# Randomized quantum measurements beyond the Clifford group

Vom Promotionsausschuss der
Technischen Universität Hamburg

zur Erlangung des akademischen Grades

Doktor der Naturwissenschaften (Dr. rer. nat.)

genehmigte Dissertation (Monografie)

von
**Mirko Arienzo**

aus
Neapel, Italien

2026

1. Gutachter: Prof. Dr. Martin Kliesch
2. Gutachter: Prof. Dr. David Gross

Tag der mündlichen Prüfung: 21. Mai 2026

doi:https://doi.org/10.15480/882.17300
ORCiD: https://orcid.org/0009-0008-3055-211X

## Abstract

Randomization techniques are a central tool in quantum information processing and in near-term applications of quantum computers. Rather than tailoring the measurement setting to a specific property of a quantum system, one can perform suitable randomized measurements and reconstruct a variety of quantum features in post-processing. This strategy is particularly effective in the current noisy intermediate-scale quantum (NISQ) era, where the characterization of quantum devices and tackling the readout problem are crucial to guarantee reliable performance. In principle, randomized protocols are most naturally formulated in terms of Haar-random unitaries followed by measurements in a fixed basis. However, their implementation quickly becomes impractical as the system size grows. In practice, one draws samples from unitary $k$-designs, i.e., structured ensembles of unitaries that mimic the behaviour of the Haar measure. In this case, the performance of randomized experiments –in particular, shadow estimation and randomized benchmarking– can often be analyzed by characterizing the associated measurement quantum channel using tools from representation theory. By inverting the channel in post-processing, estimators can be computed, and their variance determines the sampling complexity of the protocol. In discrete systems, the Clifford group is the de facto standard ensemble, as it forms a unitary 3-design, and it admits a simple description and efficient classical post-processing. However, in many situation, e.g., when protocols must respect the physical symmetries of the system, the behaviour of randomized measurements cannot be captured by standard design theory.

In this thesis, we study twirling channels arising from structured ensembles beyond group designs, focusing on applications to shadow estimation and randomized benchmarking. Shadow estimation is an attractive primitive for predicting many features of quantum states from the same experimental data. While protocols based on random Clifford unitaries yield strong practical performance, they are often restricted in practice to local random gates due to the high cost of implementing multi-qubit Cliffords. This motivates extensions to ensembles without group structure, namely, random quantum circuits. Here, we provide an analytical characterization of shadow estimation based on short random quantum circuits.

Randomized benchmarking (RB) is the most widely used protocol for the characterization of quantum gates due to its modest experimental demands and intrinsic robustness to state-preparation and measurement errors. In this thesis, we extend the protocol to photonic platforms to characterize passive Gaussian unitaries on any given particle subspace. The main technical difficulty is the symmetric nature of bosonic Hilbert spaces, which leads to nontrivial representation-theoretic features in the associated twirling channel. We derive analytical descriptions of the resulting measurement channel, highlighting inversion formulae underlying post-processing and sampling complexity guarantees. We focus on experimental settings involving Fock states and particle number resolving measurements and analyze particle loss and distinguishability as the dominant sources of noise, but also discuss Gaussian settings with either Gaussian input states or measurements and derive first results.

# Acknowledgements

First and foremost, I would like to thank my supervisor, Martin Kliesch, for introducing me to the topics of quantum system characterization and shadow estimation, and for always being supportive and a source of inspiration throughout my PhD.

I thank Markus Heinrich, who acted as an unofficial co-supervisor and mentored me during this time, and taught me about random quantum circuits and the Clifford group.

Special thanks go to my wonderful collaborators. In particular, I would like to thank Ingo Roth for the valuable insights on shadow estimation and randomized benchmarking, Dmitry Grinko for the inspiring conversations on representation theory, and Francesco Di Colandrea for introducing me to quantum simulation and for his friendship.

I would also like to thank all my colleagues, in particular Nikolai Miklin, Christopher Czedzich, Bruno Murta, Alexander Gresch, Matthias Zipper, Özgün Kum, Salwa Shaglel, Daniel Heineken, Juan Henning, and Michel Krispin, for many stimulating discussions.

Last but not least, I would like to thank my family, especially my brother Matteo and my parents, Emilia and Gennaro, as well as my friends Stefano and Vincenzo, for their unconditional support throughout my PhD.

# Contents

# Introduction to this thesis

Understanding atomic and molecular interactions is a cornerstone of modern science and engineering. Yet, the accurate simulation of microscopic systems is often beyond the possibilities of classical computers due to the unfavourable scaling in the system size. In his seminal talk, Feynman [1] introduced the idea of simulating quantum systems using another programmable quantum system. Over the past four decades, this intuition has led to the blossoming of quantum information processing and quantum computing. Foundational results in information processing, such as quantum teleportation [2], and new algorithmic techniques, such as Shor's factorization algorithm [3] and Grover's unstructured search algorithm [4], crystallized the idea that quantum information processing can deliver a genuine advantage over classical methods. However, building a quantum computer of practical value remains puzzling. Despite recent major experimental milestones [5–13], the transition from proof-of-principle demonstrations to practical applications is still elusive. The main challenges lie in the fragility of quantum devices, as interactions with the environment and imperfect control introduce noise that degrades coherence and can corrupt the information encoded in quantum states. In principle, these effects can be suppressed by encoding the quantum information into larger spaces with quantum error correcting schemes. In practice, however, this approach comes with substantial overhead beyond the capabilities of near-term quantum computers [14]. This has motivated the development of methods to assess the performance of quantum devices. In particular, by collecting sufficiently many measurement outcomes (e.g., in the form of bitstrings) on multiple copies of the system, one can reconstruct a complete mathematical description of the underlying state. However, achieving such a description requires exponential resources in the number of qubits, restricting this strategy to systems with a very moderate number of qubits [15–17]. Nevertheless, one can design more scalable strategies that infer specific properties from (fewer) measurement data. We refer to such task-specific schemes as estimation protocols, and view them within the broad framework of quantum system characterization [18–20], which comprises a landscape of protocols that benchmark properties of quantum devices depending on the initial ansatz. Similarly, the practical demands of characterization have spurred the development of techniques that mitigate the impact of noise while respecting current architectural constraints [21].

A particularly versatile approach to designing scalable protocols is based on randomized experiments [22]. Beyond mitigation and characterization, this approach enables further experimental primitives, for instance, randomized compiling [23–25], the analysis of topological invariants [26], the computation of out-of-time order correlators (OTOCs) [27], or applications in machine learning [28]. In particular, in the current noisy and intermediate scale quantum (NISQ) era, a particularly successful primitive avoids tailoring the measure-

ment setting to the properties of interest. Instead, one draws samples from a carefully chosen ensemble, whose outcomes are then post-processed through a procedure tailored to the task at hand [29], for instance, estimating overlaps between quantum states [30, 31] or purity of quantum states [32, 33], measures of entanglement [33], or probing chaotic quantum dynamics [27]. More precisely, we consider protocols that can be described in two distinct phases: First, we consider a quantum experiment that can be repeatedly performed in a lab. Each run consists of a randomized measurement where the input state is evolved under a randomly chosen unitary, and followed by a measurement in a given basis (e.g., the computational basis). The choice of input states, unitaries, and measurement is central to the design of scalable protocols, and shall match experimental capabilities. Next, the measurement outcomes are classically post-processed to infer properties of the system. In the cases of our interest, this requires the classical simulation of a quantum circuit, so it is highly desirable to consider experiments where this can be realized efficiently. In qubit systems, for instance, this often corresponds to the implementation of stabilizer circuits, which can be simulated efficiently using the Gottesman-Knill' theorem [34, 35].

While this strategy is particularly compelling for a wide variety of applications, efficient protocols with provable guarantees often rely on strong technical assumptions. More precisely, it is often convenient to draw unitaries from the uniform distribution over the unitary group, in particular, the Haar measure. In principle, this is not scalable, as approximating arbitrary unitaries requires circuits of exponential size [36]. However, in most cases, it is enough to draw samples from unitary designs, i.e., ensembles that mimic the behaviour of the Haar measure up to a certain degree, which can be implemented efficiently. Importantly, the Clifford group is the best-understood unitary design [37–41] due to its relevance across quantum information processing. However, for many tasks, implementing multi-qubit Clifford unitaries remains a major practical bottleneck: The required circuit depth typically introduces too much noise for meaningful estimation on near-term devices. Instead, short random quantum circuits can still capture non-local quantum features [42, 43] and are central, for instance, in quantum advantage proposals [5]. Beyond random quantum circuits, systems described by their physical degrees of freedom (either fermionic or bosonic) may not admit a similar randomization scheme. For instance, this is the case of continuous variable settings, where the non-existence of such designs has been proved recently [44], or particle-preserving dynamics in both fermionic and bosonic systems. The extension of a randomized protocol to such platforms is complicated by the intricacies of the associated Hilbert spaces. In particular, the unitary action describing the symmetries of such systems is often described by special classes of representations of the unitary group (i.e., symmetric or antisymmetric representations for particle-preserving dynamics of bosons and fermions, respectively), or by different groups (for instance, fermionic and bosonic Gaussian unitaries are generated by orthogonal and symplectic transformations, respectively).

In this thesis, we explore randomization techniques beyond group designs. We focus on applications in shadow estimation [45, 46] and randomized benchmarking (RB) [47, 48] that naturally fit in the randomized measurement toolbox introduced above. In particular, the data collection from quantum experiments is formally the same: We consider simple experiments where an input state (unknown for shadow estimation, fixed for RB) is subjected to random unitary evolution (for RB, using sequences of varying lengths) before measuring the circuit outcome. The outcome of this procedure is a sample pair of a random unitary (or a sequence of unitaries, for RB) and the corresponding measurement outcome. In shadow

estimation, the samples are used to compute estimators of expectation values of a given set of observables. In RB, the samples are post-processed to estimate the average quality of the implementation of the unitaries in a state preparation and measurement (SPAM) robust way: By fitting the data for different sequence lengths, decay rates can be extracted from the measurement outcomes. More precisely, in the recently proposed filtered RB framework [49, 50], the measurement outcomes are suitably postprocessed to ensure this procedure can be applied to a wide variety of gate sets. In both protocols, the experiment can be described in terms of a *measurement channel* that represents the map from the input state to the observed outcomes under the randomized procedure. Suitable estimators can be constructed by the classical inversion of the measurement channel, ideally reverting the system back to its original state. Our contributions are summarized as follows: Standard proposals for shadow estimation consider either global or local random unitaries, manifesting different regimes in which the choice of the unitary ensemble leads to efficient estimators for different features of quantum states. We interpolate between these two scenarios and characterize the measurement channel associated with short random quantum circuits. This provides a more direct construction of the classical shadows, and allows us to compare explicitly the sampling complexity of this circuit construction with the one with local Clifford unitaries. On the RB side, we bridge the gap between RB and bosonic systems, introducing the first SPAM robust protocol for the characterization of bosonic passive transformations. By extending recent advances in the RB literature [49–51], we propose a protocol that successfully benchmarks the average quality of passive Gaussian transformations on fixed number of particles using Fock states and particle number-resolving measurements. By representation-theoretic means, we derive concise formulae for post-processing and for the sampling complexity, and show that the total number of samples scales very mildly with the number of modes.

In this thesis, we focus on the mathematical characterization of such protocols. We extensively use representation theory to characterize the measurement channel (and, therefore, its inverse), as this requires the analysis of the invariant subspaces (hence, the relevant irreducible representations). The thesis is divided into three parts:

- In Part I we give a self-contained overview of representation theory and related tools that are essential for the understanding of our proofs. In Chapter 2, we discuss the basics of representation theory of compact groups. Noncommutative Fourier analysis is introduced as a tool for the analysis of the RB signal under mild noise assumptions. In Chapter 3, we analyze the structure of the irreducible representations of the unitary group and compute group twirlings for uniform distributions which will form the baseline for later generalizations. We also formally introduce group designs and review the relevant design properties of the Clifford group.

- In Part II, we focus on recent results in shadow estimation. In Chapter 5, we introduce the shadow estimation framework from the point of view of frame theory and review standard results with local and global random unitaries. These results are extended in Chapter 6, where we present the characterization of the measurement channel associated with short random quantum circuits and discuss potential extensions to deeper circuits. This chapter is largely adapted from [52]. In Chapter 7, we discuss shadow estimation for fermionic systems. We review the extension of classical shadows to the matchgate and particle-preserving passive transformation ensembles,

and discuss open problems in further extensions to randomized ensembles that respect the spin symmetry.

- Part III aims at extending randomized benchmarking to bosonic systems. In Chapter 9, we review the standard theory of RB and its extension to arbitrary compact groups by discussing the filtered RB framework [49–51]. This forms the baseline for the extension to bosonic systems discussed in Chapter 10, which is largely adapted from [53]. There, we introduce passive RB, a RB protocol to characterize the implementation of energy-preserving Gaussian unitaries using Fock states and measurements. We provide explicit post-processing procedure and workout the sampling complexity of the protocol. Lastly, in Chapter 11, we discuss how partial distinguishability of bosons affects the outcome data of passive RB, and we discuss Gaussian settings, deriving first results for RB with either input coherent states or heterodyne measurements.

# Part I

# Representation theory and group twirling

# Chapter 1

# Introduction

Representation theory of groups has long served as a unified language in theoretical physics, providing the tools to rigorously describe symmetries and their actions on vector spaces [54–56]. Group-theoretical techniques underpin a wide range of modern developments in quantum information processing, from the description of the stabilizer states [34, 35] and codes [57, 58], to the characterization of quantum devices [18, 19, 29] –for instance, tomographic protocols and benchmarking techniques– to machine learning applications [59], and analog quantum simulations [60]. Such progresses have sharpened the interest in representations of groups without a differentiable structure, namely, finite and compact groups.

In the current NISQ era, randomization techniques over unitaries have emerged as a crucial tool to enable robust characterization of quantum devices [29]. While this is well understood via the representation theory of $\mathrm{U}(d)$, for instance, via highest-weight theory or Schur-Weyl' duality, sampling Haar-random unitaries is not practical for large systems. This has motivated the theory of quantum state and unitary designs, which replicates (or approximates) averages over Haar-random unitaries up to some order. While a unitary design exists for any order and dimension [61], it is crucial that it admits efficient descriptions and implementations. This is often the case for finitely generated groups, for which each element can be written in terms of a small number of generators, and, in particular, it is the case of the Clifford group [38, 39].

Here, we provide a self-contained introduction to representation theory tailored to randomized protocols in quantum information processing. We will introduce those concept that are routinely applied to randomized techniques, while keeping the mathematical development concise and accessible.

This part is structured as follows:

- In Chapter 2, we introduce the mathematical techniques that are essential for understanding our proofs. Section 2.1 is dedicated to the notation we will use for the rest of this thesis. In Section 2.2, we discuss irreducibility and decomposition into irreducible representations. In Sections 2.3 and 2.4, we specialize to compact groups and discuss complete reducibility, orthogonality relations, and non-commutative Fourier analysis.

- Chapter 3 is dedicated to the unitary group and group twirlings. In Section 3.1, we review the representations of $\mathrm{U}(d)$. Here, the purpose is two-fold: In Section 3.1.1, we discuss the highest weights of $\mathrm{SU}(n)$ and tensor product of representations, introducing

the Clebsch-Gordan decomposition, setting the stage for Part III. Then, the remaining is dedicated to a brief review of Schur-Weyl' duality for the computation of moment operators discussed in Section 3.2. Here, we also introduce the notion of unitary design. In Section 3.4, we shortly review frame theory, a framework that encompass many randomized protocols and, in particular, shadow estimation and randomized benchmarking. Lastly, in Section 3.5, we introduce the most relevant facts about the Pauli and Clifford groups, and prove that the latter forms a unitary 2-design.

# Chapter 2

# Representation theory

Representation theory is a cornerstone in modern theoretical physics. Symmetries of a physical system are naturally encoded by a group, and the way states and observables transform under these symmetries is described by unitary representations of that group. In practice, analyzing these symmetries is crucial, as they provide a natural way to reduce the effective complexity of a problem. The Hilbert space underlying a quantum system can be decomposed into smaller irreducible subspaces, and the relevant dynamics is then restricted to these components.

In quantum information processing, group methods are ubiquitous, and randomization techniques for finding theoretical guarantees for randomized benchmarking [49, 50] and shadow estimation [45] heavily rely on the calculation of moments over the unitary group.

In this chapter, we discuss the aspects of representation theory that will be relevant throughout this thesis. We provide an overview of the notation used in the following chapters and give a short introduction to representation theory and Fourier analysis, with a particular focus on compact groups. This chapter serves as a self-contained introduction, and the well-versed reader in the topic may safely proceed to Chapter 3. We assume knowledge of linear algebra and some aspects of topology, measure theory and functional analysis.

## 2.1 Notation

In this section, we collect the most common notations used across this thesis. Some of them will be formally introduced in the upcoming sections and in the next chapter.

If $\alpha \in \mathbb{C}$, we may denote with $\bar{\alpha}$ and $\alpha^*$ its complex conjugate.

**Definition 1.** *Let $f\colon G \to \mathbb{C}$ be an integrable function on a compact group $G$. A* Haar measure *$\mu_H$ of $G$ is an invariant (Radon) measure on $G$, i.e.,*

$$\int_H d\mu_H(g) \geq 0\,, \quad \int_G f(gh)d\mu_H(g) = \int_G f(hg)d\mu_H(g) = \int_G f(g)d\mu_H(g) \tag{2.1}$$

*for all subsets $H \subseteq G$ and $h \in G$.*

We also assume the Haar measure to be normalized, i.e., $\int_G d\mu_H(g) = 1$ and use the notation $d\mu_H(g) \equiv dg$ interchangeably.

We use the standard notation for the classical Lie groups. For instance, $\mathrm{U}(d), \mathrm{SU}(n)$ denote the complex unitary and special unitary groups and $\mathrm{O}(n), \mathrm{SO}(n)$ denote the real orthogonal and special orthogonal groups, respectively. We use the notation $\mathrm{P}_n, \mathrm{Cl}_n$ to denote the Pauli and Clifford groups over $n$ qubits, respectively. Representations of groups will be mostly denoted by greek letters, e.g. $\pi, \lambda, \rho$. We denote by $\mathcal{C}(\pi) \coloneqq \{A \in \mathrm{L}(\mathcal{H}) \mid A\pi(g) = \pi(g)A \, \forall g \in G\}$ the commutant of the representation $\pi$. When $G = \mathrm{U}(d)$, we may write $U\colon \mathrm{U}(d) \to \mathrm{U}(d)$ to denote the defining (fundamental) representation. For general groups, we will also use $U$ to denote a general (possibly reducible) representation.

Let $\mathcal{H}$ be a Hilbert space. The dual space of $\mathcal{H}$ is denoted by $\mathcal{H}^*$. We denote vectors and dual vectors using the braket notation as usual, i.e. $|\psi\rangle \in \mathcal{H}$ and $\langle\psi| \in \mathcal{H}^*$. We will denote with $\mathrm{L}(\mathcal{H})$ the set of linear operators on $\mathcal{H}$ and with $\mathcal{B}(\mathcal{H})$ the set of bounded operators on $\mathcal{H}$. For a given linear operator $A \in \mathrm{L}(\mathcal{H})$, we write $A^\dagger$ for its adjoint. The identity operator is denoted by $\mathbb{1}$. In finite systems, we have $\mathcal{H} \cong \mathbb{C}^d$ for some $d \in \mathbb{N}$, and $\mathrm{L}(\mathcal{H}) \cong \mathbb{C}^{d\times d}$.

We denote the Hilbert-Schmidt inner product by a braket-like notation, namely

$$\mathrm{Tr}(A^\dagger B) \equiv (A|B) \quad A, B \in \mathrm{L}(\mathcal{H})\,. \tag{2.2}$$

Likewise, the outer product $|A)(B|$ denotes the superoperator $C \mapsto (B|C)A$. In this context, we write id for the identity superoperator. Finally, for any $k \in \mathbb{N}$, we set $[k] \coloneqq \{1, \ldots, k\}$.

## 2.2 Invariant subspaces, Schur's lemma

In the following, $\mathcal{H}$ will denote any non-trivial separable, complex Hilbert space. Recall that a group $G$ is locally compact if every every open set has a compact neighbourhood and it is Hausdorff, i.e., distinct points have disjoint neighbourhoods. We also recall that, for any directed set $A$, a net in $\{T_a\}_{a\in A} \subseteq \mathcal{B}(\mathcal{H})$ converges in the strong sense to $T \in \mathcal{B}(\mathcal{H})$ if $\|(T_a - T)|\psi\rangle\| \to 0$ for any $|\psi\rangle \in \mathcal{H}$, while we say that $\{T_a\}_{a\in A}$ converges to $T$ in the operator norm if $\|T_a - T\| \to 0$, where $\|T_a - T\| \coloneqq \sup_{\psi\in\mathcal{H}}\|(T_a - T)|\psi\rangle\|$.

**Definition 2.** *Let $G$ be a locally compact group. A (strongly) continuous homomorphism $\pi\colon G \to \mathrm{GL}(\mathcal{H})$ is a* (group) representation. *A* unitary representation *is a (strongly) continuous homomorphism from $G$ to $\mathrm{U}(\mathcal{H})$.*

We will mostly focus on unitary representations due to their prominent role in quantum theory. Moreover, in Section 2.3, we will see that for any (finite dimensional, non-unitary) representation of a compact group $G$ one can find an inner product with respect to which the representation is unitary. $\mathcal{H}$ is referred as the *carrier* space of the representation $\pi$ and $\dim\mathcal{H}$ is defined to be the dimension of $\pi$. We will also use the notation $\dim\pi$ to denote its dimension, if it is clear from the context. We remark that the strong continuity requirement is necessary, as continuity in the norm topology would be too stringent. This follows from Stone's theorem: As unitary dynamics of a quantum mechanical system is a one-parameter subgroup generated by a Hamiltonian $H$, continuity in the norm topology of a unitary representations would imply $H$ is bounded. However, physically relevant operators like $-i\frac{d}{dx}$ are necessarily unbounded, as a consequence of Stone-Von Neumann's theorem [56]. The norm-continuity prescription also poses challenges from a more abstract point of view. For instance, let $\mathrm{L}^2(G)$ be the Hilbert space of square integrable complex functions on $G$,

i.e., the space of functions $f\colon G \to \mathbb{C}$, $f \in \mathrm{L}^2(G)$ such that $\|f\|_2^2 = \int dg |f(g)|^2 < \infty$. The *left-regular representation* $\pi_L\colon G \to \mathrm{U}(\mathrm{L}^2(G))$ defined as

$$(\pi_L(g)f)(h) \coloneqq f(g^{-1}h)\,, \tag{2.3}$$

for any function $f \in \mathcal{H} \cong \mathrm{L}^2(G)$, is never continuous in the topology induced by the norm if $G$ is not discrete [62, Exercise 9.3.3].

For a given representation $\pi$ of $G$, we will also consider the representations constructed as follows:

- Let $J$ be a complex conjugation, i.e., a bijective, antilinear and inner product-preserving bounded operator. The map $\bar{\pi}\colon G \ni g \mapsto J\pi(g)J \in \mathrm{U}(\mathcal{H})$ is the *complex conjugate representation* of $\pi$.
- For any linear operator $A$, let $A^T$ denote its transpose. The map $\pi^\dagger(g) \coloneqq \pi(g^{-1})^T$ is the *dual (or contragredient) representation* of $\pi$.

Let $\pi_1 : G \to \mathrm{U}(\mathcal{H}_{\pi_1})$, $\pi_2 : G \to \mathrm{U}(\mathcal{H}_{\pi_2})$ be two unitary representations. The representations $\pi_1, \pi_2$ are said to be *intertwined* if there exists a bounded linear operator $T\colon \mathcal{H}_{\pi_1} \to \mathcal{H}_{\pi_2}$ –called the *intertwining operator*– such that $T\pi_1(g) = \pi_2(g)T$ for any $g \in G$. Let $\mathcal{C}(\pi_1, \pi_2)$ be the set of all the intertwining operators between $\pi_1$ and $\pi_2$. Note that, if $T \in \mathcal{C}(\pi_1, \pi_2)$, then $T^\dagger \in \mathcal{C}(\pi_2, \pi_1)$, because

$$T^\dagger \pi_2(g) = (\pi_2(g^{-1})T)^\dagger = (T\pi_1(g^{-1}))^\dagger = \pi_1(g)T^\dagger.$$

**Definition 3.** *Two representations $\pi_1, \pi_2$ are* unitarily equivalent *if $\mathcal{C}(\pi_1, \pi_2)$ contains a unitary operator $U$, i.e., there exists a unitary operator $U$ such that $\pi_2 = U\pi_1 U^*$. The set $\mathcal{C}(\pi) \equiv \mathcal{C}(\pi, \pi)$ is called the* commutant *or* centralizer *of the representation $\pi$.*

It is easy to see that the latter defines an equivalence relation of representations, denoted with "$\cong$". Notice that $\pi^* \cong \bar{\pi}$ on any fixed orthonormal basis as a consequence of Riesz's theorem.

**Definition 4.** *Let $\mathcal{J}$ be a closed subspace of $\mathcal{H}$. $\mathcal{J}$ is* invariant *with respect to a representation $\pi\colon G \to \mathrm{U}(\mathcal{H})$ if $\pi(g)\mathcal{J} \subseteq \mathcal{J}$ for any $g \in G$. A representation $\pi$ is* irreducible *if the only invariant subspaces are the trivial ones. Otherwise, $\pi$ is said to be* reducible*.*

We will also say that an irreducible representation is an *irrep*. In the following, we denote with $\hat{G}$ the set of inequivalent irreps of $G$, i.e.,

$$\hat{G} \coloneqq \{[\pi] \mid \pi \text{ is an irrep of } G\}\,. \tag{2.4}$$

For a non-trivial invariant subspace $\mathcal{J}$ of $\mathcal{H}$, the map $\pi_{\mathcal{J}}(g)u \coloneqq \pi(g)u$ for all $u \in \mathcal{J}$ is called a *subrepresentation* of $\pi$. Notice that if $\mathcal{J}$ is an invariant subspace, then $\mathcal{J}^\perp$ is also invariant, and the decomposition $\pi = \pi_{\mathcal{J}} \oplus \pi_{\mathcal{J}^\perp}$ holds. In fact, for vectors $u \in \mathcal{J}$ and $v \in \mathcal{J}^\perp$, one has $\langle v, \pi(g)u\rangle = \langle \pi(g)^\dagger v, u\rangle = 0$, which implies $\pi(g)v \in \mathcal{J}^\perp$. We remark that this is not true for non-unitary representations, as shown by the following canonical counter-example: The representation

$$\mathbb{R} \ni a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\,, \tag{2.5}$$

is not unitary, and the only non-trivial invariant subspace is spanned by $(1,0)^T$.

For a given group $G$, representation theory aims at classifying all the irreps of $G$ (up to equivalence) and, for reducible representations, finding how it can be decomposed into irreducible subrepresentations. General tools have been developed to answer such questions. For instance the theory of induced representations and the Mackey machine are very powerful techniques to lift irreps of a base group to a semi-direct product group having the base group as a normal factor [63, 64].

Lastly, we recall the following fundamental result that will be routinely mentioned in the following chapters:

**Lemma 5** (Schur)**.** *Let $\pi_1, \pi_2, \pi$ be unitary representations of a locally compact group $G$. Then the following facts hold true:*

*(i) $\pi$ is irreducible iff $\mathcal{C}(\pi) = \{c\mathbb{1}\}_{c\in\mathbb{C}}$.*

*(ii) Suppose $\pi_1, \pi_2$ are irreducible. If they are also unitarily equivalent, then $\mathcal{C}(\pi_1, \pi_2)$ is one-dimensional. Otherwise, $\mathcal{C}(\pi_1, \pi_2)$ is empty.*

*Proof.* (i): First, note that $\pi$ is reducible iff the orthogonal projection onto any invariant subspace is an element of $\mathcal{C}(\pi)$: Given an invariant subspace $\mathcal{H}_\lambda$ of $\mathcal{H}$, let $P_\lambda$ be the orthogonal projection on $\mathcal{H}_\lambda$. We have $\pi(g)v = \pi(g)P_\lambda v = P_\lambda\pi(g)v$ for any $v \in \mathcal{H}_\lambda$. Similarly, $P_\lambda\pi(h)v = \pi(h)P_\lambda v = 0$ for any $h \in \mathcal{H}_\lambda^\perp$, which implies $P_\lambda \in \mathcal{C}(\pi)$. Conversely, if $P_\lambda \in \mathcal{C}(\pi)$, we have that $\lambda$ is invariant since $\pi(g)v = \pi(g)P_\lambda v = P_\lambda\pi(g)v \in \mathcal{H}_\lambda$. This prove the implication from left to right, as $\mathcal{C}(\pi)$ contains nontrivial projections if $\pi$ is reducible. Conversely, if $T \in \mathcal{C}(\pi)$ and $T \neq c\mathbb{1}$, then $A \coloneqq \frac{1}{2}(T + T^*)$, $B \coloneqq \frac{1}{2i}(T - T^*) \in \mathcal{C}(\pi)$. $A$, $B$ are self-adjoint by construction, and at least one of them is not a multiple of the identity operator. Without loss of generality, suppose $A \neq c\mathbb{1}$. Thus, $\mathcal{C}(\pi)$ contains a non-trivial projection due to the spectral decomposition of $A$ [63].

(ii): Suppose $T \in \mathcal{C}(\pi_1, \pi_2)$. Hence, $T^* \in \mathcal{C}(\pi_2, \pi_1)$ as well. Then, $T^*T \in \mathcal{C}(\pi_2)$ since

$$TT^*\pi_2 = T\pi_1T^* = \pi_2TT^*.$$

Likewise, $T^*T \in \mathcal{C}(\pi_1)$, so we have $T^*T = c\mathbb{1}$ and $TT^* = c'\mathbb{1}$. Hence, it must be either $T = 0$ or $c^{-1/2}T$ is unitary. Thus, if $\pi_1$ and $\pi_2$ are inequivalent, $\mathcal{C}(\pi_1, \pi_2) = \{0\}$ and it consists of scalar multiples of unitary operators. Therefore, if $T_1, T_2 \in \mathcal{C}(\pi_1, \pi_2)$, $T_2^{-1}T_1 = T_2^*T_1 \in \mathcal{C}(\pi_1)$. Hence, $T_2^{-1}T_1 = c\mathbb{1}$, and $\dim \mathcal{C}(\pi_1, \pi_2) = 1$. □

Applications of Schur's lemma are ubiquitous in representation theory and we will discuss some of them in later sections. For now, we observe the following elementary, but useful, fact:

**Corollary 6.** *The irreps of an Abelian group $G$ are one-dimensional.*

*Proof.* In fact, suppose $\pi$ is an irreducible representation (irrep) of an Abelian group $G$. Then, $\pi(g_1)\pi(g_2) = \pi(g_2)\pi(g_1)\,\forall g_1, g_2 \in G$, which implies $\pi(G) \subseteq \mathcal{C}(\pi)$. This implies that $\pi$ is proportional to the trivial irrep of $G$. □

## 2.3 Compact groups

Analyzing unitary representations of locally compact groups is often a hard task, requiring sophisticated techniques to deal with the intricacies of infinite-dimensional Hilbert spaces. For instance, reducible representations of some classes of "pathological" groups (e.g., type II groups) may not admit a unique decomposition into irreps [63]. For more structured groups such as compact groups, however, the picture is far better: Representations are well-behaved, and decompositions are essentially unique. In what follows, we collect the key properties of compact groups that will be used throughout this thesis.

Let $G$ be a compact group with Haar measure $dg$ normalized in such a way that $\int_G dg = 1$. Note that, in this case, it is enough to consider unitary representations only. In fact, let $U\colon G \to \mathrm{GL}(\mathcal{H})$ be a representation and let $(\cdot,\cdot)$ be an inner product on $\mathcal{H}$. Then, one can define the inner product $\langle u, v\rangle \coloneqq \int_G dg\,(U(g)u, U(g)v)$ such that $U$ is a unitary representation with respect to $\mathcal{H}$ equipped with $\langle\cdot,\cdot\rangle$ since

$$\langle U(h)u, U(h)v\rangle = \int_G dg\,(U(hg)u, U(hg)v) = \int_G dg\,(U(g)u, U(g)v) = \langle u, v\rangle \tag{2.6}$$

by the left-invariance of the Haar measure. Moreover, $U$ is continuous with respect to the topology induced by Eq. (2.6) [55]. We summarize the fundamental properties of representations of compact groups:

**Theorem 7.** *Let $G$ be a compact group. The following are true:*

- *The irreps of $G$ are finite dimensional.*
- *The representations of $G$ are* completely reducible. *That is, every representation of $G$ can be decomposed in a direct sum of irreps.*

In particular, the first statement follows from the observation that, for any representation $U$ of $G$ and $|\psi\rangle \in \mathcal{H}$, the operator

$$T_\psi \coloneqq \int_G dg\, U(g)|\psi\rangle\langle\psi|U(g)^* \tag{2.7}$$

is compact, see e.g. [63, Lemma 5.1] for a proof. In fact, by Haar invariance, $T_\psi \in \mathcal{C}(U)$ and, by Schur's lemma, $T_\psi = c\mathbb{1}_\mathcal{H}$ for some scalar $c > 0$ if the representation is irreducible. Then, we observe that $\mathbb{1}_\mathcal{H}$ is compact iff $\dim\mathcal{H} < \infty$, which proves the first statement. The second statement, restricted to finite dimensional representations, can be proved by picking an invariant subspace $\lambda$ of $\mathcal{H}$ and considering the orthogonal decomposition $\lambda \oplus \lambda^\perp$. By induction on $\dim\mathcal{H}$, one obtains a decomposition of $\mathcal{H}$ into irreducible representations. The generalization to infinite dimensional representations follows from Zorn's lemma, see [63, Sec. 5.1] for more details.

Theorem 7 does not imply uniqueness in the irrep decomposition. In general, for a representation $U$, we have the decomposition $U = \bigoplus_{\pi\in\hat{G}} V_\pi$, where $V_\pi$ denotes the $\pi$-isotype defined as

$$V_\pi \coloneqq \underbrace{\mathcal{H}_\pi \oplus \cdots \oplus \mathcal{H}_\pi}_{m_\pi}, \tag{2.8}$$

with $m_\pi$ denoting the multiplicity of $\pi$ in $U$. By Schur's Lemma 5, if $\pi$ and $\tilde{\pi}$ are inequivalent, $V_\pi \perp V_{\tilde{\pi}}$. Hence, we have the canonical decomposition $\mathcal{H} = \bigoplus_\pi V_\pi$. In other terms, the

decomposition of $U$ into isotypes is unique. However, there is no canonical decomposition of isotypes into irreducible components, as, typically, this is realized by a suitable choice of an orthonormal basis inside each multiplicity subspace.

Representations of compact groups can also be understood in terms of their *characters*. For a representation $\pi$ of $G$, the associated character is the function $\chi_\pi(g) \coloneqq \mathrm{Tr}(\pi(g))$. By construction, characters are class functions, i.e., they only depend on the equivalence class of the corresponding representations. Moreover, linear operations translate naturally, e.g., $\chi_{\pi\otimes\tilde{\pi}}(g) = \chi_\pi(g)\chi_{\tilde{\pi}}(g)$.

Lastly, we comment on matrix elements of representations of compact groups. Let $U : G \to \mathrm{U}(\mathcal{H})$ be a (unitary) representation. The functions

$$c^U_{\psi,\phi} = \langle\phi\,|U(g)|\,\psi\rangle\,, \quad |\phi\rangle, |\psi\rangle \in \mathcal{H} \tag{2.9}$$

are called *matrix elements or coefficient functions* of $U$. We recall the following standard result about such coefficients that will be used in Chapter 10:

**Theorem 8** (Schur's orthogonality relations)**.** *If $\pi, \tilde{\pi}$ are irreps of $G$ and $|\phi\rangle, |\psi\rangle \in \mathcal{H}_\pi$, $|\tilde{\phi}\rangle, |\tilde{\psi}\rangle \in \mathcal{H}_{\tilde{\pi}}$, the following* orthogonality relations *hold:*

$$\int dg\, c^\pi_{\psi,\phi}(g) c^{\tilde{\pi}}_{\tilde{\phi},\tilde{\psi}}(g)^* = \begin{cases} d_\pi^{-1}\langle\tilde{\phi}|\psi\rangle\langle\phi|\tilde{\psi}\rangle\,, & \text{if } \pi \cong \tilde{\pi}, \\ 0\,, & \text{otherwise}\,. \end{cases} \tag{2.10}$$

*Proof.* For any linear map $M\colon \mathcal{H}_\pi \to \mathcal{H}_{\tilde{\pi}}$, define

$$\tilde{M} = \int_G dh\, \tilde{\pi}(h)^\dagger M \pi(h)\,. \tag{2.11}$$

By Haar invariance, $\tilde{M} \in \mathcal{C}(\pi, \tilde{\pi})$ since

$$\tilde{M}\pi(g) = \int_G dh\, \tilde{\pi}(h)^\dagger M \pi(h)\pi(g) = \int_G dh\, \tilde{\pi}(g)\tilde{\pi}(h)^\dagger M \pi(h) = \tilde{\pi}(g)\tilde{M}\,. \tag{2.12}$$

Hence, by Schur's Lemma 5, $\tilde{M} = 0$ if $\pi$ and $\tilde{\pi}$ are inequivalent, and $\tilde{M} = c\mathbb{1}$ otherwise. Moreover, by taking the trace of $\tilde{M}$ we get

$$c = \frac{1}{d_\pi}\,\mathrm{Tr}(\tilde{M}) = \frac{1}{d_\pi}\,\mathrm{Tr}(M)\,. \tag{2.13}$$

Now, let us consider $M \coloneqq |\tilde{\psi}\rangle\langle\phi|$ for $\phi \in \mathcal{H}_\pi$ and $\tilde{\psi} \in \mathcal{H}_{\tilde{\pi}}$. Then, for $\psi \in \mathcal{H}_\pi$ and $\tilde{\phi} \in \mathcal{H}_{\tilde{\pi}}$, we have

$$\begin{aligned} \langle\tilde{\phi}\,|\tilde{M}|\,\psi\rangle &= \int_G dg\, \langle\tilde{\phi}\,|\tilde{\pi}(g)^\dagger M \pi(g)|\,\psi\rangle \\ &= \int_G dg\, \langle\tilde{\phi}\,|\tilde{\pi}(g)^\dagger|\,\tilde{\psi}\rangle\langle\phi\,|\pi(g)|\,\psi\rangle \\ &= \int_G dg\, c^{\tilde{\pi}}_{\tilde{\psi},\tilde{\phi}}(g)^* c^\pi_{\psi,\phi}(g)\,. \end{aligned} \tag{2.14}$$

Then, $\langle\tilde{\phi}\,|\tilde{M}|\,\tilde{\psi}\rangle = c\langle\tilde{\phi}|\psi\rangle$, with $c = \frac{1}{d_\pi}\langle\phi|\tilde{\psi}\rangle$. □

Then, for any orthonormal basis $\{|e_i\rangle\}$ of $\mathcal{H}_\pi$, the coefficients $c^\pi_{i,j} \equiv \sqrt{d_\pi}\langle e_i|\pi(g)|e_j\rangle$ form an orthonormal basis for $\mathrm{span}\{c^\pi_{i,j}\}$. Moreover, one can prove that

$$\mathrm{L}^2(G) = \bigoplus_\pi \mathrm{span}\{c^\pi_{i,j}\}\,, \tag{2.15}$$

hence, an orthonormal basis for $\mathrm{L}^2(G)$ is given by $\bigcup_\pi\{\sqrt{d_\pi}c^\pi_{i,j} \mid i,j \in [d_\pi]\}$. This is one incarnation of Peter-Weyl's theorem [63, Thm. 5.12]. Note that this also implies orthogonality of irreducible characters, as they form an orthonormal basis for the space of square-integrable class functions.

Lastly, let us briefly review the basic facts concerning (compact) Lie groups. If a group $G$ is also a smooth manifold –namely, it is locally diffeomorphic to $\mathbb{R}^n$– and the product and inverse operations on $G$ are differentiable maps, $G$ is a (compact) *Lie group*. The *classical* matrix groups $\mathrm{GL}(d,\mathbb{C})$, $\mathrm{GL}(nd,\mathbb{R})$, $\mathrm{SL}(d,\mathbb{C})$, $\mathrm{SL}(d,\mathbb{R})$, $\mathrm{O}(d)$, $\mathrm{SO}(d)$, $\mathrm{U}(d)$, $\mathrm{SU}(d)$, $\mathrm{Sp}(2d,\mathbb{R})$ are all examples of Lie groups, with $\mathrm{O}(d)$, $\mathrm{SO}(d)$, $\mathrm{U}(d)$, $\mathrm{SU}(d)$ also being compact. The interest in Lie groups stems from the fact that their behaviour is at least partially captured by algebraic relations. Formally, each Lie group $G$ is associated with a *Lie algebra*, namely, a finite-dimensional vector space $\mathfrak{g}$ endowed with a skew-symmetric, bilinear map $[\cdot,\cdot]$ satisfying the Jacobi identity $[X,[Y,Z]]+[Y,[Z,X]]+[Z,[X,Y]]=0$ for all $X,Y,Z\in\mathfrak{g}$.

While every (finite-dimensional, real) Lie group determines a Lie algebra (unique up to isomorphisms), the converse fails in general, as a single Lie algebra can be associated with non-isomorphic Lie groups. A canonical example is provided by SO(3) and SU(2), which are non-isomorphic Lie groups (e.g., only SU(2) is simply connected) sharing the Lie algebra $\mathfrak{so}(3)\cong\mathfrak{su}(2)$. In fact, the correspondence is bijective upon restricting to simply connected Lie groups: By Cartan-Lie theorem, for each Lie algebra $\mathfrak{g}$ there exists a unique (up to isomorphism) simply connected Lie group whose Lie algebra is isomorphic to $\mathfrak{g}$, and any connected Lie group with Lie algebra $\mathfrak{g}$ is a quotient of this universal cover by a discrete central subgroup [65].

For compact connected Lie groups, irreducible representations can be classified elegantly via the highest-weight theorem; we briefly sketch the result here for later use and to keep the exposition self-contained. Let $G$ be a compact Lie group. A *maximal* torus is an Abelian subgroup (called torus) $T$ of $G$ such that $T\cong S^1\underbrace{\times\cdots\times}_{k}S^1$ for some $k\in\mathbb{N}$, where $S^1\cong\mathrm{U}(1)$ is the unit circle group, and $T$ is not properly contained in any other torus $T'\leq G$. The *rank* of $G$ is $r\coloneqq\dim T$ (as a Lie group). By construction, a (maximal) torus is a compact Lie subgroup of $G$. Hence, we can consider the corresponding Lie algebra $\mathfrak{t}$. If $\rho$ is an irrep of $G$, the restriction $\rho|_T$ to the torus $T$ decomposes into one-dimensional irreps as

$$\rho|_T \cong \bigoplus_{w\in\mathbb{Z}^r} \chi_w\otimes\mathbb{1}_{m_w}\,, \tag{2.16}$$

with $m_w$ being the multiplicity of $\chi_w$ and $\chi_w\colon G\to\mathrm{U}(1)$ being irreducible characters of $T$. The quantities $w$ are the so-called *weights* of the representation. For each $w$, the multiplicity $m_w$ of $\chi_w$ equals the dimension of the corresponding *weight space* of $w$, defined as the isotypic component $\chi_w\otimes\mathbb{1}_{m_w}$ in $\rho$. The set of weights is a poset when equipped with the following relation: First, let $\{\alpha_i\}_{i=1}^r$ be the roots of $\mathfrak{g}$ with respect to $\mathfrak{t}$ (i.e., the weights of the adjoint representation). We say that a weight $w_1$ is *higher* than a weight $w_2$, and write

$w_1 \geq w_2$, if

$$w_1 - w_2 = c_1\alpha_1 + \cdots + c_r\alpha_r\,, \tag{2.17}$$

where $c_i \geq 0$. Finally, the theorem of the highest weight [66, Thms. 9.4 and 9.5] states that every finite dimensional irrep of a compact, connected Lie group $G$ is identified by a unique highest weight, up to isomorphisms. Conversely, for any highest weight $w_H$, there exists a finite dimensional irrep of $G$. In Section 3.1.1, we discuss the weights and the irreps of $\mathrm{SU}(d)$.

## 2.4 Fourier analysis on compact groups

Fourier analysis plays a central role in representation theory and the decomposition of the space $\mathrm{L}^2(G)$ (which carries the regular representations) into its irreducible components. The standard Fourier series and transform, defined respectively as

$$f(x) = \sum_{n\in\mathbb{Z}} f_n e^{i2\pi nx}\,, \quad \hat{g}(\xi) = \int_{\mathbb{R}} dx\, g(x) e^{i2\pi x\xi}$$

for suitable integrable functions, can also be understood as the concrete application of an abstract Fourier transform for general locally compact, Abelian groups. For locally compact, Abelian groups, the construction can be understood in terms of duality theory [63]: If $G$ is Abelian, the set of characters $\hat{G} = \{[\pi] \mid \pi \text{ is a character of } G\}$ forms a group with respect to the point-wise multiplication. By Pontrjagin's duality theorem, the elements of $G$ can also be seen as characters of $\hat{G}$, establishing an isomorphism between $\mathrm{L}^2(G)$ and $L^2(\hat{G})$, which is given by the Fourier transform and its inverse

$$\hat{f}(\xi) = \int_G dg\, \xi(g)^* f(g)\,, \quad f(g) = \int_{\hat{G}} d\xi\, g(\xi)\hat{f}(\xi) \tag{2.18}$$

(this is another incarnation of Plancherel's theorem). By specifying $G$ and its dual $\hat{G}$, one can retrieve all the elementary transforms, such as the Fourier series ($G = \mathbb{Z}$ and $\hat{G} \cong \mathrm{U}(1)$), the Fourier transform ($G = \mathbb{R}$ and $\hat{G} \cong \mathbb{R}$) and the discrete Fourier transform ($G = \mathbb{Z}_n$ and $\hat{G} \cong \mathbb{Z}_n$), the latter being closely related to the quantum Fourier transform [57].

The Peter-Weyl theorem provides a natural framework to generalize standard Fourier analysis to the non-Abelian setting. Intuitively, we can extend Eq. (2.18) to non-Abelian compact groups by replacing the characters with matrix coefficients of irreps, as they form an orthonormal basis in $\mathrm{L}^2(G)$, c.f. Eq. (2.15). This is crucial for the construction of a suitable isomorphism, because $\hat{G}$ does not have an obvious group structure, and there is no clear intuition of a dual group. Hence, for any $f \in \mathrm{L}^2(G)$, we can write

$$f(g) = \sum_{\pi\in\hat{G}} \sum_{i,j=1}^{d_\pi} f^\pi_{i,j} \pi(g)_{i,j}\,, \tag{2.19}$$

with $f^\pi_{i,j} \equiv d_\pi \int_G dg\, f(g)\pi(g)^*_{i,j}$. This suggest the following, coordinate-free, notion:

**Definition 9.** *For a compact group $G$ and an irrep $\pi\colon G \to \mathrm{U}(\mathcal{H})$, the* Fourier transform *of $f \in \mathrm{L}^2(G)$ at $\pi$ is the operator*

$$\hat{f}[\pi] \coloneqq \int_G dg\, f(g)\pi(g)^\dagger\,. \tag{2.20}$$

By Eq. (2.15), Eq. (2.20) induces the coordinate-free isomorphism $\mathrm{L}^2(G) \cong \bigoplus_{\pi\in\hat{G}} \mathrm{L}(\mathcal{H}_\pi)$, where $\mathrm{L}(\mathcal{H}_\pi)$ is the space of linear operators on $\mathcal{H}_\pi$. Moreover, Eq. (2.20) admits the inversion formula

$$f(g) = \sum_{\pi\in\hat{G}} d_\pi \operatorname{Tr}\left[\hat{f}[\pi]\pi(g)\right] . \tag{2.21}$$

Note that the pointwise convergence is not guaranteed for $f \in \mathrm{L}^2(G)$ if the series is not truncated. In this thesis, we will only consider functions supported on a finite subset of irreps. For further information, we refer the reader to the discussion in [63, Lemma 5.24]. The Fourier transform (2.20) satisfies the usual properties of the standard Fourier transform:

**Definition 10.** *For two functions $f_1, f_2 \in \mathrm{L}^2(G)$ where $G$ is a compact group, we define the* convolution *of $f_1$ and $f_2$ as the map $*\colon \mathrm{L}^2(G) \times \mathrm{L}^2(G) \to \mathrm{L}^2(G)$ such that*

$$(f_1 * f_2)(g) \coloneqq \int_G dh\, f_1(gh^{-1}) f_2(h) \tag{2.22}$$

Due to non-commutativity of representations, the behaviour of the convolution under the Fourier transform is slightly different from the Abelian case:

**Proposition 11.** *The following equality holds true:*

$$\widehat{f_1 * f_2} = \hat{f}_2 \hat{f}_1 . \tag{2.23}$$

*Proof.* In fact, we have

$$\begin{aligned}
\widehat{f_1 * f_2}[\pi] &= \int_G dg\, (f_1 * f_2)(g)\pi(g)^\dagger \\
&= \int_G dg \int_G dh\, f_1(gh^{-1}) f_2(h)\pi(g)^\dagger \\
&= \int_G dg\, f_1(g) \int_G dh\, f_2(h)\pi(gh)^\dagger \\
&= \int_G dh\, f_2(h)\pi(h)^\dagger \int_G dg\, f_1(g)\pi(g)^\dagger \\
&= \hat{f}_2[\pi]\hat{f}_1[\pi] ,
\end{aligned} \tag{2.24}$$

where we mapped $g \mapsto gh$ in the third step and used the invariance of the Haar measure and Fubini-Tonelli's theorem to change the order of integration. □

It is also useful to recall Parseval's identity:

**Proposition 12.** *Let $G$ be a compact group and let $f \in \mathrm{L}^2(G)$. The following equality holds true:*

$$\|f\|_2^2 = \sum_\pi d_\pi \|\hat{f}[\pi]\|_2^2 , \tag{2.25}$$

*where the norm on the l.h.s. is the $L^2$ norm and the norm on the r.h.s. is the Hilbert-Schmidt norm.*

*Proof.* The latter follows from the inversion formula (2.21) and orthogonality relations (2.10):

$$\begin{aligned}\|f\|_2^2 &= \int_G dg \sum_{\pi,\rho} d_\pi d_\rho \operatorname{Tr}\left[\hat{f}[\pi]\pi(g)\right]^* \operatorname{Tr}\left[\hat{f}[\rho]\rho(g)\right] \\ &= \sum_{\pi,\rho} d_\pi d_\rho \sum_{i,j,k,l} f^{\pi *}_{i,j} f^{\rho}_{k,l} \int_G dg\, \pi(g)^*_{i,j}\rho(g)_{k,l} \\ &= \sum_{\pi} d_\pi \sum_{i,j} |f^{\pi}_{i,j}|^2 \\ &= \sum_{\pi} d_\pi \operatorname{Tr}\left[\hat{f}[\pi]^\dagger \hat{f}[\pi]\right] ,\end{aligned} \tag{2.26}$$

where in the third step we used orthogonality relations and the last step follows from the identification $\sum_{i,j} \overline{f^{\pi}_{i,j}} f^{\pi}_{i,j} = \operatorname{Tr}(\hat{f}[\pi]^\dagger \hat{f}[\pi])$. □

The previous discussion naturally generalizes to Fourier analysis of quantum channels. This will be central in Part III, where we discuss the form of the RB signal and regard noisy implementations of quantum gates as quantum channels. To this end, we view quantum channels as matrices and their Fourier transform as the component-wise Fourier transform defined in Eq. (2.20): Let $f\colon G \to L(\mathcal{H})$. As Eq. (2.20) is operator-valued, we shall consider the element-wise Fourier transform

$$\hat{f}[\pi]_{i,j} = \int_G dg\, \pi(g)^\dagger f_{i,j}(g) \tag{2.27}$$

(notice that the order is not relevant here, as $f_{i,j}(g) \in \mathbb{C}$). Then, $\hat{f}(\pi)$ ought to be considered as a tensor, and the previous equation justifies the following definition:

$$\hat{f}[\pi] \coloneqq \int_G dg\, \overline{\pi(g)} \otimes f(g)\,. \tag{2.28}$$

As before, we can define the convolution of matrix-valued functions as

$$f_1 * f_2(g) \coloneqq \int_G dh f_1(gh^{-1}) f_2(h)\,, \tag{2.29}$$

so we have $\widehat{f_1 * f_2} = \hat{f}_1 \hat{f}_2$ (note the we recover the standard ordering with this definition) and Parseval's identity becomes [67]

$$\int_G dg\, \|f(g)\|_2^2 = \sum_{\pi} d_\pi \|\hat{f}[\pi]\|_2^2\,, \tag{2.30}$$

which follows from orthogonality of characters.

If $\pi$ is not an irrep, we can still define $\hat{f}(\pi)$ by decomposing it into irreducible components. Specifically, by considering the decomposition

$$\pi = \bigoplus_{\lambda \in \hat{G}} \bigoplus_{i=1}^{m_\lambda} \pi_\lambda^{(i)}\,, \tag{2.31}$$

we have by linearity

$$\hat{f}[\pi] = \bigoplus_{\lambda} \bigoplus_{i=1}^{m_\lambda} \hat{f}[\pi_\lambda^{(i)}] = \bigoplus_{\lambda} \hat{f}[\pi_\lambda] \otimes \mathrm{id}_{m_\lambda} . \tag{2.32}$$

This coordinate picture justifies the following definition, which can be interpreted as a basis-free definition of Fourier transform of matrix-valued functions [50]:

**Definition 13.** *Let $G$ be compact, $\pi \colon G \to \mathrm{U}(\mathcal{H}_\pi)$ an irrep and $f \colon G \to L(\mathcal{H})$ be square integrable. The* Fourier transform *of $f$ at $\pi$ is the linear operator $\mathrm{L}(\mathcal{H}, \mathcal{H}_\pi) \to \mathrm{L}(\mathcal{H}, \mathcal{H}_\pi)$ such that*

$$\hat{f}[\pi] \coloneqq \int_G dg\, \pi(g)^\dagger(\cdot) f(g) . \tag{2.33}$$

Note that Eq. (2.33) and Eq. (2.28) are equivalent up to the composition of a suitable vectorization in a fixed orthonormal basis and a transposition [50]. The next proposition summarizes the most relevant facts for our purposes:

**Proposition 14.** *Let $\pi_\lambda \colon G \to \mathrm{U}(\mathcal{H}_\pi)$ be an irrep and let $\omega \colon G \to \mathrm{U}(\mathcal{H})$ be a representation. Then, $\hat{\omega}[\pi]$ is the orthogonal projection of $\omega$ onto the isotypic component of $\pi$ in $\omega$.*

*In particular, if $\omega$ is irreducible, then $\hat{\omega}[\pi]$ is a rank-*1 *orthogonal projector if $\omega \cong \pi$ and* 0 *otherwise.*

*Proof.* By Eq. (2.33) and the convolution theorem,

$$\begin{aligned} \hat{\omega}[\pi]^2 = \widehat{\omega * \omega}[\pi] &= \int_G dg\, \pi(g)^\dagger(\cdot)(\omega * \omega)(g) = \int_G dg\, \pi(g)^\dagger(\cdot) \int_G dh\, \omega(h)\omega(h^{-1}g) \\ &= \int_G dg\, \pi(g)^\dagger(\cdot)\omega(g) = \hat{\omega}[\pi] \end{aligned} \tag{2.34}$$

since $\int_G dh = 1$. Haar invariance also implies that $\hat{\omega}[\pi]$ is self-adjoint with respect to the Hilbert-Schmidt inner product. In fact, by cyclicity of the trace,

$$\begin{aligned} \mathrm{Tr}[\hat{\omega}(\pi_\lambda)(A)^\dagger B] &= \mathrm{Tr}\left[\int_G dg\, \left(\pi_\lambda(g)^\dagger A \omega(g)\right)^\dagger B\right] = \mathrm{Tr}\left[\int_G dg\, \omega(g)^\dagger A^\dagger \pi_\lambda(g) B\right] \\ &= \mathrm{Tr}\left[\int_G dg\, A^\dagger \pi_\lambda(g) B \omega(g)^\dagger\right] = \mathrm{Tr}\left[\int_G dg\, A^\dagger \pi_\lambda(g)^\dagger B \omega(g)\right] \\ &= \mathrm{Tr}\left[A^\dagger \hat{\omega}[\pi_\lambda](B)\right] . \end{aligned} \tag{2.35}$$

Then, suppose $\omega = \bigoplus_\eta \bigoplus_{i=1}^{m_\eta} \pi_\eta^{(i)}$.

$$\begin{aligned} \mathrm{Tr}\left[\hat{\omega}[\pi_\lambda]\right] &= \int_G dg\ \mathrm{Tr}[\pi_\lambda(g)^\dagger] \,\mathrm{Tr}[\omega(g)] = \int_G dg\ \mathrm{Tr}[\pi_\lambda(g)^\dagger] \,\mathrm{Tr}\left[\bigoplus_\eta \bigoplus_{i=1}^{m_\eta} \pi_\eta^{(i)}(g)\right] \\ &= \sum_\eta \sum_{i=1}^{m_\eta} \int_G dg\ \mathrm{Tr}[\pi_\lambda(g)^\dagger] \,\mathrm{Tr}\left[\pi_\eta^{(i)}(g)\right] = \sum_\eta \sum_{i=1}^{m_\eta} \delta_{\lambda,\eta} \\ &= m_\lambda \end{aligned} \tag{2.36}$$

by (character) orthogonality relations (2.10). The latter implies $\hat{\omega}[\pi_\lambda]$ is non-zero on the isotype $\bigoplus_{i=1}^{m_\lambda} \pi_\lambda^{(i)}$ and zero otherwise. Hence,

$$\hat{\omega}[\pi_\lambda] \cong \bigoplus_{i=1}^{m_\lambda} \int_G dg\, \pi_\lambda(g)^\dagger(\cdot)\pi_\lambda^{(i)}(g)\,. \tag{2.37}$$

Moreover, if $\omega$ is an irrep of $G$, the latter implies that $\hat{\pi}_\lambda[\pi_\lambda]$ is a rank-1 orthogonal projector. □

# Chapter 3

# Unitary group twirlings

The unitary group is ubiquitous in quantum theory. The evolution of closed systems is captured by (reversible) unitary transformations, as the dynamics described by a Hamiltonian $H$ integrates to a one-parameter unitary group $U(t) = e^{-iHt}$. At the same time, by Wigner's theorem, physical symmetries are essentially described by unitary operators [68]. Mathematically, $\mathrm{U}(d)$ is a compact Lie group, and its irreducible representations can be elegantly described using the theorem of the highest weight. In this chapter, we provide a short introduction to $\mathrm{U}(d)$, its representations, and the calculation of moment operators over the unitary group. Next, we briefly review the notion of unitary designs, provide a brief introduction to frame theory, and show that the Clifford group forms a unitary 2-design.

## 3.1 Representations of $\mathrm{U}(d)$

The group $\mathrm{U}(d)$ is the group of automorphisms of the complex vector space $\mathbb{C}^d$ endowed with the Hermitian inner product $\langle\psi|\phi\rangle = \sum_{j=1}^{d} \bar{\psi}_j \phi_j$, i.e., $\langle U\psi|U\psi\rangle = \langle\psi|\phi\rangle$ for all $U \in \mathrm{U}(d)$. This implies that $U^\dagger = U^{-1}$ and $\det U = \pm 1$. By the relation $UU^\dagger = \mathbb{1}$, it follows that the rows (and the columns) of $U$ are orthonormal and $U$ is bounded, as $|U_{jk}| \leq 1$, $j, k = 1, \ldots, d$. Since $\mathrm{U}(d)$ is a closed subgroup of $\mathrm{GL}(d, \mathbb{C})$, the latter also implies $\mathrm{U}(d)$ is compact. The irreps of $\mathrm{U}(d)$ are easily understood in terms of the ones of $\mathrm{SU}(d)$, the subgroup of unitary matrices such that $\det U = 1$. In fact, $\mathrm{SU}(d)$ is simply connected, and its irreps are identified by the highest weights, as depicted in the previous section. Then, following the observation that $\mathrm{U}(d) = \mathrm{SU}(d) \ltimes \mathrm{U}(1)$, irreps of $\mathrm{U}(d)$ are obtained from irreps of $\mathrm{SU}(d)$ extended to $\mathrm{U}(d)$ via non-trivial characters of $\mathrm{U}(1)$, e.g., the determinant representation $U \mapsto \det U$. Therefore, without loss of generality, we will consider irreps of $\mathrm{SU}(d)$.

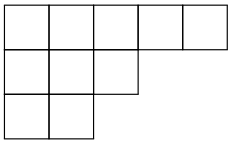
*Sections 3.1.1 and 3.1.2 are based on [53, Sec. TI.A]. The content has been adapted and broadened to provide a self-contained overview of Young diagrams, their interpretation and role in the classifications of the irreps of* $\mathrm{SU}(d)$.

### 3.1.1 Irreps of $\mathrm{SU}(d)$

**Definition 15.** *For a given $k \in \mathbb{N} \setminus \{0\}$, the* symmetric group $\mathfrak{S}_k$ *is group formed by all permutations of elements $\{1, \ldots, k\} \equiv [k]$.*

Note that $\mathfrak{S}_k$ is non-Abelian for $k \geq 3$. The importance of $\mathfrak{S}_k$ stems from the close connection with the irreps of U($d$), as we show below.

A useful tool to represent permutations is the notion of *Young diagrams*: Let $\lambda = (\lambda_1, \ldots, \lambda_m)$ be a partition of $k$, i.e. $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m \geq 0$ with $\sum_{i=0}^{m} \lambda_i = k$. We will also write $\lambda \dashv k$. Any such partition is identified with a Young diagram, namely a collection of boxes arranged in left-justified rows with a weakly decreasing number of boxes in each row, where the $i$-th row contains $\lambda_i$ boxes, e.g.,



(3.1)

corresponds to $\lambda = (5, 3, 2)$. Young diagrams are a convenient tool for studying representations of $\mathfrak{S}_k$: Its irreps are classified (up to equivalence) by partitions of $k$, or equivalently by Young diagrams with $k$ boxes [69]. In this context, many useful quantities –such as the dimension of an irrep– can be computed via combinatorial rules that can be expressed directly in terms of Young diagrams. Notably, Young diagrams also label the irreps of unitary groups (this statement will be made more precise using Schur-Weyl' duality). We will briefly discuss this fact over the next sections.

An irrep $\lambda$ of $\mathfrak{S}_k$ admits a natural orthonormal basis described as follows: A *(semi-standard) Young tableau* is a filling of Young diagram boxes, with entries in $\mathbb{N} \setminus \{0\}$, such that the entries are weakly increasing across each row and they are strictly increasing down each columns. A *standard Young tableau* is a semistandard Young tableau in which the entries are given exactly by numbers $\{1, \ldots, k\}$. In other terms, the entries in a standard Young tableau are strictly increasing across each row and down each columns. For instance, for the partition $(5, 3, 2, 1) \dashv 11$ the following are a semistandard Young tableau and a standard Young tableau, respectively:

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 2 | 4 | 6 |
| 3 | 4 | 5 | | |
| 4 | 6 | | | |
| 7 | | | | |

,

| | | | | |
|---|---|---|---|---|
| 1 | 3 | 5 | 7 | 9 |
| 2 | 4 | 6 | | |
| 8 | 10 | | | |
| 11 | | | | |

.

The dimension of $\lambda$ is the number of standard Young tableaux of this shape, which is determined as follows: Let $(i, j)$ be the row-column indices of a box in $\lambda$ and let $h_\lambda(i, j)$ be the number of boxes $(i, r)$ with $r \geq j$ and $(l, j)$ with $l \geq i$, with the $(i, j)$th box counted only once. Then, $\dim \lambda$ is determined by the formula [69]

$$d_\lambda = \frac{k!}{\prod_{(i,j)} h_\lambda(i, j)} \,. \tag{3.2}$$

This is often referred as the *hook-length formula*. For instance, for $\lambda = (5, 3, 2, 1) \dashv 11$ we have the Hook lengths

| | | | | |
|---|---|---|---|---|
| 8 | 6 | 4 | 2 | 1 |
| 5 | 3 | 1 | | |
| 3 | 1 | | | |
| 1 | | | | |

, (3.3)

where the filling of the $(i,j)$th box is in this case given by $h_{\lambda(i,j)}$. It follows that $\dim \lambda = 2310$.

Going back to the case of SU($d$), by the theorem of the highest weight, its irreps are identified by highest weight vectors. In this case, $\operatorname{rank} \mathrm{SU}(d) = d-1$ since

$$\operatorname{diag}(e^{i\theta_1}, \ldots, e^{i\theta_{d-1}}, e^{-i\sum_{j=1}^{d-1}\theta_j}) \tag{3.4}$$

is a maximal torus isomorphic to $\mathrm{U}(1)^{\times(d-1)}$, and the highest weights of SU($d$) are $(d-1)$-ples. Young diagrams uniquely determine irreps of SU($d$) up to constant shifts, namely, $(\lambda_1, \ldots, \lambda_d)$ and $(\lambda_1 + c, \ldots, \lambda_d + c)$ identify the same irrep for any integer $c$. Therefore, we assume by convention $\lambda_d = 0$ without loss of generality. In the following we will not distinguish between Young diagrams and the corresponding irreps, unless otherwise specified.

For a fixed irrep $\lambda$ of SU($d$), the semi-standard Young tableaux of shape $\lambda$ label an orthonormal basis of $\lambda$, sometimes referred as the *Weyl basis*. For instance, the Young tableaux

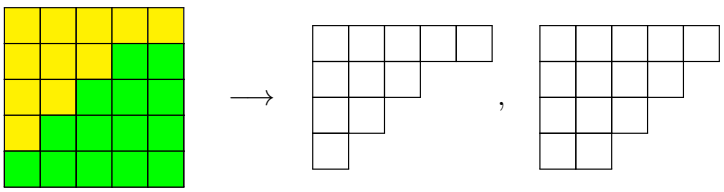
$$\begin{array}{|c|c|}\hline 1&1\\\hline 2\\\cline{1-1}\end{array},\quad \begin{array}{|c|c|}\hline 1&1\\\hline 3\\\cline{1-1}\end{array},\quad \begin{array}{|c|c|}\hline 1&2\\\hline 2\\\cline{1-1}\end{array},\quad \begin{array}{|c|c|}\hline 1&2\\\hline 3\\\cline{1-1}\end{array},$$
$$\begin{array}{|c|c|}\hline 1&3\\\hline 2\\\cline{1-1}\end{array},\quad \begin{array}{|c|c|}\hline 1&3\\\hline 3\\\cline{1-1}\end{array},\quad \begin{array}{|c|c|}\hline 2&2\\\hline 3\\\cline{1-1}\end{array},\quad \begin{array}{|c|c|}\hline 2&3\\\hline 3\\\cline{1-1}\end{array}. \tag{3.5}$$

identify an orthonormal basis for the SU(3) adjoint irrep $\lambda = (2,1,0)$.

We can compute the dimension of any irrep of SU($d$) from the shape of the corresponding Young diagram in the form of a suitable ratio of products of integers: Let $\lambda$ be a Young diagram and set $\dim \lambda = N/D$. We compute $N$ by constructing an irregular tableau of shape $\lambda$ as follows: The top left box is filled with $d$. Moving across the row, the entries increase by 1 at each step. Moving across the column, the entries decrease by 1 at each step. Then, $N$ is the product of the entries of the constructed tableau. $D$ is determined by the Hook length formula applied to $\lambda$. In the latter example, we have

$$\dim \begin{array}{|c|c|}\hline &\\\hline \\\cline{1-1}\end{array} = 8. \tag{3.6}$$

Lastly, we remark that, for a given irrep $\lambda$, the dual representation $\lambda^*$ defined as $\lambda^*(g) \coloneqq \lambda(g^{-1})^T$ acting on the dual carrier space is also irreducible. Having fixed a basis for $\lambda$, we also have $\lambda^* \cong \bar{\lambda}$, where $\bar{\lambda}(g) \coloneqq \overline{\lambda(g)}$ is the complex conjugate representation of $\lambda$. Hence, for any irrep $\lambda = (\lambda_1, \ldots, \lambda_d)$, this implies $\lambda^*$ is identified by the *dual* Young diagram $\bar{\lambda} \coloneqq (\lambda_1 - \lambda_d, \lambda_1 - \lambda_{d-1}, \ldots, \lambda_1 - \lambda_2, 0)$. More practically, $\bar{\lambda}$ is constructed by completing $\lambda$ to a $d \times \lambda_1$ rectangular Young diagram, and rotating the diagram formed by the newly added boxes by 180°. For instance,



(3.7)

are dual Young diagrams in SU(5).

**Gelfand-Tsetlin patterns.**

A more convenient way of labeling basis vectors for any irrep $\lambda = (\lambda_1, \ldots, \lambda_d)$ of SU($d$) is by *Gelfand–Tsetlin (GT) patterns*.

A GT pattern $M$ of shape $\lambda$ and length $d$ is represented by a triangular table with $d$ rows, the $j$-th row containing $j$ integers (counting from the bottom to the top)

$$M = \begin{pmatrix} M_{1,d} & & M_{2,d} & & \cdots & & M_{d-1,d} & & M_{d,d} \\ & M_{1,d-1} & & M_{2,d-1} & \cdots & M_{d-2,d-1} & & M_{d-1,d-1} & \\ & & \ddots & & \vdots & & \iddots & & \\ & & & M_{1,2} & & M_{2,2} & & & \\ & & & & M_{1,1} & & & & \end{pmatrix}, \tag{3.8}$$

and $M_{i,d} = \lambda_i$ for every $i \in [d]$ (and, in particular, $M_{d,d} = 0$ by convention). The entries satisfy the following *interlacing* or *inbetweenness* condition:

$$M_{i,j+1} \geq M_{i,j} \geq M_{i+1,j+1} \tag{3.9}$$

for every $i \in [d-1]$ and $j \in [d-1]$. We remark that by convention the indices in a GT pattern are swapped, namely the first one is the column index, increasing from left to right, as usual, while the second one is the row index, decreasing from top to bottom. We denote the set of GT patterns of shape $\lambda$ that satisfy the inbetweenness condition by GT($\lambda$).

An orthonormal basis for $\lambda$ –referred as the Gelfand–Tsetlin basis– is given by state vectors $\{|\lambda, M\rangle\}$, where $M$ is a valid GT pattern with top row $\boldsymbol{M}_1 \equiv (M_{1,1}, \ldots, M_{1,d}) = \lambda$. We will also use the notation $|\lambda, M\rangle \equiv |M\rangle$ if $\lambda$ is clear from the context. Hence, the dimension of $\lambda$ is equal to the number of such states, for which the following formula holds:

$$\dim \lambda = \prod_{1 \leq i \leq j \leq d} \left(1 + \frac{M_{i,d} - M_{j,d}}{j - i}\right). \tag{3.10}$$

In terms of the GT basis, the highest weight vector of $\lambda$ is identified by the pattern maximizing the inbetweenness conditions, namely

$$M_{\max} = \begin{pmatrix} M_{1,d} & & M_{2,d} & & \cdots & & M_{d-1,d} & & M_{d,d} \\ & M_{1,d} & & M_{2,d} & \cdots & M_{d-2,d} & & M_{d-1,d-1} & \\ & & \ddots & & \vdots & & \iddots & & \\ & & & M_{1,d} & & M_{2,d} & & & \\ & & & & M_{1,d} & & & & \end{pmatrix} \tag{3.11}$$

(likewise, the lowest weight vector of $\lambda$ is obtained by minimizing the inbetweenness conditions).

GT patterns are in one-to-one correspondence with semi-standard Young tableaux. In fact, for a given Young tableau $T$ of shape $\lambda$, the shape of the corresponding GT pattern $M$ is the same shape as $T$ and the entry $M_{j,k}$ of $M$ (remember the different indexing in (3.8) compared to matrix indices) is given by the number of entries in the $j$-th row of $T$ which are less or equal than $k$. Conversely, given a GT pattern $M$ of shape $\lambda$, the shape of the corresponding Young tableau $T$ is determined by the first row of $M$ and $M_{j,k} - M_{j,k-1}$ is the number of $k$'s in the $j$'th row of $T$. Throughout this work, we assume that all illegal coefficients are set to 0. For instance, the Young tableaux

$$\begin{array}{|c|c|c|c|c|} \hline 1 & 1 & 2 & 2 & 3 \\ \hline 2 & 2 & 3 \\ \cline{1-3} 3 & 4 \\ \cline{1-2} \end{array}, \qquad \begin{array}{|c|c|c|c|c|} \hline 1 & 1 & 1 & 1 & 1 \\ \hline 2 & 2 & 3 \\ \cline{1-3} 3 & 4 \\ \cline{1-2} \end{array} \tag{3.12}$$

corresponds to the GT patterns

$$\begin{pmatrix} 5 & & 3 & & 2 & & 0 \\ & 5 & & 3 & & 2 & \\ & & 4 & & 2 & & \\ & & & 2 & & & \end{pmatrix}, \quad \begin{pmatrix} 5 & & 3 & & 2 & & 0 \\ & 5 & & 3 & & 1 & \\ & & 5 & & 2 & & \\ & & & 5 & & & \end{pmatrix}, \tag{3.13}$$

respectively, and the Weyl basis Eq. (3.5) corresponds to the GT basis

$$\begin{array}{llll} \begin{pmatrix} 2 & & 1 & & 0 \\ & 2 & & 1 & \\ & & 2 & & \end{pmatrix}, & \begin{pmatrix} 2 & & 1 & & 0 \\ & 2 & & 0 & \\ & & 2 & & \end{pmatrix}, & \begin{pmatrix} 2 & & 1 & & 0 \\ & 2 & & 1 & \\ & & 1 & & \end{pmatrix}, & \begin{pmatrix} 2 & & 1 & & 0 \\ & 2 & & 0 & \\ & & 1 & & \end{pmatrix}, \\ \begin{pmatrix} 2 & & 1 & & 0 \\ & 1 & & 1 & \\ & & 1 & & \end{pmatrix}, & \begin{pmatrix} 2 & & 1 & & 0 \\ & 1 & & 0 & \\ & & 1 & & \end{pmatrix}, & \begin{pmatrix} 2 & & 1 & & 0 \\ & 2 & & 0 & \\ & & 0 & & \end{pmatrix}, & \begin{pmatrix} 2 & & 1 & & 0 \\ & 1 & & 0 & \\ & & 0 & & \end{pmatrix}. \end{array} \tag{3.14}$$

For a given GT pattern $M$, the *weight* of $|M\rangle$ is the $(d-1)$-tuple $w_M \coloneqq (w_1^{(M)}, \ldots, w_{d-1}^{(M)})$ as introduced before, where each entry $w_i^{(M)}$ is determined by $M$ as follows:

$$w_j^{(M)} = 2\sum_{i=1}^{j} M_{i,j} - \sum_{i=1}^{j-1} M_{i,j-1} - \sum_{i=1}^{j+1} M_{i,j+1}\,. \tag{3.15}$$

We remark weights generalizes the notion of magnetic quantum number $m$ for SU(2) in the quantum theory of angular momentum to arbitrary many modes. In the latter expression, we assume the convention that $\sum_{i=1}^{j-1} M_{i,j-1} = 0$ if $j = 1$.

All states $|M\rangle$ of the same weight $w$ form a basis of the weight space of $w$. Note that these are typically not one-dimensional, except for SU(2) [70–72]. For instance, the GT patterns

$$M = \begin{pmatrix} 3 & & 2 & & 0 \\ & 3 & & 0 & \\ & & 1 & & \end{pmatrix}, \quad \tilde{M} = \begin{pmatrix} 3 & & 2 & & 0 \\ & 2 & & 1 & \\ & & 1 & & \end{pmatrix} \tag{3.16}$$

are such that $w^M = w^{\tilde{M}} = (-1, 0)$. Thus the dimension of the weight space of $w$ (the inner multiplicity) corresponds to the number of GT states (or, equivalently, to the number of semi-standard Young tableaux) with weight $w$. These amount to Kostka's numbers, and can be computed e.g. with recursive algorithms [73].

It is worth reminding here a related definition of a *weight* for U($d$) (or GL($d$)) representations. Gelfand–Tsetlin patterns also label basis vectors of the corresponding irreps of such groups. However, the condition $M_{m,m} = 0$ is dropped. In this case, the weight of the GT pattern $M$ is defined as $w^M_{\mathrm{U}(d)} \coloneqq (w^M_{\mathrm{U}(d),1}, \ldots, w^M_{\mathrm{U}(d),d})$ with

$$w^M_{\mathrm{U}(d),j} \coloneqq \sum_{i=1}^{j} M_{i,j} - \sum_{i=1}^{j-1} M_{i,j-1}\,, \tag{3.17}$$

therefore

$$w_j^{(M)} = w^M_{\mathrm{U}(d),j} - w^M_{\mathrm{U}(d),j+1}\,. \tag{3.18}$$

An equivalent definition that will be used in this work is the following: The *tableau weight* is the $m$-tuple $w^T = (w_1^T, \ldots, w_d^T)$ where $w_i^T$ is the total number of $i$ entries in $T$. If $T$ is the semi-standard Young tableau associated with $M$, we also have

$$w_j^T \coloneqq \sum_{i=1}^{j} M_{i,j} - \sum_{i=1}^{j-1} M_{i,j-1}\,. \tag{3.19}$$

The weights $w_M$ and $w^T$ are clearly related in a similar way:

$$w_j^{(M)} = w_j^T - w_{j+1}^T \,. \tag{3.20}$$

We notice en passant that the tableau weight is always a sequence of non-negative integers, which sometimes is more convenient for combinatorics. For instance, the tableaux $T$ and $\tilde{T}$ associated with the GT patterns $M$ and $\tilde{M}$ from the former examples are

$$T = \begin{array}{|c|c|c|}\hline 1&2&2\\\hline 3&3\\\cline{1-2}\end{array}\,, \quad \tilde{T} = \begin{array}{|c|c|c|}\hline 1&2&3\\\hline 2&3\\\cline{1-2}\end{array}$$

and we have $w^T = w^{\tilde{T}} = (1,2,2)$.

**Dual GT patterns.**

For a given GT pattern $M$ of shape $\lambda$, we define the *dual* GT pattern $\bar{M}$ of shape $\bar{\lambda}$ as the pattern with entries satisfying the relation

$$\bar{M}_{i,l} \coloneqq M_{1,m} - M_{l-i+1,l} \,, \tag{3.21}$$

i.e. $\bar{M} = M_{1,d} + \tilde{M}$, where the sum shall be interpreted as the element-wise constant shift of $\tilde{M}$ by $M_{1,d}$, and $\tilde{M}$ is given by

$$\tilde{M} = \begin{pmatrix} -M_{d,d} & & -M_{d-1,d} & & \dots & & -M_{2,d} & & -M_{1,d} \\ & -M_{d-1,d-1} & & -M_{d-2,d-1} & \dots & -M_{2,d-1} & & M_{1,m-1} & \\ & & \ddots & & \vdots & & \iddots & & \\ & & & -M_{2,2} & & -M_{1,2} & & & \\ & & & & -M_{1,1} & & & & \end{pmatrix} . \tag{3.22}$$

By construction, $\bar{M}$ defines a basis state for the dual irrep $\lambda^* \cong \bar{\lambda}$. The conjugate operation is also such that each state $|M\rangle$ of $\lambda$ is associated with a unique conjugate state $|\bar{M}\rangle$ of $\bar{\lambda}$. Specifically, the conjugation operation is such that [72]

$$|M\rangle = (-1)^{\varphi(M)} |\bar{M}\rangle \,, \tag{3.23}$$

for a suitable phase function that can be determined as follows: For a GT pattern $M$, define the function

$$s_M(k) = \sum_{j=1}^{k} \sum_{i=1}^{j} M_{i,j} \,, \tag{3.24}$$

which corresponds to the sum of the labels of $M$ in the first $k$ rows (counting from bottom to top). Then [72],

$$\varphi(M) = s_M(d-1) - s_{M_{\max}}(d-1) \,, \tag{3.25}$$

where $M_{\max}$ is defined in Eq. (3.11). We remark that the latter holds up to a redefinition of every GT basis state by a global phase. In this work, we consider the Condon-Shortley convention that fixes the global phase in such a way that usual relations for SU(2) are retrieved.

### 3.1.2 Tensor product representation

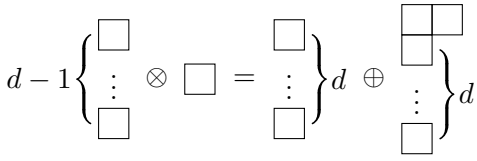
Let $\pi_1, \pi_2$ be irreps of a compact group $G$ acting on the Hilbert spaces $\mathcal{H}_{\pi_1}, \mathcal{H}_{\pi_2}$. The *tensor product* representation is the map

$$\pi_1 \otimes \pi_2 \colon G \ni g \mapsto \pi_1(g) \otimes \pi_2(g) \in \mathrm{U}(\mathcal{H}_{\pi_1} \otimes \mathcal{H}_{\pi_2})\,. \tag{3.26}$$

Note that this generalizes the unitary evolution of a quantum state described by the representation $U(\cdot)U^\dagger$, which is isomorphic to $U \otimes \bar{U}$ in a suitable orthonormal basis. The representation (3.26) is completely reducible, c.f. Theorem 7, hence,

$$\pi_1 \otimes \pi_2 \simeq \bigoplus_\lambda \lambda^{\oplus m_\lambda}\,, \tag{3.27}$$

where $m_\lambda$ is the multiplicity of $\lambda$ in $\pi_1 \otimes \pi_2$. For instance, if $U \colon \mathrm{SU}(d) \to \mathrm{U}(d)$ is the defining representation, we have $U \otimes \bar{U} = 1 \oplus \mathrm{Ad}$, where 1 is the trivial representation and $\mathrm{Ad} \colon \mathrm{SU}(d) \ni g \mapsto \mathrm{Ad}_g \in \mathrm{Aut}(\mathfrak{su}(d))$ is the adjoint representation. Roughly speaking, the decomposition is achieved by combining the two Young diagrams in all possible ways, and summing up the results. In this case, there are only two possibilities that realize allowed Young diagrams: Denoting with $\lambda_U$ and $\lambda_{\bar{U}}$ the Young diagrams associated with $U$ and $\bar{U}$, respectively, $\lambda_U$ can be attached on the right of the top row of $\lambda_{\bar{U}}$, or on the bottom of the column, i.e.




(3.28)

The first diagram on the r.h.s. is equivalent to the diagram with no boxes associated with the trivial irrep, while the second Young diagram identifies the adjoint representation acting on traceless matrices.

The general problem of finding the irrep decomposition of (3.26) for a general compact group $G$ is hard to solve, while in the particular case of the unitary groups a general solution is available in terms of Young diagrams (or, equivalently, GT patterns [74]), as the previous example suggests[1]. Specifically, *Littlewood-Richardson' rules* can be used to decompose the tensor product of two arbitrary irreps [54, 75, 76]. To spell out such rules, let $\lambda_1, \lambda_2$ be Young diagrams associated with irreps of SU($d$). The tensor product representation $\lambda_1 \otimes \lambda_2$ can be evaluated algorithmically as follows [76, Sec. 13.5.3] (or also [54, Sec. C.3]):

1. Assign distinct labels to boxes in each row of the Young diagram $\lambda_2$. For instance, the boxes in the first row will be labeled by 'a', the boxes in the second row by 'b' and so on.

2. Attach boxes labeled by $a$ to $\lambda_1$ in all possible ways such that no two $a$'s appear in the same column, and the result is still a proper Young diagram.

3. Repeat the steps above for all rows of $\lambda_2$.

[1] Note that, due to similarities in their representation theory, the same result holds for general linear groups $\mathrm{GL}(m, \mathbb{C})$, as they can be seen as the complexification of U($d$).

4. Elimination rule: For each box, assign numbers $n_a$ = number of $a$'s above and right to it, $n_b$ = number of $b$'s above and right to it, and so on. If, at any point, the relations $n_a \geq n_b \geq n_c \geq n_d \geq \ldots$ are not satisfied, discard this diagram.

5. Merging rule: If two diagrams are the same, then they are counted as the same if the labels coincide. Otherwise, they refer to distinct irreps.

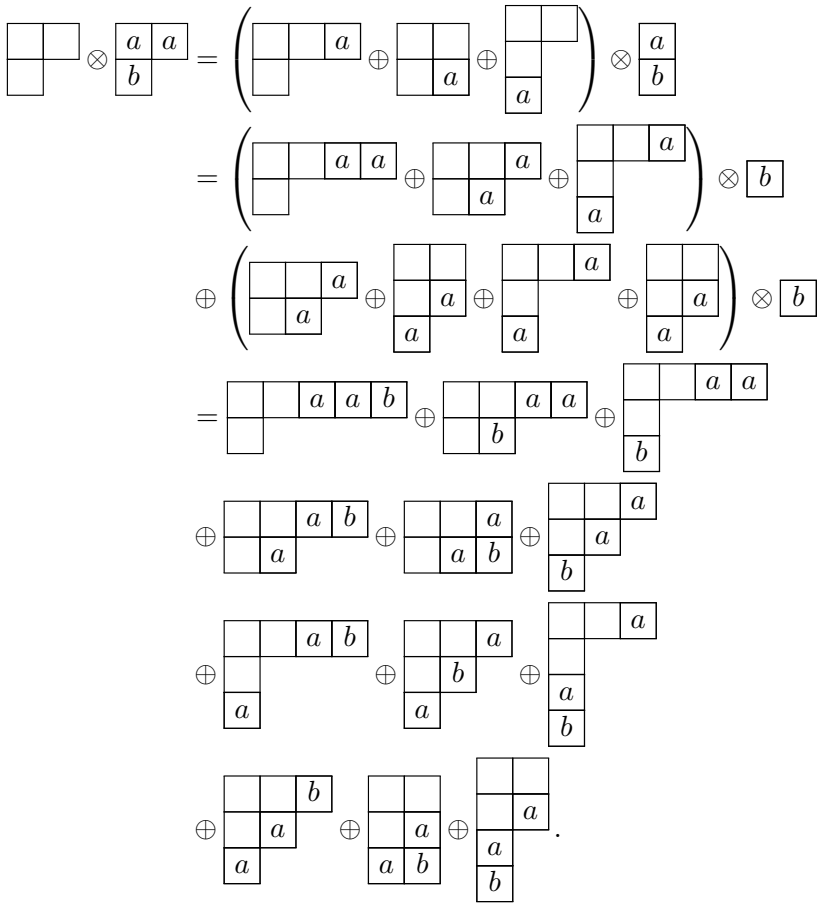
6. Cancel columns with $m$ boxes (since they correspond to constant shifts of the highest weight vector).

7. Remove all the labels after the cancellation and the merging steps.

**Example 16.** Let us consider the following diagrams:

$$\lambda_1 = \ydiagram{2,1}, \quad \lambda_2 = \ydiagram{2,1}. \tag{3.29}$$

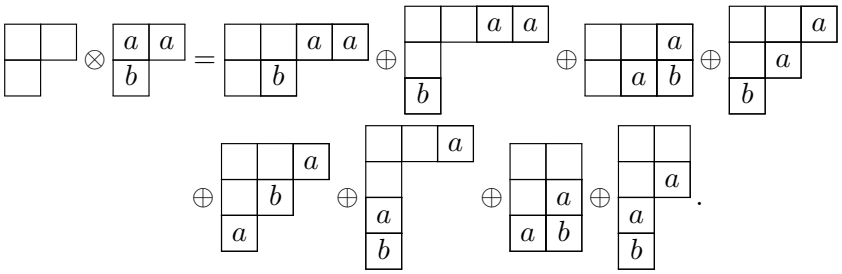
Assigning labels to $\lambda_2$ as in rule 1, and using the second and third rules, we get



(3.30)

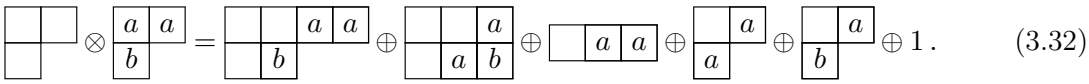
In the second step we got few equivalent diagrams with labels in the same positions, hence they have been merged according to the merging rule. Moreover, we ignored the diagrams with two $a$'s in the same column, in agreement with the symmetric constraint.

By the elimination rule, all the diagrams with a $b$ box attached on the top right shall be eliminated, yielding the following decomposition:

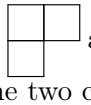



(3.31)

Finally, suppose for instance that these diagrams are associated with SU(3) irreps. Then, all columns with three boxes can be omitted, while any diagram with more than 3 boxes in a column is not allowed. This yields the following decomposition:




(3.32)

In the latter, notice that the diagram  appears with multiplicity 2 in the decomposition, as different labels are assigned to the two copies.

In the high energy literature [76], this decomposition is also written in terms of the dimension of the irrep associated with each Young diagram as

$$\mathbf{8} \otimes \bar{\mathbf{8}} = \mathbf{27} \oplus \mathbf{10} \oplus \mathbf{10'} \oplus \mathbf{8} \oplus \mathbf{8} \oplus \mathbf{1}\,. \tag{3.33}$$

Here, $\mathbf{10}$, $\mathbf{10'}$ indicates that the two irreps are inequivalent, while repeated dimensions denote the same irrep appears with a non-trivial multiplicity.

### Clebsch-Gordan's coefficients

In the context of second quantization, the decomposition of (3.26) can be interpreted as the generalization of the Clebsch-Gordan decomposition of sums of angular momenta in quantum mechanics [54, 74, 77–81]. In particular, Theorem 7 implies that there exists a unitary matrix $C$ –here referred as the *Clebsch-Gordan matrix*– that realizes the isomorphism implicit in Eq. (3.27):

$$C\,(\pi_1 \otimes \pi_2)\,C^\dagger = \bigoplus_\lambda \lambda \otimes \mathbb{1}_{m_\lambda}\,, \tag{3.34}$$

where $\mathbb{1}_{m_\lambda}$ is the $m_\lambda \times m_\lambda$ identity matrix. We explicitly define $C$ as the basis change matrix that takes the product GT basis on the left hand side of Eq. (3.34) to the union of GT bases of every $\lambda$ on the right hand side. More precisely, for GT patterns $M_1 \in \mathrm{GT}(\pi_1), M_2 \in \mathrm{GT}(\pi_2)$, we have

$$|M_1, M_2\rangle = \sum_{\lambda, r} \sum_{M \in \mathrm{GT}(\lambda)} C^{M,r}_{M_1,M_2} |M, r\rangle\,, \tag{3.35}$$

where $r \in [m_\lambda]$ denotes the $r$-th copy of $\lambda$ in $\pi_1 \otimes \pi_2$. The matrix coefficients $C^{M,r}_{M_1,M_2}$ of $C$ are called the *Littlewood-Richardson or Clebsch-Gordan's coefficients*. $C$ is uniquely defined

up to global phases, and by convention it is chosen to be real. Hence, we have the inverse transformation

$$|M, r\rangle = \sum_{M_1 \in \mathrm{GT}(\pi_1)} \sum_{M_2 \in \mathrm{GT}(\pi_2)} C^{M,r}_{M_1,M_2} |M_1, M_2\rangle \,. \tag{3.36}$$

By unitarity of $C$, the following orthogonality relations hold true:

$$\sum_{\lambda, r} \sum_{M \in \mathrm{GT}(\lambda)} C^{M,r}_{M_1,M_2} C^{M,r}_{M_3,M_4} = \delta_{M_1,M_3} \delta_{M_2,M_4} \,, \tag{3.37}$$

$$\sum_{M_1 \in \mathrm{GT}(\pi_1)} \sum_{M_2 \in \mathrm{GT}(\pi_2)} C^{M,r}_{M_1,M_2} C^{M',r'}_{M_1,M_2} = \delta_{M,M'} \delta_{r,r'} \,. \tag{3.38}$$

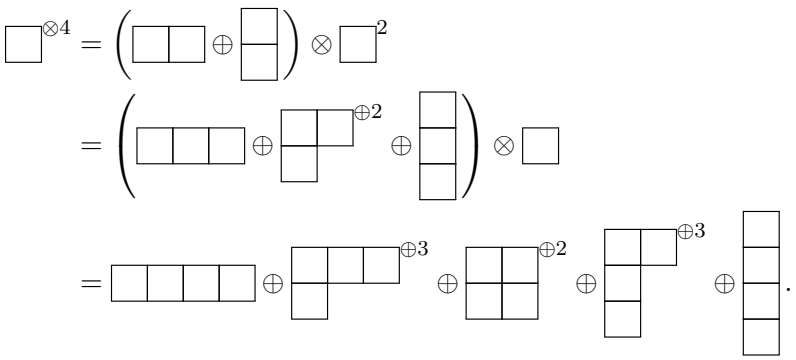
As in the case of SU(2), selection rules for Clebsch-Gordan coefficients of SU($d$) are available: For GT patterns $M_1 \in \mathrm{GT}(\pi_1), M_2 \in \mathrm{GT}(\pi_2), M \in \mathrm{GT}(\lambda)$, $C^{M,r}_{M_1,M_2} = 0$ if

$$w_M \neq w_{M_1} + w_{M_2} \,, \tag{3.39}$$

where $w_{(\cdot)}$ is the weight defined in Eq. (3.15).

### 3.1.3 The diagonal representation

The general problem of decomposing tensor product representations of U($d$) is solved by Littlewood-Richardson' rules. A case of particular interest in quantum information applications is the decomposition of the so-called *diagonal representation* of U($d$): Let $U$ be the defining representation of U($d$). The diagonal representation is defined as the map $\Delta_k \colon \mathrm{U}(d) \ni g \mapsto U(g)^{\otimes k} \in \mathrm{U}(\left(\mathbb{C}^d\right)^{\otimes k})$. Clearly, $\Delta$ is reducible for any $k \geq 2$. For instance, for $k = 4$, we have



(3.40)

The irreducible components of $\Delta_k$ can be elegantly described via *Schur-Weyl*' duality, which can be described as follows: Let $\pi_k \colon \mathfrak{S}_k \to \mathrm{U}(\left(\mathbb{C}^d\right)^{\otimes k})$ be the representation of $\mathfrak{S}_k$ that permutes the vector copies, i.e.,

$$\pi_k(\sigma) |\psi_1 \dots \psi_k\rangle \coloneqq |\psi_{\sigma^{-1}(1)} \dots \psi_{\sigma^{-1}(k)}\rangle \,. \tag{3.41}$$

By construction, $\pi_k$ commutes with $\Delta_k$, which implies $\pi_k \in \mathcal{C}(\Delta_k)$ and $\Delta_k \in \mathcal{C}(\pi_k)$. In fact, the commutants are spanned by such representations:

**Theorem 17** (Schur–Weyl's duality, Thm. 9.1.2 [82])**.** *Let $\Delta_k$ be the diagonal representation of $\mathrm{U}(d)$ and let $\pi_k$ be the representation of $\mathfrak{S}_k$ acting on the space $(\mathbb{C}^{\otimes d})^{\otimes k}$ as in Eq.* (3.41)*. Then,*

$$\mathcal{C}(\Delta_k(\mathrm{U}(d))) = \mathrm{span}\{\pi_k(\mathfrak{S}_k)\}\,, \quad \mathcal{C}(\pi_k(\mathfrak{S}_k)) = \mathrm{span}\{\Delta_k(\mathrm{U}(d))\}\,. \tag{3.42}$$

*Moreover,*

$$(\mathbb{C}^d)^{\otimes k} \cong \bigoplus_{\lambda \vdash k, l(\lambda)\leq d} W_\lambda \otimes S_\lambda\,, \tag{3.43}$$

*where $l(\lambda)$ denotes the length of the partition $\lambda$, i.e., the number of non-zero parts of $\lambda$, and $W_\lambda, S_\lambda$ are irreps of $\mathrm{U}(d), \mathfrak{S}(k)$, respectively.*

Notice that the multiplicity of $W_\lambda$ ($S_\lambda$, respectively) in $(\mathbb{C}^d)^{\otimes k}$ is determined by $\dim S_\lambda$ ($W_\lambda$, respectively), which directly follows from the duality relation in (3.42).

## 3.2 Moment operators

Theoretical guarantees in randomization protocols rely on the computation of averages over groups of unitaries. Let $d\mu_H \equiv dg$ be the normalized Haar measure on $\mathrm{U}(d)$. Throughout this work, we will make extensive use of the properties of the Fourier transform

$$\mathcal{M}(\cdot) \coloneqq \int_{\mathrm{U}(d)} dg\, \omega(g)^\dagger(\cdot)\omega(g) \tag{3.44}$$

for a fixed representation $\omega$ of $\mathrm{U}(d)$ acting on the operator space $\mathrm{L}(\mathbb{C}^{d\times d})$. By fixing an orthonormal basis, the moment operator can be expressed as

$$\mathcal{M} = \int_G dg\, \bar{\omega}(g) \otimes \omega(g)\,. \tag{3.45}$$

We will consider both forms, depending on the context. In the mathematical and quantum information literature, the latter is referred as the *group twirling* or the *moment operator* of $\mathrm{U}(d)$ with respect to $\omega$. In Section 2.4, we have seen it corresponds to a sum of orthogonal projectors onto isotypes following the irrep decomposition of $\omega$.

**Example 18** (Unitary twirl of a channel)**.** Suppose $\omega(g) = U(g)(\cdot)U(g)^\dagger$, where $U$ is the defining representation of $\mathrm{U}(d)$. Then, $\omega \cong \mathrm{id} + \mathrm{Ad}$, where Ad is the adjoint representation acting on the space of traceless operators. Then,

$$\begin{aligned}\mathcal{M}(\cdot) &= \int_G dg\, (\mathrm{id}(g) \oplus \mathrm{Ad}(g))(\cdot)(\mathrm{id}(g) \oplus \mathrm{Ad}(g)^\dagger) \\ &= \int_G dg\, \mathrm{id}(\cdot)\mathrm{id} \oplus \int_G dg\ \mathrm{Ad}(g)^\dagger(\cdot)\,\mathrm{Ad}(g) \\ &= P_{\mathbf{1}} \oplus P_{\mathrm{Ad}}\,,\end{aligned} \tag{3.46}$$

where we used the fact that $\hat{\pi}[\pi]$ is the projector onto $\pi$ for any irrep $\pi$, c.f. Proposition 14. Now, $P_{\mathbf{1}}$ projects onto the trivial subspace spanned by $\mathbb{1}$, while $P_{\mathrm{Ad}}$ projects onto the $(d^2-1)$-dimensional subspace of traceless operators, and we have $P_{\mathbf{1}} \oplus P_{\mathrm{Ad}} = \mathrm{id}$. Then, for any superoperator $\Lambda$

$$P_{\mathbf{1}}(\Lambda) = \frac{1}{d}\,\mathrm{Tr}(\Lambda)\mathbb{1}\,, \quad P_{\mathrm{Ad}}(\Lambda) = \Lambda - P_{\mathbf{1}}(\Lambda) = \Lambda - \frac{1}{d}\,\mathrm{Tr}[\Lambda]\mathbb{1}\,. \tag{3.47}$$

If $\Lambda$ is trace preserving, it follows

$$\begin{aligned}\mathcal{M}(\Lambda) &= \mathrm{Tr}[P_{\mathbf{1}}\Lambda]P_{\mathbf{1}} + \frac{1}{d^2-1}\,\mathrm{Tr}[P_{\mathrm{Ad}}\Lambda]P_{\mathrm{Ad}} \\ &= \frac{1}{d}\,\mathrm{Tr}[\Lambda]\mathbb{1} + \frac{\mathrm{Tr}[P_{\mathrm{Ad}}\Lambda]}{d^2-1}\left(\Lambda - \frac{1}{d}\mathbb{1}\right) \\ &= \frac{1}{d}(1-p_\Lambda)\mathbb{1} + p_\Lambda\Lambda\,,\end{aligned} \tag{3.48}$$

where $p_\Lambda \equiv \frac{\mathrm{Tr}[P_{\mathrm{Ad}}\Lambda]}{d^2-1}$.

In discrete variable systems, a recurrent quantity is the moment operator associated with the diagonal representation $\Delta_k$ for any $k \geq 1$

$$\mathcal{M}_k(\cdot) \coloneqq \int_{\mathrm{U}(d)} dg\, U(g)^{\otimes k\dagger}(\cdot)U(g)^{\otimes k} \cong \int_G dg\, \bar{U}(g)^{\otimes k} \otimes U(g)^{\otimes k}\,. \tag{3.49}$$

(note that for $k = 2$ this is equivalent to the previous example up to isomorphisms). Then, for any $A \in \mathrm{L}((\mathbb{C}^d)^{\otimes k})$, Schur-Weyl duality implies

$$\mathcal{M}_k(A) = \sum_{\sigma\in\mathfrak{S}_k} c_\sigma(A)\pi_k(\sigma)\,. \tag{3.50}$$

Recalling that $U(g)^{\otimes k}$ commutes with $\pi_k$, we have

$$(\pi_k(\tau)|\mathcal{M}_k(A)) = (\mathcal{M}_k(\pi_k(\tau))|A) = (\pi_k(\tau)|A)\,, \tag{3.51}$$

where the last line follows from the normalization of the Haar measure. Hence,

$$(\pi_k(\tau)|A) = \sum_{\sigma\in\mathfrak{S}_k} (\pi_k(\sigma)|A)\underbrace{(\pi_k(\tau)|\pi_k(\sigma))}_{\equiv G_{\tau,\sigma}}\,. \tag{3.52}$$

Therefore,

$$c_\sigma(A) = \sum_{\tau\in\mathfrak{S}_k} G^+_{\tau,\sigma}\,\mathrm{Tr}\left[\pi_k(\tau)^\dagger A\right]\,, \tag{3.53}$$

where $G^+$ is the Moore pseudo-inverse matrix of the Gram matrix $G$. In summary, we have

$$\mathcal{M}_k(A) = \sum_{\sigma,\tau\in\mathfrak{S}_k} G^+_{\tau,\sigma}\,\mathrm{Tr}\left[\pi_k(\tau)^\dagger A\right]\pi_k(\sigma)\,. \tag{3.54}$$

The matrix coefficients $G^+_{\tau,\sigma} \equiv \mathrm{Wg}(\sigma^{-1}\tau)$ are often referred as the *Weingarten functions* [83, 84].

**Example 19.** We can compute the first two moments as they appear frequently in applications. For $k = 1$, we clearly have that $\mathcal{M}_1$ is the projector onto the trivial subspace, i.e.,

$$\mathcal{M}_1(A) = \frac{1}{d}\,\mathrm{Tr}(A)\,\mathbb{1}\,. \tag{3.55}$$

for any $A \in \mathrm{L}(\mathbb{C}^d)$.

Next, by Schur-Weyl' duality, we have

$$\mathcal{M}_2(A) = c_{\mathrm{id}}(A)\mathrm{id} + c_{\mathbb{F}}(A)\mathbb{F} \tag{3.56}$$

for $A \in \mathrm{L}((\mathbb{C}^d)^{\otimes 2})$ (note that, up to vector spaces isomorphisms, this is equivalent to Example 18). Moreover, we can express the projectors onto the symmetric and antisymmetric subspaces as

$$P_{\mathrm{sym}^2} = \frac{1}{2}(\mathrm{id} + \mathbb{F})\,, \quad P_{\wedge^2} = \frac{1}{2}(\mathrm{id} - \mathbb{F})\,, \tag{3.57}$$

from which we obtain the relations

$$\mathrm{id} = P_{\mathrm{sym}^2} + P_{\wedge^2}\,, \quad \mathbb{F} = P_{\mathrm{sym}^2} - P_{\wedge^2}\,. \tag{3.58}$$

Then, it follows

$$\mathcal{M}_2(A) = \frac{2}{d(d+1)}\,\mathrm{Tr}[AP_{\mathrm{sym}^2}]P_{\mathrm{sym}^2} + \frac{2}{d(d-1)}\,\mathrm{Tr}[AP_{\wedge^2}]P_{\wedge^2}\,. \tag{3.59}$$

While Eq. (3.54) provides a general recipe to compute arbitrary $k$th-moment operators, this is in general complicated by the sheer amount of elements in Eq. (3.54) as $k$ increases, restricting practical applications to a few cases. Specifically, easy expressions can be computed if the operator $A$ obeys some symmetries. For instance, suppose $A \in \mathrm{L}(\mathbb{C}^d)$ and $A = |\psi\rangle\langle\psi|$ for a vector $|\psi\rangle \in \mathbb{C}^d$. Then, $\mathcal{M}_k(|\psi\rangle\langle\psi|^{\otimes k})$ is in $\mathcal{C}(U^{\otimes k}) \cap \mathcal{C}(\pi_k)$ and $P_{\mathrm{sym}^k}$ commutes with $|\psi\rangle\langle\psi|$, as $|\psi\rangle\langle\psi|^{\otimes k}$ is invariant under permutations. Then, Schur's lemma and Schur-Weyl' duality imply that $\mathcal{M}_k(|\psi\rangle\langle\psi|^{\otimes k})$ is proportional to $P_{\mathrm{sym}^k} \coloneqq \frac{1}{k!}\sum_{\sigma\in\mathfrak{S}_k}\pi_k(\sigma)$. If $|\psi\rangle \equiv |0\rangle$, this reads as

$$\mathcal{M}_k(|0\rangle\langle 0|^{\otimes k}) = \frac{\langle 0\,|P_{\mathrm{sym}^k}\,|0\rangle}{\mathrm{Tr}(P_{\mathrm{sym}^k})}P_{\mathrm{sym}^k} = \binom{k+d-1}{d-1}^{-1} P_{\mathrm{sym}^k}\,. \tag{3.60}$$

## 3.3 Unitary designs

In practical applications in quantum computing, implementing Haar random unitaries is prohibitively expensive due to the exponential size of $\mathrm{U}(d)$. In particular, a counting argument proves that implementing arbitrary unitaries requires exponentially-large circuits, see [85] or Nielsen and Chuang [57, Sec. 4.5.4.]. This motivates the following definition:

**Definition 20.** *A probability distribution $\nu$ on* $\mathrm{U}(d)$ *is a* unitary k-design *if its $k$th moment operator $\mathcal{M}_k^\nu \coloneqq \int_{\mathrm{U}(d)} d\nu(g)U(g)^{\otimes k}(\cdot)U(g)^{\dagger\otimes k}$ coincides with the $k$th Haar moment operator defined in* (3.49) *with respect to the defining representation of* $\mathrm{U}(d)$*, i.e.,*

$$\mathcal{M}_k^\nu = \int_{\mathrm{U}(d)} d\nu(g)U(g)^{\otimes k}(\cdot)U(g)^{\dagger\otimes k} = \int_{\mathrm{U}(d)} dg\,U(g)^{\otimes k}(\cdot)U(g)^{\dagger\otimes k} = \mathcal{M}_k\,. \tag{3.61}$$

Informally, a unitary $k$-design is indistinguishable from the Haar measure if we are only interested in the first $k$th moment operators. By construction, a unitary $k$-design is also a

$(k-1)$-design. In fact,

$$\begin{aligned}\mathcal{M}_{k-1} &= \int_{\mathrm{U}(d)} dg\, U(g)^{\otimes(k-1)}(\cdot)U(g)^{\dagger\otimes(k-1)} \\ &= \int_{\mathrm{U}(d)} dg\ \mathrm{Tr}_1\left[U(g)^{\otimes k}(\cdot)U(g)^{\dagger\otimes k}\right] \\ &= \int_{\mathrm{U}(d)} d\nu(g)\,\mathrm{Tr}_1\left[U(g)^{\otimes k}(\cdot)U(g)^{\dagger\otimes k}\right] \\ &= \int_{\mathrm{U}(d)} d\nu(g)\, U(g)^{\otimes(k-1)}(\cdot)U(g)^{\dagger\otimes(k-1)} \\ &= \mathcal{M}^{\nu}_{k-1}\,.\end{aligned} \tag{3.62}$$

In most relevant cases, $\nu$ is supported on a finite subset $\mathcal{U} \subset \mathrm{U}(d)$ and is taken to be the uniform distribution on $\mathcal{U}$. In such a case, it can be identified with the counting measure on $\mathcal{U}$ and $\mathcal{M}^{\nu}_k$ simply becomes

$$\mathcal{M}^{\nu}_k = \frac{1}{|\mathcal{U}|}\sum_{g\in\mathcal{U}} U(g)^{\otimes k}(\cdot)U(g)^{\dagger\otimes k}\,. \tag{3.63}$$

In this case, we will also say that $\mathcal{U}$ is a unitary $k$-design. Moreover, since $\mathrm{L}(\mathbb{C}^d) \cong \mathbb{C}^d \otimes (\mathbb{C}^d)^* \cong \mathbb{C}^d \otimes \mathbb{C}^d$, Eq. (3.61) is equivalent to the condition

$$\int_{\mathrm{U}(d)} d\nu(g) U^{\otimes k} \otimes \bar{U}^{\dagger\otimes k} = \int_{\mathrm{U}(d)} dg\, U^{\otimes k} \otimes \bar{U}^{\dagger\otimes k}\,. \tag{3.64}$$

If a unitary $k$-design $\nu$ is supported on a subset $G \subseteq \mathrm{U}(d)$ that form a group, we say that $\nu$ is a *unitary group $k$-design* or simply a *$k$-group design*. In practice, it is highly desirable that $\nu$ is a group design, as this often implies that it can be efficiently described in terms of a small number of generators, which allows for an efficient description and implementation in practice. In this case, as the moment operator $\mathcal{M}_k$ has the interpretation of a Fourier transform, definition (3.61) is equivalent to ask that the equivalence holds for all the irreps contained in $\mathrm{U}^{\otimes k}$. In other terms, since $\mathcal{M}_k$ is the projection onto the commutant of $U^{\otimes k}$, $G \subseteq \mathrm{U}(d)$ is a group design if the projections of $U^{\otimes k}$ and $U|_G^{\otimes k}$ are identical.

We note that the above notion is naturally tailored to discrete quantum systems. In particular, this stems from the choice of the defining representation in Definition 20. By contrast, in bosonic and fermionic systems, the physically relevant representations are the symmetric and antisymmetric irreps of $\mathrm{U}(d)$, which reflect the statistics of bosons and fermions, respectively. For instance, in fermionic systems, a natural set of symmetries is the group of *matchgate unitaries*, that is, unitary operators induced by orthogonal transformations describing the evolution of a quantum system under free fermionic Gaussian dynamics c.f. Chapter 7. This motivates the following natural generalization that will be useful in later chapters:

**Definition 21.** *Let $\gamma$ be a representation of a compact group $G$ and let $\nu$ be a complex Radon measure on $G$. We say that $\nu$ is a* design with respect to $\gamma$ *if*

$$\mathcal{M}^{\nu}_{\gamma} \coloneqq \int_G d\nu(g)\gamma(g) = \int_G dg\,\gamma(g) =: \mathcal{M}\,, \tag{3.65}$$

*where $\mathcal{M}$ denotes the moment operator with respect to the representation $\gamma$ as defined in Eq.* (3.44)*.*

## 3.4 Frames

Adding redundancy is a common strategy to enforce properties of (quantum) signals [16, 86]. While typical basis representations captures all the information of signals, they are often sensitive to noise or loss, so that information is easily corrupted. Mitigating this effect is crucial in practical applications where the noise cannot be completely suppressed. To make this intuition precise, consider an orthonormal basis $\{e_i\}_{i=1}^n \subset \mathcal{H}$ on a Hilbert space $\mathcal{H}$. For any vector $\psi \in \mathcal{H}$ we can consider its basis decomposition $|\psi\rangle = \sum_i \langle e_i|\psi\rangle |e_i\rangle$, which implies Parseval's identity $\|\psi\|^2 = \sum_i |\langle e_i|\psi\rangle|^2$. Now, suppose we try to recover a signal from its components $\langle e_i|\psi\rangle$. Being an orthonormal set, the loss of one of those coefficients prevents the reconstruction of $\psi$, potentially adding a significant error. Instead, we can consider a decomposition into a linearly dependent (overcomplete) set that spans the same Hilbert space:

**Definition 22.** *A set of vectors $\Phi \equiv \{f_i\}_{i=1}^m \subset \mathcal{H}$, $m \geq n = \dim \mathcal{H}$, is a* frame *for $\mathcal{H}$ if there are constants $0 < A \leq B < \infty$ such that*

$$A\|\psi\|^2 \leq \sum_i |\langle f_i|\psi\rangle|^2 \leq B\|\psi\|^2\,, \quad \forall \psi \in \mathcal{H}\,. \tag{3.66}$$

The frame is *tight* if $A = B$. Note that $\Phi$ can be an infinite set. A frame is characterized by the *frame operator* $S\colon \mathcal{H} \to \mathcal{H}$ defined by the relation $S|\psi\rangle := \sum_i \langle f_i|\psi\rangle |f_i\rangle$. By construction, $S$ is self-adjoint and it satisfies the relation $A\mathbb{1} \leq S \leq B\mathbb{1}$ since

$$\langle S\psi|\psi\rangle = \sum_i \langle f_i|\psi\rangle\langle f_i|\psi\rangle = \sum_i |\langle f_i|\psi\rangle|^2\,. \tag{3.67}$$

Then, $S$ is also positive definite and bounded, which implies $S$ is invertible. Note that if $\mathcal{H}$ is finite dimensional, $\{f_i\}_{i=1}^m$ is a frame if and only if it is a spanning set for $\mathcal{H}$. In fact, if $\psi \in \operatorname{span}\{f_i\}_i^{\perp}$, we have the implication

$$A\|\psi\|^2 \leq \sum_i |\langle f_i|\psi\rangle|^2 = 0\,, \tag{3.68}$$

which implies $\|\psi\| = 0$ since $A > 0$. Next, we can define the *dual frame* of $\{f_i\}_{i=1}^m$ to be the the set of vectors $\tilde{\Phi} \equiv \{S^{-1}f_i\}_{i=1}^m$. This is also a frame with frame operator $S^{-1}$, because the latter satisfies $B^{-1}\mathbb{1} \leq S^{-1} \leq A^{-1}\mathbb{1}$. We remark that if $\Phi$ is a tight frame $S = A\mathbb{1}$ and the dual frame operator is simply $\tilde{S} = S^{-1} = A^{-1}\mathbb{1}$. Moreover, the following *reconstruction formula* holds:

$$|\psi\rangle = \sum_i \langle f_i|\psi\rangle |\tilde{f}_i\rangle = \sum_i \langle \tilde{f}_i|\psi\rangle |f_i\rangle\,. \tag{3.69}$$

We remark that the dual frame is not uniquely specified [87, 88].

In quantum computation, frames naturally appear in characterization and tomographic protocols, for instance, in the form of mutually unbiased bases (MUBs) [89]. In this thesis, we are interested in frames associated with Haar random unitaries (or unitary designs). In particular, it is straightforward to see that, for a unitary 2-design $\nu$, the ensemble $\{U|0\rangle\langle 0|U^\dagger\}_{U\sim\nu}$ is a frame. In fact, the operator $S$ such that

$$\begin{aligned} S(A) &= \mathbb{E}_U \operatorname{Tr}[U|0\rangle\langle 0|U^\dagger A]U|0\rangle\langle 0|U^\dagger \\ &= \operatorname{Tr}_1[\mathbb{E}_U U^{\otimes 2}|0\rangle\langle 0|U^{\dagger\otimes 2} A\otimes \mathbb{1}]\,, \end{aligned} \tag{3.70}$$

is a depolarizing channel, c.f. Eq. (3.48). Hence, it can be inverted, and the positive operator-valued measure (POVM) $\{U|0\rangle\langle 0|U^\dagger\}$ is a frame.

## 3.5 The Pauli and Clifford groups

Many methods to simulate, benchmark and certify quantum systems are based on the special class of quantum circuits that entail *stabilizer states*, *Clifford unitaries* and *Pauli measurements*. These can be efficiently described in terms of the *stabilizer formalism*, which is mathematically grounded in the representation theory of the discrete phase space. In this section, we provide an introduction to the Clifford group and discuss some of its design properties. We refer to [90] for more details and proofs.

The *Pauli group* over $n$ qubits is the group $\mathcal{P}_n$ generated by all $n$-fold tensor product of Pauli operators

$$\mathcal{P}_n \coloneqq \langle \{ i^k \sigma_1 \otimes \cdots \otimes \sigma_n \mid x \in \mathbb{Z}_4, \sigma_i \in \{\mathbb{1}, X, Y, Z\}\} \rangle \,, \tag{3.71}$$

where the single-qubit Pauli operators $X, Y, Z$ have the following representation in the computational basis:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.72}$$

It is convenient to parametrize single-qubit Pauli operators by binary vectors $v = (z, x) \in \mathbb{F}_2^2$, where $\mathbb{F}_2 = \{0, 1\}$ is the binary finite field, as

$$W(0,0) \coloneqq \mathbb{1}, \qquad W(0,1) \coloneqq X, \qquad W(1,0) \coloneqq Z, \qquad W(1,1) \coloneqq Y. \tag{3.73}$$

Then, we define the $n$-qubit Pauli operators as tensor products of the single-qubit Pauli operators, indexed by vectors $v = v_1 \oplus \cdots \oplus v_n \in \mathbb{F}_2^{2n}$:

$$W(v) \coloneqq W(v_1) \otimes \cdots \otimes W(v_n) \,. \tag{3.74}$$

We refer to this notation as the phase space representation of Pauli operators (or, equivalently, as the Weyl representation), motivated by the relation

$$W(a)W(b) = (-1)^{[a,b]} W(b)W(a) \,, \tag{3.75}$$

for any $a, b \in \mathbb{F}_2^{2n}$, where $[\cdot, \cdot]$ denotes the binary symplectic product defined as

$$[a, b] \coloneqq \sum_{i=1}^{n} a_i b_{i+n} + a_{i+n} b_i \tag{3.76}$$

Formally, the operators $W(v)$ are the (projective) irreducible representations of the discrete phase space $\mathbb{F}_2^{2n}$, as they satisfy the composition law

$$W(a)W(b) = i^{\beta(a,b)} W(a+b) \,, \tag{3.77}$$

where $\beta \colon \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \to \mathbb{Z}_4$ is a suitable phase that takes into account the additional (complex) phases in the composition of two different Paulis (e.g., $ZX = iY$). As such operators are

traceless (except for the identity), it follows from the composition law that they define an orthonormal basis for the space of linear operators on $(\mathbb{C}^2)^{\otimes n}$ with respect to the Hilbert-Schmidt inner product, i.e.

$$(W(a)|W(b)) \propto \operatorname{Tr} W(a+b) = \delta_{a,b} \operatorname{Tr} \mathbb{1} \,. \tag{3.78}$$

This motivates the shorthand notation

$$|v) \equiv \frac{1}{\sqrt{d}} W(v) \tag{3.79}$$

for the normalized Pauli operators, so that the set $\{|v)\}$ denotes the orthonormal Pauli basis in $\mathbb{C}^{d\times d}$, where $d = 2^n$ is the dimension of the Hilbert space of $n$ qubits from now on.

We remark that the irreps defined by (3.77) are intimately connected with the irreps of the *Heisenberg-Weyl group* $\mathbb{H}_n(2)$ [90]. This is defined as the group of pairs $(v,t) \in \mathbb{F}_2^{2n} \times \mathbb{Z}_4$ that satisfy the composition law

$$(v_1,t_1)(v_2,t_2) \coloneqq (v_1+v_2, t_1+t_2+\beta(v_1,v_2)) \,, \tag{3.80}$$

where $\beta\colon \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \to \mathbb{Z}_4$, introduced in 3.77, is referred as a *Schur multiplier* [68]. In particular, associativity of the group multiplication implies that

$$\beta(v+w,u) + \beta(v,w) - \beta(v,u+w) - \beta(u,w) = 0 \,, \tag{3.81}$$

from which we deduce

$$\beta(v,v) = \beta(v,0) = \beta(0,v) = 0 \,, \tag{3.82}$$

$$\beta(v,w) - \beta(w,v) = 2[v,w] \,. \tag{3.83}$$

Setting $v = (v_z, v_x)$ with $v_z, v_x \in \mathbb{F}_2^n$, the unitary irreps of $\mathbb{H}_n(2)$ are given by

$$\tilde{W}(v,t) f(u) = \chi_2(v_z \cdot u)\chi_4(t + v_z \cdot v_x) f(u+v_z) \,, \tag{3.84}$$

where $\chi_2$, $\chi_4$ are characters of $\mathbb{Z}_2$ and $\mathbb{Z}_4$, respectively, and the product $v_z \cdot v_x$ is modulo 4. Then, $\tilde{W}(v,0)$ are projective irreps of $\mathbb{F}_2^{2n}$ satisfying Eqs. (3.75) and (3.77), and we use the shorthand notation $\tilde{W}(v,0) \equiv W(v)$ to denote the Weyl operators. Next, Stone-Von Neumann' theorem ensures that any irrep of $\mathbb{H}_n(2)$ that is unitarily equivalent to $\tilde{W}$ must agree with it on its centre, and vice versa. More formally, if $\phi$ is a centre-fixing automorphism of $\mathbb{H}_n(2)$, $\tilde{W} \circ \phi$ is also an irrep of $\mathbb{H}_n(2)$ that is unitarily equivalent to $\tilde{W}$. Hence, there exists a unitary operator $U$ that intertwines $W$ and $W \circ \phi$, which is uniquely determined up to a complex phase. Notably, one can prove that the centre-fixing automorphisms of $\mathbb{H}_n(2)$ are given by pairs $(g, \tilde{\alpha}_g)$, where $g \in \mathrm{Sp}(2n,2)$ and $\tilde{\alpha}_g$ is a function that satisfies the relation [90]

$$\beta(g\cdot v, g\cdot w) - \beta(v,w) = \tilde{\alpha}_g(v+w) - \tilde{\alpha}_g(v) - \tilde{\alpha}_g(w) \tag{3.85}$$

for any $g \in \mathrm{Sp}(2n,2)$ and $v, w \in \mathbb{F}_2^{2n}$. We define the Clifford group as the smallest finite subgroup of the normalizer of the discrete phase space[2]. In particular, one can prove that $\tilde{\alpha}_g = \alpha_g + [w, \cdot]$, where $\alpha_g : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ is a suitable function satisfying the compatibility

[2]More rigorously, $\mathrm{Cl}_n$ is the smallest finite subgroup of the normalizer of $\mathbb{H}_n(2)$ such that $Z(\mathrm{Cl}_n) = \mathbb{Z}_4$.

condition $\alpha_g(0) = 0$ [90, Sec. 3.3]. We remark that the latter relation can also be used to compute the phase function $\beta$ in time $\mathrm{O}(n^3)$ by fixing the values of $\alpha_g$ on an orthonormal basis [90, Sec. 4.4]. With these notations, the action of $U \in \mathrm{Cl}_n$ on Weyl operators can be written as

$$UW(v)U^\dagger \coloneqq \chi([a, v] + \alpha_g(v))W(g(v))\,, \tag{3.86}$$

where $\chi(v) \coloneqq i^{-v_z \cdot v_x}$ denotes the character of $W(v)$.

We can use the facts just summarized to show that the Clifford group is a unitary 2-design [37–39]:

**Proposition 23.** *$\mathrm{Cl}_n$ is a unitary 2-design. In particular, for $u, v \in \mathbb{F}_2^{2n}$,*

$$\mathbb{E}_{U\sim\nu}\, U^{\otimes 2}W(u) \otimes W(v)U^{\otimes 2\dagger} = \begin{cases} \mathbb{1}\,, & \text{if } u = 0 \text{ and } v = 0 \\ \frac{\delta_{u,v}}{d^2-1}\,(d\,\mathbb{F} - \mathbb{1})\,, & \text{otherwise} \end{cases}\,, \tag{3.87}$$

*where $\delta_{u,v}$ is the Kronecker $\delta$ over $\mathbb{F}_2^{2n}$, and $\mathbb{F}$ is the swap operator defined by $\mathbb{F}|\psi\rangle \otimes |\phi\rangle = |\phi\rangle \otimes |\psi\rangle$ for any $|\psi\rangle$, $|\phi\rangle \in \mathbb{C}^d$.*

*Proof.* To show that $\mathrm{Cl}_n$ is a unitary 2-design, it is enough to check this property on the Pauli basis. For $v, u \in \mathbb{F}_2^{2n}$, we have

$$\begin{aligned} &\frac{1}{|\mathrm{Cl}_n|}\sum_{U\in\mathrm{Cl}_n} U^{\otimes 2}W(u) \otimes W(v)U^{\dagger\otimes 2} \\ &\quad= \frac{1}{|\mathrm{Cl}_n|}\sum_{a\in\mathbb{F}_2^{2n}} \chi([a, v+u]) \sum_{g\in\mathrm{Sp}(2n)} \chi(\alpha_g(v) + \alpha_g(u))W(g(v)) \otimes W(g(u)) \\ &\quad= \frac{1}{2^{2n}}\sum_{a\in\mathbb{F}_2^{2n}} \chi([a, u+v]) \frac{1}{|\mathrm{Sp}(2n)|}\sum_{g\in\mathrm{Sp}(2n)} \chi(\alpha_g(v) + \alpha_g(u))W(g(v)) \otimes W(g(u)) \\ &\quad= \frac{1}{|\mathrm{Sp}(2n)|}\delta_{u,v}\sum_{g\in\mathrm{Sp}(2n)} W(v) \otimes W(v)\,. \end{aligned} \tag{3.88}$$

In the last line, we use orthogonality of characters. Then, observe that the average over $\mathrm{Sp}(2n)$ can be written as an average over the orbit of $v$ under $\mathrm{Sp}(2n)$ and, for $v \neq 0$, the actions of $\mathrm{Sp}(2n)$ over $\mathbb{F}_2^{2n} \setminus \{0\}$ is transitive, so that we obtain

$$\frac{1}{|\mathrm{Cl}_n|}\sum_{U\in\mathrm{Cl}_n} U^{\otimes 2}W(u) \otimes W(v)U^{\dagger\otimes 2} = \frac{1}{2^{2n}-1}\delta_{u,v}\sum_{v\in\mathbb{F}_2^{2n}\setminus\{0\}} W(v) \otimes W(v)\,. \tag{3.89}$$

Moreover, as we have $\mathbb{F} = 2^{-n}\sum_{v\in\mathbb{F}_2^{2n}} W(v) \otimes W(v)$, we have

$$\frac{1}{|\mathrm{Cl}_n|}\sum_{U\in\mathrm{Cl}_n} U^{\otimes 2}W(u) \otimes W(v)U^{\dagger\otimes 2} = \begin{cases} \frac{1}{2^{2n}-1}\delta_{u,v}\,(2^n\mathbb{F} - \mathbb{1})\,, & v \neq 0, \\ \delta_{u,0}\mathbb{1}\,, & v = 0\,. \end{cases} \tag{3.90}$$

On the other hand, from Eq. (3.59) we have

$$\int_{\mathrm{U}(d)} dg\, U(g)^{\otimes 2}(\cdot)U(g)^{\dagger\otimes 2} = \frac{2}{d(d+1)}|P_{\mathrm{sym}^2})(P_{\mathrm{sym}^2}| + \frac{2}{d(d-1)}|P_{\Lambda^2})(P_{\Lambda^2}|\,, \tag{3.91}$$

which implies

$$\begin{aligned}\int_{\mathrm{U}(d)} dg\, U(g)^{\otimes 2}(W(u)\otimes W(v))U(g)^{\dagger\otimes 2} \\ &= \frac{2}{d(d+1)}\operatorname{Tr}[W(u)\otimes W(v)P_{\mathrm{sym}^2}]P_{\mathrm{sym}^2} + \frac{2}{d(d-1)}\operatorname{Tr}[W(u)\otimes W(v)]P_{\Lambda^2} \\ &= \frac{1}{d(d+1)}\left(\delta_{u,0}\delta_{v,0}d^2+\delta_{u,v}d\right)(\mathbb{1}+\mathbb{F}) + \frac{1}{d(d-1)}\left(\delta_{u,0}\delta_{v,0}d^2+\delta_{u,v}d\right)(\mathbb{1}-\mathbb{F})\ .\end{aligned} \tag{3.92}$$

Hence, the equivalence follows from a case-by-case comparison. □

# Part II

# Shadow estimation beyond group designs

# Chapter 4

# Introduction to this Part

Retrieving information about the state of a quantum system is a central task in quantum technologies. Full quantum state tomography can recover a complete, precise classical description of the state but requires a large number of state copies [16, 17, 19, 91, 92], restricting concrete applications only to a small number of qubits. Moreover, for many concrete tasks, complete knowledge of the quantum state is often unnecessary [93], and estimation schemes for specific properties are often scalable, and hence, highly desirable. Building on this insight, Huang *et al.* [45], Paini and Kalev [46] introduced a novel estimation primitive, nowadays referred to as *shadow estimation*. By measuring a state $\rho$ in randomly selected bases, an approximation $\hat{\rho}$, called the *classical shadows*, capable of estimating expectation values with high probability is constructed. This approach is devised in a way that converges to full state tomography in the ideal limit of many measurements. This ensures that, by further post-processing, the classical shadows can be used to construct suitable estimators for arbitrary sets of observables. This procedure is scalable and outperforms full quantum state tomography for many different tasks. More precisely, to design a scalable shadow estimation protocol, one shall ensure the efficient experimental implementation of the protocol by considering states, unitaries and measurements that are available in labs [29, 94]. Then, we require that the sampling complexity scales favorably with system size (for instance, ensured by carefully choosing the randomized measurement to respect the symmetries of the system), and the classical post-processing can be performed in polynomial time with the system size (guaranteed by efficient classical simulation algorithms such as stabilizer simulation [34, 35]). The original examples introduced in [45] consider random unitaries drawn from subgroups of the Clifford group. By considering global Cliffords on the space of $n$ qubit, efficient and rigorous guarantees on the sampling complexity of tasks such as fidelity estimation can be formulated, while randomization over local unitaries –effectively equivalent to measuring in randomly chosen Pauli bases– yields efficient estimators for local properties[1].

In this part, we introduce the shadow estimation protocol and discuss recent developments beyond group designs. In the discrete setting of digital quantum computation, we discuss the generalization of shadow estimation to unitary ensembles without group structure, characterizing the protocol for the arguably simplest non-trivial random quantum circuit: A two-layered random circuit, in a brickwork architecture, consisting of product of 2-local random unitaries. Next, we move the discussion to fermionic systems. Firstly

[1]This paragraph has been adapted from [52].

motivated by fermionic quantum simulation, tomographic techniques based on random fermionic unitaries are particularly attractive in near-term applications for their flexibility and simple implementation [95–98]. In particular, due to their experimental friendliness and versatility, classical shadows find a natural environment of applications in many-body physics and quantum chemistry, and extensions to fermionic systems have been put forward in recent works [96, 99].

This part is structured as follows. In chapter Chapter 5, we review the general shadow estimation protocol of [45] from the point of view of frame theory. Broadly speaking, the protocol has two distinct phases: In the first one, samples from a quantum system are collected by performing suitable randomized measurements on an unknown input state. Next, these data are further elaborated to obtain estimators of classes of observables. We discuss in detail how the protocol is devised and the challenges in post-processing in Section 5.1. In Sections 5.2 and 5.3, we review shadow estimation using global Clifford circuits, respectively. Chapter 6 is adapted from [52] and it is dedicated to the analytical analysis of shadow estimation using short random circuits. Here, the characterization of the relevant measurement channel is discussed in details. In Section 6.4 we present preliminary results and attempts to extend the characterization of the frame operator of random quantum circuit or arbitrary depth. Lastly, we discuss the generalization of shadow estimation to fermionic systems in Chapter 7, and formalize preliminary results for symmetry-adapted classical shadows in spin systems.

# Chapter 5

# Shadow estimation

In practical applications, the full reconstruction of a quantum state is often unnecessary, and it typically suffices to estimate expectation values of a prescribed family of observables. Relevant quantities include, for instance, correlation functions, entanglement entropies, energy values, or fidelities with respect to a target state. This perspective motivated the development of *shadow tomography* [93], with the goal of estimating the "shadow" cast by the state on a collection of measurements, rather than reconstructing the state itself. Technically, this amounts to designing a procedure to find a POVM that accepts the input state $\rho$ with high probability whenever a given property holds, while keeping the overall error probability under control. Such a scheme can be implemented using polynomially many copies of $\rho$ in the number of qubits. Building on this insight, Huang *et al.* [45] introduced a randomized protocol, here referred to as *(classical) shadow estimation*, where a random unitary is applied to the input state, later measured in a fixed basis. A suitable classical post-processing phase guarantees the efficient prediction of many expectation values from the same measurement data. In this chapter, we discuss this protocol under the lens of frame theory, and review the most relevant mathematical aspects that will serve for further extensions in the next chapters.

## 5.1 Classical shadows formalism

The shadow estimation protocol introduced by Huang *et al.* [45] can be naturally cast in the language of frame theory discussed in Section 3.4 [52, 100]. Intuitively, instead of adapting the measurement setting to the particular properties of a quantum state, we perform random measurements sampled from a fixed ensemble. In practice, this is equivalent to perform a measurement in a randomly chosen basis. Then, the sampled data are post-processed to construct an estimator that captures some of the features of the input state. Importantly, the same set of measurement data can be used to estimate several expectation values at the same time. This intuition will also be applied later to estimate average gate fidelities with randomized benchmarking [29, 50, 100]. We summarize the two steps in a *data collection* phase and a *classical post-processing* phase:

**Data collection phase** Let $\rho$ be a given unknown state on a $n$-qubit system, let $d = 2^n$. We fix a probability measure $\nu$ on the unitary group $\mathrm{U}(d)$ and perform the following steps:

- Draw $U \sim \nu$ and apply the transformation $\rho \mapsto U\rho U^\dagger$.
- Perform a measurement in the computational basis described by the POVM $\{E_i \coloneqq |i\rangle\langle i|\}_{i\in[d]}$.
- Store the *classical snapshot* $(i, U)$.

The above primitive is repeated $T \in \mathbb{N}$ times, yielding the snapshots $\{(i_k, U_k)\}_{k=1}^T$.

**Classical post-processing** Let $O$ be an observable. To estimate $\mathrm{Tr}(O\rho)$, note that the average over $\nu$ and the computational basis measurements amounts to applying the *measurement channel*

$$S(\rho) \coloneqq \sum_{i\in[d]} \mathbb{E}_{U\sim\nu} |E_{i,U})(E_{i,U}\,|\rho) = \sum_{i\in[d]} \mathbb{E}_{U\sim\nu} \langle i\,|U\rho U^\dagger|\,i\rangle\, U^\dagger|i\rangle\langle i|U\,, \tag{5.1}$$

where $E_{i,U} \coloneqq U^\dagger E_i U$, with $E_i = |i\rangle\langle i|$. If the POVM $\{E_{i,U}\}$ is tomographically complete [101], i.e., for all states $\rho \neq \sigma$ there exists a pair $(i, U)$ such that $\langle i\,|U\rho U^\dagger|\,i\rangle \neq \langle i\,|U\sigma U^\dagger|\,i\rangle$, then, $\{E_{i,U}\}$ is a frame [19, 102], and the associated measurement channel (5.1) has the interpretation of a frame operator. In particular, $S$ is positive definite, and thus invertible. It follows that $\{\tilde{E}_{i,U} \coloneqq S^{-1}(E_{i,U})\}$ is the canonical dual frame and the identity

$$\mathrm{Tr}(O\rho) = \mathrm{Tr}(OS^{-1}S(\rho)) = \sum_i \mathbb{E}_{U\sim\nu} (O|\tilde{E}_{i,U})(E_{i,U}\,|\rho) \tag{5.2}$$

holds true. Note that $S^{-1}$ is not a quantum channel in general, as it is not necessarily completely positive. Nevertheless, it can be classically applied to the POVM element $E_{i,U}$ to obtain the dual frame elements $S^{-1}(E_{i,U})$, here referred as the *classical shadows* of $\rho$ [45]. This name is justified by the simple observation that, by definition, $\rho = \mathbb{E}[S^{-1}(U^\dagger|i\rangle\langle i|U)]$. Therefore, Eq. (5.2) can be interpreted as the expected value of $f_O(i, U) \coloneqq (O|\tilde{E}_{i,U})$ when sampling $U \sim \nu$ and $i \sim (E_{i,U}\,|\rho)$ and is, thus, the limit of the empirical average $\hat{o} = \sum_{k=1}^T f_O(i_k, U_k)$ over many experimental snapshots.

We remark that we can apply a similar procedure even if $\{E_{i,U}\}$ is *not* tomographically complete. In this case, $S$ is not necessarily invertible and we restrict to the pseudo-inverse $S^+$, defined on the range of $S$. For instance, this is the case of certain unitary ensembles drawn from subgroups $G \subset \mathrm{U}(d)$ that do not form a unitary 2-design, see e.g. [103].

Sampling complexity guarantees of shadow estimation follow from Chebyshev's inequality: $T = \mathrm{O}(\mathrm{Var}[\hat{o}]/(\epsilon^2\delta))$ suffices to ensure that $|\hat{o} - o| < \epsilon$ with high-probability $\delta$. Note that a Hoeffding bound here yields a worse bound scaling as $(v\,|S|v)^{-2}$ following from the definition of $f_O(i, U)$. This bound is sometimes formulated in terms of the *shadow norm* introduced by Huang *et al.* [45], that depends only on the target function and the measurement primitive, defined as

$$\|O\|_{\mathrm{sh}}^2 \coloneqq \max_{\rho\in\mathcal{S}(\mathcal{H})} \left( \sum_{i\in[d]} \mathbb{E}_{U\sim\nu} (O\,|S^{-1}|\,E_{i,U})^2 (E_{i,U}\,|\rho) \right). \tag{5.3}$$

If the expectation values of 'many' observables are to be estimated at once, it may be beneficial to use the *median-of-means estimator* with sampling complexity depending only

logarithmically on $\delta$ [45]. This works as follows: Split the $T$ measurement shots into $K$ equally sized batches. Typically, it is enough to choose $K = \Theta(\log(M/\delta))$, with $M$ being the number of observables. For measurement shots in each block, the empirical average is computed. The final output is the median over all batches. Intuitively, taking the median effectively filters out the contribution of outliers compared to the standard empirical average estimator, yielding only logarithmic dependence on $\delta$ and the number of observables $M$ [45, 104].

### 5.1.1 Classical post-processing

The inversion of the frame operator is central in the post-processing phase. However, it is in general a highly non-trivial task, and the analytical inversion of $S$ is often only possible in very special cases where the probability measure is very structured. For instance, if $\nu$ is the Haar measure on $\mathrm{U}(d)$, then the POVM $\{E_{i,U}\}$ is a complex projective (state) 2-design and, thus, forms a tight frame on the space of traceless Hermitian matrices, c.f. Section 3.4. As a consequence, $S$ is a depolarizing channel and can be readily inverted. A similar argument can be applied when the unitaries $U$ are drawn Haar-randomly from certain subgroups $G \subset \mathrm{U}(d)$ [50]. In the general case, analytic inversion is too complicated and one has to rely on numerical methods which are not only expensive, but may also be numerically unstable since there are no general guarantees on the condition number of $S$. In principle, the condition number can even be exponentially large [50].

Nevertheless, the inversion of $S$ is drastically simplified under certain conditions. Notably, if the measure $\nu$ is right-invariant under multiplication with Pauli operators, $S$ is diagonal in the Pauli basis $\{|v) \equiv \frac{1}{\sqrt{d}}|W(v))\}_{v\in\mathbb{F}_2^{2n}}$ [105]. To show this fact, let $\mathcal{W}(v) \coloneqq W(v)(\cdot)W(v)^\dagger$ be the action of Paulis on linear operators, let $U$ be the defining representation of $\mathrm{U}(d)$ and set $\omega = U(\cdot)U^\dagger$. Then, by right-invariance of $\nu$,

$$\begin{aligned}\mathcal{W}(v)^\dagger S\mathcal{W}(v) &= \sum_{i\in[d]} \int d\nu(g)\mathcal{W}(v)^\dagger\omega(g)^\dagger|E_i)(E_i|\omega(g)\mathcal{W}(v) \\ &= \sum_{i\in[d]} \int d\nu(g)\omega(g)^\dagger|E_i)(E_i|\omega(g) \\ &= S\,,\end{aligned} \tag{5.4}$$

Hence, $S$ is invariant under the channel twirl over the Pauli group. Therefore, it is a Pauli channel and, in particular, diagonal in the Pauli basis, which implies $S^{-1}$ can be computed via entrywise inversion of the diagonal elements $(v\,|S|\,v)$. Notice that, for Pauli invariant ensembles without group structure, it is convenient to construct the estimator according to Eq. (5.2) instead of the classical shadows $S^{-1}(\rho)$ as in [45]: For instance, this is the case of sparse observables in the Pauli basis [106], where the computation of the estimator $(O|\tilde{E}_{i,U})$ is still numerically feasible. Indeed, in the latter case, one would rely on the decomposition of $\rho$ in the Pauli basis, which usually involves exponentially many terms.

### 5.1.2 Pauli-invariant ensembles

If $O = W(v)$ is a Pauli observable (we call this task *Pauli estimation*) and if $\nu$ is Pauli invariant, the sample complexity can be analytically bounded. In particular, $S$ is diagonal

in the Pauli basis, and we have

$$f_{W(v)}(i,U) = \frac{1}{(v\,|S|\,v)}(W(v)|E_{i,U})\,. \tag{5.5}$$

Note that this expression features only a single diagonal element of the frame operator independent of $i$ and $U$. The sample complexity of the corresponding mean estimator $\hat{w}(v) \coloneqq \frac{1}{T}\sum_{j=1}^{T} f_{W(v)}(i_j,U_j)$ is determined by the variance of $f_{W(v)}(i,U)$ which is dominated by the eigenvalues of $(v\,|S|\,v)^{-1}$. In particular, we have the following fact [105]:

**Proposition 24.** *Let $\nu$ be a Pauli invariant measure. Then,* $\mathrm{Var}[\hat{w}(v)] \leq (v\,|S|\,v)^{-1}$.

*Proof.* The statement follows from the following calculation, based on the definition of $S$:

$$\begin{aligned}
\mathrm{Var}[\hat{w}(v)] &= \sum_i \mathbb{E}_U f_{W(v)}(i,U)^2 - \left[\sum_i \mathbb{E}_U f_{W(v)}(i,U)\right]^2 \\
&\leq \sum_i \mathbb{E}_U (W(v)\,|S^{-1}|\,E_{i,U})^2 (E_{i,U}|\rho) \\
&= \frac{1}{d^2}\frac{1}{(v\,|S|\,v)^2}\sum_{u\in\mathbb{F}_2^{2n}}\sum_i \mathbb{E}_U (W(u)W(v)W(u)|E_{i,U})^2 (E_{i,U}|W(u)\rho W(u)) \\
&= \frac{1}{d^2}\frac{1}{(v\,|S|\,v)^2}\sum_i \mathbb{E}_U (W(v)|E_{i,U})^2 (E_{i,U}|\sum_{u\in\mathbb{F}_2^{2n}} W(u)\rho W(u)) \\
&= \frac{1}{d}\frac{1}{(v\,|S|\,v)^2}\sum_i \mathbb{E}_U (W(v)|E_{i,U})^2 \\
&= \frac{1}{(v\,|S|\,v)}\,,
\end{aligned} \tag{5.6}$$

where we used Pauli-invariance in the third step, $W(u)W(v)W(u) \propto W(v)$ in the fourth step, and $\frac{1}{d^2}\sum_{u\in\mathbb{F}_2^{2n}} W(u)\rho W(u) = \frac{1}{d}\mathbb{1}$ as Pauli operators form a 1-design [38, 107]. Then, Chebyshev's bound ensures that the mean estimator is $\epsilon$-precise using $O((v\,|S|\,v)^{-1}\epsilon^{-2}\delta^{-1})$ many snapshots with probability $1-\delta$. □

For general observables, however, it is not easy to find strict guarantees for the sample complexity, since it is hard to analytically bound the variance, even for different classes of Pauli invariant measures. In these cases, one can rely on the weaker notion of *locally scrambled shadow norm* [106, 108, 109], which can be interpreted as the average variance over all states. In particular, since the variance is linear in the state $\rho$, the locally scrambled shadow norm thus quantifies the performance when $\rho$ is the completely mixed state.

**Proposition 25.** *Let $O$ be an observable and let $\hat{o}$ be the classical shadow estimator. Define the locally scrambled variance with respect to the completely mixed state as* $\mathrm{Var}[\hat{o}|\frac{1}{d}\mathbb{1}]_{\mathrm{lssh}} = \mathbb{E}[\hat{o}^2|\frac{1}{d}\mathbb{1}] - \mathbb{E}[\hat{o}|\frac{1}{d}\mathbb{1}]^2$. *Then,* $\mathrm{Var}[\hat{o}]_{\mathrm{lssh}} \leq \sum_u \frac{c_u^2}{(u\,|S|\,u)}$.

*Proof.* Using the decomposition in the Pauli basis $O = \frac{1}{d}\sum_{u\in\mathbb{F}_2^{2n}} c_u W(u)$ with coefficients

$c_u \equiv \mathrm{Tr}(W(u)O)$, this reads as follows:

$$\begin{aligned}\mathrm{Var}[\hat{o}]_{\mathrm{lssh}} &\leq \frac{1}{d}\sum_i \mathbb{E}_U (O\,|S^{-1}|E_{i,U})^2 (E_{i,U}|\mathbb{1}) \\ &= \frac{1}{d}\sum_i \mathbb{E}_U \sum_{u,w} \frac{c_u c_w}{(u\,|S|u)(w\,|S|w)} (W(u)|E_{i,U})(W(w)|E_{i,U}) \\ &= \sum_{u,w} \frac{c_u c_w}{(u\,|S|u)(w\,|S|w)} (u\,|S|w) \\ &= \sum_u \frac{c_u^2}{(u\,|S|u)}\,.\end{aligned} \tag{5.7}$$

□

In the remaining sections of this chapter, we will analyze revisit the results of [45] concerning local and global Clifford unitaries under the lens of the formalism here introduced.

## 5.2 Shadow estimation with global Clifford unitaries

Arguably the simplest unitary ensemble to consider for shadow estimation is the full unitary group $\mathrm{U}(d)$, i.e., $\nu \equiv \mu_H$ is the Haar measure on $\mathrm{U}(d)$. In practice, this is equivalent to sample from a unitary 2-design (or a unitary 3-design, in the case of the Clifford group $\mathrm{Cl}_n$). In particular, sampling from $\mathrm{Cl}_n$ can be achieved in polynomial time in $n$ [110, 111] and it ensures efficient classical simulability in the post-processing via Gottesman-Knill's theorem [34, 35].

In this scenario, one can compute $S$ by either characterizing its eigenvalues, or its action on quantum states. Specifically, it is possible to give a closed-form formula for the classical shadow that follows from Schur-Weyl's duality applications to the computation of moment operators, c.f. Section 3.2. In particular, we have ($v \neq 0$)

$$\begin{aligned}(v\,|S_H|v) &= \frac{1}{d}\sum_{i\in[d]} \mathbb{E}_{U\sim\mathrm{U}(d)} (v\,|\omega(g)^\dagger|E_i)(E_i\,|\omega(g)|v) \\ &= \mathbb{E}_{U\sim\mathrm{U}(d)} \langle 0\,|U^{\otimes 2} W(v)^{\otimes 2} U^{\otimes 2\dagger}|0\rangle \\ &= \frac{1}{d^2-1}\langle 0\,|d\,\mathbb{F} - \mathbb{1}|0\rangle \\ &= \frac{1}{d+1}\,,\end{aligned} \tag{5.8}$$

where we used Eq. (3.60). Hence, for Pauli estimation, we have $\mathrm{Var}[\hat{v}] \leq d+1$. On the other hand, we can compute the third moment operator to bound the shadow norm [45] (as $\mathrm{Cl}_n$ also forms a unitary 3-design). First, recall that $S$ is effectively a depolarizing channel for Haar ensembles, i.e., $S \equiv \mathcal{D}_p$ with $p = \frac{1}{d+1}$, which admits the inverse $D_p^{-1}(\cdot) \coloneqq p^{-1}(\cdot) - \mathrm{Tr}(\cdot)\mathbb{1}$. Then, we can focus on the traceless part $O_0 = O - \frac{\mathrm{Tr}(O)}{d}\mathbb{1}$ as the map $O \mapsto O_0$ is a contraction since $\mathrm{Tr}(O_0^2) = \mathrm{Tr}(O^2) - \frac{1}{d}\mathrm{Tr}(O)^2 \leq \mathrm{Tr}(O)^2$. This implies for the shadow norm

the following bound:

$$\begin{aligned}\|O_0\|_{\mathrm{sh}}^2 &\coloneqq \max_\rho \sum_i \mathbb{E}_U (S^{-1}(O_0)\,|\,E_{i,U})^2 (E_{i,U}\,|\,\rho) \\ &= (d+1)^2 \max_\rho \mathrm{Tr}\left[\rho \sum_i \mathbb{E}_U \,\mathrm{Tr}_{1,2}\left(\left(O_0^{\otimes 2}\otimes \mathbb{1}\right) U^{\otimes 3}|i\rangle\langle i|^{\otimes 3} U^{\dagger\otimes 3}\right)\right] \\ &= d(d+1)^2 \frac{6}{(d+2)(d+1)d}\,\mathrm{Tr}\left[\rho\,\mathrm{Tr}_{1,2}\left(\left(O_0^{\otimes 2}\otimes \mathbb{1}\right) P_{\mathrm{sym}^3}\right)\right] \\ &= \frac{d+1}{d+2}\max_\rho (\mathrm{Tr}\,\rho\,\mathrm{Tr}\,O_0^2 + 2\,\mathrm{Tr}(\rho O_0^2))\,.\end{aligned} \tag{5.9}$$

In the third line, we used Eq. (3.60). To compute the partial trace, we used the expression

$$P_{\mathrm{sym}^3} = \frac{1}{6}\left(\mathbb{1}^{\otimes 3} + U_{1,2} + U_{1,3} + U_{2,3} + U_{1,2,3} + U_{1,3,2}\right)\,, \tag{5.10}$$

where $U_{i,j}, U_{i,j,k}$ denote the cyclic permutations of the indeces. In particular, we have

$$\mathrm{Tr}_{1,2}(O_0^{\otimes 2}\otimes \mathbb{1} U_{1,2}) = \mathrm{Tr}(O_0^2)\mathbb{1}\,, \quad \mathrm{Tr}_{1,2}(O_0^{\otimes 2}\otimes \mathbb{1} U_{1,3}) = \mathrm{Tr}(O_0)O_0\,, \tag{5.11}$$

$$\mathrm{Tr}_{1,2}(O_0^{\otimes 2}\otimes \mathbb{1} U_{2,3}) = \mathrm{Tr}(O_0)O_0\,, \quad \mathrm{Tr}_{1,2}(O_0^{\otimes 2}\otimes \mathbb{1} U_{1,2,3}) = O_0^2\,, \tag{5.12}$$

$$\mathrm{Tr}_{1,2}(O_0^{\otimes 2}\otimes \mathbb{1} U_{1,3,2}) = O_0^2\,. \tag{5.13}$$

Then,

$$\|O_0\|_{\mathrm{sh}}^2 = \frac{d+1}{d+2}(\mathrm{Tr}(O_0^2) + 2\|O_0^2\|_\infty) \leq 3\,\mathrm{Tr}(O_0^2)\,. \tag{5.14}$$

Therefore, this measurement primitive is particularly efficient if the Frobenius norm of the observable is controlled, e.g., for fidelity estimation. However, the choice of global Cliffords is limited by practical constraints, as the implementation of such unitaries requires linear depth circuits, which are highly affected by noise.

This problem has been addressed in a recent series of works where global Cliffords are replaced by shallow circuits [43, 52, 106, 109, 112]. Specifically, Schuster *et al.* [43] proved that unitary $k$-designs can be approximated in logarithmic depth for one-dimensional circuits, effectively retaining similar sampling complexity guarantees of global Cliffords. We postpone this discussion to the next chapter.

## 5.3 Shadow estimation with local Clifford unitaries

The number of samples of shadow estimation with global Cliffords does not scale favorably for local observables. For instance, the sampling complexity of estimating Pauli observable scales as $2^n$ for all Pauli strings. In such setting, we can construct better estimators by randomizing over local unitary ensembles. Following Huang *et al.* [45], the most natural choice is to implement randomized Pauli basis measurements in the form of random local Clifford unitaries. Computing the frame operator is straightforward and very similar to the previous case, as we have a local unitary 3-design: Given $u, v \in \mathbb{F}_2^{2n}$, and denoting by $S_{\mathrm{LC}}$

the frame operator associated with local Clifford (LC) shadows, we have

$$\begin{aligned}(u\,|\,S_{\mathrm{LC}}\,|\,v) &= \frac{1}{d}\sum_i \mathbb{E}_{U\sim\mu}(u|E_{i,U})(E_{i,U}\,|\,v)\\ &= \frac{1}{d}\sum_i \mathbb{E}_{U\sim\mu}\,\mathrm{Tr}[W(u)^\dagger U|i\rangle\langle i|U^\dagger]\;\mathrm{Tr}[U|i\rangle\langle i|U^\dagger W(v)]\\ &= \mathbb{E}_{U\sim\mu}\langle 0\,|U^{\otimes 2\dagger}W(u)\otimes W(v)U^{\otimes 2}\,|0\rangle\,.\end{aligned} \tag{5.15}$$

Considering the factorization

$$W(v) = W(v_1)\otimes\cdots\otimes W(v_n)\,, \tag{5.16}$$

by Proposition 23, we have

$$\mathbb{E}_{U\sim\mu}U^{\otimes 2\dagger}W(u)\otimes W(v)U^{\otimes 2} = \delta_{u,v}\frac{1}{3^{|\mathrm{supp}_{\mathrm{LC}}(v)|}}\left(2\,\mathbb{F}-\mathbb{1}\right)^{\otimes|\mathrm{supp}_{\mathrm{LC}}(v)|}\,, \tag{5.17}$$

where $\mathrm{wt}(v)$ is the binary vector $\mathrm{wt}(v)\in\mathbb{F}_2^n$ such that $\mathrm{wt}(v)_i = 0$ iff $v_i = (0,0)$ and $\mathrm{wt}(v)_i = 1$ else, and $\mathrm{supp}_{\mathrm{LC}}(v) \coloneqq \{i \mid \mathrm{wt}(v)_i \neq 0\}$.

Therefore, it follows

$$\begin{aligned}(v\,|\,S_{\mathrm{LC}}\,|\,v) &= \frac{1}{3^{|\mathrm{supp}_{\mathrm{LC}}(v)|}}\langle 0\,|2\mathbb{F}-\mathbb{1}\,|0\rangle^{|\mathrm{supp}_{\mathrm{LC}}(v)|}\\ &= \frac{1}{3^{|\mathrm{supp}_{\mathrm{LC}}(v)|}}\,.\end{aligned} \tag{5.18}$$

From the discussion on Pauli invariant estimators, it follows that Pauli estimation is efficient provided $v$ is supported on a small number of qubit. We also remark that classical shadows for the LC ensemble is available, as $S_{\mathrm{LC}}$ amounts to a $k \equiv |\mathrm{supp}_{\mathrm{LC}}(v)|$-tensor-copies of depolarizing channels $\mathcal{D}$ by applying the result of Section 5.2 on each qubit.

Intuitively, the sample complexity scales favorably also for general local observables: It is clear that if $O$ factorizes in the form $O = O_k\otimes\mathbb{1}^{\otimes n-k}$, with $k = |\mathrm{supp}_{\mathrm{LC}}(O)|$ and $|\mathrm{supp}_{\mathrm{LC}}(O)|$ is the number of qubits on which $O$ acts non trivially, only the non-trivial part $O_k$ contributes to $\mathrm{Tr}(O\rho)$, as both local Cliffords and computational basis measurements factorize. Hence, the shadow norm factorizes in a similar fashion, and the only non-trivial contribution is associated with the non-trivial action on $O_k$. Then, Huang *et al.* [45] proved that for any observable $O$, one has $\|O\|_{\mathrm{sh}}^2 \leq 4^{\mathrm{supp}(O)}\|O\|_\infty^2$. However, the formal proof is significantly more involved, and we refer to [45, Prop. 3] for further details.

# Chapter 6

# Shadow estimation with shallow brickwork circuits

*The content of this chapter is largely adapted from [52], with the exception of the last section. The material has been reformatted for self-consistency within this thesis: Sections have been reorganized and notation has been harmonized with the rest of this work. No changes were made to the core results.*

Shadow estimation with global and local Clifford unitaries are, in a sense, two "extreme" scenarios: Randomizing through global random Cliffords provides strict sampling complexity guarantees for predicting global properties, while local Cliffords are more suitable for local observables [33, 113, 114]. While the latter is readily available in experiments [114], global Cliffords will typically introduce too much noise to be useful for estimation on near-term hardware. This stems from the fact that one needs to implement a linear depth circuit, which introduce a noise that can be limited up to some extent using robust variants of shadow estimation [115–117].

Experimentally feasible alternatives, naturally interpolating between the two extreme cases and potentially lowering the sample complexity over local Clifford unitaries, are *short Clifford circuits* [108]. However, finding expressions for classical shadows for random low-depth Clifford circuits is a challenging task. For instance, the construction by Hu *et al.* [108] involve numerically solving a large system of equations.

In this chapter, we discuss recent developments in shadow estimation using shallow random circuits. Specifically, we will focus on deriving closed-form analytic expressions for classical shadows with simple brickwork circuits consisting of two layers of product of random unitaries. In this case, we can observe that, for Pauli observables, one needs to keep track of the relative positions of supported qubit to find advantages compared to local Cliffords shadows. In fact, we will see that local Clifford unitaries yield a lower sampling complexity for sparsely distributed Pauli observables (in a precise sense), while (very short) brickwork shadows outperform the local Clifford ones when the observable is supported on sufficiently many (adjacent) qubits.

The chapter is structured as follows: As the ensemble of unitaries we consider is Pauli invariant, we work out the matrix representation of the frame operator in the Pauli basis. In particular, we can use the local 2-design property of each brick to we derive recurrence relations for subcircuits that can be analytically solved. In this way, we can identify the regime where the resulting sampling complexity outperforms shadow estimation with local

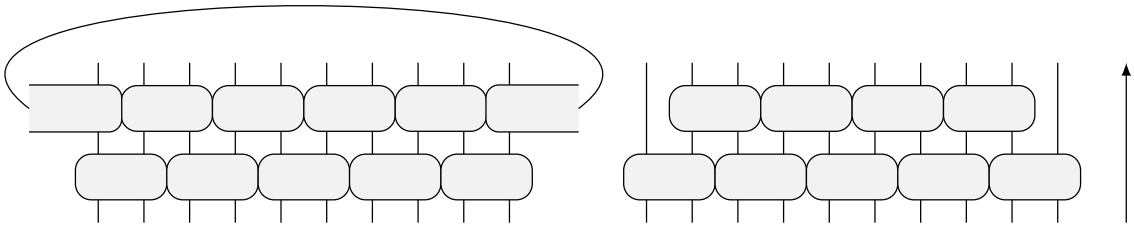


Figure 6.1: Brickwork circuits acting on $n = 10$ qubits. The left and right figures show periodic and open boundary conditions, respectively, and the arrow indicates the direction in which the circuit acts on quantum states. For both of them, the first layer is composed of $n/2$ two-qubit Haar random unitaries acting on qubits $(2i-1, 2i)$, $i \in [5]$, and the second layer is shifted by one position. On the left, the bricks in the second layer acts on qubits $(2i, 2i+1)\,, i \in [5]$, with the periodic identification $n+1 = 1$. On the right, the second layer acts on qubits $(2i, 2i+1)\,, i \in [4]$, leaving the first and the $n$th qubit untouched.

Cliffords. In the last section of this chapter, we briefly review extensions to deeper circuits and discuss preliminary unpublished results on the eigenvalues of such circuits.

## 6.1 The brickwork circuit: analytical results

We assume for simplicity that the number of qubits is even and consider one round of a one-dimensional brickwork (BW) circuit built in the following way: a first layer of $n/2$ two-local Haar random unitaries is applied to qubits $(2i-1, 2i)$ for $i \in [n/2]$. The second layer, built in the same way but shifted by one position, applies Haar random unitaries to qubits $(2i, 2i+1)$. Here, we consider two cases, see also Figure 6.1. First, the second layer has periodic boundary conditions such that qubits $n+1$ and 1 are identified, and consequently, the $n/2$th random unitary acts on the qubit pair $(n, 1)$. Second, we treat the case of open boundary conditions, where the second layer does not act on the first and the $n$th qubit. In practice, it can be more convenient to draw unitaries from a unitary 2-design, such as the Clifford group (which, for qubits systems, is even a 3-design [38, 39]). Indeed, implementing Haar-random unitaries is very hard [57] and, moreover, employing Clifford unitaries ensures one can classically post-process shadows efficiently [34]. For a given vector $v = v_1 \oplus \cdots \oplus v_n \in \mathbb{F}_2^{2n}$, we also define its *weight vector* as the binary vector $\mathrm{wt}(v) \in \mathbb{F}_2^n$ such that $\mathrm{wt}(v)_i = 0$ if $v_i = (0, 0)$ and $\mathrm{wt}(v)_i = 1$ else. In other words, $\mathrm{wt}(v)$ has a zero in the $i$th position if and only if $W(v)$ is the identity on the $i$th qubit.

In the following, we derive analytical results for the frame operator of random brickwork circuits with open and periodic boundary conditions. Both BW circuit ensembles are clearly (left and right) invariant under tensor products of single-qubit unitaries, in particular they are right-invariant under Pauli operators. By the discussion in Section 5.1.2, we thus know that the frame operator $S$ is diagonal in the Pauli basis. It is thus sufficient to compute the matrix elements $(v\,|S|v)$ for all $v \in \mathbb{F}_2^{2n}$. Moreover, both BW circuit ensembles are also invariant under local Clifford unitaries, i.e. tensor products of single-qubit Clifford gates. This implies that $(v\,|S|v)$ is invariant under the exchange of $X$, $Y$, and $Z$ operators, and hence depends only on the weight vector $\mathrm{wt}(v)$. As we show shortly, $(v\,|S|v)$ is in fact determined by non-vanishing pairs of elements in $\mathrm{wt}(v)$ corresponding to a brick in

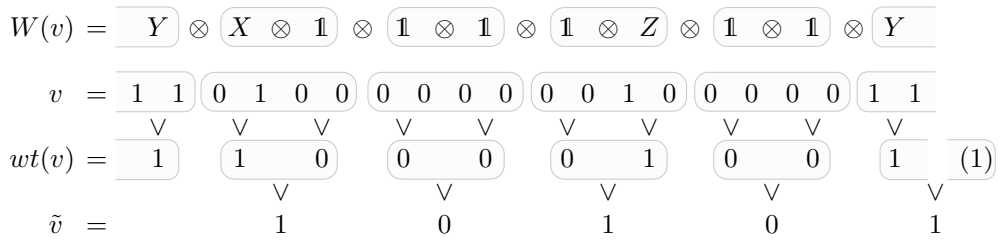



Figure 6.2: Example how the vector of supported bricks is computed from a 10-qubit Pauli operator. The structure of the shaded bricks is the one of the second layer of the circuit. First, the Pauli operator is transformed into its binary representation $v \in \mathbb{F}_2^{20}$. We apply a logical or ($\vee$) per qubit to compute the weight vector $\mathrm{wt}(v)$. Subsequently, this procedure is repeated for qubit pairs $(2i, 2i+1)$ and yields the vector of supported bricks $\tilde{v}$. For periodic boundary conditions, the last entry of $\tilde{v}$ is computed between the last and first entry of $\mathrm{wt}(v)$ (here depicted by appending the first entry at the end in parentheses). The brickwork support of this example is $\mathrm{supp}_{\mathrm{BW}}(v) = \{1, 3, 5\}$, while its partition into local factors is $\mathrm{part}_{\mathrm{BW}}(v) = (1, 2)$.

the second layer, and by their positions in the circuit. To make this precise, we have to introduce some definitions.

Let us consider a Pauli string $v = v_1 \oplus \cdots \oplus v_n \in \mathbb{F}_2^{2n}$. Roughly speaking, a brick is identified by a pair of two adjacent qubits, and it is in the support of $v$ if at least one of the qubits is in the support of $v$. More formally, we define the vector of *supported bricks* as

$$\tilde{v} = (\tilde{v}_1, \ldots, \tilde{v}_{n/2}) \in \mathbb{F}_2^{n/2}, \quad \tilde{v}_i \coloneqq \mathrm{wt}(v)_{2i} \vee \mathrm{wt}(v)_{2i+1}, \quad i \in [n/2], \tag{6.1}$$

where $x \vee y$ is the *logical or* between two bits $x, y \in \mathbb{F}_2$, i.e. $x \vee y = 1$ if $x = 1$ or $y = 1$, and 0 else. The last entry of $\tilde{v}$ is defined according to the boundary conditions of the second layer, in particular $\tilde{v}_{n/2} = \mathrm{wt}(v)_n \vee \mathrm{wt}(v)_1$ for periodic boundary conditions, and $\tilde{v}_{n/2} \equiv 0$ for open boundary conditions, see also Fig. 6.2 for an explicit example how $\tilde{v}$ is computed. We say that the $i$th brick in the second layer, with $i \in [n/2]$, *is in the support of* $v$ if $\tilde{v}_i = 1$. Then, one can define the *brickwork support* of $v \in \mathbb{F}_2^{2n}$ as $\mathrm{supp}_{\mathrm{BW}}(v) \coloneqq \{i \mid \tilde{v}_i \neq 0\}$. In the following, however, it will be equally important to keep track of sequences of consecutive supported bricks in the circuit. Hence, we introduce the following notation: A *one-component* of $\tilde{v}$ is a maximal tuple of consecutive ones in $\tilde{v}$, where "consecutive" is again meant w.r.t. the boundary conditions of the BW circuit. Then, we define the *partition of the brickwork support* $\mathrm{part}_{\mathrm{BW}}(v)$ to be the integer sequence given by the (non-unique) sizes of the one-components of $\tilde{v}$. For instance, if we have periodic boundary conditions and $\tilde{v} = (1, 0, 1, 0, 1)$ as in Fig. 6.2, then $\mathrm{part}_{\mathrm{BW}}(v) = (1, 2)$. Note that the maximal number of consecutive ones is $n/2 - 1$ and $n/2$ for open and periodic boundary conditions, respectively.

We can now state our main result:

**Theorem 26.** *Let $S$ be the frame operator associated with one round of a two-local brickwork circuit with open or periodic boundary conditions in the second layer. Then, $S$ is diagonal in the Pauli basis, and for $v \in \mathbb{F}_2^{2n}$*

$$(v\,|S|\,v) = \begin{cases} \Sigma_{\mathrm{pb}}(n), & \mathrm{part}_{\mathrm{BW}}(v) = (n/2), \\ \prod_{l \in \mathrm{part}_{\mathrm{BW}}(v)} \Sigma_{\mathrm{ob}}(2l+2), & \textit{otherwise}, \end{cases} \tag{6.2}$$

*where, for any $m \in \mathbb{N}$ even,*

$$\Sigma_{\mathrm{pb}}(m) = \frac{\left(\sqrt{41}+5\right)^{m/2} + (-1)^{m/2}\left(\sqrt{41}-5\right)^{m/2}}{(5\sqrt{2})^m}\,, \tag{6.3}$$

$$\Sigma_{\mathrm{ob}}(m) = \frac{5}{2\sqrt{41}} \frac{\left(25-3\sqrt{41}\right)\left(\sqrt{41}+5\right)^{m/2} + (-1)^{m/2+1}\left(25+3\sqrt{41}\right)\left(\sqrt{41}-5\right)^{m/2}}{\left(5\sqrt{2}\right)^m}\,. \tag{6.4}$$

Let us briefly comment on the interpretation of the matrix elements of $S$. These values, determined by the elements of $\mathrm{part}_{\mathrm{BW}}(v)$, are associated with different topologies of the effective BW circuit.

First, note that the case $\mathrm{part}_{\mathrm{BW}}(v) = (n/2)$ can occur for periodic boundary conditions only and corresponds to all bricks being in the support of $v$. In particular, for open boundary conditions, the second case in Eq. (6.2) always applies.

Next, let us motivate the second case in Eq. (6.2). Concretely, let us first assume $\mathrm{part}_{\mathrm{BW}}(v) = (n/2-1)$. In the case of open boundary conditions, this assumption corresponds to all bricks being in the support of $v$, since $\tilde{v}_{n/2} = 0$ by definition. Likewise, this situation occurs in the BW circuit with periodic boundary conditions whenever there exists exactly one $i \in [n/2]$ such that $\tilde{v}_i = 0$, see Figure 6.3. Then, we can make two observations: First, the topology of the effective circuit changes from periodic to open boundary conditions. Second, the effective circuit is equivalent –up to reordering of qubits on which it acts– to the fully supported circuit with open boundary conditions described before, which is depicted in Figure 6.1.

Suppose now we have a BW circuit with open boundary conditions, and there exists another index $i$ such that $\tilde{v}_i = 0$. Then, two cases can occur: Either, (a), $i = 1$ or $i = n/2-1$, which implies $\mathrm{part}_{\mathrm{BW}}(v) = (n/2-2)$, and we simply obtain a BW circuit with open boundary conditions on $n-4$ qubits. Otherwise, (b), $\mathrm{part}_{\mathrm{BW}}(v) = (i-1, n/2-i-1)$ and the BW circuit again factorizes into two independent BW circuits with open boundary conditions, acting on $2i$ and $n-2i$ qubits respectively.

In general, the effective circuit splits into as many independent BW circuits with open boundary conditions as the number of elements in $\mathrm{part}_{\mathrm{BW}}(v)$, and the diagonal elements of $S$ are given by products of different contributions as in Eq. (6.2). These elements also determine the number of qubits on which these subcircuits act, see Figure 6.3 for an example with $|\mathrm{part}_{\mathrm{BW}}(v)| = 2$.

As discussed in Section 5.1.2, the frame operator provides a bound on the variance of the Pauli estimation task. Specifically, denoting with $\sigma^2_{\mathrm{BW}}(v,\rho)$ the variance of the estimator $\hat{v}$ for any $v \in \mathbb{F}_2^{2n}$, we have

$$\sigma^2_{\mathrm{BW}}(v,\rho) \equiv \sigma^2_{\mathrm{BW}}(v) \leq \frac{1}{(v\,|S|\,v)}\,. \tag{6.5}$$

In Appendix A.1 we provide an alternative proof for circuits with periodic boundary conditions which holds for unitary 3-designs.

The remaining of this section is dedicated to the proof of Theorem 26. It goes through the following steps: First, in Lemma 27, we will prove that such eigenvalues are determined by $\mathrm{part}_{\mathrm{BW}}(v)$ for any $v \in \mathbb{F}_2^{2n}$. Those eigenvalues are associated with different, effective BW circuits. Exploiting the structure of the BW circuit, we can 'split' the action of the

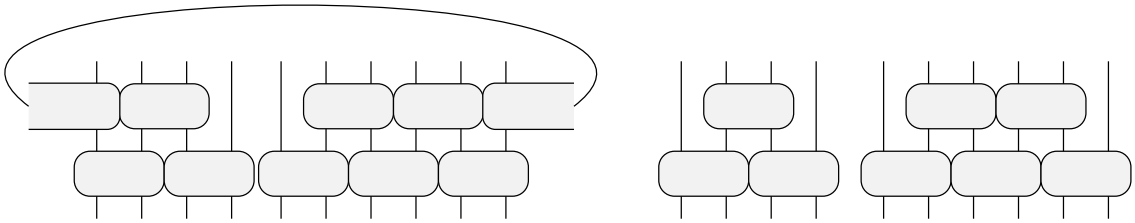


Figure 6.3: Effective brickwork circuits associated with non-fully supported Pauli operators in the case $n = 10$. On the left, the effective BW circuit associated with a $v \in \mathbb{F}_2^{20}$ such that $\tilde{v}_2 = 0$ and $\mathrm{part}_{\mathrm{BW}}(v) = (4)$. In this case, open boundary conditions apply and the circuit is topologically equivalent to the right one in Figure 6.1. On the right, the effective BW circuit associated with $v \in \mathbb{F}_2^{20}$ such that $\tilde{v}_2, \tilde{v}_5 = 0$, which implies $\mathrm{supp}_{\mathrm{BW}}(v) = \{1, 3, 4\}$ and $\mathrm{part}_{\mathrm{BW}}(v) = (1, 2)$. In this case, the circuit is the product of two smaller subcircuits with open boundary conditions. In particular, the subcircuits are defined on 4 and 6 qubits, respectively.

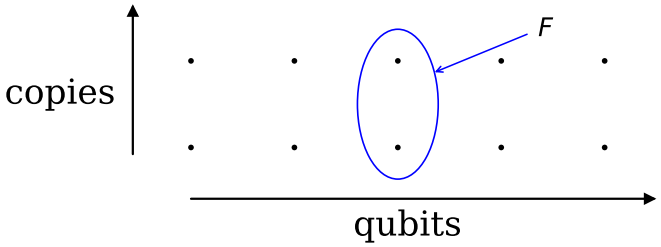



Figure 6.4: Flip operator swapping tensor factors of two copies of the third qubit site.

layers in two separate (2-local) group twirls, which can be evaluated using standard results in the computation of moment operators. Next, in Lemmas 28 and 29, using tensor network techniques, we reduce the problem of finding such eigenvalues to two different systems of recurrence relations associated with BW circuits with periodic and open boundary conditions, respectively. The latter admit closed-form analytic solutions, which lead to the explicit expression of $(v\,|S|\,v)$.

In the following, given an operator $A \in \mathrm{L}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, we denote by $A_{(2)} \equiv A \otimes A \in \mathrm{L}(\mathbb{C}^4 \otimes \mathbb{C}^4)$ the operator acting on two copies of two qubit "sites". In particular, we will extensively use the operator $\mathbb{F}_{(2)} \equiv \mathbb{F} \otimes \mathbb{F}$, where $\mathbb{F}$ is the flip operator which swaps tensor factors of $\mathbb{C}^2 \otimes \mathbb{C}^2$. The action of $\mathbb{F}$ is also depicted in Fig. 6.4.

As we observed in Section 5.1.2, the frame operator is diagonal in the Pauli basis for Pauli invariant measures [105]. However, since unitaries in the BW circuit are Haar random, we can characterize the matrix elements of the frame operator exploiting some known results about the second moment operator, c.f. Section 3.4, also see [19]. As a side note, this also implies that, in practice, we can draw unitaries from any unitary 2-design instead [37, 118], such as the Clifford group.

Then, the following holds:

**Lemma 27.** *Let $S$ be the frame operator associated with one round of a two-local brickwork circuit with periodic or open boundary conditions in the second layer. Then, $S$ is diagonal*

*in the Pauli basis, and*

$$(v\,|S|\,v) = \begin{cases} \frac{1}{(10\sqrt{3})^n}\,\mathrm{t}_{\mathrm{pb}}(n)\,, & \mathrm{part}_{\mathrm{BW}}(v) = (n/2) \\ \frac{1}{15^{|\tilde{v}|}}\prod_{l\in \mathrm{part}_{\mathrm{BW}}(v)} \frac{\mathrm{t}_{\mathrm{ob}}(2l+2)}{(2\sqrt{5})^{2l+2}}\,, & \textit{otherwise} \end{cases}\,, \tag{6.6}$$

*where $|\tilde{v}|$ is the Hamming weight of $\tilde{v}$, and*

$$\mathrm{t}_{\mathrm{pb}}(n) \coloneqq \mathrm{Tr}\Big[(\mathbb{1}+\mathbb{F}_{(2)})^{\otimes n/2}\; D_{(2)}\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes n/2} D_{(2)}^{-1}\Big]\,, \tag{6.7}$$

$$\mathrm{t}_{\mathrm{ob}}(n) \coloneqq \mathrm{Tr}\Big[(\mathbb{1}+\mathbb{F}_{(2)})^{\otimes n/2}\left\{\mathbb{1}_4\otimes\left((4\mathbb{F}_{(2)}-\mathbb{1})^{\otimes(n/2-1)}\right)\otimes\mathbb{1}_4\right\}\Big]\,, \tag{6.8}$$

*with $D|\psi_1\rangle\otimes\cdots\otimes|\psi_n\rangle \coloneqq |\psi_2\rangle\otimes\cdots\otimes|\psi_n\rangle\otimes|\psi_1\rangle$ being a cyclic shift operator.*

*Proof.* Let $\mu$ be a probability measure on the BW circuit. Hence, $\mu$ is the product of probability measures $\mu_{i_j}$, where $i = 1,\ldots,n/2$, and $j = 1,2$. In other terms, the operator corresponding to the $i_j$th brick is sampled independently from all the others. Then, given $u, v \in \mathbb{F}_2^{2n}$, we have

$$\begin{aligned}(u\,|S|\,v) &= \frac{1}{d}\sum_i \mathbb{E}_{U\sim\mu}(u\,|E_{i,U})(E_{i,U}\,|v) \\ &= \frac{1}{d}\sum_i \mathbb{E}_{U\sim\mu}\,\mathrm{Tr}[W(u)^\dagger U|i\rangle\langle i|U^\dagger]\;\mathrm{Tr}[U|i\rangle\langle i|U^\dagger W(v)] \\ &= \mathbb{E}_{U\sim\mu}\langle 0\,|U^{\otimes 2\dagger}W(u)\otimes W(v)U^{\otimes 2}|0\rangle\,.\end{aligned} \tag{6.9}$$

Consider now the following factorization of $W(v)$:

$$W(v) = W(v_{2,3})\otimes\cdots\otimes W(v_{n,1})\,, \tag{6.10}$$

where, for each $i \in [n/2]$,

$$v_{2i,2i+1} \equiv v_{2i}\oplus v_{2i+1} \in \mathbb{F}_2^2\oplus\mathbb{F}_2^2\,, \tag{6.11}$$

and each $W(v_{2i,2i+1})$ is as in Eq. (3.74). Moreover, writing $U = DU_2D^\dagger U_1$, where $U_i$ is the tensor product of two-local Haar random unitaries, it follows

$$(u\,|S|\,v) = \mathrm{Tr}\Big[\mathbb{E}_{U_1}\Big[U_1^{\otimes 2}|0\rangle\langle 0|U_1^{\otimes 2\dagger}\Big]\,D_{(2)}\,\mathbb{E}_{U_2}\Big[U_2^{\otimes 2\dagger}D_{(2)}^\dagger W(u)\otimes W(v)D_{(2)}U_2^{\otimes 2}\Big]\,D_{(2)}^\dagger\Big]\,. \tag{6.12}$$

Hence, by Eq. (3.60) and Proposition 23, we have

$$\mathbb{E}_{U_1}U_1^{\otimes 2}|0\rangle\langle 0|^{\otimes 2}U_1^{\otimes 2\dagger} = \frac{1}{10^{n/2}}P_{\mathrm{sym}^2}^{\otimes n/2}\,, \tag{6.13}$$

$$\mathbb{E}_{U_2}U_2^{\otimes 2}D_{(2)}^\dagger W(v)\otimes W(u)D_{(2)}U_2^{\otimes 2\dagger} = \delta_{u,v}\bigotimes_{i\in[n/2]} Q_{\tilde{v}_i}\,, \tag{6.14}$$

where

$$Q_{\tilde{v}_i} \coloneqq \begin{cases}\mathbb{1} & \text{if } \tilde{v}_i = 0\,, \\ \frac{1}{15}\left(4\mathbb{F}_{(2)}-\mathbb{1}\right) & \text{otherwise}\,.\end{cases} \tag{6.15}$$

Therefore, writing $P_{\mathrm{sym}^2} = \frac{1}{2}\left(\mathbb{1} + \mathbb{F}_{(2)}\right)$,

$$(v\,|S|\,v) = \frac{1}{(2\sqrt{5})^n}\,\mathrm{Tr}\left[\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes n/2} D_{(2)} \bigotimes_{i\in[n/2]} Q_{\tilde{v}_i}\, D_{(2)}^{-1}\right] \quad . \tag{6.16}$$

Finally, we distinguish cases for the latter according to $\mathrm{part}_{\mathrm{BW}}(v)$. In particular, if $\mathrm{part}_{\mathrm{BW}}(v) = (n/2)$, then $Q_{\tilde{v}_i} = \frac{1}{15}\left(4\mathbb{F}_{(2)} - \mathbb{1}\right)\ \forall i = 1,\dots,n/2$, and Eq. (6.7) reads immediately from Eq. (6.16). Next, assume $\mathrm{part}_{\mathrm{BW}}(v) = (n/2-1)$. In particular, due to invariance under translations of bricks, we can assume without loss of generality that $\tilde{v}_{n/2} = 0$, meaning $Q_{\tilde{v}_{n/2}} = \mathbb{1}$. This yields

$$(v\,|S|\,v) = \frac{1}{(2\sqrt{5})^n}\frac{1}{15^{n/2-1}}\,\mathrm{Tr}\left[\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes n/2}\mathbb{1}\otimes\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes n/2-1}\otimes\mathbb{1}\right]. \tag{6.17}$$

Consider now there exists $i \in [n/2-1]$ such that $\tilde{v}_i = 0$. Then, we distinguish between two cases. If $i = 1$ or $i = n/2-1$, then $(v\,|S|\,v)$ is still given by an expression that is morally equivalent to Eq. (6.17) up to obvious modifications determined by $\mathrm{part}_{\mathrm{BW}}(v) = (n/2-2)$. More specifically, we have

$$\begin{aligned}(v\,|S|\,v) &= \frac{1}{(2\sqrt{5})^n}\frac{1}{15^{n/2-2}}\,\mathrm{Tr}\left[\mathbb{1}+\mathbb{F}_{(2)}\right]\mathrm{Tr}\left[\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes n/2-1}\mathbb{1}\otimes\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes n/2-2}\otimes\mathbb{1}\right]\\ &= \frac{1}{(2\sqrt{5})^{n-2}}\frac{1}{15^{n/2-2}}\,\mathrm{t}_{\mathrm{ob}}(n-2)\,.\end{aligned} \tag{6.18}$$

On the other hand, if $i \in \{2,\dots,n/2-2\}$, we have $\mathrm{part}_{\mathrm{BW}}(v) = (i-1, n/2-1-i)$, and the circuit splits into two subcircuits, yielding

$$\begin{aligned}(v\,|S|\,v) &= \frac{1}{(2\sqrt{5})^n}\,\mathrm{Tr}\left[\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes i}\mathbb{1}\otimes\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes(i-1)}\otimes\mathbb{1}\right]\\ &\quad\times\mathrm{Tr}\left[\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes n/2-i}\mathbb{1}\otimes\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes n/2-1-i}\otimes\mathbb{1}\right]\\ &= \frac{1}{(2\sqrt{5})^n}\,\mathrm{t}_{\mathrm{ob}}(2i)\,\mathrm{t}_{\mathrm{ob}}(n-2i)\,.\end{aligned} \tag{6.19}$$

All other cases follow from analogous considerations. □

Note that the traces in the latter expression have two main contributions. The first one, which is proportional to the projector on the symmetric subspace $P_{\mathrm{sym}^2}$, comes from scrambling $E_i$ with the first layer of the BW circuit, and it is independent of $v$. The second layer, on the other hand, acts on $W(u)\otimes W(v)$, and the result of the scrambling for each pair of qubits is an operator that depends on $v$. This means that *effectively* the second layer determines whether the circuit factorizes at a given position, and the number of qubits on which each subcircuit is defined is determined by the corresponding first layer of random unitaries.

The next couple of technical results will give a way to evaluate the traces appearing in the previous lemma. The core steps of the proofs are most conveniently presented in terms of tensor network diagrams and deferred to Appendix A.2.

**Lemma 28.** *Let $t_1(n), t_2(n), t_3(n)$ defined as follows:*

$$t_1(n) \coloneqq \mathrm{Tr}\left[\left(\mathbb{1}\otimes\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes n/2-1}\otimes\mathbb{1}\right)\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes n/2}\right], \tag{6.20}$$

$$t_2(n) \coloneqq \mathrm{Tr}\left[\left(\mathbb{F}\otimes\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes n/2-1}\otimes\mathbb{F}\right)\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes n/2}\right], \tag{6.21}$$

$$t_3(n) \coloneqq \mathrm{Tr}\left[\left(\mathbb{1}\otimes\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes n/2-1}\otimes\mathbb{F}\right)\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes n/2}\right]. \tag{6.22}$$

*Then, $\mathrm{t}_{\mathrm{pb}}(n) = t_1(n) + t_2(n)$ and the following system of recursive relations hold true:*

$$\begin{cases} t_1(n) = 24\, t_3(n-2) \\ t_2(n) = 24\, t_3(n-2) + 60\, t_2(n-2) \\ t_3(n) = 24\, t_1(n-2) + 60\, t_3(n-2) \end{cases}, \quad n \geq 2\,, \quad n = 0 \mod 2\,, \tag{6.23}$$

*with the following base conditions:*

$$\begin{cases} t_1(2) = 0 \\ t_2(2) = 60 \\ t_3(2) = 24 \end{cases}. \tag{6.24}$$

*Proof.* The fact that $\mathrm{t}_{\mathrm{pb}}(n) = t_1(n)+t_2(n)$ is clear from the definition of $t_1$ and $t_2$. Relations (6.23) and (6.24) are proved in Appendix A.2. □

**Lemma 29.** *Let $t_1(n), t_2(n)$ be defined as follows:*

$$t_1(n) \coloneqq \mathrm{Tr}\Big[\Big\{\mathbb{1}_4\otimes\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes(n/2-1)}\Big\}\Big\{\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes(n/2-1)}\otimes\mathbb{1}_4\Big\}\Big], \tag{6.25}$$

$$t_2(n) \coloneqq \mathrm{Tr}\Big[\Big\{\mathbb{F}\otimes\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes(n/2-1)}\Big\}\Big\{\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes(n/2-1)}\otimes\mathbb{1}_4\Big\}\Big]. \tag{6.26}$$

*Then, $\mathrm{t}_{\mathrm{ob}}(n) = 4t_1(n) + 2t_2(n)$, and the following recursive relations hold true:*

$$\begin{cases} t_1(n) = 24\, t_2(n-2) \\ t_2(n) = 24\, t_1(n-2) + 60\, t_2(n-2) \end{cases} \quad n \geq 4\,, \quad n = 0 \mod 2\,, \tag{6.27}$$

*with the following base conditions:*

$$\begin{cases} t_1(4) = 48 \\ t_2(4) = 216 \end{cases}. \tag{6.28}$$

*Proof.* First, observe that

$$\begin{aligned} \mathrm{t}_{\mathrm{ob}}(n) &\coloneqq \mathrm{Tr}\Big[\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes n/2}\Big\{\mathbb{1}\otimes\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes(n/2-1)}\otimes\mathbb{1}\Big\}\Big] \\ &= \mathrm{Tr}\Big[\Big\{\mathrm{Tr}_1\big[\left(\mathbb{1}+\mathbb{F}_{(2)}\right)\big]\otimes\Big[\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes(n/2-1)}\Big]\Big\}\Big\{\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes(n/2-1)}\otimes\mathbb{1}\Big\}\Big] \\ &= \mathrm{Tr}\Big[\Big\{(4\mathbb{1}+2\mathbb{F})\otimes\left(\mathbb{1}+\mathbb{F}_{(2)}\right)^{\otimes(n/2-1)}\Big\}\Big\{\left(4\mathbb{F}_{(2)}-\mathbb{1}\right)^{\otimes(n/2-1)}\otimes\mathbb{1}\Big\}\Big] \\ &= 4\, t_1(n) + 2\, t_2(n)\,. \end{aligned} \tag{6.29}$$

Relations (6.27) and (6.28) are proved in Appendix A.2. □

*Proof of Theorem 26.* As discussed before, $S$ is diagonal in the Pauli basis, and we only need to characterize its diagonal elements $(v\,|S|\,v)$, which, by Lemma 27, are determined by $\mathrm{part}_{\mathrm{BW}}(v)$. In the first case, when $\mathrm{part}_{\mathrm{BW}}(v) = (n/2)$, the circuit retains periodic boundary conditions, and $(v\,|S|\,v)$ is proportional to $\mathrm{t}_{\mathrm{pb}}(n)$ according to Eq. (6.6). By Lemma 28, $\mathrm{t}_{\mathrm{pb}}(n)$ can be expressed as the sum of two terms that can be calculated recursively using the system of recurrence relations (6.23), and one can check that the solution of this system is given by

$$\mathrm{t}_{\mathrm{pb}}(n) = 6^{n/2}\left[\left(\sqrt{41}+5\right)^{n/2} + (-1)^{n/2}\left(\sqrt{41}-5\right)^{n/2}\right]. \tag{6.30}$$

This solution can be found with a computer algebra system, or, by hand, using the $Z$-transform [119], which maps recurrence relations to algebraic equations. Inserting Eq. (6.30) into Eq. (6.6) then shows Eq. (6.3).

Otherwise, $\mathrm{part}_{\mathrm{BW}}(v)$ determines the factorization into (possibly many) subcircuits with open boundary conditions. In particular, each entry $l \in \mathrm{part}_{\mathrm{BW}}(v)$ determines a (factorized) subcircuit acting on $2l+2$ qubits. Each such subcircuit evaluates up to a multiplicative constant to $\mathrm{t}_{\mathrm{ob}}(2l+2)$, that, by Lemma 29 fulfills the recurrence relations (6.27). These also admit a closed-form solution that can be found with the same techniques and is given as

$$\mathrm{t}_{\mathrm{ob}}(m) = \frac{6^{m/2}}{6\sqrt{41}}\left[\left(25-3\sqrt{41}\right)\left(\sqrt{41}+5\right)^{m/2} + (-1)^{m/2+1}\left(25+3\sqrt{41}\right)\left(\sqrt{41}-5\right)^{m/2}\right], \tag{6.31}$$

for any $m \equiv 2l+2$. This shows Eq. (6.4) for each subcircuit. □

As a final remark, observe that the proof of the theorem can be generalized to systems of arbitrary prime or power of prime local dimension. In particular, redefining $\tilde{v}$ according to the local dimension, Eq. (6.16) holds true with obvious modifications for any prime $p$, and the same holds for the traces Eqs. (6.7) and (6.8).

Finally, one may wonder whether it is possible to find analytical expressions for the frame operator associated with circuits with more layers. However, in this case, splitting the scrambling over multiple layers is more involved, since non-trivial 'intertwinings' between layers occur. This implies that the analytical contraction of the corresponding tensor network is more difficult compared to the calculations of Appendix A.2, and one might only resort to numerical methods to evaluate the frame operator [106, 109].

## 6.2 Discussion and comparison with local Clifford circuits

Given the closed analytic expressions for the frame operator associated with the BW circuit, we can now compare the performance with the LCs ensemble.

For LCs, the variance is exponential in the weight of the Pauli observable [45]. More precisely, for any $v \in \mathbb{F}_2^{2n}$ we define the *local Cliffords support* as the set of weighted sites of $v$, namely $\mathrm{supp}_{\mathrm{LC}}(v) \coloneqq \{i \mid \mathrm{wt}(v)_i \neq 0\}$. Then, since the LCs ensemble is clearly invariant under multiplication with Pauli operators, one can apply Eq. (5.6) to get a bound on the variance. In particular, $\sigma^2_{\mathrm{LC}}(v) \leq \frac{1}{(v\,|\,S_{\mathrm{LC}}\,|\,v)} = 3^{|\mathrm{supp}_{\mathrm{LC}}(v)|}$, where $S_{\mathrm{LC}}$ is the frame operator associated with LCs shadows (see Section 5.3 for the derivation of its matrix elements). Notice also that, although this bound corresponds to the *shadow norm* [45], one does not

need to maximize over all the states. The inequality solely originates in disregarding the square of the first-moment $(\mathbb{E}_{i,U} f_{W(v)}(i,U))^2$ which agrees by construction with $\mathrm{Tr}(W(v)\rho)^2$ for any ensemble. Therefore, we are most of the time comparing the exact expressions for the second moment $\mathbb{E}_{i,U}[f_{W(v)}(i,U)^2]$ allowing us to formally deduce lower and upper bounds. In the following, all our expressions for the variances are understood as being up to first-moment terms and we write, e.g. $\sigma^2_{\mathrm{LC}} = 3^n$.

As derived in the previous section, the variance for the brickwork circuit depends on the partitioning of the brick support into local factors. In principle, for any Pauli string $v$, we are able to compute such variance by means of Theorem 26. We also remark that the value obtained in this way are strict upper bounds, since we are only disregarding the square of the first moment term, which is upper bounded by 1. For simplicity, to compare the BW and LCs ensembles, we derive lower and upper bounds to the exact variance expression that make the asymptotic scaling transparent.

We obtain the simplest expression when $\mathrm{part}_{\mathrm{BW}}(v) = (n/2)$. In this case, Theorem 26 together with Eq. (5.6) implies that $0.8 \cdot 2^n < \sigma^2_{\mathrm{BW}} < 2.1^{n+1}$; see Appendix A.3 for details.

To compare the scaling of $\sigma^2_{\mathrm{BW}}$ to the one of $\sigma^2_{\mathrm{LC}}$, we introduce some notation to distinguish different regimes. First, recall that we say that $v \in \mathbb{F}_2^{2n}$ is supported on the $i$th brick if $\tilde{v}_i = 1$, and, by definition, $\tilde{v}_i = 1$ if at least one of $\mathrm{wt}(v)_{2i}$ and $\mathrm{wt}(v)_{2i+1}$ is non-zero. A supported brick can further be of two types. If $\mathrm{wt}(v)_{2i} \wedge \mathrm{wt}(v)_{2i+1} = 1$, namely the *logical and* between the two local weights is non-trivial, the $i$th brick is said to be *fully supported*. Otherwise, the $i$th brick is said to be *half supported* if the *logical xor* between the two local weights is non-trivial, or more formally $\mathrm{wt}(v)_{2i} \veebar \mathrm{wt}(v)_{2i+1} = 1$.

Still assuming $\mathrm{part}_{\mathrm{BW}}(v) = (n/2)$, we have two extreme cases:

- If each brick is *fully supported*, then $\sigma^2_{\mathrm{LC}} = 3^n > 2.1^{n+1} > \sigma^2_{\mathrm{BW}}$ for all $n \geq 2$. Thus, the brickwork circuits have an improved sample complexity compared to single qubit random Clifford unitaries. The number of samples is reduced by one order of magnitude for $n \geq 8$ and by a factor of about $0.5 \cdot 10^{-4}$ for $n = 20$.

- If each brick is *half-supported*, then $\sigma^2_{\mathrm{LC}} = 3^{n/2} < 1.75^n < 0.8 \cdot 2^n < \sigma^2_{\mathrm{BW}}$ for all $n \geq 2$. In this case, the BW circuit retains its periodic structure, while LCs shadow sees the 'correct' number of qubits in the support leading to a smaller sample complexity.

Similar considerations apply if $\mathrm{part}_{\mathrm{BW}}(v) = (n/2 - 1)$ i.e. when $(v\,|S|\,v)$ is given by a single term with open boundary condition. Evaluations of the expressions for both cases are summarized in Figure 6.5. We observe that the scaling for both cases only differ in a constant factor as we also explain analytically in Appendix A.3.

The two extreme cases suggest that shadows with BW circuits outperform the LCs ones when the number of fully supported bricks reaches a certain threshold. More specifically, based on our bounds, we can guarantee a lower sample complexity with BW circuits if $|\mathrm{supp}_{\mathrm{LC}}(v)| \geq 0.68(n+1)$ for the cases $\mathrm{part}_{\mathrm{BW}}(v) = (n/2)$ and $\mathrm{part}_{\mathrm{BW}}(v) = (n/2-1)$, see Appendix A.3. Furthermore, the additional constant term can be decreased for larger number of qubits. Evaluations of the threshold for up to 100 qubits are summarized in Figure 6.6.

Relaxing the restriction on $\mathrm{part}_{\mathrm{BW}}$, we can ensure that $\sigma^2_{\mathrm{BW}} \leq \sigma^2_{\mathrm{LC}}$ provided that

$$|\mathrm{supp}_{\mathrm{LC}}(v)| \geq 0.8|\,\mathrm{part}_{\mathrm{BW}}(v)| + 1.4\,|\tilde{v}|\,, \tag{6.32}$$

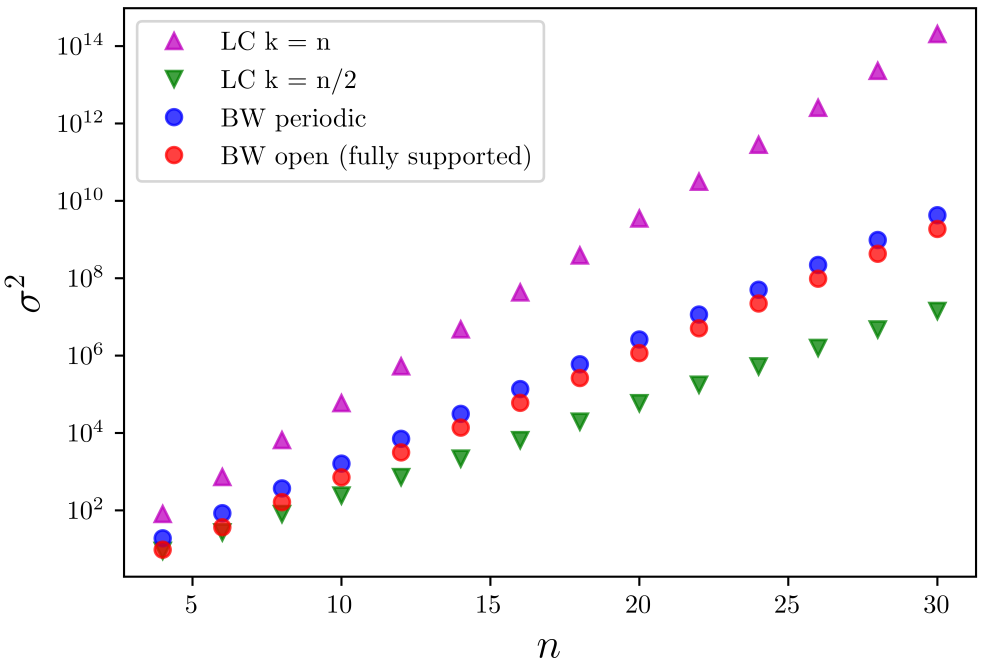



Figure 6.5: Comparison of variances (exact evaluation of second moments) calculated for brickworks and local Cliffords. For magenta and green triangles, we assumed $\mathrm{supp}_{\mathrm{LC}}(v) = n$ and $\mathrm{supp}_{\mathrm{LC}}(v) = n/2$, respectively. For blue and red dots, we assumed $\mathrm{part}_{\mathrm{BW}}(v) = (n/2)$ and $\mathrm{part}_{\mathrm{BW}}(v) = (n/2 - 1)$, respectively.

where $|\,\mathrm{part}_{\mathrm{BW}}(v)|$ is the number of entries in $\mathrm{part}_{\mathrm{BW}}(v)$ and $|\tilde{v}|$ the Hamming weight of $\tilde{v}$, i.e. the number of supported bricks in the circuit. The derivation of this criterion is given in Appendix A.3.

The main contribution (up to rescaling factors) is given by the size of $\mathrm{supp}_{\mathrm{BW}}$ (which, in turn, also influences the number of entries in $\mathrm{part}_{\mathrm{BW}}$), while the number of connected components in the effective circuit can be seen as a 'correction' to the naive comparison between the notions of supported Pauli's and bricks. In fact, by Eq. (6.16), the criterion is more likely to be satisfied if the local Pauli's are bunched together: Sparse Pauli observables are associated with (effective) BW circuits with many disjoint partitions, which imply a higher threshold. For instance, for a fixed $|\,\mathrm{supp}_{\mathrm{LC}}(v)|$, as the the number of distinct partitions increases, each subcircuit is less densely populated, and the threshold for each subcircuit becomes harder to reach. Fig. 6.7 shows two non-fully supported Pauli observables, supported on a different number of qubits, associated with the BW circuit structure. Eq. (6.32) is satisfied by the second Pauli string only.

The threshold criterion is likely to hold for random Pauli observables, since, for a fixed $n$, few additional qubits are needed to reach the threshold. On the other hand, for any random Pauli string $v \in \mathbb{F}_2^{2n}$, the probability of the $i$th brick to be fully supported is strictly larger than the probability of being half supported. Indeed, evaluating the bounds for random Pauli strings we observe that the brickwork circuit gives better performance with

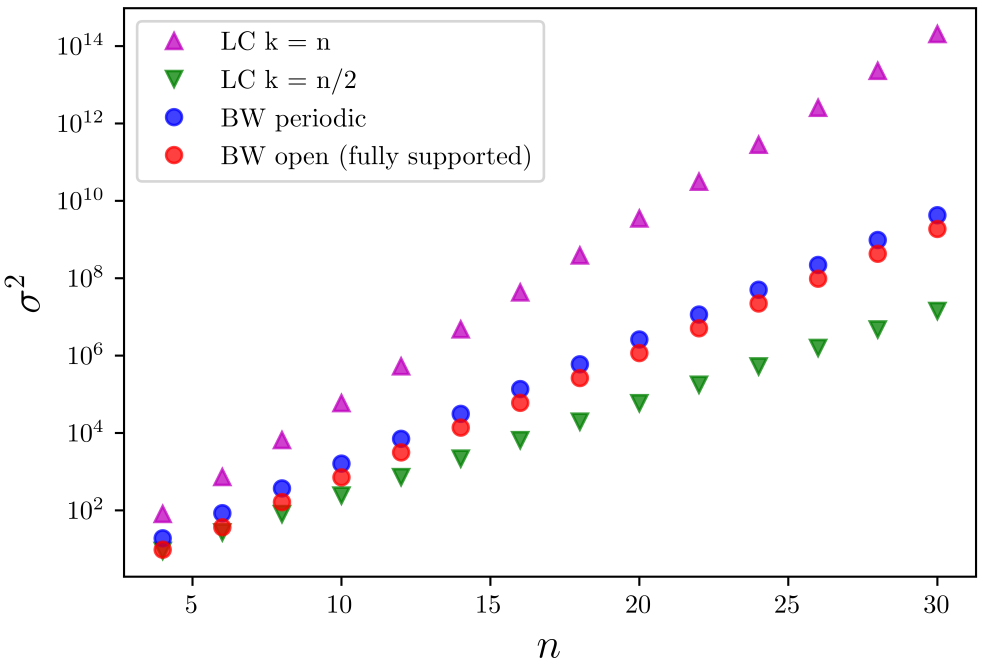



Figure 6.6: Numerical evaluation of the threshold that determines the BW sample advantage over LCs shadows in the case $\text{part}_{\text{BW}}(v) = (n/2)$. On the $x$ axis, we represent the total number of qubits. On the $y$ axis, we represent the ratio between the smallest number of qubits such that $\sigma^2_{\text{BW}} \leq \sigma^2_{\text{LC}}$ and the total number of qubits. The red line represents the ratio between the lower bound for $|\text{supp}_{\text{LC}}(v)|$ and the total number of qubits. The numerical dots are obtained by a direct comparison of $\sigma^2_{\text{BW}}$ and $\sigma^2_{\text{LC}}$: For each fixed $n$, and starting from the case where each brick is half-supported, we evaluated both of them for an increasing number of qubits (i.e. increasing the number of fully supported bricks), until the condition $\sigma^2_{\text{BW}} \leq \sigma^2_{\text{LC}}$ has been satisfied.

high probability drawing random Pauli strings, and $p(\sigma^2_{\text{BW}} \leq \sigma^2_{\text{LC}}) \xrightarrow{n \text{ big}} 1$, see Figure 6.8.

In conclusion, we showed that LCs shadows still have their own merit, in particular they are still the best choice for very sparse, local Pauli observables. However, they are significantly outperformed in all the other cases. For instance, for fully supported bricks, we observed that the variance is scaling as $\approx 2.1^n$, which is very close to the performance of a global Cliffords ensemble for a moderate number of qubits, namely global properties may be predicted using brickwork shadows. This represents a particular case of the shallow shadows presented in [106], where the authors argue that brickwork circuits (in their case, of depth $\log(n)$) are expected to have the same sample complexity as the global Clifford scheme.

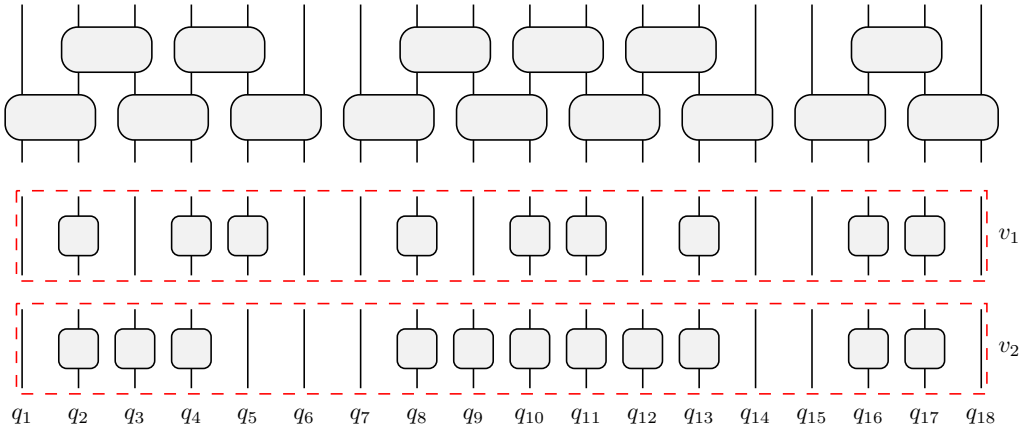



Figure 6.7: Effective circuits associated with two non-fully supported Pauli observables $v_1, v_2$. Eq. (6.32) is satisfied by $v_2$ only. In particular, we have $|\operatorname{part}_{\mathrm{BW}}(v_1)| = |\operatorname{part}_{\mathrm{BW}}(v_2)| = (2,3,1), |\operatorname{supp}_{\mathrm{BW}}(v_1)| = 9, |\operatorname{supp}_{\mathrm{BW}}(v_2)| = 11$, which imply $\sigma^2_{\mathrm{BW}}(v_1) = \sigma^2_{\mathrm{BW}}(v_2) \approx 58 \cdot 10^3, \sigma^2_{\mathrm{LC}}(v_1) \approx 19 \cdot 10^3, \sigma^2_{\mathrm{LC}}(v_2) \approx 177 \cdot 10^3$.

## 6.3 Numerical experiments

We now compare numerically performances of BW and LCs estimation procedures. For the simulation, we prepare a stabilizer input state, for simplicity, $\rho = |0\rangle\langle 0|$, and draw unitaries from the Clifford group. We choose to perform Pauli estimation for observables of $Z$-type. In this way, we can classically simulate the whole procedure efficiently using standard techniques [34, 35, 110]. The algorithms to perform the simulation work as follows: First, given $\rho = |0\rangle\langle 0|$ and a Pauli observable $W(v)$, Eq. (5.2) becomes

$$\langle 0|W(v)|0\rangle = \frac{1}{(v|S|v)} \sum_i \mathbb{E}_{U\sim\mu} \langle i|UW(v)U^\dagger|i\rangle |\langle i|U|0\rangle|^2 . \tag{6.33}$$

As discussed above, $U$ is chosen to be a Clifford operator, which is represented by a pair $(g,a)$, with $g \in \mathrm{Sp}(2n)$, and $a \in \mathbb{F}_2^{2n}$. Then, writing $U = \bigotimes_{i=1}^{n/2} \bigotimes_{j=1}^{n/2} U_1^{(i)} U_2^{(j)}$, each local symplectic matrix is sampled using König-Smolin's algorithm [110], and $a$ is a uniformly distributed vector in $\mathbb{F}_2^{2n}$. Then, samples $\{(U_j, i_j)\}_{j=1}^m$ are drawn according to standard stabilizer simulation techniques [34, 35], and the estimator is given by the following empirical average:

$$\hat{w}(v) = \frac{1}{m(v|S|v)} \sum_{j=1}^{m} \langle i_j|U_j W(v) U_j^\dagger|i_j\rangle . \tag{6.34}$$

A single estimate requires the calculation of the phase function appearing in Eq. (3.86), which can be done in time $\mathrm{O}(n^3)$ [90]. However, when the observable is of $Z$-type, we can avoid this calculation, and speed up the simulation. To prove this fact, let us consider the decomposition $\mathbb{F}_2^{2n} = Z_n \oplus X_n$, and label the computational basis by binary vectors $i \in \mathbb{F}_2^n$. Then,

$$\langle i|UW(v)U^\dagger|i\rangle = (-1)^{\alpha_g(v)+[a,gv]+(gv)_z\cdot i} 1_{Z_n}(gv) , \tag{6.35}$$

where $(gv)_z \in Z_n \simeq \mathbb{F}_2^n$ is the $Z$ part of the vector $gv \in \mathbb{F}_2^{2n}$, and $1_{Z_n}$ is the indicator function on $Z_n$. Then, suppose the outcome of the latter is non-zero, so $(gv)_x = 0$. Hence,

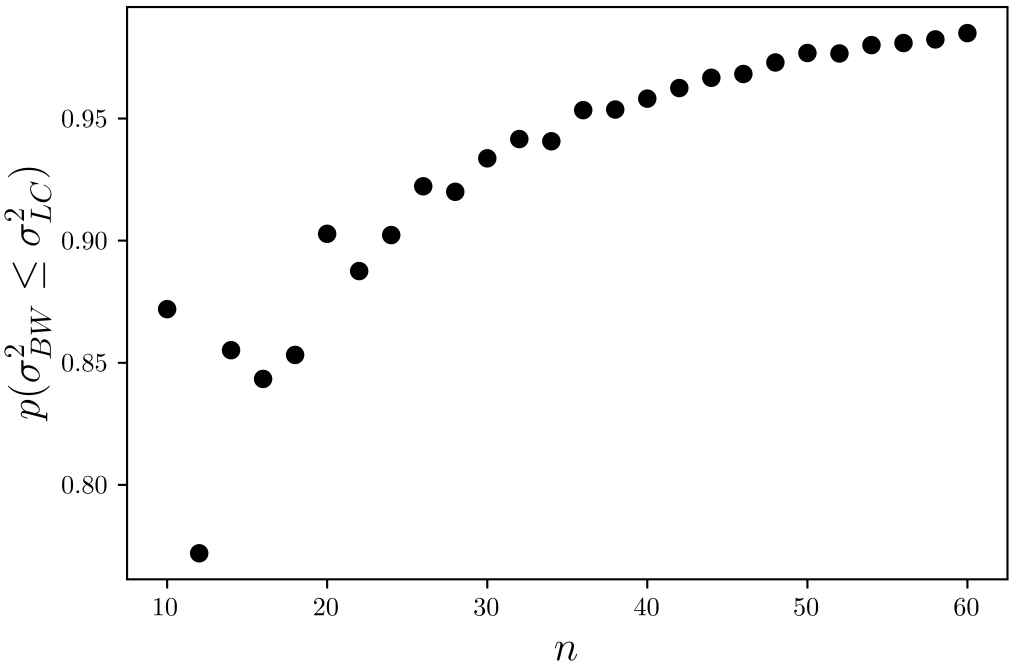



Figure 6.8: Probability of $\sigma^2_{\mathrm{BW}} \leq \sigma^2_{\mathrm{LC}}$, evaluated on $2^{16}$ random bitstrings for each value of $n$.

since $v_x = 0$ by assumption, we find:

$$\begin{aligned}[a, gv] + (gv)_z \cdot i = (gv)_z \cdot i_0 = (gv)_z \cdot \sum_j i_j (ge_j)_x \\ = \sum_j i_j [gv, ge_j] = \sum_j i_j [v, e_j] \\ = 0\,,\end{aligned} \tag{6.36}$$

where we wrote $i = i_0 + a_x$ for some $i_0 \in \mathbb{F}_2^n$, and then we considered the decomposition $i_0 = \sum_j i_j (ge_j)_z$, where $\{e_j\} \subset Z_n$ is the canonical basis.

Then, from Eq. (6.33) we get

$$\begin{aligned}(v\,|S|\,v) = \sum_i \mathbb{E}_{U\sim\mu} \langle i\,|UW(v)U^\dagger|\,i\rangle |\langle i\,|U|\,0\rangle|^2 \\ = \sum_i \mathbb{E}_{U\sim\mu} (-1)^{\alpha_g(v)} |\langle i\,|U|\,0\rangle|^2\,.\end{aligned} \tag{6.37}$$

Define now

$$p_\pm \coloneqq \frac{1}{|\mathrm{Sp}(2n)|} |\{g \in \mathrm{Sp}(2n) \mid gv \in Z_n\,,\ (-1)^{\alpha_g(v)} = \pm 1\}|\,. \tag{6.38}$$

Then,

$$\begin{aligned} p_+ + p_- &= \frac{1}{|\mathrm{Sp}(2n)|}|\{g \in \mathrm{Sp}(2n) \mid gv \in Z_n\}| \\ &= \frac{1}{|\mathrm{Sp}(2n)|}|\mathrm{STAB}(v)| \cdot |Z_n \setminus 0| \\ &= \frac{1}{|\mathrm{Sp}(2n)|}\frac{|\mathrm{Sp}(2n)|}{|\mathrm{Sp}(2n)\cdot v|} \cdot |Z_n \setminus 0| \\ &= \frac{2^n-1}{2^{2n}-1} = \frac{1}{2^n+1}\,, \end{aligned} \tag{6.39}$$

where $\mathrm{STAB}(v)$ denotes the set of stabilizers of $v$.

On the other hand, $p_+$ and $p_-$ also have the interpretation of frequencies of $\pm 1$ outcomes in Eq. (6.37) respectively. This means

$$(v\,|\,S\,|v) = p_+ - p_- = \frac{|Z_n|}{2^{2n}-1} = \frac{1}{2^n+1}\,, \tag{6.40}$$

from which it follows $p_- = 0$.

In conclusion, whenever $v_x = 0$, we only need to check if $(gv)_x$ is trivial.

Then, we consider the following setting: Fix $n = 10$ as the number of qubits. Then, we collect numerical data for three different $Z$-type operators, that we assume to be supported on each brick. In particular, we consider the following Pauli strings: $\mathrm{v}_{\mathrm{full}}$, which is supported on each qubit, $\mathrm{v}_{\mathrm{half}}$, where each brick is half supported, and $\mathrm{v}_{\mathrm{thres}}$, which is supported on 8 qubits, ensuring it satisfy the threshold criterion discussed in the last section. Notice that it does not matter where the two half supported bricks are located in $\mathrm{v}_{\mathrm{thres}}$, since all of them are supported. Then, we fix $m$ as the number of samples, and compute the empirical average over all samples as described in Section 5.1, which yields an estimator for the given observables and $\rho = |0\rangle\langle 0|$. We run this procedure 100 times, and evaluate the average of the estimators over all runs. The latter has standard deviation given by $\sigma/\sqrt{100m}$, with $\sigma = \sigma_{\mathrm{BW}}, \sigma_{\mathrm{LC}}$. Finally, the task is repeated for different values of $m$.

The results of the simulations, shown in Figs. 6.9 to 6.11, agree with the previous discussion. In particular, for circuits that are fully supported or over the threshold, the convergence to the expected values is faster using BW circuits, see Figure 6.9 and Figure 6.10, while the converse happens in the case of half supported circuits, see Figure 6.11.

## 6.4 Extension to deeper circuits

In the previous sections, we have shown clear evidence for the potential of using short circuits for shadow estimation, but also indicate limitations and the need for careful comparison in specific applications. Moreover, we expect that the direct generalization of our analytic approach to deeper circuits is considerably more involved.

To this end, the works of Akhtar *et al.* [109] and Bertoni *et al.* [106] characterize the frame operator of finite, arbitrary depth brickwork circuits with numerical methods. In particular, Akhtar *et al.* [109] applies the formalism based on entanglement features introduced by Bu *et al.* [105] and discusses average case scenario upper bounds on sample complexity based on the locally scrambled shadow norm [108]. A similar discussion, following a probabilistic interpretation of the eigenvalues of the measurement channels, can be found in [106]. In

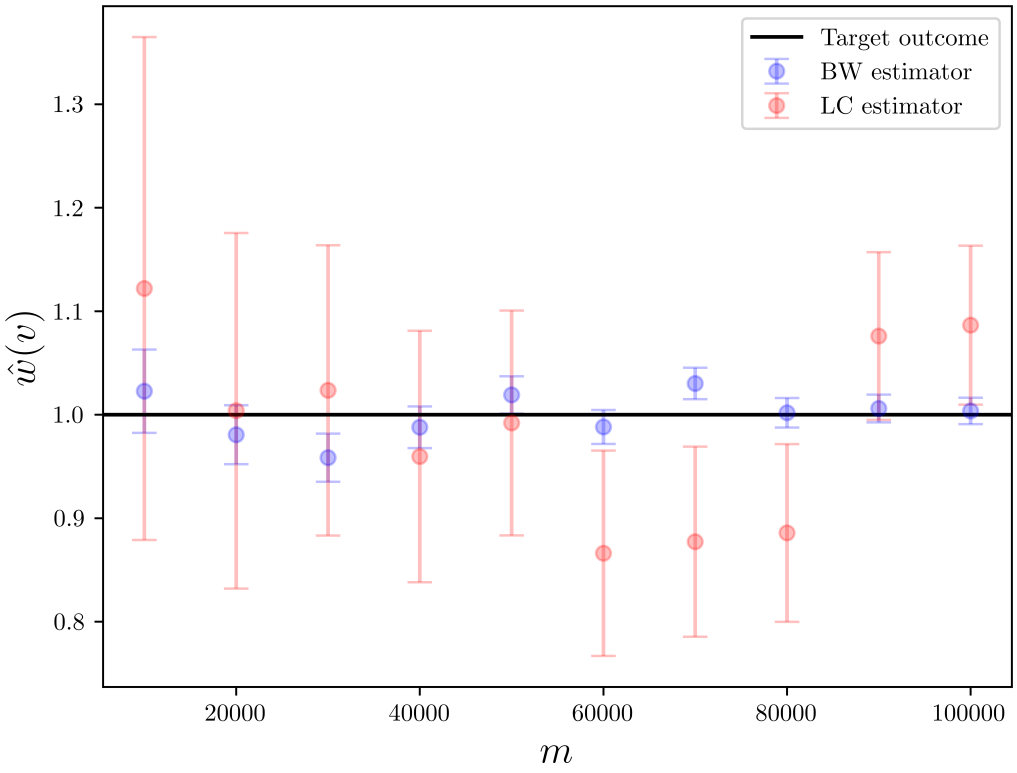



Figure 6.9: Convergence of the estimator $\hat{w}(\mathrm{v}_{\mathrm{full}})$, as defined in Section 5.1. We consider a system of 10 qubits with input state $\rho = |0\rangle\langle 0|$, ensuring we can classically simulate the whole procedure efficiently. For each fixed $m$, 100 runs have been performed and then the average over all of them, with the respective standard deviation, has been plotted. BW estimator is converging faster than the estimator using LC unitaries.

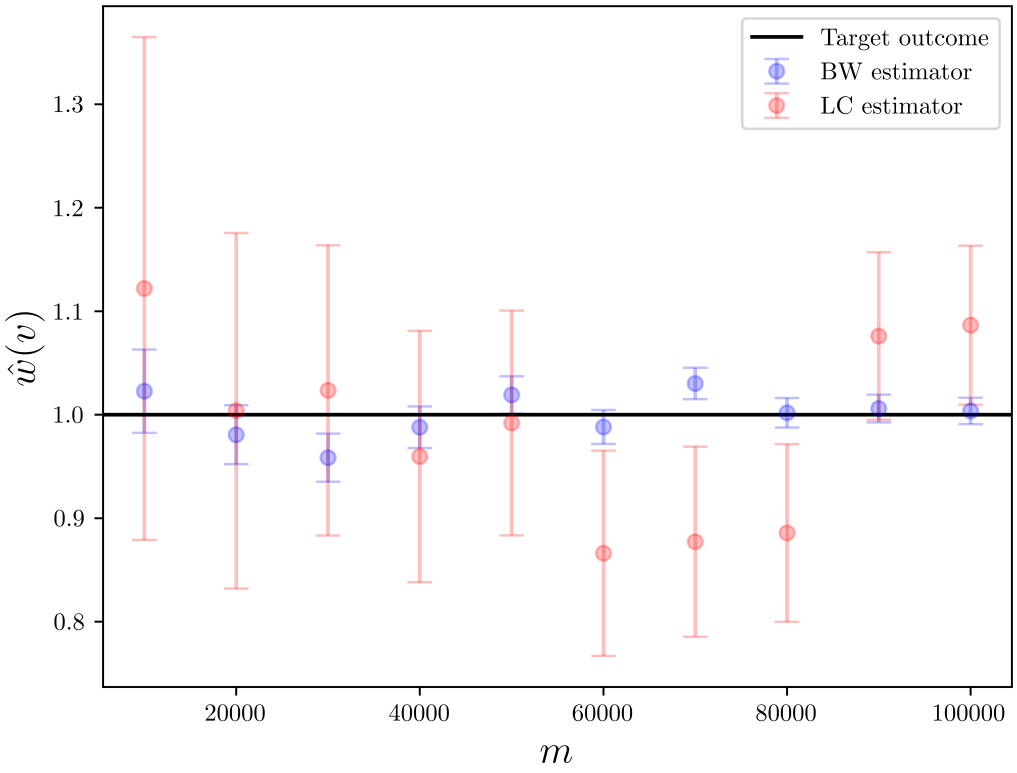



Figure 6.10: Convergence of the estimator $\hat{w}(\mathrm{v}_{\mathrm{thres}})$, as defined in Section 5.1. We consider a system of 10 qubits with input state $\rho = |0\rangle\langle 0|$, ensuring we can classically simulate the whole procedure efficiently. For each fixed $m$, 100 runs have been performed and then the average over all of them, with the respective standard deviation, has been plotted. BW estimator convergence is faster than the estimator constructed using LC unitaries.

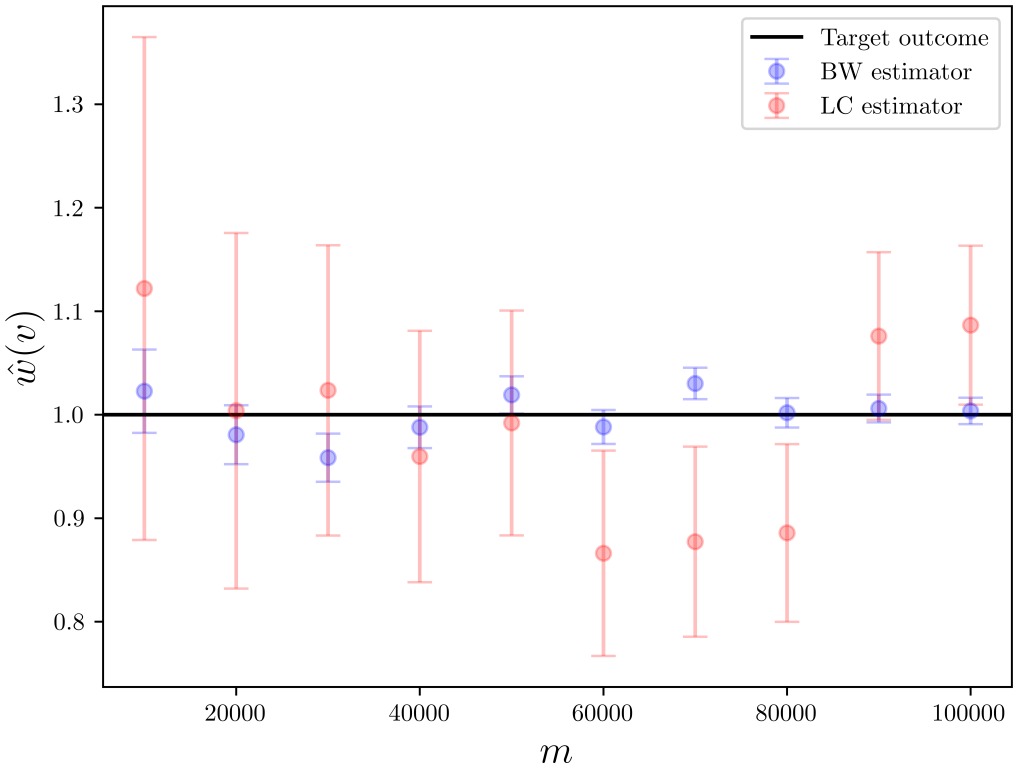



Figure 6.11: Convergence of the estimator $\hat{w}(\mathrm{v}_{\mathrm{half}})$, as defined in Section 5.1. We consider a system of 10 qubits with input state $\rho = |0\rangle\langle 0|$, ensuring we can classically simulate the whole procedure efficiently. For each fixed $m$, 100 runs have been performed and then the average over all of them, with the respective standard deviation, has been plotted. BW estimator convergence is slower than the estimator constructed using LC unitaries.

particular, Bertoni *et al.* [106] conjecture that a logarithmic depth circuit is the ideal middle ground between the local and global Cliffords ensembles. This claim is supported by the analysis of the locally scrambled shadow norm that shows that $\|O\|^2_{\text{lssh}}$ is bounded by the Frobenius norm $\|O\|^2_{\text{F}}$ for circuits of logarithmic depth. In comparison, we only focus on a single-round of a brick-layer circuits, but provide analytic expressions for the estimator of Pauli observables. A recent work by Schuster *et al.* [43] confirms this conjecture by showing that random quantum circuits form approximate unitary $k$-designs in logarithmic depth. The approximation is best controlled by the relative error $\epsilon$, see [120] and [43] for a discussion and comparison with the additive error (i.e., the diamond norm distance). Formally, denote with $U$ the defining representation of $\mathrm{U}(d)$ and recall the definition of the $k$th moment operator $\mathcal{M}_k$ from Eq. (3.49). For a probability measure $\nu_{\text{RC}}$ on $\mathrm{U}(d)$, define

$$\mathcal{M}_k^{\nu_{\text{RCS}}}(\cdot) \coloneqq \mathbb{E}_{U\sim\nu_{\text{RC}}} U^{\otimes k}(\cdot)U^{\otimes k\dagger} \tag{6.41}$$

We say that $\nu_{\text{RCS}}$ forms an $\varepsilon$-approximate unitary $k$-design (in relative error) if

$$(1-\varepsilon)\,\mathcal{M}_k \preceq \mathcal{M}_k^{\nu_{\text{RC}}} \preceq (1+\varepsilon)\,\mathcal{M}_k, \tag{6.42}$$

where $\mathcal{A} \preceq \mathcal{B}$ means that $\mathcal{B}-\mathcal{A}$ is a completely-positive map. Then, one can construct approximate unitary $k$-designs in $\log n$ depth by glueeing small brickwork circuits, which form approximate $k$-designs on $\log n$ qubits (this can be constructed in linear depth with known techniques [120]).

This construction can be applied to estimate low-rank observables with classical shadows. Recall from Section 5.2 that random global Clifford unitaries are particularly convenient to estimate low-rank observables (for instance, for fidelity estimation), but their concrete implementation is beyond near-term applications. Instead, classical shadows can be constructed from approximate designs paying a very small price: We consider an approximate unitary 3-design over $n$ qubits using random quantum circuit made up of Clifford circuits. Recall that the frame operator associated with Haar random unitaries admits the following block-diagonal representation in the Pauli basis:

$$S_H = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & s_H \mathbb{1} \end{pmatrix}, \tag{6.43}$$

with $s_H \equiv \frac{1}{d+1}$, c.f. Section 5.2. Then, by simply replacing the Haar random unitaries with a log-depth random circuit, the protocol is characterized by the frame operator

$$S_{\text{RCS}} \coloneqq \sum_{i\in[d]} \mathbb{E}_{U\sim\nu_{\text{RC}}} |E_{i,U})(E_{i,U}| \,. \tag{6.44}$$

Here, $\nu$ is approximate 2-design. Then, we can invert in post-processing with the inverse Haar-random frame operator $S_H^{-1}$ at the cost of a small bias in the shadow estimator $\hat{o}$ of $\mathrm{Tr}(\rho O)$ for any given observable $O$. In particular, one can show that the bias scales linearly in the relative error $\varepsilon$ [43]. A similar scaling also appears for the correction in the variance of the estimator.

Here, we note that the analysis of Section 6.1 can be adapted to study the eigenvalues of $S_{\text{RCS}}$. First, we observe that we can compute the eigenvalues of a short brickwork circuit in any local dimension. In other terms, Theorem 26 holds true for a suitable redefinition of the

functions $\Sigma_{\text{ob}}$ and $\Sigma_{\text{pb}}$. This follows from the fact that the recurrence relations Eqs. (6.23) and (6.27) are obtained by twirling Pauli strings with 2-local Haar random unitaries. Then, denoting with $p$ the local dimension, the systems of recurrence relations generalize to

$$\begin{cases} t_1^{\text{pb}}(n) = (p^5 - p^3)\, t_3^{\text{pb}}(n-2) \\ t_2^{\text{pb}}(n) = (p^5 - p^3)\, t_3^{\text{pb}}(n-2) + (p^6 - p^2)\, t_2^{\text{pb}}(n-2) \\ t_3^{\text{pb}}(n) = (p^5 - p^3)\, t_1^{\text{pb}}(n-2) + (p^6 - p^2)\, t_3^{\text{pb}}(n-2) \end{cases} \qquad n \geq 2\,, \quad n = 0 \mod 2\,, \tag{6.45}$$

and

$$\begin{cases} t_1^{\text{ob}}(n) = (p^5 - p^3)\, t_2^{\text{ob}}(n-2) \\ t_2^{\text{ob}}(n) = (p^5 - p^3)\, t_1^{\text{ob}}(n-2) + (p^6 - p^2)\, t_2^{\text{ob}}(n-2) \end{cases} \qquad n \geq 4\,, \quad n = 0 \mod 2\,, \tag{6.46}$$

with base conditions

$$\begin{cases} t_1^{\text{pb}}(2) = 0 \\ t_2^{\text{pb}}(2) = p^6 - p^2 \\ t_3^{\text{pb}}(2) = p^5 - p^3 \end{cases}, \quad \begin{cases} t_1^{\text{ob}}(4) = p^6 - p^4 \\ t_2^{\text{ob}}(4) = p^8 - p^5 - p^3 \end{cases}, \tag{6.47}$$

for the periodic and open boundary topologies, respectively. By solving the latter, we find the following expressions:

$$\Sigma_{\text{pb}}{}^{(p)}(m) = \frac{\left(\sqrt{(p^2+3)^2-8} + (p^2+1)\right)^{m/2} + (-1)^{m/2}\left(\sqrt{(p^2+3)^2-8} - (p^2+1)\right)^{m/2}}{(\sqrt{2}(p^2+1))^m}\,, \tag{6.48}$$

$$\Sigma_{\text{ob}}{}^{(p)}(m) = \frac{p^2+1}{2\sqrt{(p^2+3)^2-8}}\left(A_{\text{ob}}(m,p) + (-1)^{m/2} B_{\text{ob}}(m,p)\right)\,, \tag{6.49}$$

with

$$A_{\text{ob}}(m,p) \equiv \left((p^2+1)^2 - (p+1)\sqrt{(p^2+3)^2-8}\right)\left(\sqrt{(p^2+3)^2-8} + (p^2+1)\right)^{m/2}\,, \tag{6.50}$$

$$B_{\text{ob}}(m,p) \equiv \left((p^2+1)^2 + (p+1)\sqrt{(p^2+3)^2-8}\right)\left(\sqrt{(p^2+3)^2-8} - (p^2+1)\right)^{m/2}\,. \tag{6.51}$$

The main idea is to consider a sequence of depth-2 BW circuits –constructed as in Section 6.1– with increasing local dimension $p$. The rate at which $p$ increases is informally associated with the depth of a shallow BW circuit. Then, by iterating over the local dimension, we can study the convergence of the eigenvalues. Note that, in linear depth, any eigenvalue associated with a non-trivial Pauli string corresponds to an effective BW circuit realization of the Haar ensemble, hence, the convergence becomes exact at that point. In this first analysis, we study the convergence of the eigenvalues associated with fully supported circuits. In particular, we consider $v \in \mathbb{F}_2^{2n}$ such that $\text{part}_{\text{BW}}(v) = (n/2)$, c.f. Section 6.1. Note that if a $(p = 2^r)$-qudit BW circuit is fully supported, the same applies to the following

($p = 2^{r+1}$)-qudit BW circuit, as the relevant notion of locality is coarse-grained as the local dimension increases. We measure the convergence of the eigenvalues in the relative error

$$\varepsilon_{\text{eigen}} \equiv \frac{|s_{\text{RCS}} - s_H|}{s_H}\,, \tag{6.52}$$

where $s_{\text{RCQ}} \equiv (v\,|S_{\text{RCS}}|\,v)$. For simplicity, we consider a system of local dimension $p = 2^k$, with $k$ taking values in $\{2^r \mid r \in \{1, 2, \ldots, \lfloor \log_2 n \rfloor\}\}$. Note that for $k = 1$ the latter reduces to the qubit case, while the number of qubits on which each brick acts doubles at each following coarse-graining step. In general, $2k$ is the number of qubits on which each brick is supported. Intuitively, we interpret $r$ as the number of "gluing" iterations. Then, the corresponding number of qudits is $n/k$, and, setting ${\Sigma_{\text{pb}}}^{(2^k)}(m) \equiv \tilde{\Sigma}_{\text{pb}}(k, n)$, Eq. (6.48) becomes

$$\tilde{\Sigma}_{\text{pb}}(k,n) = \frac{\left(\sqrt{(4^k+3)^2-8} + (4^k+1)\right)^{\frac{n}{2k}} + (-1)^{\frac{n}{2k}}\left(\sqrt{(4^k+3)^2-8} - (4^k+1)\right)^{\frac{n}{2k}}}{(\sqrt{2}(4^k+1))^{n/k}} \tag{6.53}$$

(a similar expression holds for Eq. (6.49)). In Fig. 6.12, we numerically analyze the scaling of the relative error $|\tilde{\Sigma}_{\text{pb}}(k,n) - s_H|/s_H$, showing convergence for the eigenvalues associated with fully supported Pauli operators in logarithmic depth. If the BW circuit is not fully supported, the analysis is complicated by the effective topologies determined by the the geometry of the circuits associated with open boundary BW circuits. In particular, we observe that the log-depth convergence of the eigenvalues does not hold for all Pauli eigenoperators. For instance, this is the case of Pauli operators supported on a single qubit, which converge *exactly* to $s_H$ in linearly many steps. As a simple criterion, we identify the convergence to the fully supported topology with periodic boundary conditions as a necessary condition for convergence. In fact, this occurs at linear depth for Pauli strings supported on a single qubit, and at logarithmic depth for fully supported strings. As a rule of thumb, in general, once the effective circuit reaches this topology, convergence is ensured from $\log n$ depth on wards, in line with Fig. 6.12. However, the complete characterization of the convergence rate of the eigenvalues is still elusive. Establishing it requires a careful case-by-case analysis of the possible weight configurations in the partitions of the support (c.f., Section 6.1). We leave these questions for future work.

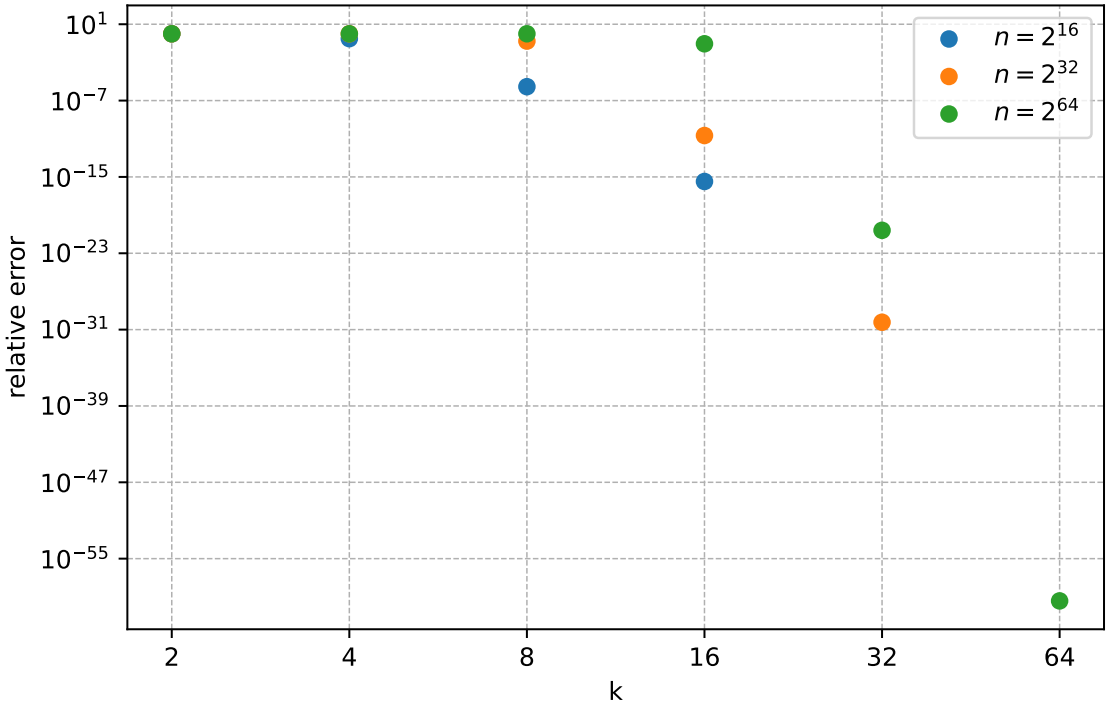



Figure 6.12: Numerical evaluation of the relative error for the eigenvalues of a fully supported Pauli basis element. The y-axis is in logarithmic scale. We plot eigenvalues of BW circuits with local dimension $p = 2^k$, where $k$ is the number of qubits on which each BW circuit acts. For convenience, we consider the number of qubits $n$ to be divisible by $k$ and we perform the computation with arbitrary accuracy using the Python library [121]. Here, $2k$ is the number of qubits on which each brick is defined, and we consider a brickwork circuit of local dimension that are associated with a random quantum circuit (RQC) with at most $\log_2 n$ layers. The relative error becomes suddenly negligible for $k \approx 2^{\log_2 n - 1}$.

# Chapter 7

# Fermionic shadows

Some of the most promising applications of quantum computers lie in the simulation of complex molecules and strongly correlated systems [122]. A deeper understanding of these systems can lead to major advances in materials science, chemistry, and engineering [123–128]. Yet, achieving accurate simulation remains challenging even for state-of-the-art classical methods. For instance, the cost of density matrix renormalization group (DMRG) techniques is too big outside favorable regimes [122]. In particular, DMRG provides a scalable route to accurate ground state approximations for local lattice Hamiltonians in one spatial dimension thanks to favorable entanglement area laws, while the same does not hold in higher dimensions. At the same time, the limitations of near-term quantum hardware motivate algorithmic approaches that trade circuit depth for additional measurements. A prominent paradigm in the NISQ regime is that of variational quantum algorithms: One prepares a parametrized quantum state and updates the parameters through a classical optimization loop, which typically requires repeated estimation of expectation values for a large collection of observables. In quantum chemistry and many-body physics, a particularly important class of target expectation values are k-reduced density matrixs (kRDMs), which encode correlations relevant, for instance, to energies [129–131]. In particular, all one-body observables, such as orbital occupations and kinetic energy, and Coulomb interactions and correlators are captured by $k = 1, 2$ kRDMs [132–134].

As such, classical shadows offer a clear path to estimating large families of fermionic observables from randomized measurements. Extending the shadow formalism to fermions, however, requires careful design choices for the unitary ensemble. Ideally, the ensemble should admit experimentally simple implementations and lead to time-efficient and scalable estimators, with tight bounds on the sampling complexity. In fermionic systems, a natural candidate is the family of fermionic Gaussian transformations, identified by matchgate unitaries [135]. Like Clifford circuits in the discrete setting, these transformations are classically efficiently simulable [136]. However, several differences arise due to the structure of the underlying groups. Moreover, it is often more practical to consider sampling from a restricted subset of matchgates.

In this chapter, we discuss the extension of classical shadows to fermionic systems, and discuss the case of symmetry-adapted fermionic shadows. The chapter is organized as follows: In Section 7.1, we fix the notation and recall the formalism of fermionic systems, with an emphasis on Gaussian unitaries. In Section 7.2 and Section 7.3, we review shadow estimation based on matchgate ensembles and on passive fermionic transformations,

respectively. Finally, in Section 7.4, we discuss adaptations of the protocol to spin-preserving ensembles, and highlight challenges posed by multiplicities that arise in the corresponding shadow estimators.

## 7.1 Gaussian transformations of fermionic systems

Let $\mathcal{H} \cong \mathbb{C}^m$ be a finite dimensional Hilbert space. A system of fermions with single-particle Hilbert space $\mathcal{H}$ is described by the $m$-modes fermionic Fock-Hilbert space defined as

$$\mathcal{H}_{\mathcal{F}}(\mathbb{C}^m) \coloneqq \bigoplus_{n=0}^{m} \bigwedge^{n}(\mathbb{C}^m)\,, \tag{7.1}$$

where $\bigwedge^n(\mathbb{C}^m)$ denotes the totally anti-symmetric subspace of $(\mathbb{C}^m)^{\otimes n}$ describing the states consisting of $n$ fermions distributed over $m$ modes. Here, $\bigwedge^0(\mathbb{C}^m) = \mathrm{span}_{\mathbb{C}}(|0\rangle)$, where $|0\rangle$ is the Fock vacuum state. For a fixed basis $\{|i\rangle\}_{i\in[m]}$ of $\mathbb{C}^m$ we define a family of creation and annihilation operators $f_j, f_j^\dagger$ acting on $\mathcal{H}_{\mathcal{F}}(\mathbb{C}^m)$, $j = 1, \ldots, m$ satisfying the canonical anti-commutation relations

$$\{f_j, f_k^\dagger\} = \delta_{j,k}\,, \quad \{f_j, f_k\} = 0 \tag{7.2}$$

for $j, k = 1, \ldots, m$. The subspace $\bigwedge^n(\mathbb{C}^m)$ –of dimension $\dim \mathcal{H}_n^m = \binom{m}{n}$– is spanned by the (fermionic) Fock states

$$|\boldsymbol{x}\rangle \coloneqq (f_1^\dagger)^{x_1}(f_2^\dagger)^{x_2} \ldots (f_d^\dagger)^{x_m}|0\rangle\,, \tag{7.3}$$

where $\boldsymbol{x} \in \{0,1\}^m$. Due to anticommutation relations, basis elements for a particle number sectors are indexed by occupation number sequences given by

$$S_{n,m} \coloneqq \{(z_1, \ldots, z_n) \mid 1 \le z_1 < z_2 < \cdots < m\}\,, \tag{7.4}$$

where each entry denotes which mode is occupied.

Fermionic Gaussian transformations correspond to the unitaries generated by Hamiltonians at most quadratic in the creation and annihilation operators. We distinguish between active and passive transformations, with the ensemble of passive transformations preserving the total number of particles in the system. Gaussian unitaries correspond to the *matchgate group*, generated by unitaries of the form $\exp(i\varphi W(v) \otimes W(u))$ with $u, v \in \mathbb{F}_2^2$ acting on nearest-neighbors qubits, and single qubit $Z$ rotations [137]. These form the metaplectic (projective) representation of $\mathrm{O}(2m)$. Due to energy conservation, the ensemble of passive Gaussian unitaries corresponds to unitary operators generated by Hamiltonians containing terms of the form $f_j^\dagger f_k + \text{h.c.}$ and are identified by unitary matrices in $\mathrm{U}(m)$ [138]. Formally, to preserve particle number, a passive Gaussian transformation is such that $f_i \mapsto \tilde{f}_i = \sum_{j=1}^m U_{i,j} f_j$, for an invertible matrix $U = (U)_{i,j}$. The transformed creation and annihilation operators still satisfy the canonical anticommutation relations, i.e., it still holds that $\{\tilde{f}_i, \tilde{f}_j^\dagger\} = \delta_{i,j}$ and $\{\tilde{f}_i, \tilde{f}_j\} = 0$. Thus, by linearity, $UU^\dagger = \mathbb{1}$. Hence, $U \in \mathrm{U}(m)$. Following the discussion in Section 3.1, we mostly restrict our attention to representations of $\mathrm{SU}(m)$, which differ from the corresponding representations of $\mathrm{U}(m)$ by an overall phase factor.

## 7.2 Matchgate shadows

Shadow estimation extends naturally to the fermionic setting due to the natural isomorphism between Pauli and Majorana operators [96]. Formally, the protocol works as in the general prescription described in Chapter 5: After preparing a fermionic input state $\rho$, randomized unitaries drawn from a suitable (group) ensemble $\mathscr{U} \subseteq \mathrm{U}(\mathcal{F}_m)$ is applied, and a measurement in the computational basis is performed. Here, the measurement is conveniently described by the fermionic Fock states POVM $\{|\boldsymbol{z}\rangle\langle\boldsymbol{z}|\}_{\boldsymbol{z}\in\mathcal{F}_m}$ under the Jordan-Wigner isomorphism. The outcome of the measurement and the drawn unitary are stored for post-processing as in Section 5.1. In practice, $\mathcal{U}$ is often chosen to be a subset of matchgate unitaries to ensure efficient sampling and post-processing via standard simulation techniques for fermionic Gaussian circuits [135, 136, 139, 140]. Therefore, for a given observable $O$, we consider the estimator of $\mathrm{Tr}(\rho O)$ defined as

$$\hat{o} = (O\,|S^{-1}\omega(g)^\dagger|E_{\boldsymbol{z}})\,, \tag{7.5}$$

with $E_{\boldsymbol{z}} \equiv |\boldsymbol{z}\rangle\langle\boldsymbol{z}|$, where $\omega$ is a suitable reference representation of $\mathcal{U}$, and

$$S \coloneqq \int_{\mathcal{U}} dg\,\omega(g)^\dagger|E_{\boldsymbol{z}})(E_{\boldsymbol{z}}|\omega(g)\,, \tag{7.6}$$

as in Chapter 5.

If the ensemble is chosen to be the matchgate group, this corresponds to sampling unitaries from the Haar random distribution on $\mathrm{O}(2m)$. Here, the relevant representation of the matchgate group acts on Majorana operators by the adjoint action of the matchgate unitary. More formally, for an $m$-modes fermionic system, the associated Majorana operators are the Hermitian operators defined as

$$\gamma_{2j-1} = f_j + f_j^\dagger\,, \quad \gamma_{2j} = -i(f_j - f_j^\dagger)\,. \tag{7.7}$$

Then, $\tau(g)$ is a matchgate unitary with $g \in \mathrm{O}(2m)$, and we consider the action of the matchgate group described by the representation $\omega = \tau(g)(\cdot)\tau(g)^\dagger$. In particular, we have $\tau(g)\gamma_j\tau(g)^\dagger = \sum_{j\in[2m]} g_{k,j}\gamma_k$. Notably, this representation decomposes into $2m$ inequivalent irreps [137] which are spanned by suitable products of Majorana operators. Formally, this is expressed as follows: Let $\gamma_i$ be a single-mode Majorana operator. Setting $A = \{i_1, \ldots, i_{|A|}\}$, one can consider the product of $A \subseteq [2m]$ Majorana operators $\gamma_A \coloneqq \gamma_{i_1}\ldots\gamma_{i_{|A|}}$ with $i_1 < \cdots < i_{|A|}$. By definition, the action of a matchgate unitary is given by

$$\tau(g)^\dagger\gamma_A\tau(g) = \sum_B \det\left(g|_{A,B}\right)\gamma_B\,, \tag{7.8}$$

with $B$ being a sequence of indices such that $|B| = |A|$ and $g|_{A,B}$ denotes the submatrix of $g$ with rows indexed by $A$ and columns indexed by $B$. Then, the irreducible subspaces of $\omega$ are of the form $\langle\gamma_A \mid A \subseteq [2m]\rangle$ and, by Schur's lemma, the frame operator is of the form $S = \sum_{l=1}^{2m} s_l|\mathbb{1}_l)(\mathbb{1}_l|$, where $|\mathbb{1}_l)(\mathbb{1}_l|$ denotes the projector onto the $l$th irreducible subspace. Then, one can show that [96]

$$S = \sum_{l=0}^{m} \binom{2m}{2l}\binom{m}{l}|\mathbb{1}_{2l})(\mathbb{1}_{2l}|\,. \tag{7.9}$$

This setting ensures efficient fidelity estimation of pure Gaussian states and Slater determinants. This follows from classical simulation techniques of fermionic circuits described within the Gaussian formalism [135]. An approach based on Grassmann's calculus lead to estimators for general observables as well [96, 136]. The third-moment operator can also be analyzed in a similar fashion, leading to tight bounds on the variance of the protocol for such observables. The same results hold if random unitaries are drawn from the ensemble of matchgate Clifford unitaries $\mathrm{O}(2m) \cap \mathrm{Cl}_m$, as these form a matchgate 3-design, c.f. Definition 21, i.e.,

$$\int_{\mathrm{O}(2m)} dg\, \tau(g)^{\otimes 3}(\cdot)\tau(g)^{\otimes 3\dagger} = \sum_{g\in \mathrm{O}(2m)\cap \mathrm{Cl}_m} \tau(g)^{\otimes 3}(\cdot)\tau(g)^{\otimes k\dagger} \tag{7.10}$$

for $k = 1, 2, 3$. Analogous results have been derived for similar ensembles of fermionic unitaries [99], for instance, by sampling random signed permutation matrices. In particular, random gates drawn from $\mathrm{O}(2m)$, $\mathrm{SO}(2m)$, $\mathrm{O}(2m) \cap \mathrm{Cl}_m$, $\mathrm{SO}(2m) \cap \mathrm{Cl}_m$ lead to equivalent estimation routines with similar variances [141].

## 7.3 Classical shadows with fermionic passive transformations

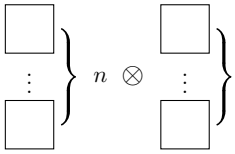
In practical tasks, exploiting symmetries of the system under examination is crucial to reduce the size of the problem, and, consequently, the sampling complexity. Let $\boldsymbol{x}, \boldsymbol{y} \in S_{n,m}$ with $|\boldsymbol{x}| = |\boldsymbol{y}| = k$. Here, $|\boldsymbol{x}|$ denotes the Hamming weight of $\boldsymbol{x}$. The task of estimating a kRDM, defined as $\mathrm{Tr}[D^{\boldsymbol{y}}_{\boldsymbol{x}}\rho]$, with

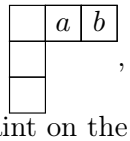
$$D^{\boldsymbol{y}}_{\boldsymbol{x}} \coloneqq f^\dagger_{x_1} \dots f^\dagger_{y_k} f_{y_k} \dots f_{x_1} \tag{7.11}$$

is relevant for the description of interacting electrons or correlation functions [95], as one and two-body observables are described by $k = 1, 2$ kRDMs. kRDMs are especially relevant for systems with a definite number of particles distributed across $m$ modes. Hence, randomizing over particle-preserving unitaries is expected to lead to improvement in the sampling complexity. In fact, Low [142] showed that, on average, the sampling complexity does not depend on the number of modes $m$, leading to a favorable scaling in tasks such as modeling dynamical correlations and simulations tasks where $m \gg n$ [143–145]. In this section, we review the characterization of the frame operator (7.6) from the point of view of the Clebsch-Gordan decomposition, c.f. Section 3.1. We refer to [142] for the construction of time-efficient simulations for the estimators of the overlaps $\mathrm{Tr}[D^{\boldsymbol{y}}_{\boldsymbol{x}}\rho]$.

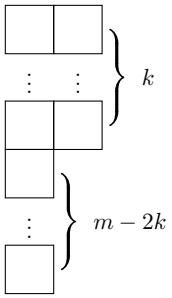
Let $n \leq m$ be the total number of particles and let $\bigwedge^n(\mathbb{C}^m)$ be the corresponding Fock subspace. We assume the unknown state $\rho$ has a well-defined number of particles $n$. The ensemble of fermionic passive Gaussian unitaries is a natural choice to construct a shadow estimator for kRDMs. Formally, we consider random unitaries $\tau(g)$ acting on $\bigwedge^n(\mathbb{C}^m)$, where $g \in \mathrm{U}(m)$, c.f. Section 7.1. The relevant representation decomposes into multiplicity-free irreps, and the frame operator can be computed (and inverted) in the basis where it is block diagonal. To see this, first recall that $\bigwedge^n(\mathbb{C}^m)$ is the carrier space of an antisymmetric irrep $\mathrm{U}(m)$, labeled by Young diagrams with only one column. For instance, $\begin{array}{|c|}\hline \\ \hline \\ \hline \end{array}$ denotes the fermionic Fock space of 3 particles distributed over $m \geq 4$ modes. Note that we can

equivalently treat this space as an antisymmetric irrep of $\mathrm{SU}(m)$ without loss of generality, c.f. Section 3.1.1. As such, the representation $\omega_n^m(g) \equiv \omega(g) \coloneqq \tau_n^m(g)(\cdot)\tau_n^m(g)^\dagger \cong \tau_n^m(g) \otimes \bar{\tau}_n^m(g)$ is given by the product

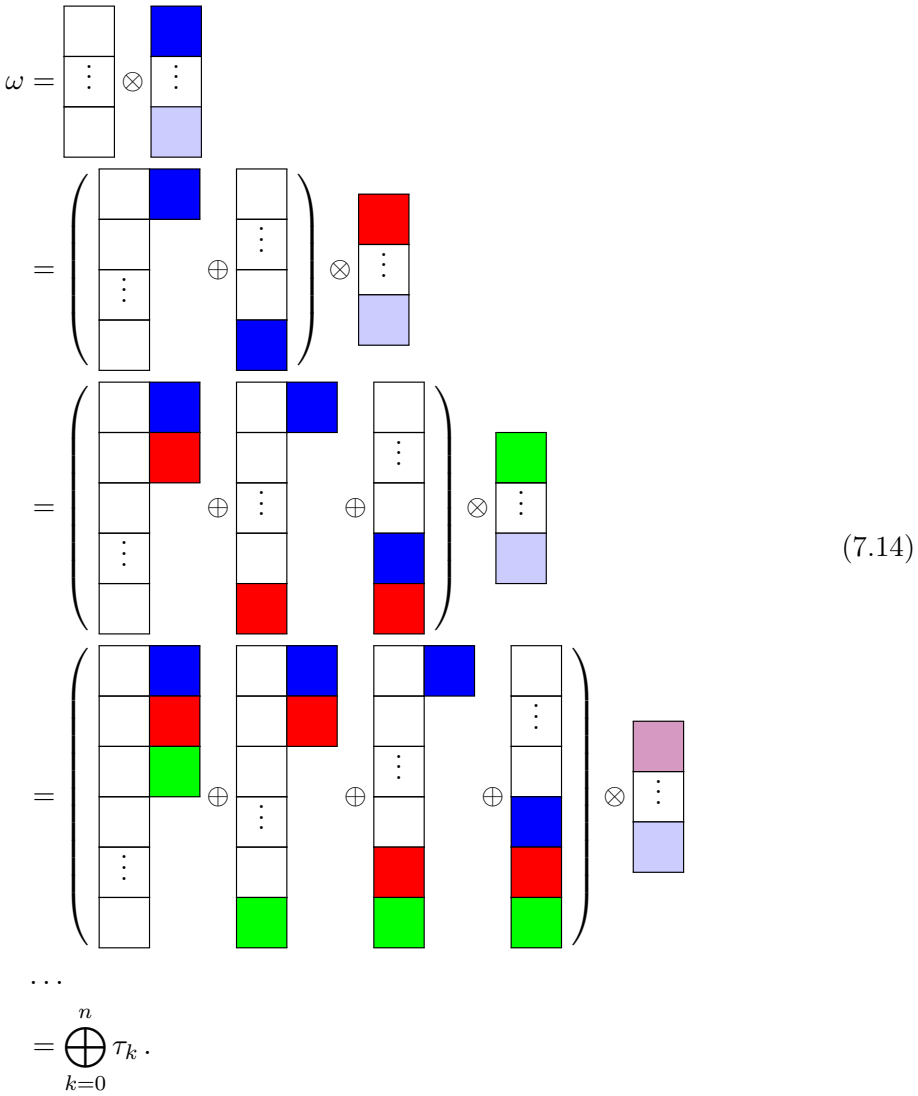
$\omega =$  (7.12)


where the second Young diagram on the right hand side is associated with $\bar{\tau}_n^m$. The irrep decomposition of the latter is multiplicity-free, c.f. Section 3.1.2: Consider a Young tableau associated with the second diagram (e.g., labeling the boxes in alphabetic order). Young diagrams with more than two columns cannot appear in the decomposition of $\omega$, as they would require to be of the type 

, for instance. Any such shape is not allowed due to the antisymmetry constraint on the rows. As a consequence, assuming $n \geq m - n$ without loss of generality, the only diagrams that can appear in the decomposition are either completely antisymmetric, or of shape

 (7.13)

for $k = 1, 2, \ldots, m - n$. More precisely, observe that



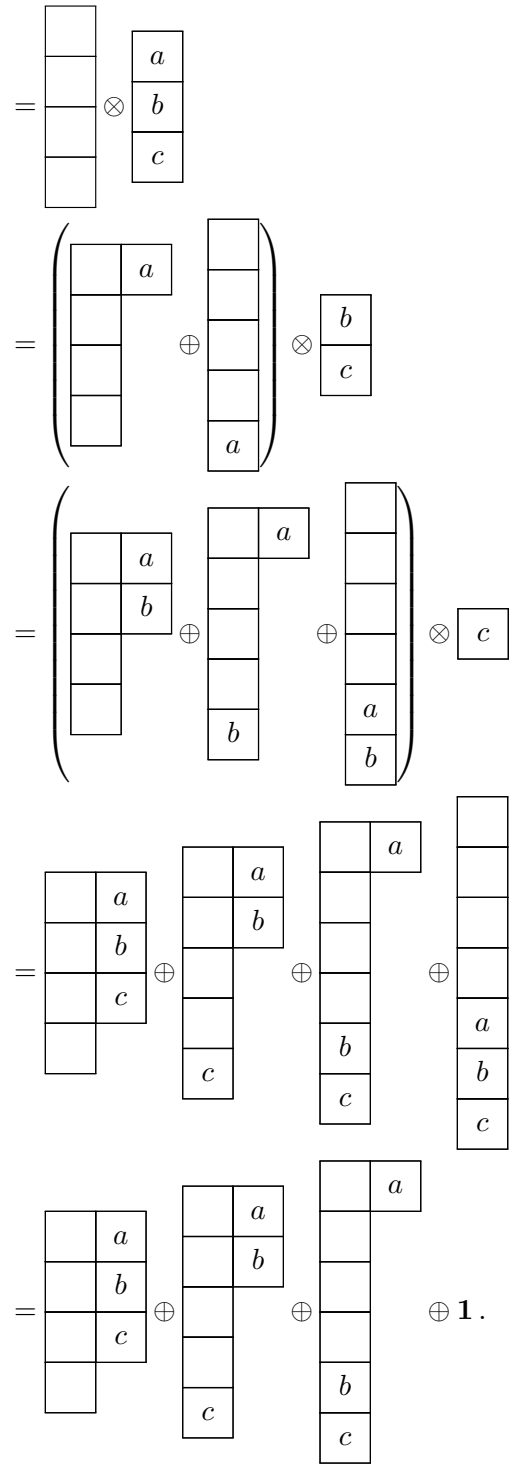
(7.14)

Note that by the elimination rule, c.f. Section 3.1.2, only the first terms in the parentheses give rise to two summands.

**Example 30.** Let $m = 7$ and consider the irrep $\tau_4^7$. Then, by Littlewood-Richardson' rules,

c.f. Section 3.1.2,

$$\omega = \tau_4^7 \otimes \bar{\tau}_4^7$$




(7.15)

We remark that in the formula

$$\omega = \bigoplus_{k=0}^{n} \tau_k \tag{7.16}$$

$\tau_0 \equiv \mathbf{1}$ is the trivial representation, and $\tau_1$ denotes the adjoint representation. By Schur's Lemma 5, it follows

$$\begin{aligned} S &\coloneqq \sum_{\boldsymbol{z}\in\mathcal{H}_n^m} \int_{\mathrm{U}(m)} dg\, \omega(g)^\dagger |E_{\boldsymbol{z}})(E_{\boldsymbol{z}}|\omega(g) \\ &= \bigoplus_{k=0}^{n} s_k \mathrm{id}_k \,, \end{aligned} \tag{7.17}$$

where $s_k = \frac{1}{d_k}\sum_{\boldsymbol{z}\in\mathcal{H}_n^m}(E_{\boldsymbol{z}}\,|P_k|\,E_{\boldsymbol{z}})$. To compute the coefficients, let us consider the vectorization $E_{\boldsymbol{z}} \cong |\boldsymbol{z},\boldsymbol{z}\rangle$ and let $Z$ be the GT pattern associated with $\boldsymbol{z}$. Let $\bar{Z}$ be the corresponding pattern in the dual representation and recall that $|Z\rangle = (-1)^{\varphi(Z)}|\bar{Z}\rangle$, c.f. Eq. (3.23). Then, as $P_k = \sum_{M\in\mathrm{GT}(\tau_k)}|M\rangle\langle M|$,

$$\begin{aligned} s_k &= d_k^{-1} \sum_{Z\in\mathrm{GT}(\tau_k)} \langle Z, Z\,|P_k|\,Z, Z\rangle \\ &= d_k^{-1} \sum_{Z\in\mathrm{GT}(\tau_k)} \langle Z, \bar{Z}\,|P_k|\,Z, \bar{Z}\rangle \\ &= \frac{1}{d_k} \sum_{Z\in\mathrm{GT}(\tau_k)} \sum_{M\in\mathrm{GT}(\tau_k)} \langle Z, \bar{Z}|M\rangle\langle Z, \bar{Z}|M\rangle \\ &= \frac{1}{d_k} \sum_{Z\in\mathrm{GT}(\tau_n^m)} \sum_{M\in\mathrm{GT}(\tau_k)} |C^M_{Z,\bar{Z}}|^2 \\ &= d_k^{-1} \sum_{M\in\mathrm{GT}(\tau_k)} \delta_{M,M} \\ &= \frac{\gamma_k(\mathbf{0})}{d_k} \,. \end{aligned} \tag{7.18}$$

The third step follows from the fact that $Z, \bar{Z}$ are weight 1 vectors. This is a simple consequence of the fact that $\tau_n^m$ is a one-column diagram: The number of Young tableaux with weight of shape $\tau_n^m$ is exactly 1 (the same applies for $\bar{\tau}_n^m$ by duality). In the fourth step, we used the definition of Clebsch-Gordan coefficients, in the fifth step we used orthogonality relations (3.37), and $\gamma_k(\mathbf{0})$ is the inner multiplicity of $\mathbf{0}$ in $\tau_k$. Moreover [146],

$$d_k = \binom{m}{k}^2 - \binom{m}{k-1}^2 , \tag{7.19}$$

and by a numerical analysis of Kostka numbers, which amounts to the inner multiplicities,

$$\gamma_k(\mathbf{0}) = \binom{m}{k} - \binom{m}{k-1} . \tag{7.20}$$

This implies

$$s_k = \frac{1}{\binom{m}{k} + \binom{m}{k-1}} = \binom{m+1}{k}^{-1} . \tag{7.21}$$

The same result follows from Weingarten calculus for the unitary group [83] and by the decomposition of the projectors $P_k$ on the $k$th irrep in elementary symmetric polynomials [142]. In particular, a polynomial-time routine to compute the estimators follows from such construction. We refer to [142] for further details.

## 7.4 Spin-adapted shadows

Fermionic systems often obey spin symmetries. This allows for further block-diagonalizations of the relevant representation according to the structure of the spin sectors. In the language of second quantization, this is modelled by considering a set of orthogonal spatial orbitals to which an additional degree of freedom, the spin, can be associated to define the spin-orbitals [147]. In this section, we use the following abstract "$\alpha$-then-$\beta$" notation: Let $\alpha$ and $\beta$ be the possible values of the spin. For $m$ spatial orbitals, we introduce $2m$ fermionic modes, labeled such that modes $1, \dots, m$ correspond to the $\alpha$ spin-orbitals, and modes $m+1, \dots, 2m$ to the $\beta$ spin-orbitals (equivalently, $f_i \equiv f_{i,\alpha}$ and $f_{i+m} \equiv f_{i,\beta}$). With this ordering, under the Jordan-Wigner transformation, each fermionic mode is mapped to one qubit, and the computational basis encodes the occupation numbers. We consider the number operators $N_\alpha \coloneqq \sum_{i=1}^{m} f_i^\dagger f_i$, $N_\beta \coloneqq \sum_{i=m+1}^{2m} f_i^\dagger f_i$. We will denote with $n_\alpha$ and $n_\beta$ the corresponding eigenvalues. Next, define the spin operators [147]

$$S_z \coloneqq \frac{1}{2}\left(N_\alpha - N_\beta\right), \quad S^2 \coloneqq S_x^2 + S_y^2 + S_z^2 \tag{7.22}$$

$$= S_- S_+ + S_z + S_z^2, \tag{7.23}$$

where $S_+ \coloneqq \sum_{i=1}^{m} f_i^\dagger f_{i+m}$ and $S_- = S_+^\dagger$. In the latter, we used the relations $S_\pm = S_x \pm i S_y$ and $[S_+, S_-] = 2S_z$. In particular, it follows

$$S^2 = \sum_{i,j=1}^{m} f_i f_j^\dagger f_{i+m}^\dagger f_{j+m} + \frac{N_\alpha - N_\beta}{2} + \frac{(N_\alpha - N_\beta)^2}{4}. \tag{7.24}$$

We are interested in the particle number-conserving unitaries that preserve the latter symmetries and the total number of particles. In particular, conservation of $S_z$ and the total number operator $N \coloneqq N_\alpha + N_\beta$ amounts to conserving $N_\alpha$ and $N_\beta$ separately. Let $n_\alpha$, $n_\beta$ be the number of spin $\alpha$ and spin $\beta$ particles, respectively. Therefore, we consider passive Gaussian transformations $\tau\colon \mathrm{SU}(2m) \to \mathrm{U}\left(\bigwedge^n(\mathbb{C}^{2m})\right)$, with $n = n_\alpha + n_\beta$, obeying the symmetries

$$[\tau(g), N_\alpha] = [\tau(g), N_\beta] = [\tau(g), S^2] = 0, \quad \forall g \in \mathrm{U}(2m). \tag{7.25}$$

For completeness, we also consider the case where $S^2$ is not conserved, although this is not typically relevant in practice. Then, we have can identify how the orbital transformations restrict in the spin-adapted setting:

**Lemma 31.** *The group of unitaries such that $N_\alpha$ and $N_\beta$ are preserved is isomorphic to $\mathrm{U}(m) \times \mathrm{U}(m)$. The group of spin-preserving transformations is isomorphic to $\mathrm{U}(m)$.*

*Proof.* We consider a fermionic system of $n_\alpha + n_\beta$ particles distributed over $2m$ modes. Let $\tau : \mathrm{U}(2m) \to \mathrm{U}(\mathcal{H}^{2m}_{n_\alpha+n_\beta})$ be the representation of a passive Gaussian transformation onto such space. Since the total number of particles is preserved by such map, we have

$$\tau(g) f_i^\dagger \tau(g)^\dagger = \sum_{j=1}^{2m} g_{j,i} f_j^\dagger, \quad \tau(g)^\dagger f_i^\dagger \tau(g) = \sum_{j=1}^{2m} \overline{g_{i,j}} f_j^\dagger. \tag{7.26}$$

for any $g \in \mathrm{U}(2m)$. Then, the conservation of $N_\alpha$ implies

$$\begin{aligned}\tau(g)N_\alpha &= \tau(g)\sum_{i=1}^{m} f_i^\dagger f_i \\ &= \sum_{i=1}^{m} \tau(g) f_i^\dagger \tau(g)^\dagger \tau(g) f_i \tau(g)^\dagger \tau(g) \\ &= \sum_{i=1}^{m} \left(\sum_{j=1}^{2m} g_{j,i} f_j^\dagger\right)\left(\sum_{k=1}^{2m} \overline{g_{k,i}} f_k\right)\tau(g) \\ &= \sum_{j,k=1}^{2m}\left(\sum_{i=1}^{m} g_{j,i}\overline{g_{k,i}}\right) f_j^\dagger f_k \tau(g)\end{aligned} \tag{7.27}$$

.

More precisely, $\tau(g)N_\alpha = N_\alpha\tau(g)$ provided that

$$\sum_{i=1}^{M} g_{j,i}\overline{g_{k,i}} = \begin{cases}\delta_{jk} & 1 \le j,k \le M\,, \\ 0 & j > M \vee k > M\,.\end{cases} \tag{7.28}$$

Similarly, we have

$$\tau(g)N_\beta = \sum_{j,k=1}^{2m}\left(\sum_{i=m+1}^{2m} g_{j,i}\overline{g_{k,i}}\right) f_j^\dagger f_k \tau(g) = N_\beta\tau(g) \tag{7.29}$$

iff

$$\sum_{i=m+1}^{2m} g_{j,i}\overline{g_{k,i}} = \begin{cases}\delta_{jk} & m+1 \le j,k \le 2m\,, \\ 0 & j \le m \vee k \le m\,.\end{cases} \tag{7.30}$$

By writing

$$g = \begin{pmatrix} A & B \\ C & D\end{pmatrix}\,, \tag{7.31}$$

Eqs. (7.28) and (7.30) are equivalent to the following relations:

$$AA^\dagger = \mathbb{1}\,, \quad AC^\dagger = 0\,, \quad BB^\dagger = 0\,, \tag{7.32}$$

$$DD^\dagger = \mathbb{1}\,, \quad BD^\dagger = 0\,, \quad CC^\dagger = 0\,. \tag{7.33}$$

In particular, it follows that $B, C = 0$ and $A, D \in \mathrm{U}(m)$.

Lastly, notice that

$$[\tau(g), S^2] = \sum_{i,j=1}^{m}[\tau(g), f_i f_j^\dagger f_{i+m}^\dagger f_{j+m}] + \frac{1}{2}[\tau(g), N_\alpha - N_\beta] + \frac{1}{4}[\tau(g), (N_\alpha - N_\beta)^2] \tag{7.34}$$

$$= \sum_{i,j=1}^{m}[\tau(g), f_i f_j^\dagger f_{i+m}^\dagger f_{j+m}]\,. \tag{7.35}$$

The latter follows from the symmetries $[\tau(g), N_\alpha] = [\tau(g), N_\beta] = 0$ and since $[A, BC] = B[A, C] + [A, B]C$ for any triple of operators $A, B, C$. Then, we have

$$\begin{aligned}\tau(g)\sum_{i,j=1}^{m} f_i f_j^\dagger f_{i+m}^\dagger f_{j+m} &= \sum_{i,j=1}^{m} \tau(g) f_i \tau(g)^\dagger \tau(g) f_j^\dagger \tau(g)^\dagger \tau(g) f_{i+m}^\dagger \tau(g)^\dagger \tau(g) f_{j+m} \tau(g)^\dagger \tau(g) \\ &= \sum_{i,j=1}^{m} \sum_{a,b,c,d} \overline{g_{a,i}} g_{b,j} g_{c,i+m} \overline{g_{d,j+m}} f_a f_b^\dagger f_c^\dagger f_d \tau(g) \\ &= \sum_{a,b,c,d} \left( \sum_{i=1}^{m} \overline{g_{a,i}} g_{c,i+m} \right) \left( \sum_{j=1}^{m} \overline{g_{d,j+m}} g_{b,j} \right) f_a f_b^\dagger f_c^\dagger f_d \tau(g) \ . \end{aligned} \tag{7.36}$$

Since $g = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}$, it follows

$$\sum_{i=1}^{m} \overline{g_{i,a}} g_{i+m,c} = \sum_{i=1}^{m} \overline{A_{i,a}} D_{i,c} = \sum_{i=1}^{m} (A^\dagger)_{a,i} D_{i,c} \,, \tag{7.37}$$

$$\sum_{j=1}^{m} \overline{g_{d,j+m}} g_{b,j} = \sum_{j=1}^{m} \overline{D_{d,j}} A_{b,j} = \sum_{j=1}^{m} A_{b,j} (D^\dagger)_{j,d} \,, \tag{7.38}$$

and $[\tau(g), \sum_{i,j=1}^{m} f_i, f_j^\dagger f_{i+m}^\dagger f_{j+m}] = 0$ provided that

$$\sum_{i=1}^{m} (A^\dagger)_{a,i} D_{i,c} = \delta_{a,c} \,, \quad \sum_{j=1}^{m} A_{b,j} (D^\dagger)_{j,d} = \delta_{b,d} \,, \tag{7.39}$$

which imply $A^\dagger D = A D^\dagger = \mathbb{1}$, respectively. Hence, $D = A$ by unitarity. □

In the remaining, we discuss modifications to fermionic shadow estimation under the symmetry-adaptations described in Lemma 31. First, let us consider a fermionic system with conservation of the spin sectors, i.e., $N_\alpha, N_\beta$ are preserved. As before, we restrict to special unitary transformations without loss of generality. In general, $\mathrm{SU}(m) \times \mathrm{SU}(m)$ acts separately on the $\alpha$ and $\beta$ sectors described by two copies of the Fock space $\bigoplus_{i=0}^{m} \bigwedge^i \mathbb{C}^m$, respectively. In particular, this action is described on the space $\left( \bigoplus_{i=0}^{m} \bigwedge^i \mathbb{C}^m \right)^{\otimes 2}$, which is naturally isomorphic to the fermionic Fock space of $2m$ modes. This follows from the fact that, for each $k \in [2m]$, $\bigwedge^k \mathbb{C}^{2m} \cong \bigoplus_{k_1+k_2=k} \bigwedge^{k_1} \mathbb{C}^m \otimes \bigwedge^{k_2} \mathbb{C}^m$ (easily verified by a dimension counting using Vandermonde's identity). More precisely, it is enough to identify the ground states of the two spaces and construct the explicit unitary map [60]:

**Proposition 32.** *Consider the Hilbert spaces $\mathbb{C}^{m_1}$, $\mathbb{C}^{m_2}$. The following isomorphism holds true:*

$$\bigoplus_{i=0}^{m_1+m_2} \bigwedge^i \mathbb{C}^{m_1+m_2} \cong \bigoplus_{i=0}^{m_1} \bigwedge^i \mathbb{C}^{m_1} \otimes \bigoplus_{i=0}^{m_2} \bigwedge^i \mathbb{C}^{m_2} \,. \tag{7.40}$$

*Proof.* Let us consider the Fock spaces $\bigoplus_{i=0}^{m_1} \bigwedge^i \mathbb{C}^{m_1}, \bigoplus_{i=0}^{m_2} \bigwedge^i \mathbb{C}^{m_2}$. These are given by the span of the bases

$$\Phi = \{ |\boldsymbol{z}^{(1)}\rangle \equiv f_{i_1}^{(1)\dagger} \dots f_{i_p}^{(1)\dagger} |\mathbf{0}_{m_1}\rangle \mid p \geq 0 \,,\, i_1 < \dots < i_p \,,\, i_k \in \mathbb{N} \,,\, k = 1, \dots p \} \,, \tag{7.41}$$

$$\Psi = \{|\boldsymbol{z}^{(2)}\rangle \equiv f_{i_1}^{(2)\dagger} \dots f_{i_p}^{(2)\dagger} |\mathbf{0}_{m_2}\rangle \mid p \geq 0\,,\, i_1 < \dots < i_p\,,\, i_k \in \mathbb{N}\,,\, k = 1, \dots p\}\,, \tag{7.42}$$

where $|\mathbf{0}_{m_1}\rangle, |\mathbf{0}_{m_2}\rangle$ denote the vacuum states of $\mathbb{C}^{m_1}$ and $\mathbb{C}^{m_2}$, respectively.

By fixing $|\mathbf{0}_{m_1+m_2}\rangle$ to be the vacuum state of $\bigoplus_{i=0}^{m_1+m_2} \bigwedge^i \mathbb{C}^{m_1+m_2}$, we have the latter is spanned by

$$\{|\boldsymbol{z}^{(1+2)}\rangle \equiv f_{i_1}^{(1)\dagger} \dots f_{i_p}^{(1)\dagger} f_{j_1}^{(2)\dagger} \dots f_{j_q}^{(2)\dagger} |\mathbf{0}_{m_1+m_2}\rangle\}\,, \tag{7.43}$$

with $0 < i_1 < \dots < i_p$, $0 < j_1 < \dots < j_q$.

Then, for any $|\psi\rangle \in \bigoplus_{i=0}^{m_1+m_2} \bigwedge^i \mathbb{C}^{m_1+m_2}$ we can define the operator $U$ such that

$$U|\psi\rangle = \sum_{i_1,\dots,i_p,j_1,\dots j_q} \langle \boldsymbol{z}^{(1+2)}|\psi\rangle |\boldsymbol{z}^{(1)}\rangle \otimes |\boldsymbol{z}^{(2)}\rangle\,, \tag{7.44}$$

which is unitary since

$$\begin{aligned}
\langle U\psi|U\phi\rangle &= \sum_{i_1,\dots,i_p,j_1,\dots j_q,k_1,\dots,k_r,l_1,\dots,k_s} \overline{\langle \boldsymbol{z}^{(1+2)}|\psi\rangle} \langle \boldsymbol{y}^{(1+2)}|\phi\rangle \langle \boldsymbol{z}^{(1)} \otimes \boldsymbol{z}^{(2)}|\boldsymbol{y}^{(1)} \otimes \boldsymbol{y}^{(2)}\rangle \\
&= \sum_{i_1,\dots,i_p,j_1,\dots j_q,k_1} \overline{\langle \boldsymbol{z}^{(1+2)}|\psi\rangle} \langle \boldsymbol{z}^{(1+2)}|\phi\rangle \\
&= \langle \psi|\phi\rangle
\end{aligned} \tag{7.45}$$

for any pair of vectors $\psi, \phi \in \bigoplus_{i=0}^{m_1+m_2} \bigwedge^i \mathbb{C}^{m_1+m_2}$. □

We now discuss the irreps of $\mathrm{SU}(m) \times \mathrm{SU}(m)$. In the following, for clarity, we use the symbol $\boxtimes$ to denote the (outer) tensor product of two representations, which is defined as follows: Let $\pi_1$, $\pi_2$ be representations of the groups $G_1$, $G_2$, respectively. The tensor product representation is defined as $\pi_1 \boxtimes \pi_2(g_1, g_2) \coloneqq \pi_1(g_1) \otimes \pi_2(g_2)$. Then, we consider

$$\tau \boxtimes \tau \colon \mathrm{SU}(m) \times \mathrm{SU}(m) \to \mathrm{U}\left( \bigoplus_{i=0}^{m} \bigwedge^i \mathbb{C}^m \otimes \bigoplus_{i=0}^{m} \bigwedge^i \mathbb{C}^m \right)\,, \tag{7.46}$$

where $\tau \colon \mathrm{SU}(m) \to \mathrm{U}(\bigoplus_{i=0}^{m} \bigwedge^i \mathbb{C}^m)$ describes the action of a passive transformation on the fermionic Fock space of $m$ modes. We remark that this picture agrees with the observation in [148, App. C] in the setting of spin-adapted fermionic Gaussian transformations. More precisely, Gaussian transformations that preserves spin $\alpha$ and $\beta$ types are still block diagonal, i.e., $O = \begin{pmatrix} O_\alpha & 0 \\ 0 & O_\beta \end{pmatrix} \in \mathrm{O}(4m)$, where $O_\alpha$, $O_\beta \in \mathrm{O}(2m)$. The action of these transformations is defined on a set of spin Majorana operators supported on the product space. The latter differs form the Majorana operators defined on each sector by a parity transformation on the $\beta$ sector that depends on the determinant of $O_\alpha$ [148, Eq. (C2)]. In our case, $\mathrm{U}(m) \cong \mathrm{SO}(2m) \cap \mathrm{Sp}(2m)$, see e.g. [149, Appendix B.1]. Hence, any passive transformation is described by a special orthogonal transformation in the basis of Majorana operators, and their action on the total Fock space is the one described in Eq. (7.46).

Next, recall that the spaces $\bigwedge^i \mathbb{C}^m$ are invariant for $i = 0, \dots, m$ and the restriction of $\tau$ to such spaces is irreducible. Then, we consider the irrep

$$\mathcal{T} \equiv \tau_\alpha \boxtimes \tau_\beta \colon \mathrm{SU}(m) \times \mathrm{SU}(m) \to \mathrm{U}\left( \bigwedge^{n_\alpha} \mathbb{C}^m \otimes \bigwedge^{n_\beta} \mathbb{C}^m \right)\,, \tag{7.47}$$

where $\tau_\alpha$ ($\tau_\beta$, respectively) is the irrep of $\mathrm{SU}(m)$ on $\bigwedge^{n_\alpha}\mathbb{C}^m$ ($\bigwedge^{n_\beta}\mathbb{C}^m$, respectively). Note that $\mathcal{T}$ is irreducible by construction, see [63, Thm. 7.12]. Then, the action of a sector-preserving unitary on quantum states is given by the representation $\mathcal{T}(\cdot)\mathcal{T}^\dagger$. By fixing a basis for the Hilbert space (in this case, the Fock basis), we have

$$\Omega \coloneqq \mathcal{T}(\cdot)\mathcal{T}^\dagger \cong \mathcal{T}\otimes\overline{\mathcal{T}}\,, \tag{7.48}$$

Then, it follows

$$\Omega \cong \mathcal{T}\otimes\overline{\mathcal{T}} \cong (\tau_\alpha\otimes\overline{\tau_\alpha})\boxtimes(\tau_\beta\otimes\overline{\tau_\beta})\,, \tag{7.49}$$

The latter decomposes according to Eq. (7.16), namely,

$$\tau_\alpha\otimes\bar{\tau}_\alpha = \bigoplus_{k=0}^{\min\{n_\alpha,m-n_\alpha\}} \tau_k\,, \quad \tau_\beta\otimes\bar{\tau}_\beta = \bigoplus_{l=0}^{\min\{n_\beta,m-n_\beta\}} \tau_l\,, \tag{7.50}$$

where $\tau_0\equiv\mathbf{1}$ and $\tau_1\equiv\mathrm{Ad}$. Therefore, we have

$$\Omega \cong \bigoplus_{k=0}^{\min\{n_\alpha,m-n_\alpha\}}\bigoplus_{l=0}^{\min\{n_\beta,m-n_\beta\}} \tau_k\boxtimes\tau_l\,. \tag{7.51}$$

It is now straightforward to compute the frame operator associated with $\Omega$:

**Proposition 33.** *Let $S$ be the frame operator of a fermionic shadow estimation protocol defined in Eq.* (5.1)*, where unitaries are drawn from $\mathrm{U}(m)\times\mathrm{U}(m)$. Then, $S = S_\alpha\otimes S_\beta$, where*

$$S_\alpha = \sum_{\boldsymbol{z}_\alpha\in\mathcal{H}^m_{N_\alpha}}\int_{\mathrm{SU}(m)} dg\,\omega_\alpha(g)^\dagger|E_{\boldsymbol{z}_\alpha})(E_{\boldsymbol{z}_\alpha}|\omega_\alpha(g)\,, \tag{7.52}$$

$$S_\beta = \sum_{\boldsymbol{z}_\beta\in\mathcal{H}^m_{N_\beta}}\int_{\mathrm{SU}(m)} dg\,\omega_\beta(g)^\dagger|E_{\boldsymbol{z}_\beta})(E_{\boldsymbol{z}_\beta}|\omega_\beta(g)\,, \tag{7.53}$$

*with $\omega_\alpha\coloneqq\tau_\alpha(\cdot)\tau_\alpha^\dagger, \omega_\beta\coloneqq\tau_\beta(\cdot)\tau_\beta^\dagger$ and $E_{\boldsymbol{z}}\equiv|\boldsymbol{z}\rangle\langle\boldsymbol{z}|$. Moreover, $S_\alpha$, $S_\beta$ admit the decompositions, c.f. Eq.* (7.17)*,*

$$S_\alpha = \bigoplus_{k=0}^{n_\alpha} s_k\mathrm{id}_k\,, \quad S_\beta = \bigoplus_{l=0}^{n_\beta} s_l\mathrm{id}_l\,. \tag{7.54}$$

*Proof.* Set $\mathcal{M} = \sum_{\boldsymbol{z}_\alpha}|E_{\boldsymbol{z}_\alpha})(E_{\boldsymbol{z}_\alpha}|\otimes\sum_{\boldsymbol{z}_\beta}|E_{\boldsymbol{z}_\beta})(E_{\boldsymbol{z}_\beta}|$. By definition of $\Omega$,

$$\begin{aligned} S &= \int_{\mathrm{U}(m)\times\mathrm{U}(m)} dg_1dg_2\,\Omega(g_1,g_2)\mathcal{M}\Omega(g_1,g_2)^\dagger \\ &= \int_{\mathrm{U}(m)\times\mathrm{U}(m)} dg_1dg_2\,\omega_\alpha\boxtimes\omega_\beta(g_1,g_2)\mathcal{M}\omega_\alpha\boxtimes\omega_\beta(g_1,g_2)^\dagger \\ &= \int_{\mathrm{U}(m)\times\mathrm{U}(m)} dg_1dg_2\,\omega_\alpha(g_1)\otimes\omega_\beta(g_2)\mathcal{M}\omega_\alpha(g_1)^\dagger\otimes\omega_\beta(g_2)^\dagger\,. \end{aligned} \tag{7.55}$$

Hence, since $\int_{\mathrm{U}(m)\times\mathrm{U}(m)} dg_1 dg_2 = \int_{\mathrm{U}(m)} dg_1 \int_{\mathrm{U}(m)} dg_2$, we have $S = S_\alpha \otimes S_\beta$. Recall now that $S_\alpha$ is the projection of $\mathcal{M}_\alpha \equiv \sum_{\boldsymbol{z}_\alpha} |E_{\boldsymbol{z}_\alpha})(E_{\boldsymbol{z}_\alpha}|$ onto the commutant of $\omega_\alpha = \sum_{k=0}^{\min\{n_\alpha, m-n_\alpha\}} \tau_k$. Schur's Lemma 5 implies

$$S_\alpha = \sum_{k=0}^{n_\alpha} S_k = \sum_{k=0}^{n_\alpha} s_k \mathbb{1}_k \,, \tag{7.56}$$

where $s_k \coloneqq d_k^{-1} \operatorname{Tr}[P_k \mathcal{M}_\alpha]$, with $P_k$ being the projector onto $\tau_k$ and $d_k = \dim \tau_k$. The latter observation holds for $S_\beta$ as well, and the assertion follows. □

Therefore, for independent spin systems with well-defined $N_\alpha$ and $N_\beta$ spin numbers, the estimator of [142] can be applied to the two spin sectors independently. Formally, if $O = O_\alpha \otimes O_\beta$, we have the following estimator:

$$\hat{o} = \operatorname{Tr}[O_\alpha \otimes O_\beta S^{-1}(E_{\boldsymbol{z},g})] = \operatorname{Tr}[O_\alpha S_\alpha^{-1}(E_{\boldsymbol{z},g_\alpha})] \operatorname{Tr}[O_\beta S_\beta^{-1}(E_{\boldsymbol{z},g_\beta})] \,, \tag{7.57}$$

where $g \equiv (g_1, g_2) \in \mathrm{U}(m) \times \mathrm{U}(m)$ and we used $S = S_\alpha \otimes S_\beta$. Note that this is the case of $k$-reduced density matrices, as $D_{\boldsymbol{q}}^{\boldsymbol{p}} \coloneqq f_{p_1}^\dagger \dots f_{p_k}^\dagger f_{q_k} \dots f_{q_1}$ is such that $d_{\boldsymbol{q},\boldsymbol{p}} \equiv \operatorname{Tr}[D_{\boldsymbol{q}}^{\boldsymbol{p}} \rho] = 0$ if the number of spin $\alpha$ and $\beta$ is not preserved. Denoting with $\hat{d}_{\boldsymbol{q},\boldsymbol{p}}$ the corresponding estimator, we have $\hat{d}_{\boldsymbol{q},\boldsymbol{p}} = \hat{d}_{\boldsymbol{q}_\alpha,\boldsymbol{p}_\alpha} \hat{d}_{\boldsymbol{q}_\beta,\boldsymbol{p}_\beta}$, where $\boldsymbol{q}_\alpha, \boldsymbol{p}_\alpha$ (respectively, $\boldsymbol{q}_\beta, \boldsymbol{p}_\beta$) are subsets of $k_\alpha$ symbols (respectively, $k_\beta$ symbols) of $\boldsymbol{q}, \boldsymbol{p}$ that lives in the $\alpha$ sector (respectively, in the $\beta$ sector) with $k = k_\alpha + k_\beta$. Each $\hat{d}_{\boldsymbol{q}_\gamma,\boldsymbol{p}_\gamma}$, with $\gamma \in \{\alpha, \beta\}$, can be computed in time $\binom{m}{k_\gamma}$ independently [142], which implies $\hat{d}_{\boldsymbol{q},\boldsymbol{p}}$ can be computed in time $\mathrm{O}\left(\max\{\binom{m}{k_\alpha}, \binom{m}{k_\beta}\}\right)$.

While this first analysis has the advantage of reducing the sampling cost of the protocol outlined in Section 7.3, it does not take fully advantage of the natural symmetries of spin systems (namely, the conservation of the total spin number). As a last topic of this part, we briefly review the case of shadow estimation with spin-adapted unitaries, described by unitary operations that preserve the total spin number $S^2$. As before, we fix the spin numbers $n_\alpha$, $n_\beta$ and consider the space $\bigwedge^{n_\alpha} \mathbb{C}^m \otimes \bigwedge^{n_\beta} \mathbb{C}^m$. By Lemma 31, the action of $\mathrm{U}(m)$ is described by the representation $\tau_\alpha \otimes \tau_\beta \colon \mathrm{U}(m) \to \mathrm{U}(\bigwedge^{n_\alpha} \mathbb{C}^m \otimes \bigwedge^{n_\beta} \mathbb{C}^m)$, where $\tau_\alpha$ (respectively, $\tau_\beta$) is again the antisymmetric irrep of $\mathrm{SU}(m)$ on the space of $n_\alpha$ (respectively, $n_\beta$) fermions. Unlike Eq. (7.47), $\tau_\alpha \otimes \tau_\beta$ is completely reducible. In fact, the latter can be seen as the restriction of $\mathcal{T}$ to the diagonal subgroup $\{(g, g) \mid g \in \mathrm{U}(m)\} \cong \mathrm{U}(m)$ of $\mathrm{U}(m) \times \mathrm{U}(m)$. Then, define the representation $\omega_{\alpha,\beta} \coloneqq \tau_\alpha \otimes \tau_\beta \otimes \bar{\tau}_\alpha \otimes \bar{\tau}_\beta$ and consider the frame operator that describes shadow estimation with spin-adapted unitaries, i.e.,

$$S_{\mathrm{spin}} \coloneqq \int_{\mathrm{U}(m)} dg\, \omega_{\alpha,\beta}(g) \mathcal{M} \omega_{\alpha,\beta}(g)^\dagger \,, \tag{7.58}$$

where $\mathcal{M} = \sum_{\boldsymbol{z}_\alpha} |E_{\boldsymbol{z}_\alpha})(E_{\boldsymbol{z}_\alpha}| \otimes \sum_{\boldsymbol{z}_\beta} |E_{\boldsymbol{z}_\beta})(E_{\boldsymbol{z}_\beta}|$. The inversion of $S_{\mathrm{spin}}$ is complicated by the insurgence of multiplicities that we observe in the following decomposition:

$$\begin{aligned} \omega &\coloneqq \omega_\alpha \otimes \omega_\beta \\ &\cong \bigoplus_{k=0}^{\min\{n_\alpha, m-n_\alpha\}} \bigoplus_{l=0}^{\min\{n_\beta, m-n_\beta\}} \tau_k \otimes \tau_l \,. \end{aligned} \tag{7.59}$$

In fact, the decomposition of $\tau_k \otimes \tau_l$ is not multiplicity-free in general. For instance, the adjoint representation $\tau_1$ appears with multiplicity 2 in $\tau_1 \otimes \tau_1$. As a consequence, the frame operator becomes [50]

$$S_{\text{spin}} = \bigoplus_r \mathrm{id}_r \otimes s_r \,, \tag{7.60}$$

where the sum runs over all the irreps in $\omega$ and $s_r$ is a positive semidefinite matrix acting on the multiplicity space of the $r$th irrep. From the isotypic decomposition of $\omega^m_{\alpha,\beta}$, and denoting with $P_r$ the projector on the $r$th irrep, it follows that $\mathrm{Tr}[s_r] = d_r^{-1} \sum_{\boldsymbol{z}} (E_{\boldsymbol{z}} \,|P_r|\, E_{\boldsymbol{r}})$. However, a further decomposition (and diagonalization) of the frame operator requires the choice of an orthonormal basis in each isotype. A suitable choice is crucial to ensure time-efficient computation of the estimators. The Clebsch-Gordan basis is a natural candidate that can solve the ambiguity of the multiplicity subspaces. In fact, if in the irrep decomposition there are non-trivial multiplicities, the Clebsch-Gordan decomposition is not unique due to the degeneracy of the subspace of highest weight vectors [77]. Gram-Schmidt orthonormalization can be used to solve such degeneracy, and, consequently, one can construct the Clebsch-Gordan basis in each irreducible subspace. However, while analytical expressions for such coefficients are available for some classes of irreps, such as the fundamental representations [150–152], this is not true in general. To our knowledge, analytical expressions for $\tau_k \otimes \tau_l$ decompositions are not known, and one must rely on the numerical computation of Clebsch-Gordan coefficients. This restrict the practical implementation to small systems due to the exponential size of the fermionic Hilbert space. Finding efficient algorithms to compute the shadow estimator remains an open question.

Lastly, we note a similar phenomenon in systems with global spin symmetry. A unitary that is symmetric under the conserved quantities $N$ and $S^2$ can be described as an element of $\mathrm{U}(m) \times \mathrm{SU}(2)$, where the two factors are a reductive dual pair in $\mathrm{U}(2m)$ (namely, their action commute on the Fock space of $2m$ modes). Therefore, the antisymmetric representation of $\mathrm{U}(2m)$ restrict to $\mathrm{U}(m) \times \mathrm{SU}(2)$ according to Howe duality, and the relevant representation is now [153–155]

$$\tau^{(N)} = \bigoplus_{S=0}^{N/2} \tau^{\mathrm{U}(m)}_{\lambda_S} \otimes \tau^{\mathrm{SU}(2)}_S \,, \tag{7.61}$$

where $\tau^{\mathrm{SU}(2)}_S$ is an irrep of $\mathrm{SU}(2)$ labeled by the total spin $S$, and $\lambda_S$ is a Young diagram with at most two columns and $N$ boxes. Then, we observe that the reference representation $\tau^{(N)}(\cdot)\tau^{(N)\dagger}$ may not decompose into multiplicity-free irreps. For instance, this is again the case if $\tau^{\mathrm{U}(m)}_{\lambda_S} \equiv \tau_1$ is the adjoint representation of $\mathrm{U}(m)$.

In conclusion, we expect the development of spin-adapted shadows to remain an important open problem requiring further investigation. Although the dimensionality reduction induced by the additional symmetries may lead to improved protocols, in the context of shadow estimation it is crucial to devise efficient classical algorithms for computing the corresponding shadow estimators. However, the emergence of non-trivial multiplicities complicates the computation of the frame operator, suggesting that more sophisticated tools are needed to design practical protocols.

# Part III

# Characterization of bosonic systems

# Chapter 8

# Introduction to this part

Bosonic quantum systems play a major role in the design of quantum technologies, such as quantum simulation [156, 157], quantum communication [158], and quantum metrology [159]. This includes photonic quantum computing as a popular proposal for scalable quantum computers [160–165]. Remarkable proposals encompass the implementation of bosonic codes to encode qubits into bosonic states, and take advantage of the "built-in redundancy" provided by the infinite-dimensional nature of the Hilbert space [166, 167], which include the Gottesmann-Knill-Preskill (GKP) code [168] capable of correcting small shifts in the quadratures of the oscillator and cat codes [159], or via the measurement-based approach to quantum computing [169–171] enabled by the implementation of cluster states in photonic platforms [172, 173]. The biggest advantages of this model rely on the implementation of particle sources, detectors, and linear optical circuits on the same integrated chips [174–177], and access to mixed schemes for quantum error correction via concatenation with quantum LDPC [178] or surface codes [179]. Alternative non-universal models of computation based on bosonic systems are also available: Boson sampling [180] and Gaussian boson sampling [181, 182] are among the most studied experiments to test quantum advantage, including practical realizations [183–185].

However, the intricacies of the bosonic Hilbert space represent a considerable challenge for the formulation of rigorous, scalable protocols for the characterization of bosonic systems [186, 187], and most common approaches rely on continuous-variable (CV) tomographic techniques based on the phase space representation of quantum mechanics [91]. Notably, the first rigorous guarantees for the latter were proven only recently [138, 188, 189]. However, practical implementations of full tomography is effectively unfeasible for non-Gaussian CV systems due to the unfavourable scaling of the number of measurement shots required [186, 190–195]. Moreover, as in discrete variable systems, the outcome of quantum process tomography depends on SPAM errors. At the same time, the design of randomized protocols is particularly challenging due to the infinite-dimensional structure of the bosonic Hilbert space that prevents a straightforward generalization of (discrete) scrambling techniques to such platforms. For instance, Gaussian unitaries only form a unitary 1-design [196, 197], and unitary 2-designs cannot exist for CV systems, unless rigged Hilbert spaces are considered [44]. Such issues constrain characterization protocols to very specific settings, as straightforward generalizations of protocols such RB require the computation of $k = 2$-moment operators, where the implemented unitary operators are only benchmarked w.r.t. a restricted set of input states [198].

In this part, we bridge this gap and extend randomized benchmarking to passive Gaussian transformations in bosonic systems. We extend recent results in the RB literature [49, 50, 199, 200] and tackle the challenges posed by bosonic systems by a careful analysis of the relevant representations describing the action of passive Gaussian transformations. In Chapter 9, we provide an introduction to the mathematical theory of randomized benchmarking. Starting from simple proposals for Clifford gates in Section 9.1, we discuss limitations of standard RB. Most notably, we discuss the signal form of RB in detail, and show that, in general, it is determined by a linear combination of exponential decays. Then, in Section 9.2, we review the recent *filtered RB* framework, designed to overcome this (and other) issue by introducing a suitable post-processing routine to isolate exponential decays [49–51]. Next, in Chapter 10, we discuss our main results by extending the filtered RB framework to bosonic systems. We propose an RB experiment akin to boson sampling and, under mild assumptions on the noise, we show how to extract decay rates and isolate particle loss rates. We also provide rigorous sampling complexity guarantees, as we show that the number of samples scales very mildly in the number of modes. This suggests that experimentally interesting implementations of the protocol are available for systems of moderate size. Lastly, in Chapter 11, we discuss extensions of the protocol by analyzing further experimental designs and noise models. In particular, we consider setups with either Gaussian states or measurements, and provide first results on the behaviour of the RB signal with distinguishable particles.

# Chapter 9

# Randomized benchmarking

Within the zoo of characterization methods for quantum processes on discrete variable systems, RB plays a special role due to its robustness against SPAM errors and its rather low demands on the measurement effort [47, 48, 199, 201–209]. Rather than certifying the behaviour of a specific process, such as in quantum process tomography, RB estimates an average metric over a set of implemented unitaries, typically summarised by one or a few parameters. Since its initial formulation, the RB formalism has developed into a family of protocols, including variants tailored to specific gate sets or designed to address specific noise models. We refer to this collection as the RB framework. It includes, for instance, protocols that assess the quality of a designated gate by interleaving it with random unitaries (interleaved RB) [205, 210–213], schemes that focus on native gates generating a given gate set [214], and variant targeting specific error models, such as coherent errors [215], or protocols designed to quantify leakage [216–218]. These protocols follow a similar prescription that is repeated many times and for quantum circuits of different depths: Given an input state, one applies a sequence of random unitary operators –terminated by an *inversion gate* that ideally trivialize the sequence– and then performs a measurement. Notably, SPAM-related contributions enter the measured signal in a way that is independent of sequence length, whereas the effect of gate imperfections accumulates with length. Fitting the length dependence thus separates gate-set properties from SPAM errors and yields parameters that reflect the average noise affecting the gate set.

Recent works led to general guarantees for RB protocols based on finite or compact groups [49–51, 200, 219, 220], revealing the structure of the RB signal beyond unitary 2-designs. In this setting, one faces the fundamental issue of dealing with linear combination of exponential decays: Estimating the corresponding decay rates becomes practically unfeasible once more than a few of them are involved.

In this chapter, we review the mathematical structure of the RB framework from a representation-theoretic perspective, highlighting both the challenges and strategies involved in extending it to bosonic systems. In Section 9.1, we introduce the standard RB protocol and discuss its limitations. We emphasize the difficulties that arise when performing RB with general groups, as well as the post-processing challenges associated with isolating exponential decays from measurement data. These issues are addressed in Section 9.2, where we review the filtered RB protocol [49, 50] –which extends previous results of character RB [51]– specializing the discussion to the case of multiplicity-free representations.

## 9.1 Standard RB

For a digital quantum computer, the aim of standard RB is to characterize a subgroup $G \subseteq \mathrm{U}(d)$ of unitary operations [47, 48, 201]. The protocol is specified by the choice of some key parameters: A quantum state $\rho$ in $\mathcal{H} = \mathbb{C}^d$ that can be prepared reliably and a POVM $M = \{E_x\}_{x\in\Omega}$. The ideal action of $G$ is described by a representation $U\colon G \to \mathrm{U}(d)$, which induces a representation of $G$ on the space $\mathrm{L}(\mathbb{C}^d)$ by the adjoint action $\omega(g) \coloneqq U(g)(\cdot)U(g)^\dagger$. We refer to the representation $\omega$ as the *reference representation*. In practice, this action is noisy, and we consider the *implementation map model* [19] to describe noisy unitary gates on $\mathrm{L}(\mathbb{C}^d)$. This is specified by a map $\phi\colon G \to \mathrm{L}(\mathrm{L}(\mathbb{C}^d))$ (the implementation map) that associates elements in $G$ with quantum channels. This model is implicitly justified by the assumption of *non-Markovian, time independent* noise. Lastly, we define a set of sequence lengths $\mathbb{L} \subset \mathbb{N}$. In the standard RB protocol, we consider the following primitive:

i. Fix a sequence length $l \in \mathbb{L}$.

ii. Prepare the input state $\rho$.

iii. Apply unitaries $g_1, \ldots, g_l \sim G$ sampled uniformly at random, followed by the *inverse* unitary $g_{\mathrm{inv}} = (g_1 \ldots g_l)^{-1}$.

iv. Perform a measurement described by a POVM $\{E_x\}$.

For each value $l$, the primitive is repeated $T$ times. In a noiseless scenario, this corresponds to implementing an identity gate and measuring the probability $\mathrm{Tr}[E_x\rho]$. In the presence of noise, this probability is reduced, so the likelihood of observing the same outcome decreases as the sequence length increases. Formally, the protocol described above amounts to sampling from the probability distribution

$$(\tilde{E}_x \,|\phi(g_{\mathrm{inv}})\phi(g_l)\ldots\phi(g_1)|\,\tilde{\rho})\,, \tag{9.1}$$

where $\tilde{\rho}, \tilde{E}_x$ are the noisy implementations of $\rho$ and $E_x$, respectively. By averaging over many samples, it follows from Eq. (2.29) and Haar invariance

$$\begin{aligned}
p(l) &\coloneqq \int dg_1 \ldots dg_l (\tilde{E}_x \,|\phi(g_{\mathrm{inv}})\phi(g_l)\ldots\phi(g_1)|\,\tilde{\rho}) \\
&= (\tilde{E}_x \,|\int dg_1 \ldots dg_l\, \phi(g_1^{-1}\ldots g_l^{-1})\phi(g_l)\ldots\phi(g_1)|\,\tilde{\rho}) \\
&= (\tilde{E}_x \,|\int dg_2 \ldots dg_l\, \phi(g_2^{-1}\ldots g_l^{-1})\phi(g_l)\cdots\int dg_1\, \phi(g_2 g_1^{-1})\phi(g_1)|\,\tilde{\rho}) \qquad (g_2 \mapsto g_2 g_1^{-1}) \\
&= (\tilde{E}_x \,|\int dg_3 \ldots dg_l\, \phi(g_3^{-1}\ldots g_l^{-1})\phi(g_l)\cdots\int dg_2\, \phi(g_3 g_2^{-1})(\phi*\phi)(g_2)|\,\tilde{\rho}) \quad (g_3 \mapsto g_3 g_2^{-1}) \\
&\;\;\vdots \\
&= (\tilde{E}_x \,|\int dg_l\, \phi(g_l^{-1} g_l)\phi^{*l}(g_l)|\,\tilde{\rho}) \\
&= (\tilde{E}_x \,|\phi^{*(l+1)}(e)|\,\tilde{\rho})\,,
\end{aligned} \tag{9.2}$$

where $e \in G$ denotes the identity. Note that RB can be understood as a power method in the Fourier space [199], as the convolution operator of maps on a group can be turned into a (matrix) multiplication using a Fourier transform.

### 9.1.1 The gate-independent noise case

The analysis of the RB data depends on the ansatz on the noise. In this section, we discuss the simple case of *gate-independent* noise. Then, there exists quantum channels $\Lambda_L$, $\Lambda_R$ such that the implementation map can be written as $\phi(g) = \Lambda_L \omega(g) \Lambda_R$ for any $g \in G$, which implies

$$\phi^{*(l+1)}(e) = \Lambda_L \left( \int_G dg\, \omega(g)^\dagger \Lambda \omega(g) \right)^l \Lambda_R \,, \tag{9.3}$$

where $\Lambda \equiv \Lambda_R \Lambda_L$ and $\mathcal{M}(\cdot) \coloneqq \int_G dg\, \omega(g)^\dagger(\cdot)\omega(g)$ is the moment operator defined in Eq. (3.49). Therefore, the RB data is fully characterized by such twirl, which amounts to the orthogonal projection onto the commutant $\mathcal{C}(\omega)$, c.f. Section 2.4.

#### RB with unitary gates

Suppose unitaries are uniformly drawn from the Haar measure on $G = \mathrm{U}(d)$. Notice that, in practice, this is equivalent to draw unitaries from a unitary 2-design, e.g., Clifford unitaries. Suppose the action of $G$ is described by the reference representation $\omega \coloneqq U(\cdot)U^\dagger$, with $U$ being the defining representation of $\mathrm{U}(d)$.

Then, we have $\omega \cong \mathrm{id} \oplus \mathrm{Ad}$, c.f. Eq. (3.28), where id, Ad denote the trivial and the adjoint representation, respectively.

Hence, $\mathcal{M}(\Lambda)$ is the depolarizing channel with depolarizing parameter $p_\Lambda = \frac{\mathrm{Tr}[P_{\mathrm{Ad}}\Lambda]}{d^2-1}$, c.f. Eq. (3.48). This is related to the average gate fidelity (AGF) in a simple way [36]: For two arbitrary maps $\mathcal{X}, \mathcal{Y}$, define the AGF as

$$F_{\mathrm{avg}}(\mathcal{X}, \mathcal{Y}) \coloneqq \int d\psi \, (\mathcal{X}(|\psi\rangle\langle\psi|) | \mathcal{Y}(|\psi\rangle\langle\psi|)) \,. \tag{9.4}$$

By setting $F_{\mathrm{avg}}(\mathcal{X}) \equiv F_{\mathrm{avg}}(\mathcal{X}, \mathrm{id})$, we have this simple fact that follows from Haar invariance and self-adjointness of $\mathcal{T}$:

$$\begin{aligned} F_{\mathrm{avg}}(\mathcal{M}(\mathcal{X})) &= \int d\psi \, (\mathcal{M}(\mathcal{X})(|\psi\rangle\langle\psi|) | \mathrm{id}(|\psi\rangle\langle\psi|)) \\ &= \int d\psi \, (\mathcal{X}(|\psi\rangle\langle\psi|) | \mathcal{M}(\mathrm{id})(|\psi\rangle\langle\psi|)) \\ &= \int d\psi \, \langle\psi| \mathcal{X}(|\psi\rangle\langle\psi|) |\psi\rangle \\ &= F_{\mathrm{avg}}(\mathcal{X}) \,. \end{aligned} \tag{9.5}$$

Setting $\mathcal{X} = \mathcal{M}(\Lambda) = \mathcal{D}_{p_\Lambda}$, we have

$$F_{\mathrm{avg}}(\mathcal{D}_{p_\Lambda}) = \int d\psi \ \mathrm{Tr}[|\psi\rangle\langle\psi| \mathcal{D}_{p_\Lambda}(|\psi\rangle\langle\psi|)] = \frac{1 - p_\Lambda}{d} + p_\Lambda \,. \tag{9.6}$$

Therefore,

$$p_\Lambda = \frac{d F_{\mathrm{avg}}(\Lambda) - 1}{d - 1} \,. \tag{9.7}$$

It is now easy to show that RB with unitary 2-designs in the presence of gate-independent noise estimates the average gate fidelity of $G$. In fact,

$$\begin{aligned}\mathcal{D}_p(\mathcal{D}_p(\rho)) &= \mathcal{D}_p(\frac{1-p}{d}\mathbb{1} + p\rho) \\ &= \frac{1-p}{d}\mathbb{1} + p\frac{1-p}{d}\mathbb{1} + p^2\rho \\ &= \frac{1-p^2}{d}\mathbb{1} + p^2\rho \\ &= \mathcal{D}_{p^2}(\rho)\,,\end{aligned} \tag{9.8}$$

for any state $\rho$. Then, by induction on $l$, we have $\mathcal{D}^l_{p_\Lambda} = \mathcal{D}_{p^l_\Lambda}$. Next, we have

$$\begin{aligned}p(l) &= (\tilde{E}_x\,|\Lambda\mathcal{D}_{p^l_\Lambda}\,|\tilde{\rho}) \\ &= p^l_\Lambda(\tilde{E}_x\,|\Lambda|\tilde{\rho}) + (1-p^l_\Lambda)(\tilde{M}\,|\Lambda|d^{-1}\mathbb{1}) \\ &= p^l_\Lambda(\tilde{E}_x\,|\Lambda|\tilde{\rho} - d^{-1}\mathbb{1}) + (\tilde{M}\,|\Lambda|d^{-1}\mathbb{1})\,.\end{aligned} \tag{9.9}$$

Here, $\tilde{\rho}, \tilde{E}_x$ denote the noisy implementations of the input state $\rho$ and the POVM element $E_x$, respectively. Therefore, we have

$$p(l) = Ap^l_\Lambda + B\,, \tag{9.10}$$

where $A \equiv (\tilde{E}_x\,|\Lambda|\tilde{\rho} - d^{-1}\mathbb{1}), B = (\tilde{E}_x\,|\Lambda|d^{-1}\mathbb{1})$ are the *SPAM* constants. Remarkably, the decay rate $p_\Lambda$ does not depend on SPAM errors, as intuitively one would expect.

### General groups and representations

For general compact groups and representation $\omega \coloneqq \tau(\cdot)\tau^\dagger$, Fourier properties of the moment operator guarantee the results of the previous section readily generalize when $\tau$ is not the defining representation. To simplify the presentation, we restrict our attention to the multiplicity-free scenario.

**Proposition 34.** *Let $\omega$ be a multiplicity-free reference representation of a compact group $G$, i.e., $\omega = \bigoplus_{\lambda\in\hat{\omega}} \tau_\lambda$. Then, the signal form of standard RB is described by the relation*

$$p(l) = s_{\mathrm{id}} + \sum_{\lambda\in\hat{\omega}\setminus\mathrm{id}} \tilde{s}_\lambda r^l_\lambda\,, \tag{9.11}$$

*for some coefficients $\tilde{s}_\lambda$.*

*Proof.* By Haar invariance, $\mathcal{M}(\Lambda)$ is in the commutant of $\omega$. Hence, by Schur's lemma 5, it must be of the form $\bigoplus_{\lambda\in\hat{\omega}} r_\lambda \mathrm{id}_\lambda$, where $\mathrm{id}_\lambda$ is the (unnormalized) projector onto the $\lambda$th irrep. Let us denote with $\{|\lambda M\rangle\}_{M\in\mathcal{H}_\lambda}$ an orthonormal basis in $\mathcal{H}_\lambda$ and let $C$ be the matrix that realizes the changes of basis. We have $\mathcal{M}(\Lambda) = CDC^{-1}$, where $D$ is diagonal in the basis of operators $\{|\lambda_1 M_1\rangle\langle\lambda_2 M_2| \mid \lambda_1, \lambda_2 \in \hat{\omega}\,,\ M_1 \in \mathcal{H}_{\lambda_1},\, M_2 \in \mathcal{H}_{\lambda_2}\}$, namely

$$D = \sum_{\lambda\in\hat{\omega}} r_\lambda \sum_{M\in\mathcal{H}_\lambda} |\lambda M\rangle\langle\lambda M|\,. \tag{9.12}$$

The RB data reads as

$$\begin{aligned} p(l) &= (\tilde{E}_x \,|\mathcal{M}(\Lambda)^l|\, \tilde{\rho}) \\ &= (\tilde{E}_x \,|CD^lC^{-1}|\, \tilde{\rho}) \\ &= \sum_{\lambda\in\hat{\omega}} r_\lambda^l \sum_{M\in\mathcal{H}_\lambda} \langle \lambda M \,|C^{-1}(\tilde{\rho})C^\dagger(\tilde{E}_x)|\, \lambda M\rangle \,. \end{aligned} \tag{9.13}$$

In the first line, we absorbed $\Lambda_L$ and $\Lambda_R$ in the SPAM terms. By writing $C^\dagger(\tilde{E}_x), C^{-1}(\tilde{\rho})$ in the same operator basis, i.e.,

$$C^\dagger(\tilde{E}_x) = \sum_{\lambda_1,\lambda_2} \sum_{M_1\in\mathcal{H}_{\lambda_1}} \sum_{M_2\in\mathcal{H}_{\lambda_2}} a^{\lambda_1,\lambda_2}_{M_1,M_2} |\lambda_1 M_1\rangle\langle\lambda_2 M_2| \,, \tag{9.14}$$

$$C^{-1}(\tilde{\rho}) = \sum_{\lambda_3,\lambda_4} \sum_{M_3\in\mathcal{H}_{\lambda_3}} \sum_{M_4\in\mathcal{H}_{\lambda_4}} b^{\lambda_3,\lambda_4}_{M_3,M_4} |\lambda_3 M_3\rangle\langle\lambda_4 M_4| \,, \tag{9.15}$$

and by the orthogonality relations $\langle \lambda_i M_j \,|\lambda_k M_l\rangle = \delta_{i,k}\delta_{j,l}$, we have

$$p(l) = \sum_{\lambda\in\hat{\omega}} \tilde{s}_\lambda r_\lambda^l = s_{\mathrm{id}} + \sum_{\lambda\in\hat{\omega}\setminus[\mathrm{id}]} \tilde{s}_\lambda r_\lambda^l \,, \tag{9.16}$$

where $\tilde{s}_\lambda = \sum_{\tilde{\lambda}\in\hat{\omega}} \sum_{M\in\mathcal{H}_\lambda} \sum_{\tilde{M}\in\mathcal{H}_{\tilde{\lambda}}} a^{\lambda,\tilde{\lambda}}_{M,\tilde{M}} b^{\tilde{\lambda},\lambda}_{\tilde{M},M}$, and in the r.h.s. we isolated the contribution from the trivial representation in $\omega$. □

We remark that the latter results holds also if the decomposition of $\omega$ is not multiplicity-free. If the reference representation decomposes as $\bigoplus_\lambda \bigoplus_{r=1}^{m_\lambda} \tau_\lambda^{(r)}$, where $m_\lambda$ is the multiplicity of $\tau_\lambda$ in $\omega$, by Proposition 14, $\mathcal{M}$ projects onto $\mathcal{C}(\omega)$ and it is such that

$$\mathcal{M} = \bigoplus_{\lambda\in\hat{\omega}} P_\lambda \otimes \mathrm{id}_{m_\lambda} \,, \tag{9.17}$$

where $\mathrm{id}_{m_\lambda}$ is the $m_\lambda \times m_\lambda$ identity on the multiplicity subspace. In particular França and Hashagen [219] consider the Jordan decomposition [221]

$$C\mathcal{M}(\Lambda)C^{-1} = D + N \,, \tag{9.18}$$

where $D$ is diagonal, $N$ is nilpotent, and $[D, N] = 0$. Then, one can repeat the same analysis as before and, by fixing the intertwining operators that block-diagonalize $\omega$, the RB signal can be expressed as a linear combination of *matrix* exponential decays associated with the isotypes in $\omega$. Specifically, the nilpotent part vanishes if $l \geq \max r_\lambda$, and the same derivation applies.

### 9.1.2 The gate-dependent noise model

The analysis so far relies on the unrealistic assumption of gate-independent noise. While this is convenient, it is typically a poor approximation in practice, and a more careful treatment is required. In general, the analysis of the RB signal becomes significantly more involved once gate-dependent noise is taken into account. Nevertheless, if the implemented gates are not too noisy, the standard RB signal is still well approximated by the same linear

combination of (matrix) exponential decays, up to an error that is exponentially suppressed in the sequence length [49, 200, 222]. Here, we outline the underlying intuition, and refer to [222, Thm. 4] for a formal proof in the case of unitary 2-designs, and [49, Thm. 8], [200, Thm. 1] for the analysis of finite and compact groups, respectively.

RB under gate-dependent noise can be analyzed using matrix Fourier analysis introduced in Section 2.4. The key steps can be summarized as follows [49, 199, 200]: Following the decomposition of $\omega$ into irreps, one shall consider the Fourier inversion formula [49, 199]

$$\phi(g) = \sum_{\lambda \in \hat{G}} d_\lambda \operatorname{Tr}_\lambda \left( \hat{\phi}[\tau_\lambda] \bar{\tau}_\lambda(g^{-1}) \otimes \mathbb{1} \right) . \tag{9.19}$$

In the Fourier space, the convolution is mapped to a product, and one has

$$\begin{aligned} p(l) &= (\tilde{E}_x \,|\, \phi^{*(l+1)}(e) \,|\, \tilde{\rho}) \\ &= \sum_{\lambda \in \hat{G}} d_\lambda (\tilde{E}_x \,|\, \tilde{\rho}) (\tilde{E}_x \,|\, \operatorname{Tr}_\lambda (\hat{\phi}[\tau_\lambda]^{l+1} \, \bar{\tau}_\lambda(g)^{-1} \otimes \mathbb{1}) \,|\, \tilde{\rho}) \, . \end{aligned} \tag{9.20}$$

Crucially, if the implementation map is sufficiently 'good', $\hat{\phi}$ can be interpreted as a perturbation of $\hat{\omega}$. Formally, one can write $\hat{\phi} = \hat{\omega} + E$, with $E \equiv \hat{\phi} - \hat{\omega}$ being a perturbation term that is small enough in a given norm. Recall that $\hat{\omega}$ is effectively a direct sum of projectors, each associated with a $\lambda$-isotype for $\lambda \in \hat{G}$. Then, $\hat{\phi}$ is close to being a projector, in the sense that $\hat{\phi}[\tau_\lambda]$ is also block-diagonal, i.e. $\hat{\phi}[\tau_\lambda] \approx \operatorname{diag}(I_\lambda, O_\lambda)$, with the error from the diagonal components of $\hat{\omega}[\tau_\lambda]$ being well-controlled. Moreover, the second term constitutes a sub-dominant term that is exponentially suppressed in the sequence length provided the perturbation is small. This implies that for some super-operators $\hat{\Phi}, \hat{\Omega}$ we have a functional form given by

$$p(l) = (\tilde{E}_x \,|\, \hat{\Phi} - \hat{\Omega} \,|\, \tilde{\rho}) + \text{ exponentially suppressed error} \, . \tag{9.21}$$

By fixing a basis in the space of the representation, as in Section 9.1.1, it is possible to prove that

$$p(l) = \sum_{\lambda \in \hat{G}} \operatorname{Tr}(A_\lambda M_\lambda^l) + \text{ exponentially suppressed error} \, . \tag{9.22}$$

In next section, we provide further details on the application of matrix perturbation theory in the context of RB.

### 9.1.3 Fitting procedure

For Haar random unitaries (or unitary 2-designs), the decay rates may be associated with suitably-defined average gate fidelities on each invariant subspace. If $G$ is not a 2-design, it is convenient to combine the decay rates $r_\lambda$ in a single measure of the quality of the implementation map in terms of the entanglement fidelity $F_e$ of the noise channel $F_e(\mathcal{T}) \coloneqq (E_\Omega \,|\, \mathcal{T} \otimes \mathrm{id} \,|\, E_\Omega)$, where $E_\Omega \equiv |\Omega\rangle\langle\Omega|$ and $|\Omega\rangle \coloneqq \frac{1}{\sqrt{d}} \sum_{i \in [d]} |i, i\rangle$ is the maximally

entangled state. Specifically, we have

$$\begin{aligned} F_e(\mathcal{M}(\Lambda)) &\coloneqq (E_\Omega \,|\Lambda \otimes \mathrm{id}|\, E_\Omega) \\ &= \sum_{i,j,k,l\in[d]} (|i\rangle\langle j| \otimes |i\rangle\langle j| \,|\mathcal{M}(\Lambda) \otimes \mathrm{id}||k\rangle\langle l| \otimes |k\rangle\langle l|) \\ &= \sum_{i,j} (|i\rangle\langle j| \,|\mathcal{M}(\Lambda) \otimes \mathrm{id}||i\rangle\langle j|) \\ &\equiv \mathrm{Tr}(\mathcal{M}(\Lambda)) \\ &= \mathrm{Tr}(\Lambda)\,. \end{aligned} \tag{9.23}$$

As $\mathcal{M}$ is a direct sum of projectors, by Lemma 5, it follows [219]

$$F_e(\Lambda) = \frac{1}{d^2} \sum_{\lambda\in\hat{\omega}} d_\lambda r_\lambda\,. \tag{9.24}$$

Then, by fitting the curve to experimental data one could obtain estimates on the eigenvalues of $\mathcal{M}(\Lambda)$. However, the post-processing phase incurs in some relevant issues that undermine the feasibility of standard RB. Extracting decay rates requires fitting noisy data points $\{x_i\}_{i=1}^{l}$ to a model of the form

$$p(l) = c_0 + \sum_{i=1}^{|\hat{\omega}|} c_i e^{-b_i x_i}\,. \tag{9.25}$$

Despite the progress made over the last few years [223], the signal form poses significant challenges in practical applications, as this non-linear fitting problem is affected by several sources of numerical instability. For instance, the convergence of most algorithms strongly depends on the choice of a good initial point. Similarly, numerical instabilities may arise if the eigenvalues $r_\lambda$ are close [219]. Moreover, given pairs of experimental data $\{l, \hat{p}(l)\}_{l\in\mathbb{N}}$, it is hard to establish which parameter corresponds to which irrep in the decomposition of $\omega$. This poses additional issues in the reconstruction of the (entanglement) fidelity of the gate set. In the gate-dependent setting, such issues persist. Moreover, when the decomposition of $\omega$ is not multiplicity-free, the signal is more intricate, and fitting matrix exponential decays becomes numerically unstable in practice, even for small multiplicities, rendering the analysis effectively unfeasible [49].

A related question is whether RB decay parameters always coincide with average gate fidelities. The answer is subtle and depends on the choice of a *gauge*, i.e., a change of basis for the implementation map. In particular, gate fidelities are not gauge-invariant, unlike decay parameters [206]. Nevertheless, such interpretation of the decay parameters can always be recovered by a suitable change of basis, at the cost of the resulting map not being necessarily completely positive [49]. However, whether such interpretation is justified or not cannot be deduced from RB results alone, and additional information, e.g., on the noise sources, is necessary. From this point on wards, we take the point of view of [49], and view the decay rates as quantities that provide a benchmark for the quality of the implementation in their own right.

## 9.2 Filtered RB

Extracting exponential decays from the output signal of standard RB in practical applications is a challenging task, and the protocol is limited to a handful of gate sets for which the reference representation decomposes into a very moderate number of irreps. For instance, this proves to be hard to implement on analog simulators, and a different approach must be taken.

In what follows, we describe techniques to isolate exponential decays and thereby reduce the burden on the fitting procedure. In recent work, this problem has been addressed by developing post-processing techniques that avoid some of the complications of standard RB. Notably, character RB [51] omits the inversion gate and instead performs a suitable post-processing of the data, where contributions associated to individual irreps are isolated by effective projections onto the corresponding invariant subspaces. Other approaches include cycle RB [213], its Pauli channel variant [224] and dyhedral RB [225]. In the setting of non-uniform sampling, Helsen *et al.* [49] and Heinrich *et al.* [50] generalize character RB by introducing a post-processing procedure based on *filter functions* to isolate decay rates and generalize the framework to random quantum circuits.

### 9.2.1 Description of the protocol

Filtered RB differs from standard RB in a few key ingredients. Most importantly, it includes a non-trivial post-processing procedure that allows to isolate individual decay rates. Moreover, it does not include an inversion gate at the end of the sequence. Instead, the inversion is performed in post-processing. This has significant practical advantages, as implementing the actual inverting gate may be expensive even if the random sequence is restricted to generators of the group. The protocol is characterized by the choice of the following hyperparameters:

- A compact group $G$, representing the unitaries that can be implemented experimentally.
- An input state $\rho$ and a POVM $\{E_x\}_{x\in\Omega}$, where $\Omega$ is a suitable sample space.
- A reference representation $\omega$ of $G$ on the space of linear operators determined by the chosen state and measurement. Accordingly, an implementation map $\phi$ describing the noisy implementation of $\omega$ that depends on the specifics of the experiment.
- A set of sequence lengths $\mathbb{L} \in \mathbb{N}$ specifying the lengths of the random sequences implemented in each iteration of the experiment.
- A probability distribution $\nu$ over $G$ that controls the random sampling of group elements in RB.
- The total number of samples $T \in \mathbb{N}$, ideally chosen according to sampling complexity guarantees associated with the protocol.

To fix the ideas, it suffices to restrict to the case $\nu \equiv \mu_H$, i.e., the Haar measure. At the end of this section, we will comment on the differences arising in the general case. As in the classical shadow protocol, we distinguish two separate phases, c.f. Section 5.1: In the *data*

*collection* phase, one performs a quantum experiment described by the chosen input state $\rho$ and POVM $M = \{E_x \equiv |x\rangle\langle x|\}_{x\in\Omega}$, and a sequence of random unitaries (without inversion). This primitive is repeated $T$ times, yielding a collection of samples $\{(g_1^{(i)}, \ldots, g_l^{(i)}, x^{(i)})\}_{i=1}^T$. Next, in the *post-processing* phase, one computes the mean estimator of the so-called *filter function* $f_\lambda$, which depends on an irrep $\lambda \in \hat{G}$. To simplify the notation, we will only consider the case of multiplicity-free representations. More precisely, the aim of filtered RB is to construct the empirical mean estimator

$$\hat{F}_\lambda(l) = \frac{1}{T}\sum_{i=1}^{T} f_\lambda(x, g_1^{(i)} \ldots g_l^{(i)}) \tag{9.26}$$

by repeating the data collection phase for different sequence lengths $l \subset \mathbb{N}$.

Formally, suppose $\omega = \bigoplus_{\lambda\in\hat{G}} \tau_\lambda$, and let $P_\lambda$ be the projection onto the $\lambda$th irrep. We define the *filter function*

$$f_\lambda(x, g|\rho) \coloneqq (\rho\,|P_\lambda S^+ \omega(g)^\dagger|\,E_x)\,, \tag{9.27}$$

where $S$ is the frame operator defined as in Chapter 5. Then, we define the *filtered survival probabilities*

$$F_\lambda(l) \coloneqq \int_\Omega dx \int_G d\nu(g_1)\ldots d\nu(g_l) f_\lambda(x, g_1 \ldots g_l)\tilde{p}(g_1 \ldots g_l|x, \rho)\,, \tag{9.28}$$

with

$$\tilde{p}(g_1 \ldots g_l|x, \rho) \coloneqq (\tilde{E}_x\,|\phi(g_l)\ldots\phi(g_1)|\,\tilde{\rho})\,. \tag{9.29}$$

Hence, collecting samples $\{(x^{(i)}, g_1^{(i)}, \ldots, g_l^{(i)})\}$ from Eq. (9.29), the estimator Eq. (9.26) yields an unbiased estimator of Eq. (9.28).

Under mild assumptions on the noise, one can fit the estimated filtered survival probabilities and extract individual decay rates associated with irreps. Definitions (9.28) and (9.26) also determine the sampling complexity. In particular, under the assumption of non-fine-tuned noise, the second moment $\mathbb{E}[f_\lambda^2]$ is upper bounded by the ideal second moment [50]

$$\mathbb{E}[f_\lambda^2]_{\text{ideal}} \coloneqq \int_\Omega dx \int_G d\nu(g_1)\ldots d\nu(g_l)(\rho\,|P_\lambda S_\lambda^\dagger \omega(g_1 \ldots g_l)^\dagger|\,E_x)^2(E_x\,|\omega(g_1 \ldots l)|\rho)\,. \tag{9.30}$$

In this case, $\hat{F}_\lambda$ can be bounded by Chebyshev's inequality, yielding sampling complexity guarantees as

$$T \geq \frac{1}{\varepsilon^2\delta}\mathbb{E}[f_\lambda^2]_{\text{ideal}}\,. \tag{9.31}$$

The choice of the filter function (10.9) made by Heinrich *et al.* [50] is determined by the

following observation in the case of noise-free implementations:

$$\begin{aligned} F_\lambda(l) &= \int_\Omega dx \int_G d\nu(g) f_\lambda(x,g) p(g|x,\rho) \\ &= \int_\Omega dx \int_G d\nu(g) (\rho \,|P_\lambda S^+ \omega(g)^\dagger| E_x)(E_x \,|\omega(g)|\rho) \\ &= (\rho|P_\lambda S^+ \int_G \omega(g)^\dagger \int_\Omega dx |E_x)(E_x|\omega(g)|\rho) \\ &= (\rho|P_\lambda S^+ \int_G \omega(g)^\dagger \mathcal{M} \omega(g)|\rho) \\ &= (\rho \,|P_\lambda S^+ S|\,\rho)\,. \end{aligned} \tag{9.32}$$

In particular, if the POVM $\{\omega(g)^\dagger(E_x)\}$ is informationally complete, we have $S^+ = S^{-1}$, and

$$F_\lambda(l) = (\rho \,|P_\lambda|\,\rho)\,. \tag{9.33}$$

In other terms, the output of the ideal filtered RB signal is the overlap of $\rho$ with the $\lambda$th irrep, while this is restricted to the span of the POVM if the latter is not informationally complete. Notice that by summing over all irreps in the decomposition of $\omega$ one recovers exactly the standard RB signal. In this sense, standard RB is a particular instance of filtered RB with projection onto $\omega$ itself.

### 9.2.2 Signal form of filtered randomized benchmarking

Under mild assumptions on the noise, $F_\lambda$ is well-approximated by a (matrix) exponential decay [49, 50]. In this section, we review the derivation of Heinrich *et al.* [50] of this fact in the simplified scenario of reference representations admitting multiplicity-free irrep decompositions. While considering the general case of non-trivial multiplicities is formally equivalent, practical implementations incur in numerical instabilities. To keep the notation as simple as possible, we also restrict to the case of Haar-random unitaries.

The analysis of $F_\lambda$ follows from the key observation that, provided the noise is not too strong, the implementation function is *close* to the ideal reference representation, and can be viewed as a perturbation of the latter [49, 50, 226]. More formally, consider the Fourier transform $\hat{\omega}[\tau_\lambda] = \int_G dg\, \tau_\lambda(g)^\dagger(\cdot)\omega(g)$ (c.f. Eq. (2.33)). By Proposition 14, there exist unitary matrices $A = [A_1, A_2]$, $B = [B_1, B_2]$ such that

$$\begin{bmatrix} A_1^\dagger \\ A_2^\dagger \end{bmatrix} \hat{\omega}[\tau_\lambda][B_1, B_2] \cong \begin{pmatrix} \mathrm{id} & 0 \\ 0 & 0 \end{pmatrix}. \tag{9.34}$$

Then, for a perturbation matrix $E$ that is small enough, i.e., $\|E\|_\infty < 1/4$, one can find matrices $R = [R_1, R_2]$, $L = [L_1, L_2]$ satisfying $L^\dagger = R^{-1}$, and matrices $I$, $O$ such that

$$\begin{bmatrix} L_1^\dagger \\ L_2^\dagger \end{bmatrix} (\hat{\omega} + E)[R_1, R_2] = \begin{pmatrix} I & 0 \\ 0 & O \end{pmatrix}. \tag{9.35}$$

This is ensured by the fact that the block-diagonalizing matrices $L$, $R$ are 'close' to the unperturbed ones. In particular, this argument yields the bounds

$$\|I - \mathrm{id}\|_\infty < 2\|E\|_\infty\,, \tag{9.36}$$

$$\|O\|_\infty < 2\|E\|_\infty\,, \tag{9.37}$$

$$\|L_2\|_\infty\|R_2\|_\infty \leq \|E\|_\infty\,(1-\|E\|_\infty) + \frac{1+\|E\|_\infty}{1-4\|E\|_\infty}\,. \tag{9.38}$$

**Theorem 35** (Thm. 16 in [49], Thm. 8 [50])**.** *Let $G$ be compact and let $\omega$ be a reference representation. In particular, suppose the decomposition $\omega = \bigoplus_{\lambda\in\hat{\omega}} \tau_\lambda$ holds. Consider now a non-trivial irrep $\tau_\lambda \in \hat{\omega}$, and suppose $\|\hat{\phi}[\tau_\lambda] - \hat{\omega}[\tau_\lambda]\|_\infty \leq \delta_\lambda < 1/4$. Then, the filtered signal in Eq.* (9.28) *is such that*

$$F_\lambda(l) \approx a_\lambda r_\lambda^l + \alpha_\lambda\,, \tag{9.39}$$

*where the additive error $\alpha_\lambda \geq 0$ which is suppressed exponentially in $l$, $a_\lambda \in \mathbb{R}$, $r_\lambda \in (0,1]$. Moreover $a_\lambda$ does not depend on the initial state and measurement.*

For $\tau\colon G \to \mathrm{U}(\mathbb{C}^d)$, we note that $\omega \coloneqq \tau(\cdot)\tau^\dagger$ is a real representation, as it is equivariant under the involution $J(X) \coloneqq X^\dagger$. Let $\tau_\lambda$ be an irrep in $\omega$. It follows that either $\tau_\lambda$ is an irrep of real type, or also the dual $\tau_\lambda^\dagger$ appears in the decomposition of $\omega$. Similarly, if $\tau_\lambda \in \hat{\omega}$ is a complex representation, equivariance under $J$ implies $\tau_\lambda^\dagger \in \hat{\omega}$ as well, and the corresponding multiplicities $m_\lambda$, $m_{\lambda^\dagger}$ coincide. We note that $\tau_\lambda$, in our setting, cannot be a quaternionic irrep, i.e., a self-dual irrep that is equivariant under a quaternionic structure defined by an antilinear map $j : \mathcal{H}_\lambda \to \mathcal{H}_\lambda$ such that $j^2 = -1$. In fact, one can prove that quaternionic irreps may only appear in the decomposition of $\omega$ with even multiplicities, due to the structure of the multiplicity subspaces and equivariance under $J$.

*Proof of Theorem 35.* Let $P_\lambda$ be the projector onto $\tau_\lambda$ and let $X_\lambda$ be the partial isometry such that $P_\lambda = X_\lambda^\dagger X_\lambda$. By construction, $X_\lambda$ commutes with both $S^+$ and $\omega$. Hence, we observe the following fact:

$$\begin{aligned}
F_\lambda(l) &= \int_\Omega dx \int_G dg_1 \dots dg_l f_\lambda(x, g_1 \dots g_l)\tilde{p}(x|g_1,\dots,g_l) \\
&= (\rho\,|P_\lambda S^+ \left(\int dg\omega(g)^\dagger(\cdot)\phi(g)\right)^l (\tilde{M})\,|\tilde{\rho}) \\
&= (\rho\,|P_\lambda S_\lambda^+ \hat{\phi}[\tau_\lambda]^l(\tilde{M})\,|\tilde{\rho}) \\
&= (\rho\,|X_\lambda S_\lambda^+ \hat{\phi}[\tau_\lambda]^l(X_\lambda\tilde{M})\,|\tilde{\rho}) \\
&= (\rho\,|X_\lambda S_\lambda^+ \hat{\phi}[\tau_\lambda]^l(\tilde{M}_\lambda)\,|\tilde{\rho}) \\
&= \mathrm{Tr}\left[\hat{\phi}[\tau_\lambda]^l|\tilde{M}_\lambda)(\tilde{R}_\lambda|\right]\,,
\end{aligned} \tag{9.40}$$

where $\tilde{M}_\lambda \equiv X_\lambda\tilde{M}$ and $\tilde{R}_\lambda = |\tilde{\rho})(\rho|X_\lambda S_\lambda^+$. Let $E = \hat{\phi}[\tau_\lambda] - \hat{\omega}[\tau_\lambda]$, so that we can write $\hat{\phi}[\tau_\lambda] = \hat{\omega}[\tau_\lambda] + E$. As $\|E\|_\infty \leq \delta_\lambda$, $\hat{\phi}[\tau_\lambda]$ is a perturbation of $\hat{\omega}[\tau_\lambda]$. Hence, the eigenspaces of $\hat{\omega}[\tau_\lambda]$ are approximately invariant, and we can write

$$\hat{\phi}[\tau_\lambda] = R_1^\lambda r_\lambda L_1^{\lambda\dagger} + R_2^\lambda O_\lambda L_2^{\lambda\dagger}\,, \tag{9.41}$$

where $L^{\lambda\dagger}R^\lambda = \mathrm{id}$. In particular, the multiplicity-free assumption implies that $r_\lambda$ is a $1\times 1$ block, and thus $R_1^\lambda r_\lambda L_1^{\lambda\dagger} = r_\lambda R_1^\lambda L_1^{\lambda\dagger} \equiv r_\lambda P_\lambda$, where $P_\lambda$ is a projector on the perturbed range of $\hat{\omega}[\tau_\lambda]$. The latter implies

$$\hat{\phi}[\tau_\lambda]^l = d_\lambda^{-1} P_\lambda r_\lambda^l + R_2^\lambda O_\lambda^l L_2^{\lambda\dagger}\,. \tag{9.42}$$

Hence,

$$F_\lambda(l) = a_\lambda r_\lambda^l + (\tilde{R}_\lambda \,|\, R_2^\lambda O_\lambda^l L_2^{\lambda\dagger} \,|\, \tilde{M}_\lambda)\,, \tag{9.43}$$

where $a_\lambda = d_\lambda^{-1}(\tilde{R}_\lambda \,|\, P_\lambda \,|\, \tilde{M}_\lambda)$. By construction, $|r_\lambda - 1| < 2\delta_\lambda$ and $O_\lambda$ is bounded as $\|O_\lambda\|_\infty \leq 2\delta_\lambda$, c.f. Eq. (9.36).

The exponential suppression of the subdominant term follows from the following observation:

$$\begin{aligned} |(\tilde{R}_\lambda \,|\, R_2^\lambda O_\lambda^l L_2^{\lambda\dagger} \,|\, \tilde{M}_\lambda)| &\leq \|L_2^{\lambda\dagger}|\tilde{M}_\lambda)(\tilde{R}_\lambda|R_2^\lambda\|_1 \|O_\lambda\|_\infty^l \\ &\leq \|L_2^{\lambda\dagger}(\tilde{M}_\lambda)\|_2 \|R_2^{\lambda\dagger}(\tilde{R}_\lambda)\|_2 \|O_\lambda\|_\infty^l \\ &= \|L_2^\lambda\|_\infty \|R_2^\lambda\|^\infty \|X_\lambda^\dagger \tilde{M}\|_2 \|S_\lambda^+ X_\lambda|\rho)(\tilde{\rho}|\|_2 \|O_\lambda\|_\infty^l\,. \end{aligned} \tag{9.44}$$

Let us analyze the latter term-by-term: First, Eq. (9.36) implies the bound $\|L_2^\lambda\|_\infty \|R_2^\lambda\|_\infty < (1 - 4\delta_\lambda)\delta_\lambda + \frac{1+\delta_\lambda}{1-4\delta_\lambda}$. Next, we have

$$\|S_\lambda^+ X_\lambda|\rho)(\tilde{\rho}|\|_2 \leq \|S_\lambda^+\|_\infty \|X_\lambda \rho\|_2 \|\tilde{\rho}\|_2 \leq \|S_\lambda^+\|_\infty \sqrt{(\rho \,|\, P_\lambda \,|\, \rho)}\,. \tag{9.45}$$

Finally, recall $\tilde{M} = M\mathcal{E}_M$ is the noisy measurement channel, with $M = \sum_x |E_x)(E_x|$ being a projector by construction. Then, as $P_\lambda = X_\lambda X_\lambda^\dagger$,

$$\|X_\lambda^\dagger \tilde{M}\|_2^2 = \mathrm{Tr}[P_\lambda M \mathcal{E}_M \mathcal{E}_M^\dagger M] = (P_\lambda \,|\, M\mathcal{E}_M\mathcal{E}_M^\dagger M)\,. \tag{9.46}$$

In particular, $P_\lambda$ projects onto a non-trivial subspace of Hermitian operators. Hence, the components of $M\mathcal{E}_M\mathcal{E}_M^\dagger M$ aligned with the $\lambda$th subspace contribute non-trivially. Moreover, $M$ is unital. Hence, non-trivial contributions are associated with the unital, trace-preserving components of $\mathcal{E}_M\mathcal{E}_M^\dagger$ and one has $\|\mathcal{E}_M\mathcal{E}_M^\dagger\|_\infty = 1$ [227]. It follows from Hölder's inequality $\|X_\lambda^\dagger \tilde{M}\|_2^2 \leq \|P_\lambda M\|_1 \leq \min\{d_\lambda, d\}$. □

In principle, one can extract decay rates from Eq. (9.39) by choosing sequence lengths large enough to suppress the additive error $\alpha_\lambda$. In practice, $F_\lambda(l)$ can be small (e.g., for small irreps), and it is more convenient to look at the relative error $\alpha_\lambda/(a_\lambda r_\lambda)$, as we expect it to decay with $l$ as well. In particular, it is sufficient to choose the sequence length as [50, 53]

$$l \geq \frac{\log \frac{d_\lambda}{s_\lambda} + 2\log\frac{1}{\alpha} + 4}{2\log(\frac{1}{\delta_\lambda})}\,. \tag{9.47}$$

The extension of Theorem 35 to irreps $\lambda$ with non-trivial multiplicities is straightforward. In this case, $\hat{\omega}[\tau_\lambda]$ is just the projector onto the $\lambda$-isotypic component of $\omega$ with rank given by the multiplicity $m_\lambda$, c.f. Proposition 14. Hence the output data is described by

$$F_\lambda(l) = \mathrm{Tr}[A_\lambda I_\lambda^l] + \mathrm{Tr}[B_\lambda O_\lambda^l]\,, \tag{9.48}$$

where the SPAM constants $A_\lambda, B_\lambda$ can be obtained as before, and $I_\lambda$ is now a $m_\lambda \times m_\lambda$ matrix.

Lastly, we remark that the filtered RB framework is designed to extend RB to non-uniform sampling and, in particular, to sampling from random quantum circuits. This requires the following modification: Instead of considering the Fourier transform

$$\hat{\omega}[\omega] = \int_G dg\, \omega(g)^\dagger(\cdot)\omega(g)\,,$$

sampling from a probability distribution $\nu \neq \mu_H$ means that the relevant quantity is now the moment operator defined as

$$\hat{\omega}_\nu[\omega] \coloneqq \int_G d\nu(g)\omega(g)^\dagger(\cdot)\omega(g)\,. \tag{9.49}$$

If $\nu$ is supported on generators, and denoting with $V_{\mathbf{1}}$ the trivial isotype in $\omega$, it can be shown that $\hat{\omega}_\nu[\omega]$ admits the decomposition [50]

$$\hat{\omega}_\nu[\omega] = \begin{pmatrix} \mathrm{id} & 0 \\ 0 & \hat{\omega}_\nu[\omega \ominus \mathbf{1}] \end{pmatrix}, \tag{9.50}$$

where $\hat{\omega}_\nu[\omega \ominus \mathbf{1}] = \int_G d\nu(g)\,(\omega \ominus \mathbf{1})(g)^\dagger(\cdot)\omega(g)$ and $\omega \ominus \mathbf{1} = \sum_{\lambda \in \hat{\omega}\setminus \mathbf{1}} \tau_\lambda$ is the representation on the orthogonal complement of $V_{\mathbf{1}}$. The difference between the latter and the moment operator defined with respect to the Haar measure is determined by the spectral gap $\Delta$ of $\nu$, i..e,

$$\|\hat{\omega}_\nu[\omega] - \hat{\omega}[\omega]\|_\infty \leq 1 - \Delta\,. \tag{9.51}$$

Then, it is sufficient that $\nu$ defines a random walk on $G$ that converges to $\mu_H$, that is $\nu^{*l} \to \mu_H$ for $l \to \infty$. In fact, by the right invariance of the Haar measure, observe that

$$\begin{aligned} \hat{\omega}_\nu[\omega]\hat{\omega}[\omega] &= \int_G d\nu(g)\omega(g)^\dagger \int_G dh\,\omega(h)^\dagger(\cdot)\omega(h)\omega(g) \\ &= \int_G d\nu(g) \int_G dh\,\omega(h)^\dagger(\cdot)\omega(h) \\ &= \hat{\omega}[\omega]\,, \end{aligned} \tag{9.52}$$

and the same holds for $\hat{\omega}[\omega]\hat{\omega}_\nu[\omega]$ by left invariance. As a consequence,

$$\begin{aligned} \|\hat{\omega}_{\nu^{*l}}(\omega) - \hat{\omega}[\omega]\|_\infty &= \|\hat{\omega}_\nu[\omega]^l - \hat{\omega}[\omega]\|_\infty \\ &= \|(\hat{\omega}_\nu[\omega] - \hat{\omega}[\omega])^l\|_\infty \\ &\leq (1-\Delta)^l\,. \end{aligned} \tag{9.53}$$

Hence, a suitable choice of $\nu$ ensures the spectral distance decays exponentially in the sequence length.

This approach offers practical advantages as, for instance, sampling from generators may be easier, as not all unitaries may be equally simple to implement. We remark that, in this case, the quality of the approximation in the signal form and condition on the length of the sequences depend on the spectral gap $\Delta$.

# Chapter 10

# Bosonic randomized benchmarking

*This chapter is mostly adapted from [53]. Only formatting (typesetting) and structural modifications (e.g., rearranging sections to eliminate redundancy) have been made. The research findings, analysis, and core content remain unchanged. Section 10.1 has been added for a self-contained presentation of the results. Any further alterations to terminology or minor adjustments were solely for stylistic consistency within this thesis and the most recent literature.*

Very recently, a bosonic randomized benchmarking protocol using random phase-space displacements has been put forward [228]. The protocol follows the prescription of standard RB and is summarized as follows: For a fixed $l \in \mathbb{N}$, initialize a bosonic mode in the ground state $|0\rangle\langle 0|$ and applies $l$ random displacement operators $D(\alpha_i) \coloneqq e^{i(\alpha a^\dagger - \bar{\alpha} a)}$, with $|\alpha_i| = |\alpha_0|$ for each $i$ and the phases are uniformly drawn from $\{0, \pi/2, \pi, 3\pi/2\}$. The sequence is terminated by the inversion gate $D(-\sum_{i=1}^{l} \alpha_i)$. The overlap with the ground state is then measured to benchmark the fidelity between the initial and the evolved state. Due to the Abelian character of the (projective) Heisenberg-Weyl group, the complicated behaviour involving many decays is avoided, and common noise models e can be analyzed. In particular, analytical error models for heating and dephasing noise are derived, and dominant noise mechanisms can be extracted from the RB data.

In the non-Abelian setting, the peculiarities of the infinite dimensional Hilbert spaces prevents a straightforward generalization of randomization techniques to bosonic systems, and one cannot hope for such a simple analysis. Moreover, the analysis is complicated by the fact that, in separable infinite-dimensional Hilbert spaces, Gaussian ensembles do not form CV 2-designs [196, 197]. In fact, this is in fact a special case of a no-go result in CV systems, which states the non-existence of CV $t$-designs for any $t \geq 2$, unless rigged Hilbert spaces are considered [44]. However, the results presented in Chapter 9 extend the RB framework to general compact groups when revisited under the lens of representation theory. Hence, we take this point of view, and generalize filtered RB to symmetric representations of unitary groups to benchmark passive bosonic (Gaussian) transformations. We refer to the protocol introduced in this way as *passive bosonic RB*, or short *passive RB*. In contrast to the discrete variable systems explicitly considered in Ref. [50], reasonable guarantees for a filtered RB protocol in bosonic systems are harder to obtain. This is because the action of passive transformation on the full bosonic Hilbert space is considerably more complicated than, e.g., the action of the qubit Clifford group, and thus a well-behaved protocol requires a careful identification of relevant and feasible experimental settings. In

the passive RB protocol, we navigate these complications by considering experiments where the input state is a number state and particle number-resolving (PNR) measurements are performed, resembling boson sampling experiments [180]. For practical reasons, we propose to use collision-free states with at most one particle per mode. We then show that the passive RB successfully benchmarks the average quality of passive transformations on a fixed number of particles, thereby separating the effect of particle number-preserving noise from particle loss using different post-processing of the same experimental data. In general, we prove that there are as many decay rates as we have particles in the experiments – however it is sufficient to only estimate a constant number of them in practice. By representation-theoretic means, we derive explicit and concise formulas for the functions used in the post-processing. As the protocol involves non-Gaussian elements, the classical post-processing requires the computation of matrix permanents, and it is therefore generally inefficient [180]. Specifically, we expect the post-processing to be feasible for $\approx 30$ particles and modes, thus allowing the protocol to target an experimentally interesting regime. The inefficiency of the post-processing should not be unexpected, as a similar behaviour can be found in linear cross-entropy benchmarking [50, 229]. There, the post-processing involves the simulation of random circuit sampling, which is also known to be computationally hard [5, 230–232]. We simulate the passive RB protocol for a small number of modes, demonstrating that it works as intended. Finally, we analyze the sampling complexity of our protocol by computing the relevant variances. We evaluate the obtained expressions numerically and find a very mild scaling with the number of modes $m$ which seems be logarithmic.

The remainder of this chapter is structured as follows: In Section 10.1, we set the stage for the remaining of this part, introducing the most common notation and facts concerning bosonic systems. We do not assume previous knowledge on bosonic systems, and introduce all the building blocks that are necessary for the comprehension of this chapter. Section 10.2 and Section 10.3 are the main sections of this chapter. In Section 10.2, we formulate our passive RB protocol in full detail. In Section 10.3, we analyze our protocol, discuss the role of the input states, and prove rigorous guarantees, including bounds on its sampling complexity. We conclude with a brief overview on potential extensions of the protocol, some which we address in the next chapter, in Section 10.4. The technical details and proofs are deferred to Section 10.5.

## 10.1 Bosonic quantum systems

We consider a bosonic system of $m \in \mathbb{N}_{\geq 2}$ modes described by annihilation and creation operators $a_k$ and $a_k^\dagger$ $(k = 1, \dots, m)$, respectively, satisfying the canonical commutation relations (CCRs)

$$[a_k, a_l^\dagger] = \delta_{kl}\,, \quad [a_k, a_l] = [a_k^\dagger, a_l^\dagger] = 0\,, \quad k, l = 1, \dots, m\,,$$

where $\delta_{k,l}$ is the Kronecker delta. These operators act on the Fock-Hilbert space $\mathcal{F}_m \coloneqq \bigoplus_{n=0}^{\infty} \mathcal{H}_n^m$, where $\mathcal{H}_n^m$ is the subspace of $n$ bosons distributed over $m$ modes of dimension $\dim \mathcal{H}_n^m = \binom{n+m-1}{n}$ spanned by the *Fock* or *number states*

$$|\boldsymbol{n}\rangle \equiv |n_1, \dots, n_m\rangle \coloneqq \prod_{k=1}^{m} \frac{1}{\sqrt{n_k!}} a_k^{\dagger n_k} |\boldsymbol{0}\rangle\,, \tag{10.1}$$

where $|\boldsymbol{n}| \coloneqq \sum_{i=1}^{m} n_i = n$ and $|\boldsymbol{0}\rangle \equiv |0, \ldots, 0\rangle$ denotes the vacuum state of $m$ decoupled one-dimensional harmonic oscillators [233]. The collection of Fock states $\{|\boldsymbol{n}\rangle\}_{\boldsymbol{n}\in\mathbb{N}^m}$ forms an orthonormal basis in $\mathcal{F}_m$. Equivalently, $\mathcal{H}_n^m$ can be identified with the *symmetric* $n$-fold tensor product of a single-particle Hilbert space $\mathcal{H} \cong \mathbb{C}^m$, obtained by projecting $\otimes^n\mathcal{H}$ onto the completely symmetric subspace. Such symmetrization encodes the indistinguishability of bosons and is formally justified by the spin-statistic theorem [60]. This implies that a unitary transformation on a bosonic system is associated with described by a maximally symmetric Young diagram.

As $\mathcal{F}_m$ is infinite-dimensional, the space of quantum states is extremely rich and includes infinite-dimensional quantum states as well. Here, we find various families of states that can be routinely prepared in a lab are of special importance in quantum optics are among the most thoroughly studied, including coherent states (as generated by lasers) and thermal states (describing, for instance, black-body radiation). All these states, and many others of practical relevance, can be efficiently described by Gaussian phase-space distributions, and are therefore collectively referred as *Gaussian states*. Formally, define the *displacement operators*

$$D(\alpha) \coloneqq e^{\alpha a^\dagger - \bar{\alpha} a} \quad \alpha \in \mathbb{C} \tag{10.2}$$

(the generalization to the multimode case is straightforward). A state $\rho$ is Gaussian if the *characteristic function* $\chi_\rho(\alpha) \coloneqq \mathrm{Tr}[\rho D(-\alpha)]$ is a Gaussian function (notice that $D(-\alpha) = D(\alpha)^\dagger$). Importantly, one can check that *coherent states*, defined as

$$|\alpha\rangle \coloneqq D(\alpha)|0\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle\,, \tag{10.3}$$

are eigenstates of the annihilation operator $a$, and therefore are Gaussian states.

### 10.1.1 Gaussian transformations

Gaussian transformations are a fundamental class of bosonic channels [234]. Those are the channels that preserve Gaussianity, i.e., map Gaussian states to Gaussian states. Formally, they are generated by Hamiltonians that are at most quadratic in the field mode operators [235], such as

$$H = \sum_{k=1}^{N} g_k a_k^\dagger + \sum_{k>l=1}^{N} f_{kl} a_k^\dagger a_l + \sum_{k,l=1}^{N} h_{kl} a_k^\dagger a_l^\dagger + \text{h.c.}\,. \tag{10.4}$$

Such Hamiltonians generate two broad classes of unitaries. The first class, associated with Hamiltonians of the form $g_k a_k^\dagger$ + h.c., gives rise to displacement operators, and they are formally given by the irreps of the Heisenberg group $\mathrm{H}_n(\mathbb{R})$ [233]. The second corresponds to transformations that permute displacement operators among themselves, which can be identified with the (projective) representations of $\mathrm{Sp}(2m, \mathbb{R})$ [236]. Informally, for $g \in \mathrm{Sp}(2m, \mathbb{R})$, one has $U(g)D(\alpha)U(g)^\dagger \propto D(g \cdot \alpha)$, up to a global phase. This representation, called the *metaplectic representation* or *Weil representation* or *oscillating representation*, plays a central role in the representation-theoretical aspects of Gaussian states. It decomposes into two infinite-dimensional irreps, and the interplay with randomized techniques is not yet fully understood. Symplectic transformations can be further divided into *passive* and *active* ones, depending on whether they preserve the total energy of

the system. Active transformations –formally generated by symmetric operators– do not conserve the energy and corresponds to unitaries generated by Hamiltonians of the form $h_{kl}a^k a^l + \text{h.c.}$. In standard optical setups, these are the single-mode and two-mode squeezing operations. In contrast, passive transformations are energy-preserving and are generated by number-conserving quadratic Hamiltonians. Practically, these can also be thought as multimode interferometers, which can be decomposed in quadratically many two-modes interferometers and phase shift transformations only [164, 237–240]. In this thesis, our focus is on passive transformations. By definition, they form the group of unitary operators on $\mathcal{F}_m$ that leave the total number of particles invariant. These are exactly the unitaries that induce a transformation of the bosonic operators as $a_k \mapsto \sum_{l=1}^m U_{lk} a_l$ for a unitary matrix $U = (U_{lk})_{l,k=1}^m \in \mathrm{U}(m)$. Hence, the group of passive transformations can be identified with the unitary group $\mathrm{U}(m) \cong \mathrm{Sp}(2m, \mathbb{R}) \cap \mathrm{O}(2m)$ via the representation $\tau^m \colon \mathrm{U}(m) \to \mathrm{U}(\mathcal{F}_m)$ [236]. The above representation on $\mathcal{F}_m$ is *completely reducible* as $\mathrm{U}(m)$ is compact and $\tau^m$ is infinite-dimensional. In particular, we observe that the number operator $\hat{n} \coloneqq \sum_{i=1}^m a_i^\dagger a_i$ commutes with $\tau^m(g)$ for any $g \in \mathrm{U}(m)$. This implies that $\tau^m|_{\mathcal{H}_n^m} \equiv \tau_n^m$ is invariant and, in particular, one can show that the Fock-subspaces are indeed irreducible [241].

### 10.1.2 Observables

In this work, we are mostly interested in two families of POVMs. The first one, is represented by the *Fock-states POVM*, which is implemented by *single-mode* PNR detectors, measuring the number of photons in each mode. The ideal POVM for a single-mode detector is simply given by the projector-valued measure (PVM) $\{|k\rangle\langle k|\}_{k\in\mathbb{N}}$ [242, 243]. In the case of a photodetector with efficiency $0 < \eta < 1$, the probability to detect $k$ photons is

$$p(k \mid n) = \binom{n}{k} \eta^k (1-\eta)^{m-k}\,, \tag{10.5}$$

therefore the POVM elements are in this case given by statistical mixtures of projective measurements, namely [244]

$$M_k = \sum_{m=k}^{\infty} \binom{m}{k} \eta^k (1-\eta)^{m-k} |m\rangle\langle m|\,. \tag{10.6}$$

Often, it is enough to truncate the sum to a maximum number of detected photons, as a real detector reach saturation after it exceeds the counting.

The second family of POVMs we consider is given by collections of Gaussian states, referred as *Gaussian POVMs*: Measuring a Gaussian state with such measurements provide Gaussian-distributed outcomes [245]. Experimentally, they are realized by appending the input state with an ancilla, evolving the global system with Gaussian unitaries, and measuring the quadrature operators. In practice, the relevant Gaussian POVMs are homodyne detectors, where the measurement is realized on one of the two quadrature operators, and heterodyne detectors, where the measurement is described by the coherent state POVM $\{|\alpha\rangle\langle\alpha|\}_{\alpha\in\mathbb{C}}$ [246]. Notice that the ideal detectors homodyne and heterodyne detectors correspond to sampling from the Wigner and Husimi Q distribution, respectively, [91]. Using the framework of $s$-ordered quasi-distributions, the noisy counterparts can be described by convolutions of the POVM elements with a suitable Gaussian distribution that summarizes the imperfections in the device [234].

## 10.2 The passive randomized benchmarking protocol

### 10.2.1 Description of the protocol

The passive RB protocol follows the general procedure of the filtered RB framework discussed in Section 9.2, adapted to the group of passive transformations acting on bosonic systems. Additionally, we use post-selection to isolate particle loss rates., see Sec. 10.2.2 and 10.2.3 for details. Later, we also discuss preliminary results concerning the problem of distinguishable particles, that mostly affect the state preparation phase, see Chapter 11.

As for any filtered RB protocol, passive RB consists of two phases: During the data collection phase, we use a fixed number state $\rho = |\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|$ as an input to passive transformations, and particle number-resolving (PNR) measurements $\{|\boldsymbol{n}\rangle\langle\boldsymbol{n}|\}_{\boldsymbol{n}\in\mathbb{N}^m}$ are performed on the output. Motivated from boson sampling experiments, we propose to use a *collision-free* input state $\boldsymbol{n}_0 = (1, 1, 1, \ldots, 1, 0, \ldots, 0)$ with $n \leq m$ particles [180], see also the discussion in Section 10.3.2 below.

The collected data then undergoes the post-processing phase depicted in Section 9.2. In particular, we fix a suitable irrep $\lambda$ of $\mathrm{U}(m)$ and use its *filter function* $f_\lambda(\boldsymbol{n}, g|\rho)$, as defined in Eq. (9.27). Assuming the data $\{(\boldsymbol{n}^{(i)}, g_1^{(i)}, \ldots, g_l^{(i)})\}_{i=1}^T$ has been gathered, we compute the mean estimator

$$\hat{F}_\lambda(l) = \frac{1}{T'}\sum_{i=1}^{T} f_\lambda(\boldsymbol{n}^{(i)}, g_1^{(i)} \cdots g_l^{(i)}|\rho)\,, \tag{10.7}$$

where $T' \leq T$ is given in Section 10.2.2 below (note that this generalizes the estimator defined in Eq. (9.26)). The data series $(l, \hat{F}_\lambda(l))_{l\in\mathbb{L}}$ constitutes the (filtered) *RB signal*. Finally, perform an exponential fit according to the model $\hat{F}_\lambda(l) = A_\lambda r_\lambda^l$ to extract the *decay rate* $r_\lambda$. Repeat for different irreps $\lambda$ as needed.

We remark that we resort to the Haar measure to simplify the presentation. The generalization to non-uniform sampling is straightforward, as this work builds on the filtered RB framework. Using a gapped probability measure $\nu$ instead of the Haar measure, typically has some advantages in practice. For instance, it might be easier to sample and to take some practical limitations into account (perhaps not all passive transformations are equally simple to implement). In particular, one can simply generate passive transformations using random beam splitters and single-mode rotations. Note that in such a case, the sequence length $l$ changes its interpretation from the number of passive transformation to be applied to the number of *elementary* transformations. The filtered RB framework, c.f. Section 9.2, then predicts that the sequence of elementary transformations has to be sufficiently long in order to "appear random enough" and this threshold $l_0$ scales with the inverse spectral gap $\Delta^{-1}$. In practice, $l_0$ seems to be reasonable small such that we expect that already very short random sequences can be used for passive RB. In particular, this should outperform the quadratic depth needed to decompose Haar-random passive transformations in terms of elementary transformations.

Additionally, the protocol inherits from the filtered RB framework the interpretation of the decay rates into an average performance measure of passive transformations on the $n$-particle subspace using the formula for the entanglement fidelity described in Eq. (9.24) cf. Refs. [219, Cor. 10] and [49, Eq. (242)], that reads as

$$F = (\dim \mathcal{H}_n^m)^{-2} \sum_\lambda d_\lambda r_\lambda\,, \tag{10.8}$$

where the sum runs over all relevant irreps $\lambda$ with dimensions $d_\lambda$, c.f. Eq. (9.24). We remind the reader that caution is advised if $F$ is interpreted as the average entanglement fidelity of passive transformations due to inherent gauge freedom of RB, c.f. Section 10.3. Besides the mentioned interpretational issues, let us note that, for discrete variable systems, a suitable affine transformation is typically applied to Eq. (10.8) to produce a proxy for the better-known *average gate fidelity*. This relies on the relation $F_{\text{avg}} = \frac{dF+1}{d+1}$ for discrete variable systems in $d$ dimensions. In the here considered setting, such a transformation would result in an expression akin to the average gate fidelity, where the average is performed over input states in the $n$-particle subspace.

As $F$ corresponds to a weighted average, it is typically sufficient to only consider the largest weights which coincide with largest irreps. This means that it may not be necessary to run the post-processing phase (II) of the protocol for *every* irrep $\lambda$. We justify this statement and make it more precise later in Section 10.3.2. We refer to Section 9.2.2 for a discussion on the interpretation of $F$ and the gauge freedom aspects of RB.

For now, we restrict our attention to number state inputs and PNR measurements and justify this choice in more detail in Section 10.2.2. In Chapter 11, we discuss extensions of the passive RB protocol to Gaussian states or measurements.

Finally, the procedure described above is sometimes referred to as *single-shot estimation*, in the sense that only a single shot (or measurement) is taken per sequence. In practice, it is often advantageous to use *multi-shot estimation* instead, where multiple shots per sequence are recorded. Then, the estimator (10.7) changes in an obvious way, but converges to the same expectation value as (10.7). Except for the sampling complexity discussion in Section 10.3.4 all results of this work also apply to the multi-shot estimator.

### 10.2.2 Details of the protocol

Choosing a number state $|\boldsymbol{n}_0\rangle$ as input to the protocol has the advantage that –*ideally*– the dynamics should happen on the finite-dimensional $n$-particle subspace $\mathcal{H}_n^m \subset \mathcal{F}_m$ only, where $n = |\boldsymbol{n}_0|$. On $\mathcal{H}_n^m$, the passive transformations $\mathrm{U}(m)$ act via the totally symmetric irrep $\tau_n^m$. To describe noise, we transition to the density operator formalism, in which this action is described by conjugation, $\omega_n^m(g)(\rho) \coloneqq \tau_n^m(g)\rho\,\tau_n^m(g)^\dagger$. If we assume – for the sake of the argument – that the noise is particle number-preserving, we can model the noisy transformations by quantum channels $\phi_n^m(g)$ on the space of bounded operators $\mathcal{B}(\mathcal{H}_n^m)$, provided that the noise is time-stationary and Markovian. Regarding the $\phi_n^m(g)$ as (small) perturbations of $\omega_n^m(g)$, the filtered RB framework [50] then predicts RB decays in one-to-one correspondence with the irreps of the *reference representation* $\omega_n^m$. As we show in Section 10.5.3, the latter decomposes into exactly $n+1$ distinct irreps $\lambda_k$[1] and this is the number of decays to expect.

Arguably, *particle loss* is one of the major noise sources in, e.g., photonic systems, hence assuming particle-number preserving noise is unrealistic. This can nevertheless be accounted for in our framework, as we are performing PNR measurements: By post-selecting on particle number-preserving events, we obtain effective dynamics described by completely positive, *trace non-increasing* maps $\phi_n^m(g)$ on $\mathcal{B}(\mathcal{H}_n^m)$ and we can again rely on the results in Ref. [50]. Note that this reasoning also applies to noisy PNR measurements by modelling them as a sub-normalized POVM. This approach is justified as long as the product of the

[1]Here, $\lambda_0 = \mathbf{1}$ is the trivial irrep and $\lambda_1 = \mathrm{Ad}$ is the adjoint irrep of $\mathrm{U}(m)$.

photon loss probability and the one of photon *gain* (e.g. through thermal noise in detectors) is very small such that the error introduced by ignoring photon gain is comparable to the shot noise. We expect this to be the case in modern photonic chips.

Finally, we introduce the *filter function* which isolates the exponential decays for each irrep $\lambda = \lambda_k$ in the post-processing of the collected data. Let $P_\lambda$ be the projector on the carrier space of $\lambda$ and let $d_\lambda$ be its dimension. Then, given the measurement channel $\mathcal{M}(A) \coloneqq \sum_{n\in\mathbb{N}^m} \langle \boldsymbol{n}\,|A|\boldsymbol{n}\rangle |\boldsymbol{n}\rangle\langle \boldsymbol{n}|$, the filter function defined in Eq. (9.27) becomes

$$\begin{aligned} f_\lambda(\boldsymbol{n}, g|\rho) &\coloneqq s_\lambda^{-1} \langle \boldsymbol{n}\,|\omega_n^m(g) \circ P_\lambda(\rho)\,|\boldsymbol{n}\rangle\,, \\ s_\lambda &\coloneqq d_\lambda^{-1} \operatorname{Tr}[P_\lambda \mathcal{M}] \in \mathbb{R}_{\geq 0}\,. \end{aligned} \tag{10.9}$$

We will often simply write $f_\lambda(\boldsymbol{n}, g|\rho) \equiv f_\lambda(\boldsymbol{n}, g)$ once the input state $\rho$ is fixed. We give a more concise formula for $f_\lambda$ in Section 10.3 as Theorem 36. In particular, we show that $s_\lambda > 0$ as long as the number of modes $m$ is strictly larger than 1. As the filter function is automatically zero if $|\boldsymbol{n}| \neq n$ due to $P_\lambda$, we can formally describe the post-selection on particle number-preserving events by defining

$$T_{\mathrm{pr}} \coloneqq |\{i \in [T]\,|\,|\boldsymbol{n}^{(i)}| = n\}|\,, \tag{10.10}$$

and using the mean estimator Eq. (10.7) with the choice $T' = T_{\mathrm{pr}}$.

### 10.2.3 Estimation of particle loss rates

The same post-processing procedure can also be used to capture the estimation of particle loss rates as follows. Define the filter function to be the indicator function[2]

$$f(\boldsymbol{n}) \coloneqq \begin{cases} 1 & \text{if } |\boldsymbol{n}| = n, \\ 0 & \text{else,} \end{cases} \tag{10.11}$$

and set $T' = T$. Thus, the associated mean estimator $\hat{F}(l)$, cf. Eq. (10.7), simply yields the ratio $T_{\mathrm{pr}}/T$. To see that this leads to the wanted result, let us model particle loss by a beam splitter with transmittivity $\sqrt{p}$ in every mode (i.e. $p$ is the probability of *not* loosing a particle). In addition, we assume transmittivities $\sqrt{p_{\mathrm{SP}}}$ and $\sqrt{p_{\mathrm{M}}}$ associated with state preparation and measurement, respectively. Hence, the probability that a sequence of $l$ passive transformations preserves the particle number is $p_{\mathrm{SP}}^n p_{\mathrm{M}}^n p^{nl} = \mathbb{E}[T_{\mathrm{pr}}/T] = \mathbb{E}[\hat{F}(l)]$. Therefore, we can extract the transmittivity $\sqrt{p}$ from the data $(l, \hat{F}(l))_{l\in\mathbb{L}}$ using an exponential fit as before.

Note that the original filtered RB protocol does not perform the post-selection in Section 10.2.2 above (i.e. $T' = T$ in Eq. (10.7)). This leads to a mixing of the decay rate of particle-preserving noise with the particle loss rate, resulting in a combined decay $(p^n r_\lambda)^l$. By performing post-selection, we can consider these decays individually.

## 10.3 Analysis and guarantees

The filtered RB framework [50] implies a number of guarantees for the passive RB protocol, which we specialize and extend in the following. We rely on the *implementation map* noise

[2] Note that this conicides with a suitably rescaled filter function (10.9) for the trivial irrep $\lambda_0$.

model which we justified using the post-selection argument in Section 10.2. In this model, the noise is modeled by replacing the representation $\omega_n^m$ with an implementation map $\phi_n^m$ on $\mathrm{U}(m)$, which takes values in the set of completely positive, trace non-increasing superoperators on $\mathcal{H}_n^m$. This model allows for highly gate-dependent noise, which, however, needs to be stationary and Markovian.

In the following, we use the short-hand notations $\omega \equiv \omega_n^m$, $\tau \equiv \tau_n^m$, and $\phi \equiv \phi_n^m$ whenever the parameters $n$ and $m$ are clear from the context.

### 10.3.1 The RB signal

In the filtered RB framework [50], noise is measured by the operator norm $\delta_\lambda \coloneqq \|\tilde{T}_\lambda - T_\lambda\|_\infty$ and "weak noise" is such that $\delta_\lambda \leq 1/5$. Then, Ref. [50] gives more precise conditions on the error suppression in the expected signal. In particular, it is sufficient to choose the sequence length as

$$l \geq \frac{\log \frac{d_\lambda}{s_\lambda} + 2\log \frac{1}{\alpha} + 4}{2\log \frac{1}{2\delta_\lambda}}\,. \tag{10.12}$$

where $d_\lambda$ is the dimension of the irrep and $s_\lambda$ is as in Eq. (10.9). In the technical part of this work, Section 10.5, Proposition 39 and Theorem 41, we prove the following explicit formulae for $\lambda = \lambda_k$:

$$d_{\lambda_k} = \frac{2k+m-1}{m-1}\binom{k+m-2}{k}^2, \tag{10.13}$$

$$s_{\lambda_k} = \frac{m-1}{2k+m-1}\binom{k+m-2}{k}^{-1}. \tag{10.14}$$

In particular, we have (for $m > 1$):

$$\frac{d_{\lambda_k}}{s_{\lambda_k}} = \left(\frac{2k+m-1}{m-1}\right)^2 \binom{k+m-2}{k}^3. \tag{10.15}$$

Hence, it is sufficient to take sequences of length $O(k \log \frac{k+m-2}{k})$ which is $O(m \log m)$ in the *non-collision regime* $n \leq m$ (as $k \leq n$). However, we expect that these bounds are not tight. In fact, Eq. (10.12) is not tight in the first place [50], nevertheless improving the bound is hard in the gate-dependent noise setting. Based on the experience with discrete variable RB, we expect that already very short sequences are sufficient and conjecture that the dependence on $d_{\lambda_k}/s_{\lambda_k}$ in Eq. (10.12) can in fact be dropped, meaning that constant-length sequences are sufficient.

The signal form is concretely shown in Fig. 10.1, where we show the results of a simulation of the protocol with $|\boldsymbol{n}_0\rangle = |\mathbf{1}\rangle_4 \equiv |1111\rangle$, assuming lossy gates for different values of the transmittivity. By performing exponential fits, we retrieve values of the transmittivity $\sqrt{p}$ using $T = 10000$ samples, matching the used transmittivities up to an error of $10^{-3}$. We also simulated an experiment where the transmittivity is chosen at random for each transformation, resulting in decay rates that match the average over the allowed random decay rates. We provide additional details on numerical experiments in Appendix B.4.

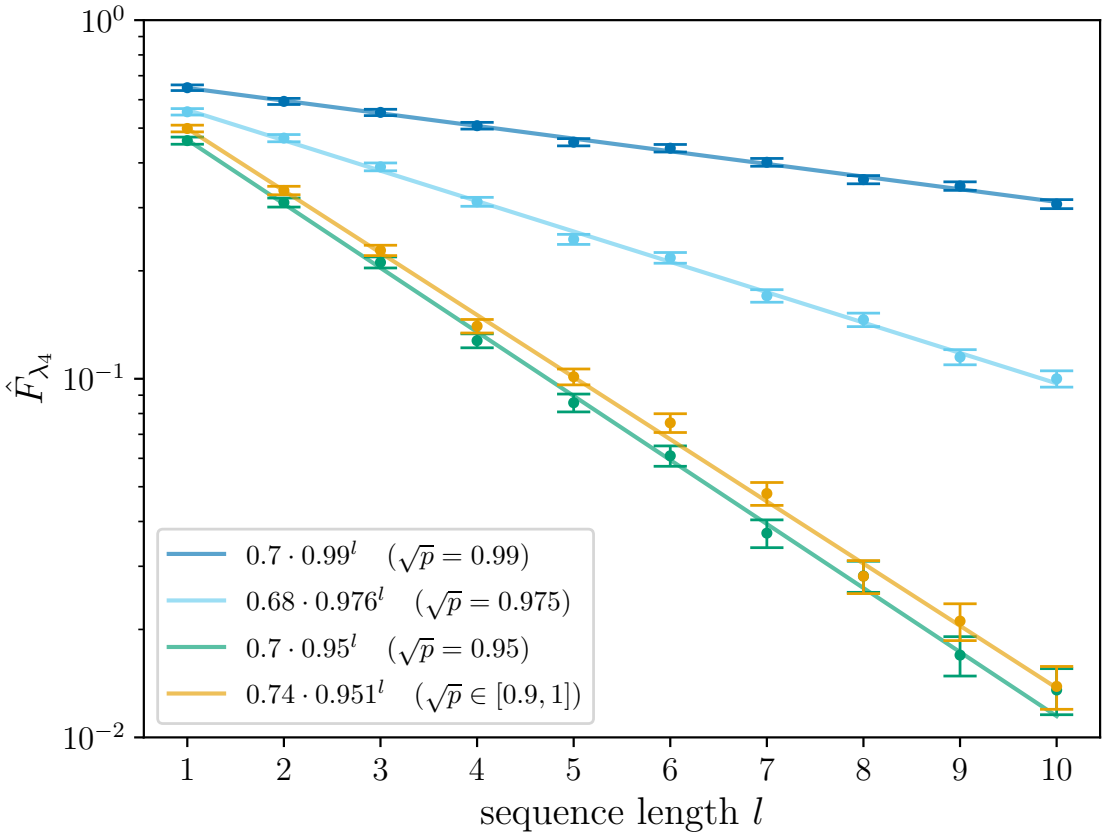



Figure 10.1: Passive RB signal (10.7) using $n = m = 4$ and input state $|\mathbf{1}_4\rangle \equiv |1111\rangle$ in the presence of particle loss noise, using $T = 10000$ samples. The last (yellow) data set corresponds to simulated gate-dependent noise where the transmittivities $\sqrt{p}$ are drawn uniformly at random from $[0.9, 1]$ for every transformation in the sequence. More details can be found in Appendix B.4.

### 10.3.2 Choice of input state

For standard RB on discrete variable systems, the input state is typically chosen to be the all-zeros state $|0^n\rangle$, and, in fact, the choice of input state plays a minor role in this case. The underlying reason is that we typically have a single non-trivial irrep (i.e., the adjoint irrep) with respect to which all states are equivalent.

In the finite-dimensional bosonic setting, we show in Lemma 38 in Section 10.5.3 that $\omega_n^m$ decomposes into $n + 1$ irreps and thus there is a certain freedom in choosing the input state $\rho = |\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|$. In principle, the passive RB protocol is agnostic of the input state. However, its choice influences the overall magnitude of the RB signal since the latter scales with the overlap of the state with the irrep of interest [50]. As the variance of $F_\lambda$ exhibits the same scaling behaviour, the mean estimator $\hat{F}_\lambda(l)$ also converges more rapidly for smaller overlaps and hence the overall scale set by the overlap does not influence the sampling complexity of the protocol, see also Section 10.3.4. Nevertheless, it may happen that the input state has vanishing overlap with an irrep, in which case the RB signal is identically zero and no information about decay rates can be extracted. Moreover, very small overlaps,

and thus signals, may lead the numerical issues in the post-processing.

Our proposal of using a collision-free state $\boldsymbol{n}_0 = \mathbf{1}_n = (1, 1, 1, \ldots, 1, 0, \ldots, 0)$ is motivated by practical considerations as generating higher Fock states can be a challenging task [247–249]. In Fig. 10.2 and Fig. 10.3, we show its overlaps with the relevant irreps for $n = m$ and for $n \leq m$ with $m$ fixed, respectively. We see that the largest overlap is always attained with the largest irrep $k = n$ and typically decreases with $k$, leading to small overlaps for $k \ll n$ if $m$ is not too small. Generally, one can show that the collision-free state for $n = m$ particles always has zero overlap with the $\lambda_1$ (adjoint) irrep. This behaviour can be avoided by optimizing $\boldsymbol{n}_0$, however likely leading to an input state that is hard to prepare in experiments.

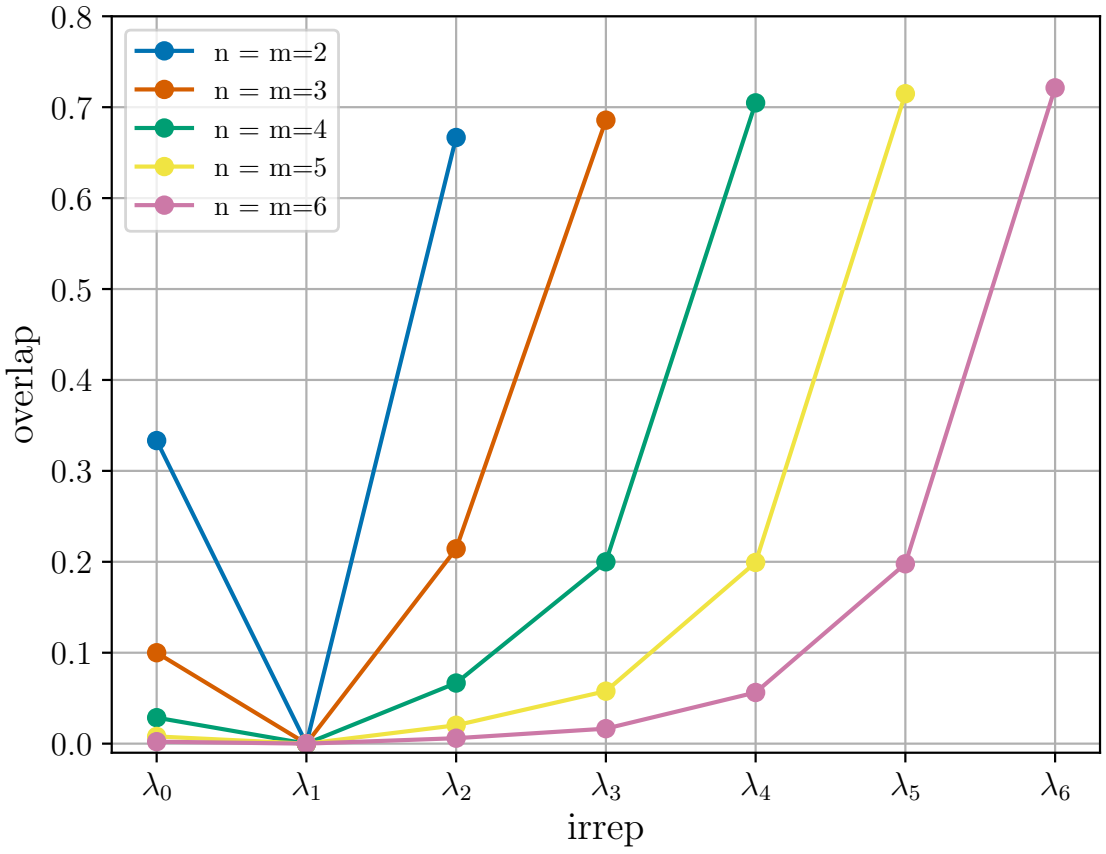



Figure 10.2: Overlaps of the collision-free $n$-particle state $\mathbf{1}_n = (1, \ldots, 1, 0, \ldots, 0)$ with the irreps $\lambda_k, k = 0, \ldots, m$. Lines are shown to enhance readability of data points and their relationships. For $n = m$, we observe no overlap with the adjoint irrep $\lambda_1$. For each $m$, the overlap is maximized by the largest irrep.

As a matter of fact, the problem of vanishing and very small overlaps of the collision-free state is not severe: Recall that the overall benchmarking quantity $F$, cf. Eq. (10.8), is given as a weighted average of the decay rates $r_{\lambda_k}$, where the weights are given by the irrep dimension $d_{\lambda_k}$. Since irreps with small $k$ also have small dimension, their contribution to the weighted average may be neglected. More precisely, if we only take into account the $u$

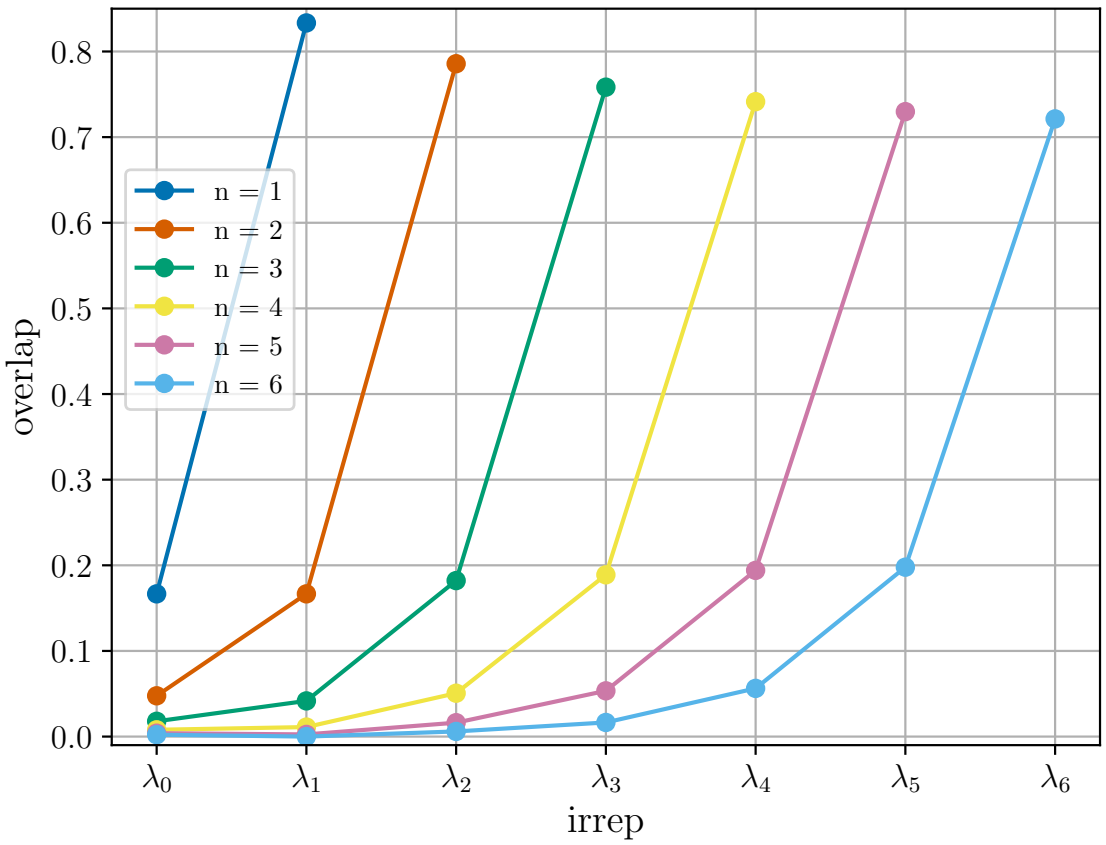



Figure 10.3: Overlaps of the collision-free $n$-particle state $\mathbf{1}_n = (1, \ldots, 1, 0, \ldots, 0)$ with the irreps $\lambda_k, k = 0, \ldots, m$ for $n \leq m = 6$. As before, the maximum overlap is obtained for the largest irrep $\lambda_n$. Note that the overlap with $\lambda_1$ is trivial only for $n = m$.

largest irreps, their combined weight can be readily computed as

$$(\dim \mathcal{H}_n^m)^{-2} \sum_{i=0}^{u-1} d_{\lambda_{n-i}} = 1 - \left[ \prod_{i=1}^{u} \frac{n-i+1}{n+m-i} \right]^2 . \tag{10.16}$$

In particular, if $n$ is fixed and $m \to \infty$, this converges to 1 for any $u$, and if $n = m \to \infty$, the weight converges to $1 - 4^{-u}$. As the convergence is fast in both cases, taking only a constant number of irreps (the largest ones) into account gives an exponentially good approximation to $F$, already for a moderate number of modes. For instance, for $n = 5$ particles in $m = 10$ modes, taking the 3 largest irreps covers 99.9% of the total weight. This also implies that it is sufficient to perform the post-processing phase (II) in the passive RB protocol, Section 10.2, only a constant number of times.

### 10.3.3 Evaluation of the filter function

At the heart of the the passive RB protocol, Section 10.2, lies the evaluation of the filter function (10.9) in the post-processing phase. We briefly sketch the central steps of

its computation leading to Theorem 36 in the following and refer to the technical part, Section 10.5, for more details and proofs.

First, note that $\omega \simeq \tau \otimes \bar{\tau}$ can be explicitly decomposed into irreps using a suitable generalization of the Clebsch-Gordan decomposition for the sum of two angular momenta in quantum mechanics [54, 77]. This yields the following expansion of Fock states

$$|\boldsymbol{n}\rangle\langle\boldsymbol{n}| \simeq |\boldsymbol{n},\boldsymbol{n}\rangle = \sum_{\lambda} \sum_{M_\lambda} \tilde{C}^{M_\lambda}_{\boldsymbol{n},\bar{\boldsymbol{n}}} |M_\lambda\rangle\,, \tag{10.17}$$

where $\lambda$ runs over the irreps of $\omega$ and the $|M_\lambda\rangle$ form a suitable basis of $\lambda$. The $\tilde{C}^{M_\lambda}_{\boldsymbol{n},\bar{\boldsymbol{n}}}$ correspond to (generalized) SU($m$) Clebsch-Gordan coefficients, up to a phase. Then, the projection onto a specific irrep $\lambda$ acts by selecting only the corresponding terms in Eq. (10.17). Re-expressing the $|M_\lambda\rangle$ in terms of Fock states and inserting the expansion into Eq. (10.9) produces so-called *permanents*, which are defined for an arbitrary $r \times r$ matrix $A$ as

$$\mathrm{Per}(A) \coloneqq \sum_{\pi \in S_r} \prod_{i=1}^{r} A_{i\,\pi(i)}\,, \tag{10.18}$$

where $S_r$ denotes the symmetric group over $r$ symbols. Let us define $A_{\boldsymbol{n},\boldsymbol{m}}$ to be the matrix obtained from $A$ by taking $m_j$ copies of the $j$-th column of $U$ and then taking $n_i$ copies of the $i$-th row of the resulting matrix. Then, the appearance of permanents is due to the well-known fact that $\sqrt{\boldsymbol{n}!}\sqrt{\boldsymbol{m}!}\,\langle \boldsymbol{n}\,|\tau(g)|\,\boldsymbol{m}\rangle = \mathrm{Per}(g_{\boldsymbol{n},\boldsymbol{m}})$ [250], where we used the multi-index notation $\boldsymbol{n}! \coloneqq n_1! \ldots n_m!$.

Finally, we have the following concise formula that can be used for numerical computation:

**Theorem 36** (PNR filter function – informal)**.** *The filter function* (10.9) *is given as*

$$f_{\lambda_k}(\boldsymbol{n}, g) = \frac{1}{s_{\lambda_k}} \sum_{M} \tilde{C}^{M}_{\boldsymbol{n}_0,\bar{\boldsymbol{n}}_0} \sum_{\boldsymbol{n}_1 \in \mathcal{H}^m_n} \tilde{C}^{M}_{\boldsymbol{n}_1,\bar{\boldsymbol{n}}_1} \frac{|\mathrm{Per}(g_{\boldsymbol{n},\boldsymbol{n}_1})|^2}{\boldsymbol{n}!\boldsymbol{n}_1!}\,. \tag{10.19}$$

*Here, $M$ labels a so-called* Gelfand-Tsetlin *basis of the irrep $\lambda_k$ and the coefficients $\tilde{C}$ coincide with Clebsch-Gordan coefficients for* SU($m$) *up to a phase.*

We refer to Section 3.1.1 for more details on the Gelfand-Tsetlin basis, the computation of Clebsch-Gordan coefficients, and the occurring phases, and formally prove Theorem 36 in Section 10.5.5. We also give an alternative formula for $f_{\lambda_k}$ in Corollary 44 using matrix coefficients of the irrep $\lambda_k$. These also correspond to permanents, however, of a different dimension [251].

Generally speaking, the computation of filter functions of the form (10.9) requires to simulate the entire experiment. As the proposed protocol involves non-Gaussian elements, the computation of filter functions is expected to be generally inefficient. This is manifest in the occurrence of permanents in our filter functions. The computational complexity of evaluating permanents is central to the complexity-theoretic arguments for boson sampling. It is known that even approximating permanents is computationally hard [180, 232]. Nevertheless, these quantities can be computed efficiently in some scenarios [252–257].

This finding should not come as a surprise, as we find a similar behaviour in the discrete setting – namely linear cross-entropy benchmarking [50, 229]. There, the post-processing

requires the simulation of random circuit sampling which is known to be computationally hard, analogous to boson sampling [5, 230–232].

In practice, Clebsch-Gordan coefficients can be computed in polynomial time in the dimension of $\lambda$ [77]. This can be significantly sped up by taking advantage of the symmetries of the weight diagrams under the action of the Weyl group of $\mathrm{SU}(m)$ [258]. Specifically, we expect this to be feasible for $m \approx 20 - 30$ modes. In such regime, the computation of the permanents appearing in Eq. (10.19) is also still possible, as we consider $n \leq m$ particles and, by Ryser's formula, it can be computed in time $\mathrm{O}(n \cdot 2^n)$ [259, 260].

### 10.3.4 Sampling complexity

In the following, we discuss the sample complexity of passive RB, i.e. the number of samples needed to guarantee that the estimator $\hat{F}_\lambda(l)$ is $\epsilon$-close to its expected value $F_\lambda(l)$ with high probability. Recall from Eq. (10.7) that $\hat{F}_\lambda(l)$ is a mean estimator for the filter function $f_\lambda$. Since the latter is only poorly bounded, we compute the variance $\mathrm{Var}[\hat{F}_\lambda(l)] = \mathrm{Var}[f_\lambda]/L$ (here the variance is still taken over length-$l$ sequences). Then, we can use Chebyshev's inequality to ensure $|\hat{F}_\lambda(l) - F_\lambda(l)| < \epsilon$ with probability $1 - \delta$ given $L \geq \epsilon^{-2}\delta^{-1}\,\mathrm{Var}[f_\lambda]$ samples.

In general, analyzing the variance $\mathrm{Var}[f_\lambda]$ – more precisely the second moment $\mathbb{E}[f_\lambda^2]$ – can be quite cumbersome, as the underlying probability distribution is given by Born probabilities involving the noisy input state, the noisy transformations, and the noisy measurements. In the filtered RB framework [50] it is however shown that – under reasonable assumptions on the noise[3] – this problem can be reduced to analyzing the second moment $\mathbb{E}[f_\lambda^2]_{\mathrm{ideal}}$ in the ideal, noiseless case. In other words, the presence of noise cannot decrease the efficiency of filtered RB. Using this assumption, we have the following result bounding the variance of passive RB:

**Theorem 37** (Variance bound – informal)**.** *The variance of the passive RB protocol is bounded as*

$$\mathrm{Var}[f_{\lambda_k}] \leq \mathbb{E}[f_{\lambda_k}^2]_{\mathrm{ideal}} = s_{\lambda_k}^{-2} \sum_{\boldsymbol{n} \in \mathcal{H}_n^m} \tilde{g}_k(\boldsymbol{n}, \boldsymbol{n}_0)\,, \tag{10.20}$$

*where $\tilde{g}_k(\boldsymbol{n}, \boldsymbol{n}_0)$ is a function of Clebsch-Gordan coefficients of the representations $\omega$ and $\lambda_k^{\otimes 2}$.*

A formal version of Theorem 37 is given as Theorem 48 in the technical part and also proven there. It relies on expressing the second moment $\mathbb{E}[f_{\lambda_k}^2]_{\mathrm{ideal}}$ as a suitable integral of the representations $\lambda_k^{\otimes 2}$ and $\omega_n^m$ over $\mathrm{SU}(m)$ [50, 199]. Schur's lemma then implies that the non-trivial contributions to this integral are given by the irreps of $\lambda_k^{\otimes 2}$ which are also contained in $\omega$. We determine these irreps which allows us to finally write $\mathbb{E}[f_{\lambda_k}^2]_{\mathrm{ideal}}$ in terms of suitable Clebsch-Gordan coefficients.

Arguably, Eq. (10.20) is not very explicit and it is thus not clear how $\mathbb{E}[f_{\lambda_k}^2]$ scales with $k$, $n$, and $m$. Finding a meaningful bound for the expression in Eq. (10.20) turns out to be difficult and we are left with the trivial bound

$$\mathbb{E}[f_{\lambda_k}^2] \leq s_{\lambda_k}^{-2} = \left(1 + \frac{2k}{m-1}\right) \binom{k+m-2}{k}^2\,, \tag{10.21}$$

[3] This is necessary as specially engineered noise can drastically change the behavior of the RB signal, for instance by relabeling the measurement outcomes. Similar assumptions can be found throughout the RB literature [208, 224].

which suggests an exponential scaling like $2^{4m}$ in the worst case $k = n = m$. This bound is however very loose: A numerical evaluation of the second moment (see below) reveals that the upper bound (10.21) already overestimates the second moment for $m = 2$ by a factor of 10 and by a factor of $10^4$ for $m = 5$.

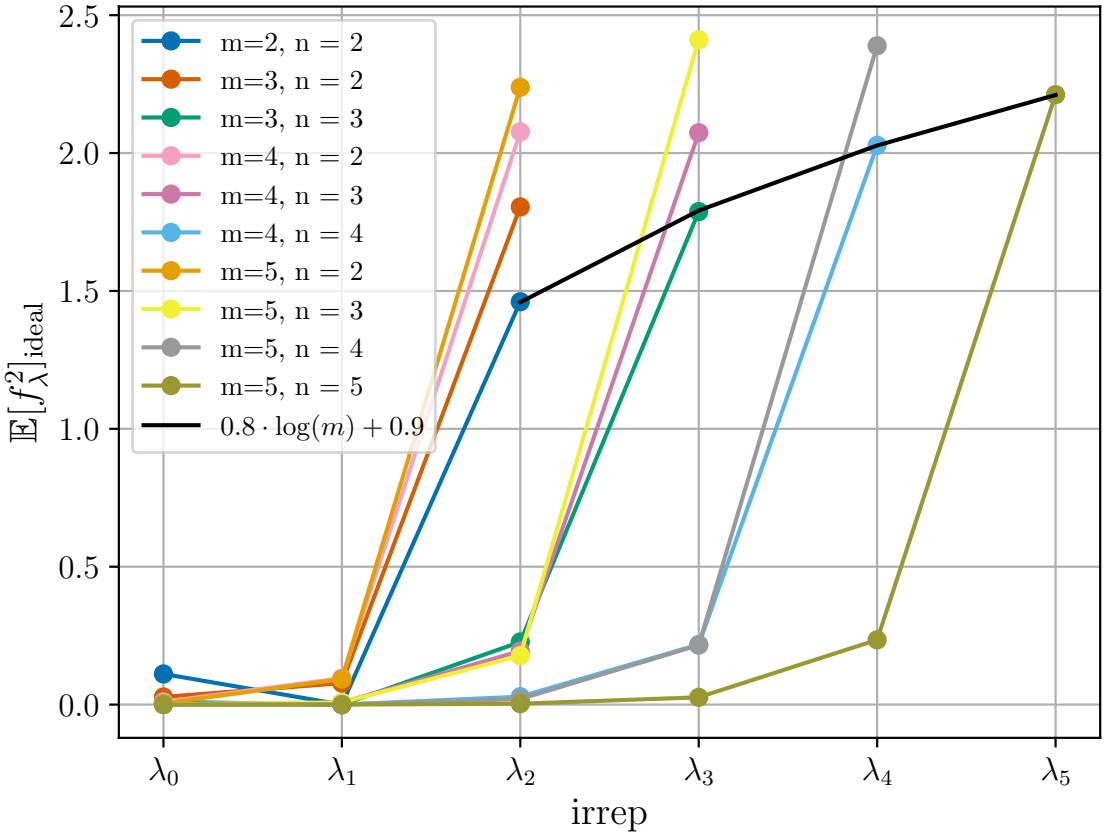



Figure 10.4: Empirical second moment of the filter function $f_{\lambda_k}$ with $T = 10000$ samples for different values of $n \leq m$ and $m \leq 6$. The largest second moment (for fixed $m$) is always attained at the largest irrep $k = n$. The scaling of the second moment for $m = n = k$ with $m$ seems to be logarithmic, however there is insufficient data the make a definite conclusion. Lines are shown to enhance readability of data points and their relationships.

The shear number of Clebsch-Gordan coefficients that need to be evaluated for the formula (10.20) however limits a numerical study to very low values of $k$, $n$, and $m$ using standard algorithms [77].[4] To increase the available data a bit, we furthermore estimate the variance empirically using $T = 10000$ samples from the noiseless outcome distributions. From Fig. 10.5, we can observe that this number of samples is already enough to give reasonable estimates of $\mathbb{E}[f_{\lambda_k}^2]_{\text{ideal}}$. In Fig. 10.4, we show the empirical second moments for $m \leq 5$ using a collision-free input state $\mathbf{1}_n$ with $n \leq m$ particles (cf. Appendix B.4 for further details on the sampling procedure). Similar to the behaviour for the ideal first moments (overlaps) in Figs. 10.2 and 10.3, the second moment for a fixed $m$ is maximized

[4]We expect Eq. (10.20) can be evaluated for a moderate number of modes exploiting the symmetries of the weight diagrams under the action of the Weyl group [258].

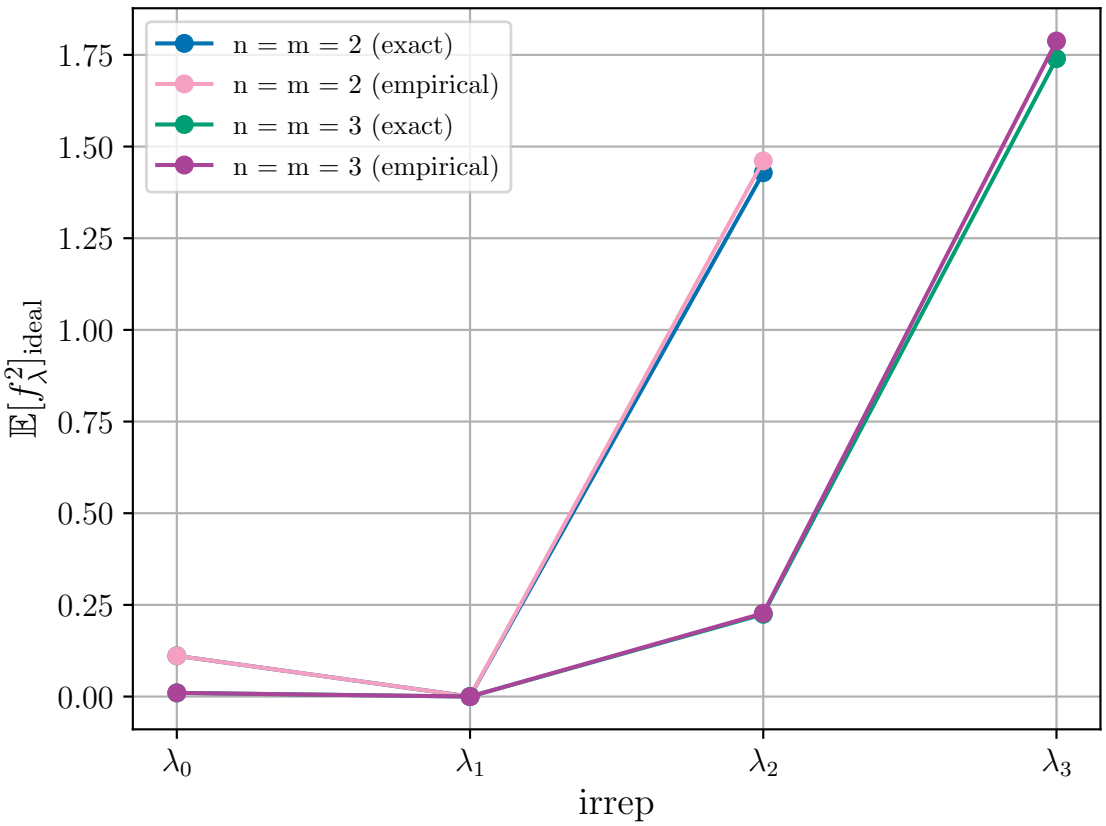



Figure 10.5: Empirical second moment with $T = 10000$ samples compared to the exact second moment (10.20) for $n = m \leq 3$. We observe that this number of samples is already sufficient to give reasonable approximations of the second moment. Lines are shown to enhance readability of data points and their relationships.

at the largest irrep $k = n$. In addition, we analyzed the scaling scaling of the empirical second moments for $m = n = k$ with $m$. Although we have too few data points to make a conclusive statement, we find that the scaling is best compatible with a logarithmic scaling in $m$ (or a polynomial of very small degree $\approx m^{1/20}$). This would be a double-exponential improvement over the trivial bound (10.21).

## 10.4 Extensions of the protocol

Arguably, the most straightforward –and experimentally simplest– protocol would involve a Gaussian input state and measurement. However, this would correspond to a classical linear optics experiment and one should not expect to capture errors which would occur in a quantum setting. Hence, it is more instructive to consider a variation of the passive RB protocol, in which either the input state or the measurement is made Gaussian.

However, one needs to be careful when leaving the effectively finite-dimensional setting which we explored in this chapter. Indeed, an 'inherently infinite-dimensional' RB protocol is ill-behaved for the following reason: Any passive transformation $U \in \mathrm{U}(m)$ is represented

as a unitary operator $\tau^m(U)$ on the full Fock space $\mathcal{F}_m := \bigoplus_{n=0}^{\infty} \mathcal{H}_n^m$. Since $\mathrm{U}(m)$ is compact, $\tau^m$ is completely reducible, and decomposes into infinitely many finite-dimensional irreps acting on the boson number subspaces [261]. Then, the conjugation representation $\omega \equiv \tau^m(\,\cdot\,)\tau^{m\dagger}$ decomposes into infinitely many irreps, too. This means we may find infinitely many decay rates (each associated to one irrep) and it is unclear how to truncate those with a regularization argument, as the irreps lack a clear physical interpretation. On top of that, the decomposition of $\omega$ is not multiplicity-free,[5] which may complicate the post-processing and affect its numerical stability [49].

In the next chapter, as a first step, we consider a passive RB protocol with a number input state and a balanced heterodyne measurement at the end of each mode, and a passive RB protocol with coherent states and PNR measurements.

Lastly, we comment on the extension to other groups. Broadly speaking, *active* Gaussian transformations play a fundamental role in CV systems, for instance in GKP encoding of qubits in bosonic states [166], or in the preparation of input states for Gaussian boson sampling experiments [181, 182, 262]. However, randomized benchmarking of general Gaussian transformations faces many challenging issues, most strikingly the fact that this group – the symplectic group $\mathrm{Sp}(2m, \mathbb{R})$ on $m$ modes– is *non-compact*. As a consequence, a Haar probability measure cannot exist, and thus it is not even clear how to 'randomize' in this context. Hence, the filtered RB framework focuses on compact groups [50]. Some of the ideas in Ref. [50] nevertheless carry over to the non-compact case if one considers suitable random walks on $\mathrm{Sp}(2m, \mathbb{R})$. By the central limit theorem for reductive Lie groups [263], such random walks converge to a Gaussian distribution on $\mathrm{Sp}(2m, \mathbb{R})$. However, this does not clarify –to the best of our knowledge– the behaviour and convergence of the moment/twirling operator. Since $\mathrm{Sp}(2m, \mathbb{R})$ has Kazhdan's property (T) [264], the characterization of the relevant representation theory – capturing the action of active transformations onto density operators– plays a central role. This involves the well-known metaplectic (or oscillator) representation of $\mathrm{Sp}(2m, \mathbb{R})$ and can – in principle – be approached using Howe duality [265, 266]. Due to infinite-dimensional irreps [56] and open convergence questions, it is however far from obvious whether a meaningful RB protocol can be developed for active transformations. We leave the resolution of these questions for future work.

## 10.5 Technical details and proofs

Here, we provide proofs for the theorems introduced in Section 10.2: In Section 10.5.5 we prove Theorem 36 and in Section 10.5.6 we prove Theorem 37 based on notation and technical tools introduced in Section 3.1.1. Throughout this section we assume that the number of modes is $m \geq 2$.

### 10.5.1 Further notations

As the Clebsch-Gordan decomposition is naturally related with the direct sum decomposition of an Hilbert space of the form $\mathcal{H}_1 \otimes \mathcal{H}_2$, it will be convenient to introduce a vectorized notation for operators and super-operators on $\mathcal{H}_n^m$.

[5] Note that $\omega$ restricted to $\mathcal{B}(\mathcal{H}_n^m)$ is equal to $\omega_n^m$ and –as mentioned in Section 10.2.2– each $\lambda_k$ appears in all $\omega_n^m$ for $n \geq k$.

We consider the basis of linear operators for $\mathcal{B}(\mathcal{H}_n^m)$ given by $\Phi = \{|\boldsymbol{n}\rangle\langle\boldsymbol{m}|\}_{\boldsymbol{n},\boldsymbol{m}\in\mathbb{N}^m}$ with $\sum_{i=1}^m n_i = \sum_{i=1}^m m_i = n$. Any linear operator $A \in \mathcal{B}(\mathcal{H}_n^m)$ can be vectorized to an element $|A\rangle \in \mathcal{H}_n^m \otimes \mathcal{H}_n^m$ w.r.t. $\Phi$ as

$$|A\rangle = \sum_{\boldsymbol{n},\boldsymbol{m}} \langle \boldsymbol{n}\,|A|\boldsymbol{m}\rangle |\boldsymbol{n},\boldsymbol{m}\rangle\,, \quad |\boldsymbol{n},\boldsymbol{m}\rangle \equiv |\boldsymbol{n}\rangle \otimes |\boldsymbol{m}\rangle\,. \tag{10.22}$$

Under vectorization, we have the induced mapping $\tau_n^m(\cdot)\tau_n^{m\dagger} \mapsto \tau_n^m \otimes \bar{\tau}_n^m$, where $\bar{\tau}_n^m$ denotes the complex conjugate representation of $\tau_n^m$ (in the Fock basis $\phi$). Moreover, as long as it is clear from the context, we will not distinguish between super-operators and their corresponding quantities acting on $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Then, the filter function defined in Eq. (10.9) becomes

$$f_\lambda(\boldsymbol{n}, g) = \frac{1}{s_\lambda} \langle \boldsymbol{n}_0, \boldsymbol{n}_0\,|P_\lambda(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger|\,\boldsymbol{n},\boldsymbol{n}\rangle\,, \tag{10.23}$$

where $\rho = |\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0| \cong |\boldsymbol{n}_0,\boldsymbol{n}_0\rangle$ is the input state and $s_\lambda = (d_\lambda)^{-1} \sum_{\boldsymbol{n}\in\mathbb{N}^m} \langle \boldsymbol{n},\boldsymbol{n}\,|P_\lambda|\,\boldsymbol{n},\boldsymbol{n}\rangle$.

### 10.5.2 Symmetric irreps in $\mathrm{SU}(m)$.

In this section, we summarize a few basic facts concerning symmetric irreps of $\mathrm{SU}(m)$, as they are of central importance throughout this work. By construction, the space of $n$ particles over $m$ modes is maximally symmetric under permutations over the modes. This implies that the action of $g \in \mathrm{SU}(m)$ on such space is described by the irrep

$$\tau_n^m \equiv (n, \underbrace{0,\ldots,0}_{m-1}) = \underbrace{\square\cdots\square}_{n}\,, \tag{10.24}$$

where the number of boxes has the interpretation of the number of particles in the system. Formally, the Young diagram on the r.h.s. labels the maximally symmetric irrep in $\mathrm{SU}(m)$. Notably, the weights of the maximally symmetric irreps uniquely identify GT basis elements, as it can be easily checked via the associated tableaux weights.

In $\mathcal{H}_n^m$, a common orthonormal basis is the *Fock basis*, given by Fock states $\{|\boldsymbol{n}\rangle \mid \boldsymbol{n} \in \mathbb{N}^m, \sum_{i=1}^m n_i = n\}$. We remark that the GT basis, as well as the Weyl basis, labels the same set of orthonormal vectors as the Fock basis. In fact, for symmetric irreps, $\boldsymbol{n}$ is exactly the tableau weight of the corresponding Young tableau, i.e. $n_i$ is the number of boxes filled with $i$ for each $i \in [m]$, e.g.

$$|3,2,1\rangle = \Big|\begin{array}{|c|c|c|c|c|c|}\hline 1&1&1&2&2&3\\\hline\end{array}\Big\rangle\,, \tag{10.25}$$

from which follows the correspondence with the GT basis. In particular, for any Fock state $|\boldsymbol{n}\rangle = |n_1,\ldots,n_m\rangle$, the corresponding GT pattern –that will be denoted by $N$ throughout this work– is given as follows:

$$N = \begin{pmatrix} n & & 0 & & \ldots & 0 & 0 \\ & \sum_{i=1}^{m-1} n_i & & 0 & \ldots\ 0 & & 0 \\ & & \ddots & & \vdots & \iddots & \\ & & & n_1+n_2 & 0 & & \\ & & & & n_1 & & \end{pmatrix}. \tag{10.26}$$

The complex conjugate representation (dual representation) on $\mathcal{H}_n^m \cong (\mathcal{H}_n^m)^*$ is identified by the Young diagram

$$\bar{\tau}_n^m = \begin{array}{l} \\ m-1 \\ \\ \\ \end{array}\!\!\left\{\begin{array}{c} \square\cdots\square \\ \vdots\ \ \cdots\ \ \vdots \\ \underbrace{\square\cdots\square}_{n} \end{array}\right. . \tag{10.27}$$

Note that although $\bar{\tau}_n^m$ acts on $\mathcal{H}_n^m$, it is not symmetric (unless $m = 2$). We can construct the dual GT basis labeled by GT patterns $\bar{N}$ of the form (cf. Eqs. (3.21) and (10.26))

$$\bar{N} = \begin{pmatrix} n & & n & & \cdots & & & n & & 0 \\ & n & & n & \cdots & & n & & n_m & \\ & & \ddots & & \vdots & & & \iddots & & \\ & & & n & & \sum_{i=3}^m n_i & & & & \\ & & & & \sum_{i=2}^m n_i & & & & & \end{pmatrix} . \tag{10.28}$$

By Eq. (3.23), the dual GT basis again coincides with the Fock basis of $\mathcal{H}_n^m$, but modified with the phase function Eq. (3.25).

Finally, unlike the general case of arbitrary irreps of $\mathrm{SU}(m)$, the weight spaces of symmetric irreps are clearly one-dimensional: Each Fock state corresponds to one and only one Young tableau, as there are no degrees of freedom for box-labeling. Weight spaces of dual symmetric irreps have the same property by duality.

### 10.5.3 Clebsch-Gordan decomposition of the reference representation

In this section, we study the irrep decomposition of $\omega_n^m$. From the previous discussion, we have

$$\omega_n^m = \tau_n^m(\,\cdot\,)\tau_n^{m\dagger} \cong \tau_n^m \otimes \bar{\tau}_n^m\,, \tag{10.29}$$

where again complex conjugate representation is taken in the Fock basis. We can restrict our focus to the irreps of $\mathrm{SU}(m)$ (or, equivalently, its corresponding Lie algebra $\mathfrak{su}(m)$) as $\tau_n^m$ can be extended to irreps of $\mathrm{U}(m)$ using nontrivial characters of the unit circle group (roughly speaking, resulting in a multiplication by a global phase which vanishes in the conjugate action of $\mathcal{B}(\mathcal{H}_n^m)$). The decomposition of $\omega_n^m$ into irreps can be computed using *Littlewood-Richardson' rules*, a general tool to classify the decomposition of tensor product representations. We refer to Section 3.1.1 for a brief overview on how they can be employed in the context of $\mathrm{SU}(m)$.

**Lemma 38.** *Let $\tau_n^m : \mathrm{SU}(m) \to \mathrm{U}(\mathcal{H}_n^m)$ be the irreducible representation of $\mathrm{SU}(m)$ on the space of $n$ bosons distributed over $m$ modes as in Eq.* (10.24)*. Define the Young diagram*

$$\lambda_k \equiv \begin{array}{l} \\ m-1 \\ \\ \\ \end{array}\!\!\left\{\begin{array}{c} \overbrace{\square\cdots\square}^{k}\overbrace{\square\cdots\square}^{k} \\ \vdots\ \ \ddots\ \ \vdots \\ \square\cdots\square \end{array}\right. , \tag{10.30}$$

*where $\lambda_0$ and $\lambda_1$ denote the trivial irrep and the adjoint irrep of* $\mathrm{SU}(m)$*, respectively. Then, for any* $n, m \in \mathbb{N} \setminus \{0\}$*,*

$$\omega_n^m = \bigoplus_{k=0}^{n} \lambda_k \,, \tag{10.31}$$

*where each* $\lambda_k$*,* $k = 0, \ldots, n$*, appears exactly one time.*

*Proof.* We will prove the following equivalent fact by induction:

$$\omega_n^m = \lambda_n \oplus \omega_{n-1}^m \,, \quad \forall n \in \mathbb{N} \setminus \{0\} \,. \tag{10.32}$$

First, notice that

$$\omega_1^m = \; m-1 \left\{ \begin{array}{c} \square\square \\ \vdots \\ \square \end{array} \right. \oplus \mathbf{1} \equiv \lambda_1 \oplus \omega_0^m \,, \tag{10.33}$$

as $\omega_0^m = \mathbf{1}$ trivially.

The conjugate representation is associated with the tensor product of Young diagrams

$$m-1 \left\{ \begin{array}{c} \overbrace{\square \cdots \square}^{n} \\ \vdots \quad \ddots \quad \vdots \\ \square \cdots \square \end{array} \right. \otimes \underbrace{\square \cdots \square}_{n} \tag{10.34}$$

(swapping tensor factors does not influence the result). By Littlewood-Richardson' rules, we first have

$$\begin{aligned} m-1 \left\{ \begin{array}{c} \overbrace{\square \cdots \square}^{n} \\ \vdots \quad \ddots \quad \vdots \\ \square \cdots \square \end{array} \right. \otimes \overbrace{\boxed{a} \cdots \boxed{a}}^{n} = \; & m-1 \left\{ \begin{array}{c} \overbrace{\square \cdots \square}^{n}\boxed{a} \\ \vdots \quad \ddots \quad \vdots \\ \square \cdots \square \end{array} \right. \otimes \overbrace{\boxed{a} \cdots \boxed{a}}^{n-1} \\ & \oplus \; m-1 \left\{ \begin{array}{c} \overbrace{\square \cdots \square}^{n-1} \\ \vdots \quad \ddots \quad \vdots \\ \square \cdots \square \end{array} \right. \otimes \overbrace{\boxed{a} \cdots \boxed{a}}^{n-1} \,. \end{aligned} \tag{10.35}$$

Note that the second term in the r.h.s. is by definition $\omega_{n-1}^m$. Hence, we shall only prove that

$$m-1 \left\{ \begin{array}{c} \overbrace{\square \cdots \square}^{n}\boxed{a} \\ \vdots \quad \ddots \quad \vdots \\ \square \cdots \square \end{array} \right. \otimes \overbrace{\boxed{a} \cdots \boxed{a}}^{n-1} = \oplus_{k=0}^{n} \lambda_k \,. \tag{10.36}$$

For this purpose, let us consider the factor

$$\tilde{\lambda}_r^{(s)} \coloneqq \; m-1 \left\{ \begin{array}{c} \overbrace{\square \cdots \square}^{r} \overbrace{a \cdots a}^{s} \\ \vdots \quad \ddots \quad \vdots \\ \square \cdots \square \end{array} \right. . \tag{10.37}$$

Clearly, $\tilde{\lambda}_r^{(r)} = \lambda_r$ and $\tilde{\lambda}_0^{(0)} = \mathbf{1}$. Notice that

$$\begin{aligned} \tilde{\lambda}_r^{(s)} \otimes \tau_l^m &= \left( m-1 \left\{ \begin{array}{c} \overbrace{\square \cdots \square}^{r} \overbrace{a \cdots a}^{s+1} \\ \vdots \quad \ddots \quad \vdots \\ \square \cdots \square \end{array} \right. \oplus \; m-1 \left\{ \begin{array}{c} \overbrace{\square \cdots \square}^{r-1} \overbrace{a \cdots a}^{s} \\ \vdots \quad \ddots \quad \vdots \\ \square \cdots \square \end{array} \right. \right) \otimes \overbrace{a \cdots a}^{l-1} \\ &= \left( \tilde{\lambda}_r^{(s+1)} \oplus \tilde{\lambda}_{r-1}^{(s)} \right) \otimes \tau_{l-1}^m \,. \end{aligned} \tag{10.38}$$

With this notation, expanding the l.h.s. of Eq. (10.36) we get

$$\begin{aligned} \tilde{\lambda}_n^{(1)} \otimes \tau_{n-1}^m &= \left( m-1 \left\{ \begin{array}{c} \overbrace{\square \cdots \square}^{n} a \, a \\ \vdots \quad \ddots \quad \vdots \\ \square \cdots \square \end{array} \right. \oplus \; \begin{array}{c} \overbrace{\square \cdots \square}^{n-1} a \\ \vdots \quad \ddots \quad \vdots \\ \square \cdots \square \end{array} \right) \otimes \overbrace{a \cdots a}^{n-2} \\ &= \left( \tilde{\lambda}_n^{(2)} \oplus \tilde{\lambda}_{n-1}^{(1)} \right) \otimes \tau_{n-2}^m \\ &= \left( \tilde{\lambda}_n^{(3)} \oplus \tilde{\lambda}_{n-1}^{(2)} \oplus \tilde{\lambda}_{n-1}^{(2)} \oplus \tilde{\lambda}_{n-2}^{(1)} \right) \otimes \tau_{n-3}^m \\ &= \left( \tilde{\lambda}_n^{(3)} \oplus \tilde{\lambda}_{n-1}^{(2)} \oplus \tilde{\lambda}_{n-2}^{(1)} \right) \otimes \tau_{n-3}^m \\ &\vdots \\ &= \left( \tilde{\lambda}_n^{(i)} \oplus \tilde{\lambda}_{n-1}^{(i-1)} \oplus \cdots \oplus \tilde{\lambda}_{n-i+1}^{(1)} \right) \otimes \tau_{n-i}^m \\ &\vdots \\ &= \bigoplus_{i=0}^{n} \tilde{\lambda}_{n-i}^{(n-i)} \\ &= \bigoplus_{k=0}^{n} \lambda_k \,. \end{aligned} \tag{10.39}$$

In the latter, we used the merging rule for Young diagrams, see Section 3.1.1. Finally, we have

$$\omega_n^m = \sum_{k=0}^{n} \lambda_k \oplus \omega_{n-1}^m = \sum_{k=0}^{n} \lambda_k \oplus \sum_{l=0}^{n-1} \lambda_l = \lambda_n \oplus \omega_{n-1}^m \,, \tag{10.40}$$

by the merging rule again. □

For instance, we have the following explicit decomposition for $n = m = 3$:

$$\omega_3^3 = \mathbf{1} \oplus \ydiagram{2,1} \oplus \ydiagram{4,2} \oplus \ydiagram{6,3}\,, \tag{10.41}$$

since:

$$\ydiagram{3,3} \otimes \begin{array}{|c|c|c|}\hline a & a & a \\ \hline \end{array} = \left( \ydiagram{4,3} \oplus \ydiagram{2,2} \right) \otimes \begin{array}{|c|c|}\hline a & a \\ \hline \end{array} \tag{10.42}$$

$$= \left( \ydiagram{5,3} \oplus \ydiagram{3,3} \oplus \ydiagram{1,2} \right) \otimes \begin{array}{|c|}\hline a \\ \hline \end{array} \tag{10.43}$$

$$= \ydiagram{6,3} \oplus \ydiagram{4,3} \oplus \ydiagram{2,2} \oplus \mathbf{1}\,. \tag{10.44}$$

The dimension of $\lambda_k$ admits a nice closed-form expression in terms of the dimension of the number subspace,

$$\dim \mathcal{H}_k^m = \binom{k+m-1}{k}\,, \tag{10.45}$$

as follows:

**Proposition 39.** *For any $k \in \mathbb{N}$, set $d_{\lambda_k} \equiv \dim \lambda_k$. Then, the following holds:*

$$d_{\lambda_k} = \left(1 - \frac{k^2}{(k+m-1)^2}\right) (\dim \mathcal{H}_k^m)^2 = \frac{2k+m-1}{m-1} \binom{k+m-2}{k}^2 . \tag{10.46}$$

We prove this fact in Appendix B.1.

We remark that for the one-to-one correspondence of RB decays with irreps, it is important that the reference representation $\omega_n^m$ decomposes into *multiplicity-free* irreps [49, 50]. Moreover, these irreps should be of *real type*. This is the case for the irreps $\lambda_k, k = 1, \ldots, n$, because each term in the decomposition is self-dual and multiplicity free (this can also be checked using e.g. [69, Proposition 26.24], where all the complex, real, and quaternionic irreps of SU($m$) are classified). In general, both conditions are not necessarily fulfilled, which can lead to more than one decay per irrep that may also be complex (i.e. oscillating).

### 10.5.4 The passive frame operator

As the reference representation $\omega = \omega_n^m := \tau_n^m(\cdot)\tau_n^{m\dagger}$ of $G = \mathrm{U}(m)$ preserves the number of particles, $S$ acts non-trivially on the $n$-th Fock sector only, i.e.

$$S = \begin{pmatrix} \mathbf{0} & & & & & \\ & \ddots & & & & \\ & & \mathbf{0} & & & \\ & & & S^{(n)} & & \\ & & & & \mathbf{0} & \\ & & & & & \ddots \end{pmatrix}, \tag{10.47}$$

where $S^{(n)}$ is obtained via the restriction of $\mathcal{M}$ to the subspace of $n$ particles. Moreover, since $\omega_n^m$ decomposes as $\bigoplus_{k=0}^n \lambda_k$ (see Lemma 38), Schur's lemma implies [50]:

$$S^{(n)} = \bigoplus_{\lambda} S_\lambda^{(n)}, \quad S_\lambda^{(n)} = s_\lambda \mathrm{id}_\lambda, \tag{10.48}$$

where the direct sum is over all irreps of $\omega_n^m$ and, in general [50],

$$s_\lambda = d_\lambda^{-1} \operatorname{Tr}[P_\lambda \mathcal{M}] = d_\lambda^{-1} \int_\Omega d\boldsymbol{x} \, \operatorname{Tr}\left[|\boldsymbol{x}\rangle\langle\boldsymbol{x}| P_\lambda(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|)\right]. \tag{10.49}$$

Here, $d_\lambda \equiv \dim \mathcal{H}_\lambda$, with $\lambda \in \{\lambda_k\}_{k=0}^n$, and $P_\lambda$ is the corresponding projector onto its carrier space. In the second step, we used the fact that the Bochner integral commutes with the trace since the latter is a continuous linear operator in the trace norm and the trace of $[|\boldsymbol{x}\rangle\langle\boldsymbol{x}|P_\lambda(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|)]$ is finite.

### 10.5.5 Filter function for passive RB with PNR measurements

As the irrep decomposition of $\omega_n^m$ can be computed for any $n$ and $m$ (cf. Lemma 38), we can evaluate explicit expressions for the filter function. This will provide the proof of Theorem 36.

By construction, $\omega_n^m = \tau_n^m(\cdot)\tau_n^{m\dagger} \cong \tau_n^m \otimes \bar{\tau}_n^m$ acts on elements $|\boldsymbol{n}, \boldsymbol{n}\rangle$ (from here on referred as the uncoupled basis). However, as pointed out in the Section 3.1.1, the second entry shall be suitably interpreted as a basis element of $\bar{\tau}_n^m$, which requires the specification of the relative phases between states of $\tau_n^m$ and its dual. In particular, we have

$$|\boldsymbol{n}\rangle = |N\rangle = (-1)^{\varphi(N)}|\bar{N}\rangle, \tag{10.50}$$

where $|N\rangle$ is the GT pattern defined in Eq. (10.26), $|\bar{N}\rangle$ is the dual state, cf. Eq. (3.21), and the relative phase is given in Eq. (3.25). For the rest of this work, we fix the following notation: For each Fock state $|\boldsymbol{m}\rangle$, the corresponding GT pattern will be denoted with the corresponding Latin capital letter, namely the identification $|\boldsymbol{m}\rangle \equiv |M\rangle$ holds.

From previous considerations, it follows

$$\rho \cong |\boldsymbol{n}_0, \boldsymbol{n}_0\rangle = |N_0, N_0\rangle = (-1)^{\varphi(N_0)}|N_0, \bar{N}_0\rangle = (-1)^{\varphi(N_0)} \sum_{k=0}^{n} \sum_{M \in \mathrm{GT}(\lambda_k)} C_{N_0,\bar{N}_0}^{M} |M\rangle, \tag{10.51}$$

with $\{|M\rangle\}_{M\in\mathrm{GT}(\lambda_k)}$ being an orthonormal basis (referred as the coupled basis from here on) for the carrier space of $\lambda_k$. Notice that in Eq. (10.51) we do not need to specify the multiplicity index of states and Clebsch-Gordan coefficients since $\lambda_k$ is multiplicity free for each $k = 0, \dots, n$.

Then, for a fixed irrep $\lambda \in \{\lambda_k\}_{k=0}^n$, we have $P_\lambda = \sum_{M\in\mathrm{GT}(\lambda)} |M\rangle\langle M|$ and the following relation holds true:

$$P_\lambda |N_0, \bar{N}_0\rangle = \sum_{M\in\mathrm{GT}(\lambda)} C^M_{N_0,\bar{N}_0} |M\rangle\,, \tag{10.52}$$

We remark that – by the selection rules of Clebsch-Gordan coefficients Eq. (3.39) – the sum is restricted to all the basis vectors such that the associated weight corresponds to the sum of the weights of the states $|N_0\rangle$ and $|\bar{N}_0\rangle$, Cf. Eq. (3.39). Specifically, by Eq. (3.21), $C^M_{N_0,\bar{N}_0}$ is possibly nonzero provided that

$$\begin{aligned} w_j^{(M)} &= w_j^{(N_0)} + w_j^{(\bar{N}_0)} \\ &= 2\sum_{i=1}^{j} N^{(0)}_{i,j} - \left(\sum_{i=1}^{j-1} N^{(0)}_{i,j-1} + \sum_{i=1}^{j+1} N^{(0)}_{i,j+1}\right) + 2\sum_{i=1}^{j} \bar{N}^{(0)}_{i,j} - \left(\sum_{i=1}^{j-1} \bar{N}^{(0)}_{i,j-1} + \sum_{i=1}^{j+1} \bar{N}^{(0)}_{i,j+1}\right) \\ &= 2\sum_{i=1}^{j} N^{(0)}_{1,m} - \left(\sum_{i=1}^{j-1} N^{(0)}_{1,m} + \sum_{i=1}^{j+1} N^{(0)}_{1,m}\right) \\ &= 0 \end{aligned} \tag{10.53}$$

for each $j = 1, \dots, m$, i.e. $w_{N_0} + w_{\bar{N}_0} = \mathbf{0}$.

Moreover, for the $\mathbf{0}$ weight spaces, the inner multiplicity $\gamma_{\lambda_k}(\mathbf{0})$ of $\mathbf{0}$ in $\lambda_k$ can be easily computed, as we prove the following fact:

**Lemma 40.** *Let $\lambda_k$ be an irrep of $\mathrm{SU}(m)$ as in Eq. (10.30) for any $k \in \mathbb{N}$. Then,*

$$\gamma_{\lambda_k}(\mathbf{0}) = \binom{k+m-2}{k}\,. \tag{10.54}$$

We prove this fact in Appendix B.2. This provides the number of (possibly) non-zero terms in Eq. (10.52) and is relevant for the evaluation of the eigenvalues of the frame operator of passive RB with PNR measurements, for which we obtain the following simple expression:

**Theorem 41.** *Let $\lambda_k$, $k = 0, \dots, n$ be an irrep in $\omega_n^m$. For a PNR measurement setting, the eigenvalues of the frame operator of the passive RB protocol are given by*

$$s_{\lambda_k} = \frac{m-1}{2k+m-1}\gamma_{\lambda_k}(\mathbf{0})^{-1}\,, \tag{10.55}$$

*where $\gamma_{\lambda_k}(\mathbf{0})$ is as in Eq. (10.54).*

*Proof.* First, recall that a single mode (ideal) PNR detector measures the number of particles in such mode [243]. In the case of $m$ modes, the (ideal) POVM is therefore given by $\{|\mathbf{n}\rangle\langle\mathbf{n}|\}_{\mathbf{n}\in\mathbb{N}^m}$ and the (vectorized) measurement channel can be written as

$$\mathcal{M} \coloneqq \sum_{\mathbf{n}\in\mathbb{N}^m} |\boldsymbol{n},\boldsymbol{n}\rangle\langle\boldsymbol{n},\boldsymbol{n}| = \sum_{n=0}^{\infty} \sum_{n\in\mathrm{GT}(\tau_n^m)} |N,N\rangle\langle N,N|\,. \tag{10.56}$$

Denoting by $P_{\lambda_k}$ the projector onto $\lambda_k \in \hat{\omega}_n^m$, we have the following:

$$s_{\lambda_k} = \frac{1}{d_{\lambda_k}} \sum_{\boldsymbol{n}\in\mathbb{N}^m} \langle \boldsymbol{n}, \boldsymbol{n} \,|P_{\lambda_k}|\, \boldsymbol{n}, \boldsymbol{n}\rangle \tag{10.57}$$

$$= \frac{1}{d_{\lambda_k}} \sum_{N\in \mathrm{GT}(\tau_n^m)} \langle N, N \,|P_{\lambda_k}|\, N, N\rangle \tag{10.58}$$

$$= \frac{1}{d_{\lambda_k}} \sum_{N\in \mathrm{GT}(\tau_n^m)} (-1)^{2\varphi(N)} \langle N, \bar{N} \,|P_{\lambda_k}|\, N, \bar{N}\rangle \tag{10.59}$$

$$= \frac{1}{d_{\lambda_k}} \sum_{N\in \mathrm{GT}(\tau_n^m)} \sum_{M\in \mathrm{GT}(\lambda_k)} |C^M_{N,\bar{N}}|^2 \,, \tag{10.60}$$

where in the second step we used the fact that $P_{\lambda_k}$ acts non-trivially on the $n$ particle subspace, and in the fourth step we used the fact that the phases $\varphi(N)$ introduced in the labeling of GT dual patterns are integers by construction, see Eq. (3.25). Finally, recall that the non-trivial Clebsch-Gordan coefficients are determined by the selection rule $w_M = w_N + w_{\bar{N}} = 0$. Moreover, symmetric irreps of $\mathrm{SU}(m)$ –and their dual– preserve the 1-to-1 correspondence between weights and basis vectors, see Section 10.5.2. This implies

$$\sum_{N\in \mathrm{GT}(\tau_n^m)} |C^M_{N,\bar{N}}|^2 = \sum_{N\in \mathrm{GT}(\tau_n^m)} \sum_{\bar{N}'\in \mathrm{GT}(\bar{\tau}_n^m)} C^M_{N,\bar{N}'} C^M_{N,\bar{N}'} = 1 \tag{10.61}$$

by orthogonality relations, cf. Eq. (3.37). Therefore,

$$s_{\lambda_k} = \frac{\gamma_{\lambda_k}(\mathbf{0})}{d_{\lambda_k}} \tag{10.62}$$

and the assertion follows from Eq. (10.54) and Proposition 39. □

Notice that $s_{\lambda_k}$ scales exponentially in both $k$ and $m$. In particular, in the case $k = n = m$, it is proportional to the $m$-th Catalan number, and it scales as $\mathrm{O}(4^m/\sqrt{m})$ for large values of $m$.

**Theorem 42** (Restatement of Theorem 36 - PNR version)**.** *Let $\rho = |\boldsymbol{n}_0\rangle\langle \boldsymbol{n}_0| \cong |\boldsymbol{n}_0, \boldsymbol{n}_0\rangle = |N_0, N_0\rangle$ be a $m$ modes state and let $\{|\boldsymbol{n}\rangle\langle \boldsymbol{n}|\}_{\boldsymbol{n}\in\mathbb{N}^m}$ be the Fock state POVM. Let $N$ be the GT pattern associated with $\boldsymbol{n}$. Then, for a given irrep $\lambda_k \in$ in $\omega_n^m$, and assuming $s_{\lambda_k} \neq 0$,*

$$f_{\lambda_k}(\boldsymbol{n}, g) = \frac{1}{s_{\lambda_k}} \frac{(-1)^{\varphi(N_0)}}{\boldsymbol{n}!} \sum_{M\in \mathrm{GT}(\lambda_k)} C^M_{N_0,\bar{N}_0} \sum_{N'\in \mathrm{GT}(\tau_n^m)} \frac{(-1)^{\varphi(N')}}{\boldsymbol{n}'!} C^M_{N',\bar{N}'} |\mathrm{Per}(g_{\boldsymbol{n},\boldsymbol{n}'})|^2 \tag{10.63}$$

*where $s_{\lambda_k}$ is evaluated in Theorem 41, the sums are restricted to all basis states such that Eq.* (10.53) *is satisfied and $\mathrm{Per}(g_{\boldsymbol{n},\boldsymbol{m}})$ denotes the permanent of the matrix obtained by $g$ by taking $m_j$ copies of the $j$-th column of $U$ and then by taking $n_i$ copies of the $i$-th row of the resulting matrix, and we used the multi-index notation $\boldsymbol{n}! := n_1! \dots n_m!$.*

*Proof.* By Eq. (10.51), and denoting by $N_0$ and $N$ the GT patterns associated with $\boldsymbol{n}_0$ and $\boldsymbol{n}$, respectively, the filter function defined in Eq. (10.9) becomes

$$f_{\lambda_k}(N, g) = \frac{1}{s_{\lambda_k}} \langle N_0, N_0 \,|P_{\lambda_k} \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger\,|\, N, N\rangle \tag{10.64}$$

$$= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N_0)} \sum_{M\in \mathrm{GT}(\lambda_k)} C^{M}_{N_0,\bar{N}_0} \langle M\,|(\tau\otimes\bar{\tau})(g)^\dagger|N,N\rangle \tag{10.65}$$

$$= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N_0)} \sum_{M\in \mathrm{GT}(\lambda_k)} C^{M}_{N_0,\bar{N}_0} \sum_{N_1,N_2\in\mathrm{GT}(\tau_n^m)} C^{M}_{N_1,\bar{N}_2} \langle N_1,\bar{N}_2\,|\tau_n^m\otimes\bar{\tau}_n^m(g)^\dagger|N,N\rangle \tag{10.66}$$

$$= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N_0)} \sum_{M\in \mathrm{GT}(\lambda_k)} C^{M}_{N_0,\bar{N}_0} \sum_{N_1,N_2\in\mathrm{GT}(\tau_n^m)} (-1)^{\varphi(N_2)} C^{M}_{N_1,\bar{N}_2} \tag{10.67}$$
$$\times \langle N_1,N_2\,|\tau_n^m\otimes\bar{\tau}_n^m(g)^\dagger|N,N\rangle\,,$$

where in Eq. (10.64) we used Eq. (10.52) and relabeled the second entries as dual basis vectors by introducing the corresponding relative phases (Cf. Eq. (3.25)). In Eq. (10.65), we used the Clebsch-Gordan decomposition $M = \sum_{N_1,N_2} C^{M}_{N_1,\bar{N}_2}|N_1,\bar{N}_2\rangle$, and in Eq. (10.66) we relabeled $\bar{N}_2$ as a basis vector for $\tau_n^m$. In particular, the latter implies that $f_{\lambda_k}$ is manifestly related to the computation of permanents [250], as each inner product resembles the boson sampling problem when expressed in the Fock basis:

$$\langle N_1,N_2\,|\tau_n^m\otimes\bar{\tau}_n^m(g)^\dagger|N,N\rangle = \langle \boldsymbol{n}_1,\boldsymbol{n}_2\,|\tau_n^m\otimes\bar{\tau}_n^m(g)^\dagger|\boldsymbol{n},\boldsymbol{n}\rangle \tag{10.68}$$

$$= \langle \boldsymbol{n}_1\,|\tau_n^m(g)^\dagger|\boldsymbol{n}\rangle\langle \boldsymbol{n}\,|\tau_n^m(g)|\boldsymbol{n}_2\rangle \tag{10.69}$$

$$= \frac{1}{\boldsymbol{n}!\sqrt{\boldsymbol{n}_1!\boldsymbol{n}_2!}}\,\mathrm{Per}(g^\dagger_{\boldsymbol{n}_1,\boldsymbol{n}})\,\mathrm{Per}(g_{\boldsymbol{n},\boldsymbol{n}_2})\,, \tag{10.70}$$

Finally, since weights for symmetric irreps of $\mathrm{SU}(m)$ uniquely identify basis vectors, by selection rules of Clebsch-Gordan coefficients we have that $N_2 = N_1$ (see also Eq. (10.61)), and the assertion follows by plugging in Theorem 41. □

Clebsch-Gordan coefficients can be calculated in polynomial time [77] for $\approx 20$ modes before memory overhead limits the application of such algorithms [258]. We remark that –using exact formulae for CG coefficients for $\tau_n^m\otimes\bar{\tau}_n^m$ from [150]– one can compute the necessary Clebsch-Gordan coefficients for higher number of modes $m$. Hence, the computational hardness of $f_{\lambda_k}$ comes from the evaluation of the permanents appearing in Eq. (10.63).

Alternatively, $f_{\lambda_k}$ can be expressed as a linear combination of matrix coefficients of $\lambda_k$ (in the corresponding GT basis). To show this fact, we introduce the following technical result that will be used extensively in the rest of this work:

**Lemma 43.** *Let $N, X$ be GT patterns, and let $\bar{N},\bar{X}$ be their dual, respectively. Let $\tau_n^m$ be the n-particles maximally symmetric irrep of* $\mathrm{SU}(m)$ *and consider $\lambda_k \in \omega_n^m \cong \tau_n^m\otimes\bar{\tau}_n^m$. Let $P_{\lambda_k}$ be the projector onto $\lambda_k$. Then, the following holds:*

$$\langle N,\bar{N}\,|P_{\lambda_k}(\tau_n^m\otimes\bar{\tau}_n^m)(g)^\dagger|X,\bar{X}\rangle = \sum_{M\in\mathrm{GT}(\lambda_k)} C^{M}_{N,\bar{N}} \sum_{M'\in\mathrm{GT}(\lambda_k)} C^{M'}_{X,\bar{X}} \langle M\,|\lambda_k(g)^\dagger|M'\rangle\,. \tag{10.71}$$

*Proof.* By construction, $P_{\lambda_k}$ selects the $\lambda_k$-th component of $|N,\bar{N}\rangle$, which can be conveniently isolated by the Clebsch-Gordan decomposition of $\omega_n^m \cong \tau_n^m\otimes\bar{\tau}_n^m$. This implies

$$\langle N,\bar{N}\,|P_{\lambda_k}(\tau_n^m\otimes\bar{\tau}_n^m)(g)^\dagger|X,\bar{X}\rangle = \sum_{M\in\mathrm{GT}(\lambda_k)} C^{M}_{N,\bar{N}} \langle M\,|\tau_n^m\otimes\bar{\tau}_n^m(g)^\dagger|X,\bar{X}\rangle\,. \tag{10.72}$$

To compute the inner product, recall that $\tau_n^m \otimes \bar{\tau}_n^m = \bigoplus_{l=0}^n \lambda_l$ (Cf. Eq. (10.31)). In particular, observe that $M$ is a basis element in $\lambda_k$, which implies the only non trivial contributions from $\tau_n^m \otimes \bar{\tau}_n^m$ are associated with its $\lambda_k$-th component. Likewise, the only relevant contributions to the inner product coming from $|X, \bar{X}\rangle$ are associated with its restriction to $\lambda_k$ that can be expressed as

$$|X, \bar{X}\rangle\big|_{\lambda_k} = \sum_{M' \in \mathrm{GT}(\lambda_k)} C_{X,\bar{X}}^{M'} |M'\rangle \,. \tag{10.73}$$

Hence,

$$\langle M \,|\tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger|\, X, \bar{X}\rangle = \sum_{M' \in \mathrm{GT}(\lambda_k)} C_{X,\bar{X}}^{M'} \langle M \,|\lambda_k(g)^\dagger|\, M'\rangle \,, \tag{10.74}$$

from which the assertion follows. □

As mentioned before, a first consequence is the following explicit expression for the filter function:

**Corollary 44.** *For a given irrep $\lambda_k \in \hat{\omega}_n^m$, and assuming $s_{\lambda_k} \neq 0$, the following holds true:*

$$f_{\lambda_k}(\boldsymbol{n}, g) = \frac{1}{s_{\lambda_k}} (-1)^{\varphi(N_0)+\varphi(N)} \sum_{M \in \mathrm{GT}(\lambda_k)} C_{N_0,\bar{N}_0}^{M} \sum_{M' \in \mathrm{GT}(\lambda_k)} C_{N,\bar{N}}^{M'} \langle M \,|\lambda_k(g)^\dagger|\, M'\rangle \,, \tag{10.75}$$

*where the sums are restricted to all basis states such that Eq.* (10.53) *is satisfied.*

*Proof.* By Eq. (10.51), and denoting by $N_0$ and $N$ the GT patterns associated with $\boldsymbol{n}_0$ and $\boldsymbol{n}$, respectively, the filter function defined in Eq. (10.9) becomes

$$\begin{aligned} f_{\lambda_k}(N, g) &= \frac{1}{s_{\lambda_k}} \langle N_0, N_0 \,|P_{\lambda_k}(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger|\, N, N\rangle & (10.76)\\ &= \frac{1}{s_{\lambda_k}} (-1)^{\varphi(N_0)+\varphi(N)} \langle N_0, \bar{N}_0 \,|P_{\lambda_k}(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger|\, N, \bar{N}\rangle & (10.77)\\ &= \frac{1}{s_{\lambda_k}} (-1)^{\varphi(N_0)+\varphi(N)} \sum_{M \in \mathrm{GT}(\lambda_k)} C_{N_0,\bar{N}_0}^{M} \sum_{M' \in \mathrm{GT}(\lambda_k)} C_{N,\bar{N}}^{M'} \langle M \,|\lambda_k(g)^\dagger|\, M'\rangle \,. & (10.78) \end{aligned}$$

In the last line, we used Lemma 43. □

Notably, explicit expressions for the matrix elements of irreps of $\mathrm{SU}(m)$ are also available, see for instance [151, Chapter 3] for $\mathrm{SU}(2)$ and [152, Chapter 9] for $\mathrm{SU}(m)$. Moreover, numerical implementations of the bosonic realization of $\mathfrak{su}(m)$ are available [251] and matrix coefficients can be expressed as suitable permanents of $\lambda_k(g)$.

### 10.5.6 Moments of the filter function for PNR measurement settings

In this section, we provide explicit expressions for the first two moments of the filter function (10.9) w.r.t the ideal probability distribution $p(\boldsymbol{n}|g) = \langle \boldsymbol{n} \,|\omega_n^m(g)(\rho)|\boldsymbol{n}\rangle$, $\boldsymbol{n} \in \mathbb{N}^m$. In particular, the ideal second moment will provide an upper bound to the sampling complexity of the protocol, Cf. Section 10.3. Throughout this section $dg$ denotes the Haar measure on $\mathrm{SU}(m)$.

The following technical result will be useful:

**Lemma 45.** *Let $N, X$ be GT patterns, and let $\bar{N}, \bar{X}$ be their dual, respectively. Let $\tau_n^m$ be the $n$-particles maximally symmetric irrep of $\mathrm{SU}(m)$ and let $\lambda_k$ be an irrep in $\omega_n^m$. Then, the following holds:*

$$\langle X, \bar{X} \,|(\tau_n^m \otimes \bar{\tau}_n^m)(g)|\, N, \bar{N}\rangle = \sum_{j=0}^{n} \sum_{M,M' \in \mathrm{GT}(\lambda_j)} C_{X,\bar{X}}^{M} C_{N,\bar{N}}^{M'} \langle M \,|\lambda_j(g)|\, M'\rangle \,. \tag{10.79}$$

*Proof.* The expression follows immediately from the Clebsch-Gordan decomposition. More specifically, we have

$$|N, \bar{N}\rangle = \sum_{i=0}^{n} \sum_{M \in \mathrm{GT}(\lambda_i)} C_{N,\bar{N}}^{M} |M\rangle \,, \quad |M, \bar{M}\rangle = \sum_{j=0}^{n} \sum_{M' \in \mathrm{GT}(\lambda_j)} C_{X,\bar{X}}^{M'} |M'\rangle \,, \tag{10.80}$$

$$\tau_n^m \otimes \bar{\tau}_n^m = \bigoplus_{k=0}^{n} \lambda_k \,, \tag{10.81}$$

Cf. Eq. (10.51) and Eq. (10.31). Hence, since $M$ and $M'$ are basis elements of $\lambda_i$ and $\lambda_j$, respectively,

$$\langle M \,|\lambda_k(g)|\, M'\rangle \neq 0 \tag{10.82}$$

only if $i = j = k$, from which the assertion follows. □

We will also need the following standard result in the representation theory of compact groups, often referred as Schur's orthogonality relations, see [63, Thm. 5.8]: For a given irrep $\lambda$ of $\mathrm{SU}(m)$ (or, in general, of any compact group $G$), if $M_1, M_2, M_1', M_2' \in \mathrm{GT}(\lambda)$, then the following relation holds true:

$$\int dg \, \langle M_1 \,|\lambda(g)|\, M_1'\rangle \langle M_2 \,|\lambda(g)^\dagger|\, M_2'\rangle = \frac{1}{d_\lambda} \delta_{M_1,M_2} \delta_{M_1',M_2'} \,, \tag{10.83}$$

where $dg$ denotes the Haar measure on $G$.

Before we prove the main results of this section, it is worth to quickly consider the first moment $\mathbb{E}[f_{\lambda_k}]$, as the proof scheme is the same, but in the case of the second moment is hidden behind additional technical details concerning the representations involved.

**Lemma 46.** *For a PNR measurement setting, $\rho = |\boldsymbol{n}_0\rangle\langle \boldsymbol{n}_0|$ as input state, and an irrep $\lambda_k$ of $\omega^{(n)} = \tau_n^m(\,\cdot\,)\tau_n^{m\dagger}$, the following holds:*

$$\mathbb{E}[f_{\lambda_k}] = \sum_{M \in \mathrm{GT}(\lambda_k)} |C_{N_0,\bar{N}_0}^{M}|^2 \,, \tag{10.84}$$

*where $N_0$ is the GT pattern associated with $\boldsymbol{n}_0$, and $\bar{N}_0$ is its dual.*

*Proof.* Since $\rho$ is an $n$-particle state and $\omega_n^m$ is a passive transformation, the outcome of a PNR measurement must also be an $n$-particle Fock state. Hence, we have

$$\mathbb{E}[f_{\lambda_k}] \coloneqq \frac{1}{s_{\lambda_k}} \sum_{\boldsymbol{n} \in \mathcal{H}_n^m} \int dg \, \langle \boldsymbol{n}_0, \boldsymbol{n}_0 \,|P_{\lambda_k}(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger|\, \boldsymbol{n}, \boldsymbol{n}\rangle \langle \boldsymbol{n}, \boldsymbol{n} \,|(\tau_n^m \otimes \bar{\tau}_n^m)(g)|\, \boldsymbol{n}_0, \boldsymbol{n}_0\rangle \tag{10.85}$$

$$= \frac{1}{s_{\lambda_k}} \sum_{N\in \mathrm{GT}(\tau_n^m)} \int dg \, \langle N_0, \bar{N}_0 \,|P_{\lambda_k}(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger| N, \bar{N}\rangle\langle N, \bar{N}\,|(\tau_n^m \otimes \bar{\tau}_n^m)(g)|N_0, \bar{N}_0\rangle \tag{10.86}$$

$$= \frac{1}{s_{\lambda_k}} \sum_{M\in \mathrm{GT}(\lambda_k)} C^M_{N_0,\bar{N}_0} \sum_{N\in \mathrm{GT}(\tau_n^m)} \int dg \, \langle M \,|\lambda_k(g)^\dagger| N, \bar{N}\rangle\langle N, \bar{N}\,|\bigoplus_{j=0}^{n} \lambda_j(g)|N_0, \bar{N}_0\rangle \,. \tag{10.87}$$

The second line follows since the relative phases between $|M\rangle$ and $|\bar{M}\rangle$ highlighted in Eq. (3.23) are integers and they appear an even number of times. In the third step, we projected $|N_0, \bar{N}_0\rangle$ onto its $\lambda_k$-th component, see Eq. (10.52). Accordingly, the only non-trivial contribution to the integral is determined by the $\lambda_k$-th component of $\tau_n^m \otimes \bar{\tau}_n^m$. Similarly, by orthogonality relations, the integral is non-zero only if $\lambda_j = \lambda_k$. Hence, it is enough to consider the restricted Clebsch-Gordan decomposition to the $\lambda_k$-th irrep, and the following holds:

$$\mathbb{E}[f_{\lambda_k}] = \frac{1}{s_{\lambda_k}} \sum_{M\in \mathrm{GT}(\lambda_k)} C^M_{N_0,\bar{N}_0} \sum_{N\in \mathrm{GT}(\tau_n^m)} \int dg \, \langle M \,|\lambda_k(g)^\dagger| N, \bar{N}\rangle\langle N, \bar{N}\,|\lambda_k(g)|N_0, \bar{N}_0\rangle \tag{10.88}$$

$$= \frac{1}{s_{\lambda_k}} \sum_{M\in \mathrm{GT}(\lambda_k)} C^M_{N_0,\bar{N}_0} \sum_{N\in \mathrm{GT}(\tau_n^m)} \sum_{M_1,M_2,M_3\in \mathrm{GT}(\lambda_k)} C^{M_1}_{N,\bar{N}} C^{M_2}_{N,\bar{N}} C^{M_3}_{N_0,\bar{N}_0} \tag{10.89}$$

$$\times \underbrace{\int dg \, \langle M \,|\lambda_k(g)^\dagger| M_1\rangle\langle M_2\,|\lambda_k(g)|M_3\rangle}_{=\frac{1}{d_{\lambda_k}}\delta_{M,M_3}\delta_{M_1,M_2}} \tag{10.90}$$

$$= \frac{1}{d_{\lambda_k}} \frac{1}{s_{\lambda_k}} \sum_{M\in \mathrm{GT}(\lambda_k)} |C^M_{N_0,\bar{N}_0}|^2 \sum_{N\in \mathrm{GT}(\tau_n^m)} \sum_{M_1\in \mathrm{GT}(\lambda_k)} |C^{M_1}_{N,\bar{N}}|^2 \tag{10.91}$$

$$= \sum_{M\in \mathrm{GT}(\lambda_k)} |C^M_{N_0,\bar{N}_0}|^2. \tag{10.92}$$

In the second step, we expanded $|N, \bar{N}\rangle, |N_0, \bar{N}_0\rangle$ in the coupled basis, and restricted the decompositions to the $\lambda_k$-th components. In the third step, we used Schur's orthogonality relations to compute the integral, and in the final step we used the definition of the frame operator, and in particular the result in Theorem 41. □

In general, finding explicit expressions for the second moment $\mathbb{E}[f_\lambda^2]$ is more involved and the following technical result is necessary:

**Lemma 47.** *Let $\lambda_k$ be a Young diagram as in Eq.* (10.30) *labeling an irrep of* $\mathrm{SU}(m)$, $m \geq 3$. *Then,*

$$\lambda_k \otimes \lambda_k = \bigoplus_{l=0}^{k} \lambda_l^{(l+1)} \oplus \bigoplus_{l=k+1}^{2k} \lambda_l^{(2k-l+1)} \oplus L \,, \tag{10.93}$$

*where $\lambda_0 \equiv \mathbf{1}$, $\lambda_1 \equiv \mathrm{Ad}$, $\lambda_j^{(i)}$ denotes the $i$-th copy of $\lambda_j$ in $\lambda_l^{\otimes 2}$, and $L$ is a suitable direct sum of irreps which are not of the form $\lambda_l$ for any $l \in \mathbb{N}$.*

Specifically, all irreps $\lambda_l$ in $\lambda_k^{\otimes 2}$ are computed by identifying all admissible ways of combining two copies of $\lambda_k$ to a fixed shape using Littlewood-Richardson' rules. This result is proved in Appendix B.3.

Hence, we derive an explicit expression for $\mathbb{E}[f_{\lambda_k}^2]$ using Eq. (2.10):

**Theorem 48.** *For a PNR measurement setting, $\rho = |\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|$ as input state, and an irrep $\lambda_k$ of $\omega_n^m$, the following holds:*

$$\mathbb{E}[f_{\lambda_k}^2] = \frac{1}{s_{\lambda_k}^2}(-1)^{\varphi(N_0)} \sum_{N\in \mathrm{GT}(\tau_n^m)} (-1)^{\varphi(N)} g_k(N, N_0)\,, \tag{10.94}$$

*where $g_k(N, N_0)$ is a function of Clebsch-Gordan coefficients of the representations $\tau_n^m \otimes \bar{\tau}_n^m$ and $\lambda_k^{\otimes 2}$ given by*

$$g_k(N, N_0) = \sum_{l=0}^{\min(n,2k)} \frac{1}{d_{\lambda_l}} \sum_{r=1}^{m_l} \sum_{\substack{M,M'\in \mathrm{GT}(\lambda_k)\\ L,L'\in \mathrm{GT}(\lambda_k)\\ R,R'\in \mathrm{GT}(\lambda_l)}} C^{M}_{N_0,\bar{N}_0} C^{M'}_{N_0,\bar{N}_0} C^{R}_{N_0,\bar{N}_0} C^{L}_{N,\bar{N}} C^{L'}_{N,\bar{N}} C^{R'}_{N,\bar{N}} C^{R,r}_{M,M'} C^{R',r}_{L,L'} \tag{10.95}$$

*where $m_l$ is the multiplicity of $\lambda_l$ in $\lambda_k^{\otimes 2}$ as in Lemma 47 and $d_{\lambda_l} \equiv \dim \lambda_l$.*

*Proof.* For any irrep $\lambda_k \in \hat{\omega}_n^m$, and by relabeling the second entries as basis elements of the dual irrep $\bar{\tau}_n^m$, the second moment can be expressed as follows:

$$\begin{aligned}
\mathbb{E}[f_{\lambda_k}^2] &\coloneqq \frac{1}{s_{\lambda_k}^2} \sum_{\boldsymbol{n}\in\mathcal{H}_n^m} \int dg\, \langle \boldsymbol{n}_0, \boldsymbol{n}_0 | P_{\lambda_k}(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger | \boldsymbol{n}, \boldsymbol{n}\rangle^2 \langle \boldsymbol{n}, \boldsymbol{n} | \tau_n^m \otimes \tau_n^m(g) | \boldsymbol{n}_0, \boldsymbol{n}_0\rangle \\
&= \frac{1}{s_{\lambda_k}^2} \sum_{N\in \mathrm{GT}(\tau_n^m)} \int dg\, \langle N_0, N_0 | P_{\lambda_k}(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger | N, N\rangle^2 \langle N, N | \tau_n^m \otimes \tau_n^m(g) | N_0, N_0\rangle \\
&= \frac{1}{s_{\lambda_k}^2} \sum_{N\in \mathrm{GT}(\tau_n^m)} (-1)^{\varphi(N_0)+\varphi(N)} \int dg\, \langle N_0, \bar{N}_0 | P_{\lambda_k}(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger | N, \bar{N}\rangle^2 \\
&\times \langle N, \bar{N} | \tau_n^m \otimes \tau_n^m(g) | N_0, \bar{N}_0\rangle \\
&= \frac{1}{s_{\lambda_k}^2}(-1)^{\varphi(N_0)} \sum_{N\in \mathrm{GT}(\tau_n^m)} (-1)^{\varphi(N)} g_k(N, N_0)\,,
\end{aligned} \tag{10.96}$$

where

$$g_k(N, N_0) \equiv \int dg\, \langle N_0, \bar{N}_0 | P_{\lambda_k}(\tau_n^m \otimes \bar{\tau}_n^m)(g)^\dagger | N, \bar{N}\rangle^2 \langle N, \bar{N} | \tau_n^m \otimes \tau_n^m(g) | N_0, \bar{N}_0\rangle\,. \tag{10.97}$$

By Lemmas 43 and 45, we obtain

$$\begin{aligned}
g_{k,l}(N, N_0) = &\sum_{M,M'\in \mathrm{GT}(\lambda_k)} C^{M}_{N_0,\bar{N}_0} C^{M'}_{N_0,\bar{N}_0} \sum_{L,L'\in \mathrm{GT}(\lambda_k)} C^{L}_{N,\bar{N}} C^{L'}_{N,\bar{N}} \sum_{j=0}^{n} \sum_{J,J'\in \mathrm{GT}(\lambda_j)} C^{J}_{N,\bar{N}} C^{J'}_{N_0,\bar{N}_0} \\
&\times \underbrace{\int dg\, \langle M, M' | \lambda_k(g)^{\dagger\otimes 2} | L, L'\rangle \langle J | \lambda_j(g) | J'\rangle}_{\equiv I}
\end{aligned} \tag{10.98}$$

We compute the integral with Schur's orthogonality relations. Specifically, this requires the irrep decomposition of $\lambda_k^{\otimes 2}$: By Lemma 47, we have

$$\langle M, M' | \lambda_k(g)^{\dagger \otimes 2} | L, L' \rangle = \langle M, M' | \bigoplus_{l=0}^{2k} \lambda_l^{\oplus m_l}(g)^\dagger | L, L' \rangle \,, \tag{10.99}$$

where $m_l \in \{0, 1, \ldots, k\}$ is the multiplicity of $\lambda_l$ in $\lambda_k^{\otimes 2}$ worked out in Lemma 47. Then, consider the following Clebsch-Gordan decompositions:

$$|M, M'\rangle = \sum_{i=0}^{2k} \sum_{r_i=1}^{m_i} \sum_{R \in \mathrm{GT}(\lambda_i)} C_{M,M'}^{R,r_i} |R, r_i\rangle \,, \quad |L, L'\rangle = \sum_{h=0}^{2k} \sum_{r_h=1}^{m_h} \sum_{R' \in \mathrm{GT}(\lambda_h)} C_{L,L'}^{R',r_h} |R', r_h\rangle \,, \tag{10.100}$$

where $r_i, r_h$ denote the $r_i$-th and $r_h$-th copies of $\lambda_i$ and $\lambda_h$ in $\lambda_k^{\otimes 2}$, respectively. By orthogonality of irreps, it follows

$$\langle M, M' | \lambda_k(g)^{\dagger \otimes 2} | L, L' \rangle = \sum_{l=0}^{2k} \sum_{r=1}^{m_l} \sum_{R, R' \in \mathrm{GT}(\lambda_l)} C_{M,M'}^{R,r} C_{L,L'}^{R',r} \langle R, r | \lambda_l^{(r)}(g)^\dagger | R', r \rangle \,. \tag{10.101}$$

By Schur's orthogonality relations, this implies that the only non trivial contributions in $I$ are associated with irreps $\lambda_l$ which appears in the intersection of the sets of irreps of $\tau_n^m \otimes \bar{\tau}_n^m$ and $\lambda_k \otimes \lambda_k$, i.e. $j = l$ provided that $\lambda_l$ appears in both decomposition. More specifically,

$$\begin{aligned} I &= \sum_{l=0}^{2k} \sum_{r=1}^{m_l} \sum_{R, R' \in \mathrm{GT}(\lambda_l)} C_{M,M'}^{R,r} C_{L,L'}^{R',r} \int dg \, \langle R, r | \lambda_l^{(r)}(g)^\dagger | R', r \rangle \langle J | \lambda_j(g) | J' \rangle \\ &= \sum_{l=0}^{2k} \delta_{l,j} \sum_{r=1}^{m_l} \sum_{R, R' \in \mathrm{GT}(\lambda_l)} C_{M,M'}^{R,r} C_{L,L'}^{R',r} \int dg \, \langle R, r | \lambda_l^{(r)}(g)^\dagger | R', r \rangle \langle J | \lambda_l(g) | J' \rangle \\ &= \sum_{l=0}^{2k} \frac{1}{d_{\lambda_l}} \delta_{l,j} \sum_{r=1}^{m_l} \sum_{R, R' \in \mathrm{GT}(\lambda_l)} C_{M,M'}^{R,r} C_{L,L'}^{R',r} \delta_{R,J'} \delta_{R',J} \,. \end{aligned} \tag{10.102}$$

Therefore, we have

$$\begin{aligned} g_k(N, N_0) = & \sum_{M, M' \in \mathrm{GT}(\lambda_k)} C_{N_0,\bar{N}_0}^{M} C_{N_0,\bar{N}_0}^{M'} \sum_{L, L' \in \mathrm{GT}(\lambda_k)} C_{N,\bar{N}}^{L} C_{N,\bar{N}}^{L'} \sum_{j=0}^{n} \sum_{J, J' \in \mathrm{GT}(\lambda_j)} C_{N,\bar{N}}^{J} C_{N_0,\bar{N}_0}^{J'} \\ & \times \sum_{l=0}^{2k} \frac{1}{d_{\lambda_l}} \delta_{l,j} \sum_{r=1}^{m_l} \sum_{R, R' \in \mathrm{GT}(\lambda_l)} C_{M,M'}^{R,r} C_{L,L'}^{R',r} \delta_{R,J'} \delta_{R',J} \\ = & \sum_{l=0}^{\min(n,2k)} \frac{1}{d_{\lambda_l}} \sum_{r=1}^{m_l} \sum_{M, M' \in \mathrm{GT}(\lambda_k)} C_{N_0,\bar{N}_0}^{M} C_{N_0,\bar{N}_0}^{M'} \sum_{L, L' \in \mathrm{GT}(\lambda_k)} C_{N,\bar{N}}^{L} C_{N,\bar{N}}^{L'} \\ & \times \sum_{R, R' \in \mathrm{GT}(\lambda_l)} C_{N_0,\bar{N}_0}^{R} C_{N,\bar{N}}^{R'} C_{M,M'}^{R,r} C_{L,L'}^{R',r} \,, \end{aligned} \tag{10.103}$$

from which the assertion follows. □

### 10.5.7 A worked out example

In the case of 2 modes systems, Clebsch-Gordan coefficients reduce to the usual ones, and the analysis of the filter function and its moments drastically simplifies. In this section, we show explicit expressions for such a case, which will highlight some technicalities implicit in the general case of SU($m$).

In the SU(2) case, it is convenient to switch from the bosonic realization of the SU(2) algebra to its spin realization, where Clebsch-Gordan coefficients are naturally introduced. This task is accomplished by the Jordan-Schwinger map [261]: For given annihilation operators $a_1, a_2$ acting on a 2 mode system and satisfying the CCRs, the Jordan-Schwinger map is such that

$$J_1 \coloneqq \frac{1}{2}\left(a_2^\dagger a_1 + a_1^\dagger a_2\right), \quad J_2 \coloneqq \frac{1}{2}\left(a_2^\dagger a_1 - a_1^\dagger a_2\right), \quad J_3 \coloneqq \frac{1}{2}\left(a_1^\dagger a_1 - a_2^\dagger a_2\right), \tag{10.104}$$

where $[J_i, J_j] = i\epsilon_{ijk}J_k$, $\epsilon$ is the Levi-Civita's pseudo-tensor, and

$$J^2 = J_1^2 + J_2^2 + J_3^2 = \frac{n}{2}\left(\frac{n}{2}+1\right), \quad n = n_1 + n_2\,,\, n_i = a_i^\dagger a_i\,. \tag{10.105}$$

This implies the normalized states $|n_1, n_2\rangle$ correspond to the eigenstates $|jm\rangle$ of $J^2$ and $J_3$, with the identification [78, 79]

$$n_1 = j + m\,, \quad n_2 = j - m\,, \tag{10.106}$$

hence, in this section, we will consider an input state $\rho = |jm\rangle\langle jm|$ and the Fock state POVM becomes $\{|j'm'\rangle\langle j'm'|\}$, where $j' \in \frac{1}{2}\mathbb{N}$ and $m' = -j', \ldots, j'$. A spin state $|jm\rangle$ and its dual are identified by the GT patterns

$$\begin{pmatrix} 2j & & 0 \\ & j+m & \end{pmatrix}, \quad \begin{pmatrix} 2j & & 0 \\ & j-m & \end{pmatrix}, \tag{10.107}$$

respectively, which implies the following relation:

$$|jm\rangle = (-1)^{j-m}|j-m\rangle\,. \tag{10.108}$$

Moreover, given any irrep $\lambda_J$ of SU(2), the following relations hold:

$$P_J = \sum_{M=-J}^{J} |JM\rangle\langle JM|\,, \quad s_J = \frac{1}{2J+1}\,. \tag{10.109}$$

In particular, the expression for $s_J$ follows from Eq. (10.55), the fact that the inner multiplicities of SU(2) basis vectors are 1 (or, equivalently, each weight is uniquely associated with a unique weight vector).

In this case, with the identification $|x_1, x_2\rangle \mapsto |j\,l\rangle$, Eq. (10.63) becomes

$$f_J(l, g) = \frac{1}{2J+1}(-1)^{2j-m-l} C^{J0}_{jm,j-m} C^{J0}_{jl,j-l} \langle J0\,|\,\lambda_J(g)^\dagger\,|\,J0\rangle\,, \tag{10.110}$$

or, equivalently, it can be expressed as (Cf. Eq. (10.75))

$$\begin{aligned} f_J(l,g) &= \frac{(-1)^{2j-m}}{2J+1} C^{J0}_{jm,j-m} \sum_{m'=-j}^{j} (-1)^{-m'} C^{J0}_{jm',j-m'} \langle jm', j-m' \,|(\tau_n^2 \otimes \bar{\tau}_n^2)(g)^\dagger| x_1, x_2\rangle \\ &= \frac{(-1)^{2j-m}}{2J+1} C^{J0}_{jm,j-m} \sum_{m'=-j}^{j} (-1)^{-m'} C^{J0}_{jm',j-m'} |\langle x_1, x_2 \,|\tau_n^2(g)\,| n_1', n_2'\rangle|^2 \\ &= \frac{1}{2J+1} \frac{(-1)^{2j-m}}{x_1! x_2!} C^{J0}_{jm,j-m} \sum_{m'=-j}^{j} \frac{(-1)^{-m'}}{n_1'! n_2'!} C^{J0}_{jm',j-m'} |\mathrm{Per}(g_{(n_1',n_2'),(x_1,x_2)})|^2 \,, \end{aligned} \tag{10.111}$$

where we set $|jm'\rangle = |n_1', n_2'\rangle$ by the inverse Jordan-Schwinger map.

The second moment expression also simplifies significantly. First, notice that, for a given representation $\lambda_J \otimes \lambda_J$, each $\lambda_K$, with $K \in \{0, \ldots, 2J\}$, is multiplicity free as all such irreps are clearly maximally symmetric. This implies the decomposition of $\lambda_J^{\otimes 2}$ is formally the same as the one of $\tau_n^2 \otimes \bar{\tau}_n^2$, i.e.

$$\underbrace{\square \cdots \square}_{K} \otimes \underbrace{\square \cdots \square}_{K} = 1 \oplus \square\square \oplus \square\square\square\square \oplus \cdots \oplus \underbrace{\square \cdots \square}_{2K} \tag{10.112}$$

and the second moment expression of Theorem 48 simplifies to

$$\mathbb{E}[f_J^2] = \frac{1}{s_J^2} (-1)^{2j} |C^{J0}_{jm,j-m}|^2 \sum_{l=-j}^{j} (-1)^{m+l} |C^{J0}_{jl,j-l}|^2 \sum_{K=0}^{2\min(J,j)} \frac{1}{2K+1} C^{K0}_{jl,j-l} C^{K0}_{jm,j-m} |C^{K0}_{J0,J0}|^2 \,. \tag{10.113}$$

# Chapter 11

# Open problems in bosonic RB

The passive RB protocol introduced in Chapter 10 allows for SPAM robust characterization of passive Gaussian unitaries using very few samples. However, passive RB relies on the preparation of Fock states and measurements to isolate particle loss rates. Fock states, in particular, are often subjected to (partial) distinguishability [267–272]: Imperfections in state preparation, for instance, the individual particles may have different polarizations, can make the bosons distinguishable. In this regime, the system is no longer described by the standard bosonic Hilbert space, and further modeling is required to capture the correct behaviour. Another challenge of passive RB is the computational effort in post-processing that restricts concrete applications to a moderate number of modes. While the computation of Clebsch-Gordan coefficients still offers room for optimization, the computation of permanents ultimately constitutes the main bottleneck towards scalability.

In this chapter, we collect first results and outline future directions aimed at extending passive RB towards relevant noise models and alternative, more practical, implementations of bosonic RB. In Section 11.1, we briefly review how the decay rates can be used to obtain information about relevant quantum channels. A particularly notable approach is the reconstruction of tomographic information of a fixed quantum channel using RB data [220, 273, 274]. In Section 11.2, we present a first analysis of the passive RB signal in the presence of distinguishability. We derive expressions for the SPAM component of the signal when the input state consists of (partially) distinguishable bosons. These expressions can be used to benchmark the implementation of input states. Further, we discuss preliminary results using Gaussian measurements, appearing in [53], and present first steps towards passive RB using coherent states and PNR measurements.

## 11.1 Interpretation of decay rates

In Chapter 10, we discussed how one can extract decay parameters to benchmark the implementation of bosonic passive transformations. Besides particle loss, the interpretation of such parameters requires further assumptions on the noise model. Interestingly, a noise model may behave differently in different irreducible subspaces, see e.g. [275] for a discussion on leakage in a trapped-ion platform. As this is a transversal topic throughout the RB literature, in this section, we provide a brief overview in the general setting.

Beyond gate-set properties, RB techniques can be adapted to estimate the quality of the implementation of a specific gate. Let $G$ be a compact group, $\omega$ a reference representation

and $\phi$ the corresponding implementation map. A common variant is interleaved RB [205, 212], where an estimate of the quality of the implementation of a target gate $g_t$ is obtained in a SPAM-robust way (we can assume for simplicity $g_t \in G$ here). This is realized by inserting $g_t$ after every random gate in the RB sequence. Formally, the output data assumes the following form:

$$\int_G dg_1 \dots dg_l (\tilde{E}_x \,|\phi(g_{\text{inv}})\phi(g_t)\phi(g_l)\dots\phi(g_t)\phi(g_1)|\,\tilde{\rho})\,, \tag{11.1}$$

where $g_{\text{inv}} = (g_t g_l \dots g_t g_1)^{-1}$ and $\phi$ is a given implementation function. Concretely, the implementation of $g_t$ is benchmarked in a two-step procedure by first benchmarking the average gate fidelity of the implementation of $G$, and then implementing the interleaved sequence to obtain an estimate of the average gate fidelity of $g_t$. In the gate-independent scenario, this idea can be extended to obtain a tomographic reconstruction of a fixed quantum channel from average gate fidelities estimated via RB [273, 274]. However, finding rigorous guarantees is challenging, as this approach features steep exponential decays, which translates mathematically in the fact that the implementation map is not closed to a reference representation, see [49, Sec. VI.C].

An alternative approach put ideas from shadow estimation and RB together in a unified framework [220]: The samples collected from an RB experiment are post-processed into suitable correlation functions where a fixed superoperator is interleaved in post-processing. Formally, for an input state $\rho$, POVM element $E_x$, reference representation $\omega$ and a superoperator $C$, one defines

$$f_{C,\lambda}(x, g_1, \dots, g_l) \coloneqq \frac{1}{s_\lambda}(\rho\,|P_\lambda \omega(g_l)^\dagger C \omega(g_{l-1})^\dagger C \dots C\omega(g_1)|E_x)\,, \tag{11.2}$$

where $\lambda$ is an irrep in $\omega$. Here, the superoperator $C$ encodes some features of the gate set that can be summarized in the decay parameters of the estimator associated with different irreps. Then, the post-processing is formally equivalent to filtered RB: By collecting samples $\{x^{(j)}, g_1^{(j)}, \dots, g_l^{(j)}\}_{j\in T}$, one can construct the estimator

$$\hat{F}_{C,\lambda} = \frac{1}{T}\sum_{i=1}^{T} f_{\lambda,C}(x^{(j)}, g_1^{(j)}, \dots, g_l^{(j)}) \tag{11.3}$$

of $F_{C,\lambda}(l) \coloneqq \sum_x \int_G dg_1 \dots dg_l\, f_{C,\lambda}(x, g_1, \dots, g_l)\tilde{p}(g_1 \dots g_l \mid x, \rho)$, where $\tilde{p}(g_1 \dots g_l \mid x, \rho)$ is defined as in Eq. (9.29) (this can be improved using the median-of-means estimator, as in shadow estimation [220]). Fitting $\hat{F}_{C,\lambda}$ for different values of $l \in \mathbb{N}$, one can extract decay rates for each irrep $\lambda$ of $G$. We remark that, as for the filter functions and the estimators in shadow protocols, the computation of the correlation functions typically requires the simulation of the quantum experiment (restricted to the $\lambda$th irreducible subspace). However, in the same spirit as shadow estimation, the same sampled data can be reused to estimate many properties at once. Specifically, it is possible to reconstruct a unitary approximation of a quantum channel from average gate fidelities (with respect to Clifford unitaries) [220, 273, 274]. As in RB approaches, the analysis is significantly more involved with more complicated noise models. In particular, in the gate-dependent noise scenario, in principle, a perturbative analysis may shed light on the output under general gate-dependent, Markovian, time-independent noise. However, finding rigorous guarantees

on the signal form is still an open problem. In particular, it is unclear how 'strong' can the noise be (in the sense of Theorem 35) before the perturbative approach is not viable anymore. Moreover, this comes at the cost of the interpretability of the decay rates due to the inherent gauge choice issue that is common to SPAM-robust protocols. Besides such issues, in the bosonic setting, the derivation of sampling complexity guarantees is complicated by the structure of its twirling, even in the gate-independent case. How the noise affects the different irreducible subspaces is still an open question.

## 11.2 Distinguishable particles in bosonic RB

Indistinguishability, and therefore symmetry under particle exchange, is the defining property of bosons. This has immediate consequences in quantum computation, as for, instance, hardness of boson sampling is a direct consequence of indistinguishability, while it can be efficiently simulated in the regime of distinguishable particles [270, 276, 277]. Intuitively, distinguishability carries over the "which-path information" of otherwise identical particles, effectively destroying quantum interference and leading to deviations in the output statistics [278]. In the case of two particles interfering on a beam-splitter, their indistinguishability is completely characterized by the Hong-Ou-Mandel experiment, which reflects on the architecture of photonic quantum computers [160], while for larger systems lead to more complicated behaviour, where the particles may be partially distinguishable by a restricted set of internal degrees of freedom.

As in Chapter 10, we consider a finite-dimensional bosonic system of $n$ particles distributed across $m$ modes. By construction, the associated Hilbert space is maximally symmetric under permutations over the modes. This implies that the action of a passive Gaussian unitary $g \in \mathrm{SU}(m)$ on such space is described by the maximally symmetric irrep $\tau_n^m$ defined in Section 10.5.2. In the ideal case, the reference representation is $\omega_n^m \equiv \tau_n^m(\,\cdot\,)\tau_n^{m\dagger} \cong \tau_n^m \otimes \bar{\tau}_n^m = \bigoplus_{k=0}^n \lambda_k$, where the irrep decomposition follows from the Clebsch-Gordan decomposition discussed in Section 10.5.3. In this setting, we model distinguishability between the modes of $\mathcal{H}_n^m$ by introducing additional modes, corresponding to internal degrees of freedom. These may represent, for instance, the polarization of the bosons, temporal modes induced by different emission times, or differences in central frequency. In the extreme scenario, all $n$ bosons are completely distinguishable. In this case, the number of internal degrees of freedom (or 'label') is exactly $n$, so that each boson can be correlated to a unique label. Consequently, the system is described by $m \times n$ modes (or, in general, $m \times t$ modes for partial $t$-distinguishability), and the corresponding Hilbert space is a subspace of $\mathcal{H}_n^{mn}$ (respectively, $\mathcal{H}_n^{mt}$). In principle, the internal degrees of freedom are not relevant for the description of experiments using passive unitaries and PNR detectors, namely, they remain unchanged and unobserved in such experiments. However, if particles are (partially) distinguishable, by tracing out the internal degrees of freedom, one can observe decoherence in the system [279].

We model distinguishable particles by considering passive unitaries that mix the internal modes as follows: In a partially distinguishable system, let $t$ be the additional modes modeling internal degrees of freedom (in the general case, $t = n$). The internal modes are initialized in the vacuum state. Without loss of generality, if $\rho = |\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|$ with $n_{0,i} = 1$ for

each $i = 1, \dots, m$, we have

$$n_{0,i} \mapsto \boldsymbol{n}_{0,i} = (n_{0,i}, \underbrace{0, \dots, 0}_{t-1 \text{ times}}) \tag{11.4}$$

and the input state in this enlarged Hilbert space is $\tilde{\rho} = \otimes_{i=1}^{m} |\boldsymbol{n}_{0,i}\rangle\langle \boldsymbol{n}_{0,i}|$. Then, we include the action of a passive transformation $V$ on the internal modes so that the (partially distinguishable) input state we consider is

$$|\boldsymbol{n}_{0,i}\rangle \mapsto \sum_{\boldsymbol{m}_i \in \mathcal{H}^t_{n_i}} V_{\boldsymbol{n}_{0,i}}(\boldsymbol{m}_i) |\boldsymbol{m}_i\rangle \tag{11.5}$$

and set $\tilde{\boldsymbol{n}}_0 \equiv \bigotimes_{i=1}^{m} |\boldsymbol{n}_{0,i}\rangle$. Hence,

$$\begin{aligned} \tilde{\rho} = & \sum_{\substack{\boldsymbol{m}_1, \boldsymbol{l}_1 \in \mathcal{H}^t_{n_{0,1}} \\ \dots \\ \boldsymbol{m}_m, \boldsymbol{l}_m \in \mathcal{H}^t_{n_{0,m}}}} V_{\boldsymbol{n}_{0,1}}(\boldsymbol{m}_1) |\boldsymbol{m}_1\rangle\langle \boldsymbol{l}_1| V_{\boldsymbol{n}_{0,1}}(\boldsymbol{l}_1)^\dagger \otimes \cdots \otimes V_{\boldsymbol{n}_{0,m}}(\boldsymbol{m}_m) |\boldsymbol{m}_m\rangle\langle \boldsymbol{l}_m| V_{\boldsymbol{n}_{0,m}}(\boldsymbol{l}_m)^\dagger \\ \equiv & \sum_{\substack{\boldsymbol{m}_1, \boldsymbol{l}_1 \in \mathcal{H}^t_{n_{0,1}} \\ \dots \\ \boldsymbol{m}_m, \boldsymbol{l}_m \in \mathcal{H}^t_{n_{0,m}}}} \mathcal{V}_{\tilde{\boldsymbol{n}}_0}(\boldsymbol{m}_1, \dots, \boldsymbol{m}_m) |\tilde{\boldsymbol{m}}\rangle\langle \tilde{\boldsymbol{l}}| \mathcal{V}_{\tilde{\boldsymbol{n}}_0}(\boldsymbol{l}_1, \dots, \boldsymbol{l}_m)^\dagger \,, \end{aligned} \tag{11.6}$$

where $|\tilde{\boldsymbol{m}}\rangle \equiv \otimes_{i=1}^{m} |\boldsymbol{m}_i\rangle$ and $\mathcal{V}_{\tilde{\boldsymbol{n}}_0}(\boldsymbol{m}_1, \dots, \boldsymbol{m}_m) \equiv V_{\boldsymbol{n}_{0,1}}(\boldsymbol{m}_1) \otimes \cdots \otimes V_{\boldsymbol{n}_{0,m}}(\boldsymbol{m}_m)$.

We consider a POVM that is able to resolve only the external modes. Hence, the ideal POVM element $|\boldsymbol{n}\rangle\langle \boldsymbol{n}|$ with $|\boldsymbol{n}\rangle \in \mathcal{H}^m_n$ is such that

$$n_i \mapsto \sum_{\boldsymbol{n}_i \in \mathcal{H}^t_{n_i}} |\boldsymbol{n}_i\rangle \,. \tag{11.7}$$

It follows that

$$|\boldsymbol{n}\rangle\langle \boldsymbol{n}| \mapsto \bigotimes_{i=1}^{m} \left( \sum_{\boldsymbol{n}_i \in \mathcal{H}^t_{n_i}} |\boldsymbol{n}_i\rangle\langle \boldsymbol{n}_i| \right) = \sum_{\substack{\boldsymbol{n}_1 \in \mathcal{H}^t_{n_1} \\ \dots \\ \boldsymbol{n}_m \in \mathcal{H}^t_{n_m}}} |\boldsymbol{n}_1 \dots \boldsymbol{n}_m\rangle\langle \boldsymbol{n}_1 \dots \boldsymbol{n}_m| \,. \tag{11.8}$$

We can now consider a passive RB experiment where we assume the input state is partially distinguishable. In this preliminary analysis, it is enough to consider distinguishability as an effect of imperfect preparation of the input state, as it typically arises from single photons generated by different sources [280–282]. Hence, to analyze the contribution of distinguishability, it is enough to compute how the SPAM constants are thereby affected. These amount to the overlap of $\rho$ with a fixed irrep $\lambda_k$. Specifically, we consider the scenario where the probability distribution is determined by the action of $\omega_n^{m \otimes t} \equiv \tilde{\omega}$, while the filtering in the post-processing is performed using the same filter function as in Chapter 10. In this setting, the SPAM constants are given by

$$\mathrm{Tr}(A_{\lambda_k}) = (\rho \,|\, P_{\lambda_k} S^{-1} \hat{\tilde{\omega}}[\omega](\tilde{\mathcal{M}}) \,|\, \tilde{\rho}) \,, \tag{11.9}$$

where $\rho$ is the ideal input state and $\tilde{\rho}$ is the corresponding partially distinguishable state, $\hat{\tilde{\omega}}$ is the Fourier transform of the representation $\tilde{\omega}$ and $\tilde{\mathcal{M}} = \sum_{\boldsymbol{n}} |E_{\boldsymbol{n}})(E_{\tilde{\boldsymbol{n}}}|$ is the measurement

channel determined by the PNR (distinguishable) measurement that projects onto the ideal, indistinguishable, Fock state $|\boldsymbol{n}\rangle$. Then, by vectorizing with respect to the Fock basis,

$$\begin{aligned}\mathrm{Tr}(A_{\lambda_k}) = \frac{1}{s_{\lambda_k}} \int dg \sum_{\boldsymbol{n}\in\mathcal{H}_n^m} \langle \boldsymbol{n}_0, \boldsymbol{n}_0 | P_{\lambda_k} \omega(g)^\dagger | \boldsymbol{n}, \boldsymbol{n}\rangle \sum_{\substack{\boldsymbol{m}_1,\boldsymbol{l}_1\in\mathcal{H}^t_{n_{0,1}} \\ \cdots \\ \boldsymbol{m}_m,\boldsymbol{l}_m\in\mathcal{H}^t_{n_{0,m}}}} \mathcal{V}_{\tilde{\boldsymbol{n}}_0}(\tilde{\boldsymbol{m}})\mathcal{V}_{\tilde{\boldsymbol{n}}_0}(\tilde{\boldsymbol{l}})^* \sum_{\substack{\boldsymbol{n}_1\in\mathcal{H}^t_{n_1} \\ \cdots \\ \boldsymbol{n}_m\in\mathcal{H}^t_{n_m}}} \\ \times \langle \boldsymbol{n}_1 \dots \boldsymbol{n}_m, \boldsymbol{n}_1 \dots \boldsymbol{n}_m | \tilde{\omega}(g) | \boldsymbol{m}_1 \dots \boldsymbol{m}_m, \boldsymbol{l}_1 \dots \boldsymbol{l}_m\rangle\end{aligned} \tag{11.10}$$

(note that we are using the general language of filtered RB that includes non-trivial multiplicities. This is due to the structure of $\tilde{\omega}$).

By unfolding Eq. (11.10) and setting $\omega_n^m \equiv \omega$, the SPAM constants are determined by the integrals

$$\begin{aligned}I_k^{(t)} &\equiv \int_{\mathrm{U}(m)} dg\, \langle \boldsymbol{n}_0, \boldsymbol{n}_0 | P_{\lambda_k} \omega(g)^\dagger | \boldsymbol{n}, \boldsymbol{n}\rangle \langle \boldsymbol{n}_1 \dots \boldsymbol{n}_m, \boldsymbol{n}_1 \dots \boldsymbol{n}_m | \tilde{\omega}(g) | \boldsymbol{m}_1 \dots \boldsymbol{m}_m, \boldsymbol{l}_1 \dots \boldsymbol{l}_m\rangle \\ &= \int_{\mathrm{U}(m)} dg\, \langle \boldsymbol{n}_0, \boldsymbol{n}_0 | \lambda_k(g)^\dagger | \boldsymbol{n}, \boldsymbol{n}\rangle \langle \boldsymbol{n}_1 \dots \boldsymbol{n}_m, \boldsymbol{n}_1 \dots \boldsymbol{n}_m | \omega(g)^{\otimes t} | \boldsymbol{m}_1 \dots \boldsymbol{m}_m, \boldsymbol{l}_1 \dots \boldsymbol{l}_m\rangle\,,\end{aligned} \tag{11.11}$$

where the $i$th copy of $\omega$ acts on the $i$th internal modes, i.e., setting $|n_1^{(i)}, \dots, n_m^{(i)}\rangle \equiv |\boldsymbol{n}^{(i)}\rangle$ where $\boldsymbol{n}_a \equiv (n_a^{(1)}, \dots, n_a^{(t)})$, we have

$$\langle \boldsymbol{n}_1 \dots \boldsymbol{n}_m, \boldsymbol{n}_1 \dots \boldsymbol{n}_m | \omega(g)^{\otimes t} | \boldsymbol{m}_1 \dots \boldsymbol{m}_m, \boldsymbol{l}_1 \dots \boldsymbol{l}_m\rangle = \prod_{i=1}^t \langle \boldsymbol{n}^{(i)}, \boldsymbol{n}^{(i)} | \omega(g) | \boldsymbol{m}^{(i)}, \boldsymbol{l}^{(i)}\rangle\,. \tag{11.12}$$

To this end, we need the decomposition of $\omega^{\otimes t}$ that can be inferred from multiple iterations of Proposition 50. In this setting, we obtain that $I_k^{(t)}$ is a linear combination of Clebsch-Gordan coefficients associated with the relevant irrep decompositions (of $\omega$ and $\omega^{m\otimes t}$). We motivate this fact by analyzing the reference representation in the case $t = 2$, i.e., 2 internal degrees of freedom may be assigned to the particles. In this case, the relevant reference representation is

$$\omega^{\otimes 2} = \bigoplus_{k,l=0}^n \lambda_k \otimes \lambda_l\,, \tag{11.13}$$

that admits the decomposition $\sum_r \lambda_r^{m_r} \oplus R$, where $m_r$ is the multiplicity of $\lambda_r$ and $R$ is the direct sum of irreps that are not associated with Young diagrams of shape. Specifically, we can prove this result by generalizing the proof of Lemma 47 to the case of different pairs $\lambda_k$ and $\lambda_l$:

**Lemma 49.** *Let $\lambda_k$ be a Young diagram as in Eq.* (10.30) *labeling an irrep of* $\mathrm{SU}(m)$, $m \geq 3$. *Then, for each $k, l \geq 0$,*

$$\lambda_k \otimes \lambda_l = \bigoplus_{j=0}^{\min\{k,l\}} \lambda^{(j+1)}_{|k-l|+j} \oplus \bigoplus_{j=\min\{k,l\}+1}^{k+l} \lambda^{(k+l-j+1)}_{|k-l|+j} \oplus R\,, \tag{11.14}$$

*where $\lambda_0 \equiv \mathbf{1}$, $\lambda_1 \equiv \mathrm{Ad}$, $\lambda_j^{(i)}$ denotes the $i$-th copy of $\lambda_j$ in $\lambda_k \otimes \lambda_l$, and $R$ is a suitable direct sum of irreps which are not of the form $\lambda_l$ for any $l \in \mathbb{N}$.*

The proof follows from an analysis of the possible Young diagrams obtained by applying Littlewood-Richardson' rules and is discussed in Appendix B.5. Then, the following decomposition follows immediately:

**Proposition 50.** *For any $m \geq 3$ and $n \in \mathbb{N}$, $\omega_n^{m\otimes 2}$ decomposes as*

$$\omega^{\otimes 2} = \bigoplus_{k,l=0}^{n} \left[ \bigoplus_{j=0}^{\min\{k,l\}} \lambda_{|k-l|+j}^{(j+1)} \oplus \bigoplus_{j=\min\{k,l\}+1}^{k+l} \lambda_{|k-l|+j}^{(k+l-j+1)} \right] \oplus R\,. \tag{11.15}$$

Note that the multiplicities do not depend on the number of modes provided that $m \geq 3$. An explicit expression of the SPAM constants is provided in Appendix B.6 for the case $t = 2$.

In principle, the contribution of distinguishability in state-preparation can be estimated by computing the SPAM error contributions in the distinguishable and indistinguishable settings (the latter being computed in Section 10.5.6, as the SPAM constant corresponds to the expected value of the filter function). However, we note that this approach is limited in practice by the sheer amount of Clebsch-Gordan coefficients associated with the high-dimensional representations appearing in the decomposition of $\omega, \omega^{\otimes t}$, as well as by their multiplicities. This is already apparent from the decomposition of $\omega^{\otimes 2}$, c.f. the dimension formula Proposition 39. In fact, the generalization of Proposition 50 to more than 2 internal degrees of freedom is straightforward by virtue of Lemma 49. In principle, only the first $n$ irreps of the form $\lambda_k$ contribute to the SPAM constant since, following the post-processing procedure of passive RB, we filter the experimental data with respect to the irreps appearing in $\omega$. Nevertheless, the post-processing is complicated by the further multiplicities arising in $\omega^{\otimes t}$, which lead to additional non-trivial overlaps while filtering. A more detailed analysis of this scenario is left to future work.

## 11.3 Passive RB with heterodyne measurement

*The technical results shown in this section are adapted from [53, App. E]. Only formatting and structural modifications have been made.*

Throughout this section, we will use the usual multi-index notation [283, Sec. 9.1]: For elements $\boldsymbol{n}_1, \boldsymbol{n}_2 \in \mathcal{H}_n^m$, $\boldsymbol{n}_1 + \boldsymbol{n}_2$ denotes the component-wise sum. The multi-index factorial of $\boldsymbol{n} \in \mathcal{H}_n^m$ is defined as $\boldsymbol{n}! \coloneqq n_1! \dots n_m!$. Also, for a given $\boldsymbol{\alpha} \in \mathbb{C}^m$, we consider the power $\boldsymbol{\alpha}^{\boldsymbol{n}} \coloneqq \alpha_1^{n_1} \dots \alpha_m^{n_m}$, and we set $|\boldsymbol{\alpha}|^p \coloneqq \alpha_1^p + \dots + \alpha_m^p$ for $p \geq 1$. With this notation, the multi-mode coherent state $|\boldsymbol{\alpha}\rangle$ can be expanded as

$$|\boldsymbol{\alpha}\rangle = e^{-|\boldsymbol{\alpha}|^2/2} \sum_{\boldsymbol{n}\in\mathcal{F}_m} \frac{\boldsymbol{\alpha}^{\boldsymbol{n}}}{\sqrt{\boldsymbol{n}!}} |\boldsymbol{n}\rangle\,. \tag{11.16}$$

Lastly, we recall the identification between Fock states and GT patterns: we will write $|\boldsymbol{n}_i\rangle = |N_i\rangle$, meaning that $N_i = N_i(\boldsymbol{n}_i)$.

Although Gaussian experiments involving Gaussian states and measurements lead to technical challenges in the benchmarking of passive unitaries related to the dimension of the bosonic Fock state, 'partial' settings using either Gaussian states or Gaussian measurements may be considered. In this section and the following one, we provide first results in this direction.

We consider a filtered RB experiment with (balanced) heterodyne measurements, described by the POVM $\{E_{\boldsymbol{\alpha}} \equiv |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|\}_{\boldsymbol{\alpha}\in\mathbb{C}^m}\}$, where $|\boldsymbol{\alpha}\rangle$ is a $m$-mode coherent state. Specifically, we consider an experiment where we prepare a Fock input state $\rho = |\boldsymbol{n}\rangle\langle\boldsymbol{n}|$, apply a sequence of (noisy) passive Gaussian unitaries, and then perform heterodyne measurements at the end of each mode.

As before, the filter function (9.27) plays a central role and here assumes the following form:

$$f_{\lambda_k}(\boldsymbol{\alpha}, g) = \frac{1}{s_{\lambda_k}} \langle \boldsymbol{n}_0, \boldsymbol{n}_0 \,| P_{\lambda_k} \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,| \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle \,, \tag{11.17}$$

where $\rho = |\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|$ is the input state, $\lambda_k$ is an irrep in $\tau_n^m \otimes \bar{\tau}_n^m \cong \tau_n^m(\cdot)\tau_n^{m\dagger} =: \omega_n^m$ and $\boldsymbol{\alpha} \in \mathbb{C}^m$ denotes an $m$-modes coherent state.

The coherent state POVM $\{|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|\}_{\alpha\in\mathbb{C}^m}$ is informationally complete [284], which implies $s_{\lambda_k} \neq 0$ for any $\lambda_k \in \hat{\omega}_n^m$ [50]. Then, we can compute the filter function as in Eq. (10.63):

**Theorem 51** (Restatement of Theorem 36 - heterodyne version)**.** *Let $\rho = |\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|$ be a $m$ modes state and let $\{|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|\}_{\boldsymbol{\alpha}\in\mathbb{C}^m}$ be the coherent state POVM. Let $\lambda_k$ an irrep of $\tau_n^m \otimes \bar{\tau}_n^m$ as in Eq.* (10.30)*. Then, the filter function* (10.9) *is given by*

$$f_{\lambda_k}(\boldsymbol{\alpha}, g) = \frac{(-1)^{\varphi(N_0)}}{s_{\lambda_k}} \sum_{M\in \mathrm{GT}(\lambda_k)} C^M_{N_0,\bar{N}_0} \sum_{N'\in\mathrm{GT}(\tau_n^m)} (-1)^{\varphi(N')} C^M_{N',\bar{N}'} |\langle \boldsymbol{\alpha} \,| \tau_n^m(g) |\boldsymbol{n}'\rangle|^2 \,, \tag{11.18}$$

*where $|\boldsymbol{n}'\rangle = |N'\rangle$.*

*Proof.* The proof is analogous to the PNR case. By a slight generalization of Lemma 43 to include coherent state measurements, we have

$$\begin{aligned}
f_{\lambda_k}(\boldsymbol{\alpha}, g) &= \frac{1}{s_{\lambda_k}} \langle \boldsymbol{n}_0, \boldsymbol{n}_0 \,| P_{\lambda_k} \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,| \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle && (11.19)\\
&= \frac{1}{s_{\lambda_k}} (-1)^{\varphi(N_0)} \langle N_0, \bar{N}_0 \,| P_{\lambda_k} \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,| \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle && (11.20)\\
&= \frac{1}{s_{\lambda_k}} (-1)^{\varphi(N_0)} \sum_{M\in\mathrm{GT}(\lambda_k)} C^M_{N_0,\bar{N}_0} \langle M \,| \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,| \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle && (11.21)\\
&= \frac{1}{s_{\lambda_k}} (-1)^{\varphi(N_0)} \sum_{M\in\mathrm{GT}(\lambda_k)} C^M_{N_0,\bar{N}_0} \sum_{N_1,N_2\in\mathrm{GT}(\tau_n^m)} C^M_{N_1,\bar{N}_2} \langle N_1, \bar{N}_2 \,| \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,| \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle && (11.22)\\
&= \frac{1}{s_{\lambda_k}} (-1)^{\varphi(N_0)} \sum_{M\in\mathrm{GT}(\lambda_k)} C^M_{N_0,\bar{N}_0} && (11.23)\\
&\times \sum_{N_1,N_2\in\mathrm{GT}(\tau_n^m)} (-1)^{\varphi(N_2)} C^M_{N_1,\bar{N}_2} \langle N_1, N_2 \,| \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,| \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle && (11.24)\\
&= \frac{1}{s_{\lambda_k}} (-1)^{\varphi(N_0)} \sum_{M\in\mathrm{GT}(\lambda_k)} C^M_{N_0,\bar{N}_0} && (11.25)\\
&\times \sum_{N_1\in\mathrm{GT}(\tau_n^m)} (-1)^{\varphi(N_1)} C^M_{N_1,\bar{N}_1} \langle N_1, N_1 \,| \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger \,| \boldsymbol{\alpha}, \boldsymbol{\alpha} \rangle \,. && (11.26)
\end{aligned}$$

In Eq. (11.20), we used the identification with GT patterns and introduced the phases described in Eq. (3.25). In Eq. (11.21), we projected $|N_0, \bar{N}_0\rangle$ onto $\lambda_k$, c.f. Eq. (10.52). In Eq. (11.22), we applied the Clebsch-Gordan decomposition

$$|M\rangle = \sum_{N_1,N_2\in \mathrm{GT}(\tau_n^m)} C^M_{N_1,\bar{N}_2} |N_1, N_2\rangle\,. \tag{11.27}$$

In Eq. (11.23), we used again Eq. (3.25), and in Eq. (11.25) we used selection rules for Clebsch-Gordan coefficients, since $N_1, N_2 \in \mathrm{GT}(\tau_n^m)$. By the identification $|\boldsymbol{n}_1\rangle = |N_1\rangle$, we have

$$\langle N_1, N_1\,|\tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger|\boldsymbol{\alpha},\boldsymbol{\alpha}\rangle = |\langle \boldsymbol{n}_1\,|\tau_n^m(g)|\boldsymbol{\alpha}\rangle|^2\,, \tag{11.28}$$

and the assertion is proved. □

We remark that an expression analogous to Eq. (10.75) as a weighted sum of matrix coefficients of $\lambda_k$ can be worked out by considering the expansion of $|\boldsymbol{\alpha}\rangle$ in the Fock basis.

Similarly, explicit expressions for the first two moments of probability of the filter function (10.9) in the case of heterodyne measurements with respect to the ideal probability distribution is $p(\boldsymbol{\alpha}|g) = \langle \boldsymbol{\alpha}\,|\omega_n^m(g)(\rho)|\boldsymbol{\alpha}\rangle$, $\boldsymbol{\alpha} \in \mathbb{C}^m$ can be computed. In particular, the ideal second moment will provide an upper bound to the sampling complexity of the protocol, Cf. Section 10.3. As in Section 10.5.6, the proofs rely on the application of Schur's orthogonality relations (2.10). While the general functional form is similar to the PNR setting, the expressions are complicated by the decomposition of coherent states in the Fock basis. We refer to Lemma 63 and Theorem 64 for explicit statements and proofs.

From Eq. (11.18), we observe that the overlap between $|\boldsymbol{\alpha}\rangle$ and $|\boldsymbol{n}'\rangle$ can be easily computed. Hence, the filter function can be computed more efficiently for representations of moderate size. Moreover, heterodyne measurements are more easily experimentally accessible compared to PNR detectors. However, isolating loss contributions is more subtle. In fact, while this is straightforward in the PNR setting, coherent states have non-trivial overlaps with all Fock basis states, and further analysis is required with heterodyne measurements.

## 11.4 Passive RB with coherent states

Heterodyne measurements can reduce the experimental effort in passive RB, but, at the same time, introduce further challenges in the estimation of average particle loss rates and distinguishability due to the experimental setup with Fock input states. A natural, alternative approach considers coherent states instead, which can be implemented reliably in experiments. For this RB experiment, we consider a coherent input state that goes through a sequence of (noisy) passive unitaries. At the end of the sequence, we resolve the total number of particles in each mode.

Formally, let $\rho = |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|$, let $\omega_n^m \coloneqq \tau_n^m(\cdot)\tau_n^{m\dagger}$ be the usual reference representation on $\mathrm{L}(\mathcal{H}_n^m)$ and let us consider the Fock states POVM $\{|\boldsymbol{n}\rangle\langle\boldsymbol{n}|\}_{\boldsymbol{n}\in\mathbb{N}^m}$. The latter POVM implies that the eigenvalues of the frame operator are again given by

$$s_{\lambda_k} = \frac{1}{d_{\lambda_k}} \sum_{\boldsymbol{n}} \langle \boldsymbol{n}, \boldsymbol{n}\,|P_{\lambda_k}|\boldsymbol{n},\boldsymbol{n}\rangle = \frac{m-1}{2k+m-1}\binom{k+m-2}{k}^{-1}, \tag{11.29}$$

c.f. Section 10.3. This simplifies the computation of the filter function compared to the heterodyne setting, c.f. Theorem 51. In particular, using the fact that the projector $P_\lambda$ onto the $\lambda$th irrep of $\omega \equiv \omega_n^m \coloneqq \tau_n^m(\cdot)\tau_n^{m\dagger}$ commutes with $\omega$, following the same steps as in the proof of Theorem 51, we have

$$\begin{aligned}
f_{\lambda_k}(\boldsymbol{n}, g) &= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N)}\langle \boldsymbol{\alpha}, \boldsymbol{\alpha}\,|\tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger P_{\lambda_k}|N, \bar{N}\rangle \\
&= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N)} \sum_{M\in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \langle \boldsymbol{\alpha}, \boldsymbol{\alpha}\,|\tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger|M\rangle \\
&= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N)} \sum_{M\in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \sum_{N_1,N_2\in \mathrm{GT}(\tau_n^m)} C^M_{N_1,\bar{N}_2} \langle \boldsymbol{\alpha}, \boldsymbol{\alpha}\,|\tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger|N_1, \bar{N}_2\rangle \\
&= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N)} \sum_{M\in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \sum_{N_1\in \mathrm{GT}(\tau_n^m)} (-1)^{\varphi(N_1)} C^M_{N_1,\bar{N}_1} \\
&\times \langle \boldsymbol{\alpha}, \boldsymbol{\alpha}\,|\tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger|N_1, N_1\rangle \\
&= \frac{1}{s_{\lambda_k}}(-1)^{\varphi(N)} \sum_{M\in \mathrm{GT}(\lambda_k)} C^M_{N,\bar{N}} \sum_{N_1\in \mathrm{GT}(\tau_n^m)} (-1)^{\varphi(N_1)} C^M_{N_1,\bar{N}_1} |\langle \boldsymbol{\alpha}\,|\tau(g)|\boldsymbol{n}_1\rangle|^2 .
\end{aligned} \tag{11.30}$$

We outline first considerations for analyzing particle loss in this experimental setup. Recall that the photon-number distribution of a coherent state $|\boldsymbol{\alpha}\rangle$ is given by

$$|\langle \boldsymbol{\alpha}\,|\boldsymbol{n}\rangle|^2 = e^{-|\boldsymbol{\alpha}|^2}\frac{|\boldsymbol{\alpha}|^2}{\boldsymbol{n}!} \tag{11.31}$$

We remark that the number of photons in each mode is independently Poisson distributed with mean value $|\alpha_j|^2$. For simplicity, we say that the distribution of photons around the average $\|\boldsymbol{\alpha}\|_2^2 = n$ is described by the latter Poisson distribution. We also recall that the action of passive Gaussian unitaries maps coherent states to coherent states. In particular, let $|\boldsymbol{\alpha}\rangle = D(\boldsymbol{\alpha})|\boldsymbol{0}\rangle$ be a coherent state, where $D(\boldsymbol{\alpha}) \coloneqq e^{\boldsymbol{\alpha}^T\boldsymbol{a}^* - \bar{\boldsymbol{\alpha}}^T\boldsymbol{a}}$ is the multimode displacement operator introduced in Section 10.1 and $\boldsymbol{a} \equiv (a_1, \ldots, a_m)$ is the vector of annihilation operators. A passive transformation $g \in \mathrm{U}(m)$ is such that $\tau^m(g)^\dagger \boldsymbol{a}\tau^m(g) = g\cdot\boldsymbol{a}$, where $\tau^m\colon \mathrm{U}(m) \to \mathrm{U}(\mathcal{F}_m)$ is the representation of $g$ on the bosonic Fock space. Then, we have $\tau^m(g)|\boldsymbol{\alpha}\rangle = |g\cdot\boldsymbol{\alpha}\rangle \equiv |\boldsymbol{\alpha}'\rangle$ and, by unitarity, $\|\boldsymbol{\alpha}'\|_2^2 = \|\boldsymbol{\alpha}\|_2^2$.

In the lossless case, the average number of particles detected is distributed with confidence level $1-\delta$ around $\|\boldsymbol{\alpha}\|_2^2$ according to the quantile function with $n$ degrees of freedom. Let us now consider lossy gates and let $p$ be the probability of *not* losing a particle. After $l$ gates, the probability of preserving the particle number is $p^{nl}$, ignoring SPAM contributions, and the output distribution $|\langle \boldsymbol{\alpha}'\,|\boldsymbol{n}_0\rangle|^2$, where $\boldsymbol{\alpha}'$ denotes the amplitude of the coherent state after evolution (assuming only Gaussian processes) is centered around

$$\|\boldsymbol{\alpha}'\|_2^2 = p^{nl}\cdot n = \langle \hat{n}\rangle . \tag{11.32}$$

By a suitable definition of confidence intervals around the (input) mean, the output statistics can highlight photon loss events (assuming that contributions from particle gain, such as, for instance, thermal light, are negligible).

Moreover, by the Clebsch-Gordan decompositions of $\tau_n^m(\cdot)\tau_n^{m\dagger}$, we can compute the first two moments associated with the filter function with coherent states and PNR measurements, assuming that the reference representation is $\omega_n^m \coloneqq \tau_n^m(\cdot)\tau_n^{m\dagger}$.

**Theorem 52** (First moment)**.** *Let $\rho = |\alpha\rangle\langle\alpha|$ be a $m$ modes state and let $\{|\boldsymbol{n}\rangle\langle\boldsymbol{n}|\}_{\boldsymbol{n}\in\mathbb{N}^m}$ be the Fock state POVM. Let $\lambda_k$ an irrep of $\tau_n^m \otimes \bar{\tau}_n^m$. Then,*

$$\mathbb{E}[f_{\lambda_k}] = e^{-2|\boldsymbol{\alpha}|^2} \sum_{\boldsymbol{n}_1,\ldots,\boldsymbol{n}_4} \frac{\bar{\boldsymbol{\alpha}}^{\boldsymbol{n}_1+\boldsymbol{n}_2}\boldsymbol{\alpha}^{\boldsymbol{n}_3+\boldsymbol{n}_4}}{\sqrt{\boldsymbol{n}_1!\boldsymbol{n}_2!\boldsymbol{n}_3!\boldsymbol{n}_4!}}(-1)^{\varphi(N_2)+\varphi(N_4)} \sum_M C^M_{N_1,\bar{N}_2} C^M_{N_3,\bar{N}_4}\,. \tag{11.33}$$

*Proof.* By the general theory of filtered RB, we have $\mathbb{E}[f_{\lambda_k}] = (\rho\,|P_{\lambda_k}|\,\rho)$. Hence,

$$\begin{aligned}
\mathbb{E}[f_{\lambda_k}] &= \langle\alpha,\alpha\,|P_{\lambda_k}|\,\alpha,\alpha\rangle \\
&= e^{-2|\boldsymbol{\alpha}|^2} \sum_{\boldsymbol{n}_1,\ldots,\boldsymbol{n}_4} \frac{\bar{\boldsymbol{\alpha}}^{\boldsymbol{n}_1+\boldsymbol{n}_2}\boldsymbol{\alpha}^{\boldsymbol{n}_3+\boldsymbol{n}_4}}{\sqrt{\boldsymbol{n}_1!\boldsymbol{n}_2!\boldsymbol{n}_3!\boldsymbol{n}_4!}}\langle\boldsymbol{n}_1,\boldsymbol{n}_2\,|P_{\lambda_k}|\,\boldsymbol{n}_3,\boldsymbol{n}_4\rangle \\
&= e^{-2|\boldsymbol{\alpha}|^2} \sum_{\boldsymbol{n}_1,\ldots,\boldsymbol{n}_4} \frac{\bar{\boldsymbol{\alpha}}^{\boldsymbol{n}_1+\boldsymbol{n}_2}\boldsymbol{\alpha}^{\boldsymbol{n}_3+\boldsymbol{n}_4}}{\sqrt{\boldsymbol{n}_1!\boldsymbol{n}_2!\boldsymbol{n}_3!\boldsymbol{n}_4!}}(-1)^{\varphi(N_2)+\varphi(N_4)}\langle N_1,\bar{N}_2\,|P_{\lambda_k}|\,N_3,\bar{N}_4\rangle \\
&= e^{-2|\boldsymbol{\alpha}|^2} \sum_{\boldsymbol{n}_1,\ldots,\boldsymbol{n}_4} \frac{\bar{\boldsymbol{\alpha}}^{\boldsymbol{n}_1+\boldsymbol{n}_2}\boldsymbol{\alpha}^{\boldsymbol{n}_3+\boldsymbol{n}_4}}{\sqrt{\boldsymbol{n}_1!\boldsymbol{n}_2!\boldsymbol{n}_3!\boldsymbol{n}_4!}}(-1)^{\varphi(N_2)+\varphi(N_4)} \sum_M C^M_{N_1,\bar{N}_2} C^M_{N_3,\bar{N}_4}\,.
\end{aligned} \tag{11.34}$$

□

Lastly, one can show that the same analysis of the third moment as in Theorem 48 leads to the following result:

**Theorem 53.** *For a PNR measurement setting, $\rho = |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|$ as input state, and an irrep $\lambda_k$ of $\omega_n^m$, the following holds:*

$$\begin{aligned}
\mathbb{E}[f^2_{\lambda_k}] = \frac{e^{-3|\boldsymbol{\alpha}|^2}}{s^2_{\lambda_k}} \sum_N (-1)^{\varphi(N)} \sum_{N_1,\ldots,N_6} \frac{\bar{\boldsymbol{\alpha}}^{\boldsymbol{n}_1+\cdots+\boldsymbol{n}_4}\boldsymbol{\alpha}^{\boldsymbol{n}_5+\boldsymbol{n}_6}}{\sqrt{\boldsymbol{n}_1!\ldots\boldsymbol{n}_6!}}(-1)^{\varphi(N_2)+\varphi(N_4)+\varphi(N_6)} \\
\times \sum_{\lambda_l}\sum_r \sum_{M,\tilde{M}}\sum_{L_1,L_2}\sum_{M_1,M_2} \frac{1}{d_{\lambda_l}} C^M_{N,\bar{N}} C^{\tilde{M}}_{N,\bar{N}} C^{M_1}_{N_1,\bar{N}_2} C^{M_2}_{N_3,\bar{N}_4} C^{L_1,r}_{M_1,M_2} C^{L_1}_{N,\bar{N}} C^{L_2,r}_{M,\tilde{M}} C^{L_2}_{N_5,\bar{N}_6}\,.
\end{aligned} \tag{11.35}$$

We note that passive RB with coherent states is suited for experimental realizations in the context of, for instance, Gaussian boson sampling. In particular, its appeal lies in the less demanding experimental requirements and more efficient post-processing scheme compared to the scheme discussed in Chapter 10. However, so far, we assumed that we filter on the irreps associated with a specific particle-number subspace. In general, a coherent state is supported on all Fock subspaces, and the concrete implementation is complicated by the onion-like structure of the irreducible subspaces over different particle subspaces under the action of the reference representation. In particular, the reference representation acts on coherent states as $\tau^m = \bigoplus_{n=0}^{\infty} \tau_n^m$, and an irrep $\lambda_k$ appears exactly once in each subspace associated with $n \geq k$ particles. As a result, a naive filtering onto a fixed $\lambda_k$ may cause oscillations in the outcome signal induced by effective multiplicities across different particle subspaces. One possible solution comes from the observation that the structure of the bosonic Fock space induces a natural decomposition of the $\lambda_k$th isotype, and the measurement setting is effectively projecting the signal onto a number subspace. This comes at the cost of an increase in the sampling complexity. Determining the number of samples needed to isolate individual irrep contributions with high probability remains an open problem.

# Conclusions

Randomized measurements are a fundamental tool for near-term quantum computing, finding applications in estimation tasks, many-body quantum systems, and machine learning. Notably, shadow estimation and randomized benchmarking stand out as experimentally-accessible frameworks that leverage randomized measurements for efficient estimation of quantum features and SPAM-robust characterization of quantum processes. In their simplest form, these protocols often assume access to Haar random unitaries or, equivalently, unitary (group) designs. However, extending these ideas to physical platforms, for instance, photonic quantum computers, requires additional care. In these cases, the moment operator arising from random unitaries may not coincide with the one obtained from uniform twirling in the discrete settings due to the additional physical constraints on the Hilbert space.

In this thesis, we contributed to generalizations of shadow estimation and RB that go beyond group designs and, more concretely, the standard setting of random Clifford unitaries. In Chapter 6, we discussed explicit expressions and guarantees for shadow estimation with short random quantum circuits: We derived closed-form analytic expressions for the frame operator (and its inverse) associated with one round of a brickwork circuit. In particular, these can be used to calculate the classical shadow and the corresponding linear estimators. This allowed us, in contrast to numeric approaches, to explicitly work out the sample complexity of Pauli estimation, giving rise to a simple criterion to identify regimes with a scaling advantage over shadow estimation with local Clifford unitaries. Our results provide clear evidence for the potential of using short circuits in well-defined regimes, while also motivating the need for careful comparison in specific applications. Finally, we observed that the recurrence relations can be adapted to more general random quantum circuits: The generalization of our construction to arbitrary local dimensions leads to first steps towards an analytical characterization of the corresponding frame operators. Then, in Chapter 7, we turned to extensions of classical shadows to fermionic systems. Standard approaches to randomization use either matchgate unitaries [96] for efficient implementations [136] or fermionic passive transformations [142]. Motivated by common symmetries in quantum chemistry and many-body systems, one could instead consider spin-preserving fermionic (passive) Gaussian unitaries. Notably, when the total spin-squared operator $S^2$ is conserved, non-trivial multiplicities arise from the relevant representations. This complicates the classical inversion of the frame operator, as, in particular, it requires the choice of an orthonormal basis within each isotypic component. A natural candidate is the Clebsch-Gordan basis. While analytic expressions exist for certain families of Clebsch-Gordan coefficients of SU($m$), no such closed-form formulae appear to be available for the relevant irreps in the spin-adapted setting. To the best of our knowledge, the required coefficients must therefore be obtained numerically, complicating the classical post-processing phase.

Our next major contribution lies within the randomized benchmarking framework, discussed in Part III. We introduced passive RB, the first SPAM-robust protocol for the characterization of bosonic passive transformations. While a naive adaptation of discrete RB to this setting would result in complicated signals, we combined techniques from filtered RB with careful choices of initial state and measurement to propose an experimental setting in which a meaningful benchmark is possible. By using collision-free $n$-particle states as input and PNR measurements, we effectively restricted the dynamics to a finite-dimensional setting in which the RB signal consists of $(n+1)$ decays that can be isolated with filtering techniques by projecting onto the relevant invariant subspaces. We showed that estimating a constant number of these decays suffices to produce a meaningful benchmark for passive transformations on $n$ particles, and the same procedure can be used to estimate particle loss rates. In addition, by computing the relevant variances, we observed that the sampling complexity of passive RB scales very mildly with the number of modes, hinting that meaningful experiments are possible with a small number of samples. The primary bottleneck is the computation of the filter functions, which requires the calculation of Clebsch-Gordan coefficients and the simulation of boson sampling experiments. We expect this is feasible for a moderate and experimentally interesting number of particles, in analogy with the simulation of random circuit sampling in discrete systems, by speeding up the computation of Clebsch-Gordan coefficients using symmetries [285], and reducing the permanents to the relevant irreps. Ultimately, however, the scaling is limited by the computation of permanents in post-processing. This limitation is not a proof artifact, as it is intrinsic to the experimental setting, much like the classical hardness of random circuit sampling [229]. We also discussed an extension of the mathematical framework of passive RB to incorporate (partially) distinguishable bosons, which primarily arises from imperfections in state preparation. Lastly, we outlined preliminary results that address the post-processing bottleneck of passive RB. We considered experimentally convenient setups that replace either the input state or the measurement with Gaussian resources, and provided initial results by computing the first two moments of the associated filter functions. In the setting with coherent input states, distinguishability effects from state preparation become negligible. However, the analysis of lossy processes becomes more subtle because coherent states do not have a fixed particle number. In fact, the nested irrep structure across different particle-number subspaces may induce multiplicities in the filtered RB signals. The analysis of a post-processing strategy that resolves these effects remains an open direction for future work.

# Part IV

# Appendices

# Appendix A

# Additional calculations for shadow estimation with brickwork circuits

## A.1 Another take on the variance bound

In this section, we provide an alternative proof of the bound in Eq. (6.5) in the case of BW circuits with periodic boundary conditions that relies on the 3-design property of the multiqubits Clifford group. In particular, it is based on the following result:

**Lemma 54.** *Let $n \in \mathbb{N}$ and let $d = 2^n$ be the dimension of a $n$-qubits system. If $0 \neq v \in \mathbb{F}_2^{2n}$, then*

$$\mathbb{E}_{U \in \mathrm{Cl}_n(2)} U^{\otimes 3} \left( W(v)^{\otimes 2} \otimes W(u) \right) (U^\dagger)^{\otimes 3} = \frac{1}{d^2 - 1} \delta_{u,0} \left( d\, \mathbb{F} - \mathbb{1}_{d^2} \right) \otimes \mathbb{1}_d \quad \forall u \in \mathbb{F}_2^{2n} . \tag{A.1}$$

*Moreover,*

$$\mathbb{E}_{U \in \mathrm{Cl}_n(2)} U^{\otimes 3} \left( \mathbb{1}_d^{\otimes 2} \otimes W(u) \right) (U^\dagger)^{\otimes 3} = \delta_{u,0} \mathbb{1}_{d^3} \quad \forall u \in F_2^{2n} . \tag{A.2}$$

*Proof.* First, we recall notations for the phase space representation of Clifford operators, c.f. Section 3.5.

Let $[\cdot, \cdot] : \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \to \mathbb{F}_2$ be the standard symplectic product over $\mathbb{F}_2^{2n}$. Let $\tilde{\alpha}_g : \mathbb{F}_2^{2n} \to \mathbb{Z}_4$ be a centre fixing automorphism of the associated Heisenberg-Weyl group, where $g \in \mathrm{Sp}(2n)$. One can prove that $\tilde{\alpha}_g = \alpha_g + [w, \cdot]$, where $\alpha_g : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ is a suitable function satisfying the compatibility condition $\alpha_g(0) = 0$ [90, Sec. 3.3]. Notice also that $|\mathrm{Cl}_n(2)| = d^2 |\mathrm{Sp}(2n)|$.

With these notations, the action of $U \in \mathrm{Cl}_n(2)$ on Weyl operators can be written as

$$U W(v) U^\dagger \coloneqq \chi([a, v] + \alpha_g(v)) W(g(v)) , \tag{A.3}$$

where $\chi(v) \coloneqq i^{-v_z \cdot v_x}$ denotes the character of $W(v)$.

Hence,

$$\begin{aligned}
&\mathbb{E}_{U\in \mathrm{Cl}_n(2)} U^{\otimes 3}\left(W(v)^{\otimes 2}\otimes W(u)\right)(U^\dagger)^{\otimes 3} \\
&\quad= \frac{1}{|\mathrm{Cl}_n(2)|}\sum_{a\in\mathbb{F}_2^{2n}}\chi([a,2v+u])\sum_{g\in \mathrm{Sp}(2n)}\chi(2\alpha_g(v)+\alpha_g(u))W(g(v))^{\otimes 2}\otimes W(g(u)) \\
&\quad= \frac{1}{2^{2n}}\sum_{a\in\mathbb{F}_2^{2n}}\chi([a,u])\frac{1}{|\mathrm{Sp}(2n)|}\sum_{g\in \mathrm{Sp}(2n)}\chi(\alpha_g(u))W(g(v))^{\otimes 2}\otimes W(g(u)) \\
&\quad= \frac{1}{|\mathrm{Sp}(2n)|}\,\delta_{u,0}\sum_{g\in \mathrm{Sp}(2n)} W(g(v))^{\otimes 2}\otimes W(g(u)) \\
&\quad= \frac{1}{|\mathrm{Sp}(2n)\cdot v|}\,\delta_{u,0}\sum_{w\in \mathrm{Sp}(2n)\cdot v} W(w)\otimes W(w)\otimes \mathbb{1}_2\,.
\end{aligned} \tag{A.4}$$

Going from the third to the fourth line, we used $\sum_{a\in\mathbb{F}_2^{2n}}\chi([a,u]) = d^2\delta_{u,0}$. In the last step, we wrote the average over $\mathrm{Sp}(2n)$ as an average over the orbit of $v$ under $\mathrm{Sp}(2n)$. Notice that, since $v\neq 0$, $\mathrm{Sp}(2n)$ acts transitively on $\mathbb{F}_2^{2n}\setminus 0$ [90], the average over such orbit can be rewritten as an average over $\mathbb{F}_2^{2n}\setminus 0$. Moreover, recalling that the flip operator has the following Pauli expansion:

$$\mathbb{F} = \frac{1}{d}\sum_{w\in\mathbb{F}_2^{2n}} W(w)\otimes W(w)\,, \tag{A.5}$$

it holds that

$$\mathbb{E}_{U\in \mathrm{Cl}_n(2)} U^{\otimes 3}\left(W(v)^{\otimes 2}\otimes W(u)\right)(U^\dagger)^{\otimes 3} = \frac{1}{d^2-1}\,\delta_{u,0}\,(d\mathbb{F}-\mathbb{1}_{d^2})\otimes\mathbb{1}_d. \tag{A.6}$$

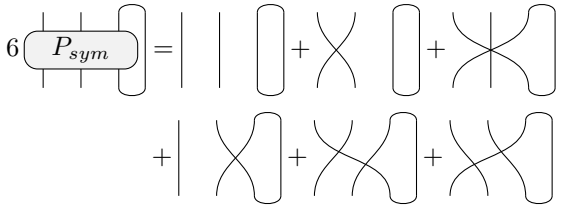
If $v=0$, the assertion follows trivially from previous considerations. □

We will also need the following calculation:

**Lemma 55.** *Given two copies of a system of* 3 *qubits, it holds*

$$\mathrm{Tr}_3\, P_{\mathrm{sym}^3} = \frac{d+2}{6}\,(\mathbb{1}+\mathbb{F})\,. \tag{A.7}$$

*Proof.* We prove the latter using tensor network diagrams. First, let us consider the decomposition $P_{\mathrm{sym}^3} = \frac{1}{6}\left(\mathbb{1}+P_{(1,2)}+P_{(1,3)}+P_{(2,3)}+P_{(1,2,3)}+P_{(1,3,2)}\right)$, $P_{(\cdot)}$ are unitary operators associated with elements of the permutation group $\mathfrak{S}_3$, and each $a\in\mathfrak{S}_3$ is represented in cyclic notation. Then,




$$= (d+2)(\mathbb{1}+F)\,.$$

□

**Proposition 56.** *For any state $\rho$, estimate $W(v)$ using BW shadows with periodic boundary conditions. Then, the variance of the estimator depends only on $v \in \mathbb{F}_2^{2n}$, and*

$$\sigma^2_{\mathrm{BW}}(v) \leq \frac{1}{(v\,|S|\,v)}\,. \tag{A.8}$$

*Proof.* In the following, we will denote by $D$ the cyclic shift operator between Hilbert spaces as before, so that a random brickwork unitary is given by $U = DU_2D^\dagger U_1$, where $U_i,\ i = 1, 2$, is the tensor product of two-local Haar random unitaries. For a given operator $A \in \mathrm{L}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, we will also consider the operator acting on three copies of two qubit sites $A_{(3)} \coloneqq A \otimes A \otimes A \in \mathrm{L}(\mathbb{C}^8 \otimes \mathbb{C}^8)$.

According to the shadow estimation protocol, we estimate the expectation value $\mathrm{Tr}[W(v)\rho]$ of some Pauli observable $W(v)$ by measuring $\rho$ many times in the computational basis after having applied $U \sim \mu$, where $\mu$ is a probability measure on the ensemble of BW operators. Then, a single such sample has a variance $\sigma^2_{\mathrm{BW}}(v, \rho)$ bounded as

$$\begin{aligned}
\sigma^2_{\mathrm{BW}}(v,\rho) &\coloneqq \sum_i \mathbb{E}_{U\sim\mu}(W(v)\,|\tilde{E}_{i,U})^2(E_{i,U}\,|\rho) - \mathrm{Tr}[W(v)\rho]^2 \\
&\leq \sum_i \mathbb{E}_{U\sim\mu}\,\mathrm{Tr}\Big[S^{-1}(W(v))U^\dagger E_i U\Big]^2\ \mathrm{Tr}\Big[U^\dagger E_i U\rho\Big] \\
&= d\,\mathbb{E}_{U\sim\mu}\,\mathrm{Tr}\Big[U^{\otimes 3\dagger}|0\rangle\langle 0|^{\otimes 3}U^{\otimes 3}\left(S^{-1}(W(v))^{\otimes 2}\otimes\rho\right)\Big] \\
&= \frac{d}{(v\,|S|\,v)^2}\,\mathbb{E}_{U\sim\mu}\,\mathrm{Tr}\Big[U^{\otimes 3\dagger}|0\rangle\langle 0|^{\otimes 3}U^{\otimes 3}\left(W(v)^{\otimes 2}\otimes\rho\right)\Big] \\
&= \frac{1}{(2\sqrt{5})^n}\frac{d}{(v\,|S|\,v)^2}\,\mathbb{E}_{U_2}\,\mathrm{Tr}\Big[P_{\mathrm{sym}^3}^{\otimes n/2}D_{(3)}\,U_2^{\otimes 3}\left(D_{(3)}^\dagger W(v)^{\otimes 2}\otimes\rho\,D_{(3)}\right)U_2^{\otimes 3\dagger}D_{(3)}^\dagger\Big]\,,
\end{aligned} \tag{A.9}$$

where in the last step we applied again Eq. (3.60) and $U = DU_2D^\dagger U_1$. Notice that $P_{\mathrm{sym}^3}$ acts on triples of two neighboring qubit sites.

Consider now the expansion in the Pauli basis $\rho = \sum_{u\in\mathbb{F}_2^{2n}} c_u W(u)$, where $c_u \coloneqq \frac{1}{d}\,\mathrm{Tr}(W(u)\rho)$, and for any $w \in \mathbb{F}_2^{2n}$ consider the decomposition

$$D^\dagger W(w) D = W(w_{2,3}) \otimes \cdots \otimes W(w_{n,1})\,, \tag{A.10}$$

which agrees with the structure of the second layer of the BW circuit. Then, by Lemma 54, we have

$$\mathbb{E}_{U_2}U_2^{\otimes 3}\left(D_{(3)}^\dagger W(v)^{\otimes 2}\otimes W(u)\,D_{(3)}\right)U_2^{\otimes 3\dagger} = \delta_{u,0}\bigotimes_{i\in[n/2]} Q_{\tilde{v}_i}\otimes\mathbb{1}_d\,, \tag{A.11}$$

from which it follows

$$\sigma^2(v,\rho) \leq \frac{1}{(2\sqrt{5})^n}\frac{d}{(v\,|S|\,v)^2}\,c_0\ \mathrm{Tr}\left[P_{\mathrm{sym}^3}^{\otimes n/2}\ D_{(3)}\bigotimes_{i\in[n/2]} Q_{\tilde{v}_i}\,D_{(3)}^{-1}\otimes\mathbb{1}_d\right], \tag{A.12}$$

where $Q_{\tilde{v}_i}$ is defined in Eq. (6.15). Hence, $\sigma^2(v,\rho) \equiv \sigma^2(v)$, since $c_0 = 1/d$. According to Lemma 54, this means that each Clifford unitary in the second layer depolarizes any dependency from the corresponding two-qubits Weyl operator appearing in the decomposition of

$\rho$ in the Pauli basis; periodic boundary conditions ensure that this applies to each pair of qubits. Finally, by Lemma 55,

$$\begin{aligned}\sigma^2(v) &\leq \frac{1}{(2\sqrt{5})^n}\frac{1}{(v\,|S|\,v)^2}\ \mathrm{Tr}\left[\mathrm{Tr}_3(P_{\mathrm{sym}^3}^{\otimes n/2})\ D_{(2)}\bigotimes_{i\in[n/2]} Q_{\tilde{v}_i}\,D_{(2)}^{-1}\right]\\ &= \frac{1}{(2\sqrt{5})^{2n}}\frac{1}{(v\,|S|\,v)^2}\ \mathrm{Tr}\left[(\mathbb{1}+\mathbb{F})^{\otimes n/2}\ D_{(2)}\bigotimes_{i\in[n/2]} Q_{\tilde{v}_i}\,D_{(2)}^{-1}\right]\\ &= \frac{1}{(v\,|S|\,v)}\,,\end{aligned} \tag{A.13}$$

□

Finally, notice that Lemma 54 does not hold for arbitrary values of the local dimension. Indeed, in odd dimensions, the flip operator has the Weyl expansion

$$\mathbb{F} = \frac{1}{d}\sum_{v\in\mathbb{F}_p^2} W(v)\otimes W(-v)\,, \tag{A.14}$$

meaning the operator $\frac{1}{d}\sum_{v\in\mathbb{F}_2^{2n}} W(v)\otimes W(v)$ admits a nice expression for fields of characteristic 2 only, and the proof of Proposition 56 holds for qubit systems only.

## A.2 Tensor networks for Lemma 28 and 29

In this section, we show how $t_1, t_2, t_3$ (respectively, $t_1, t_2$) appearing in Lemma 28 (respectively, Lemma 29) can be written as a system of recurrence relations using tensor networks.

First, notice that each operator in the traces Eqs. (6.7) and (6.8) acts on two copies of 2 qubits. That means that each brick is represented by two overlapping copies, see Fig. A.1. Next, given (the two copies of) a brick, we set for notational purpose

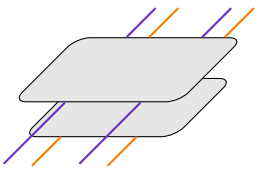
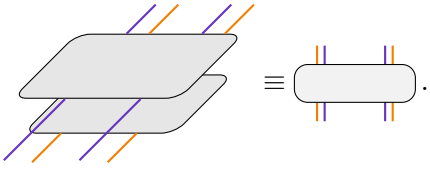


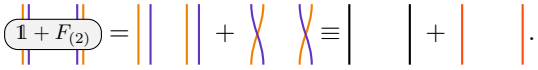
Figure A.1: Each local operator corresponds to two overlapping copies of a brick in the BW circuit.



Now notice that each brick is made up of identities and flips, the latter is usually represented as

$$\mathbb{F} = \quad . \tag{A.15}$$

Finally, $\mathrm{t}_{\mathrm{pb}}(n)$ and $\mathrm{t}_{\mathrm{ob}}(n)$ will be simplified exploiting linearity and separability of bricks. For this purpose, and to simplify the notation, we rewrite each pair of lines corresponding to the same qubit as a single one. In particular, if two lines are straight (the identity operator is applied), we summarize them as a single black line, otherwise as a red line when the flip operator is applied. For instance, for a brick $\mathbb{1} + \mathbb{F}$ in the first layer of the circuit (here $\mathbb{F} \equiv \mathbb{F}_{(2)}$ for simplicity), we have

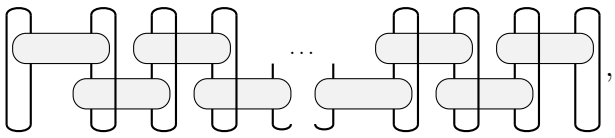



### A.2.1 Proof of relations (6.23) and (6.24)

We show how to derive recurrence relations in Lemma 28. First, recall the following definitions:

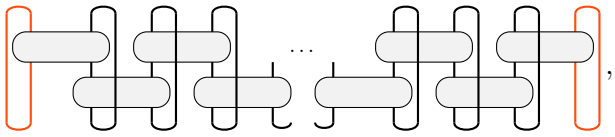
$$t_1(n) \coloneqq \mathrm{Tr}\left[\left(\mathbb{1} \otimes \left(\mathbb{1} + \mathbb{F}_{(2)}\right)^{\otimes n/2-1} \otimes \mathbb{1}\right)\left(4\mathbb{F}_{(2)} - \mathbb{1}\right)^{\otimes n/2}\right] \tag{A.16}$$

$$= \tag{A.17}$$



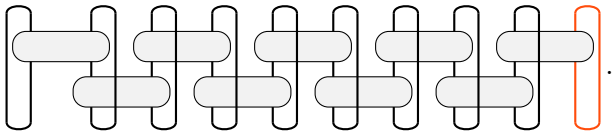
$$t_2(n) \coloneqq \mathrm{Tr}\left[\left(\mathbb{F} \otimes \left(\mathbb{1} + \mathbb{F}_{(2)}\right)^{\otimes n/2-1} \otimes \mathbb{F}\right)\left(4\mathbb{F}_{(2)} - \mathbb{1}\right)^{\otimes n/2}\right] \tag{A.18}$$

$$= \tag{A.19}$$

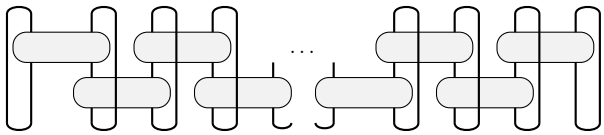


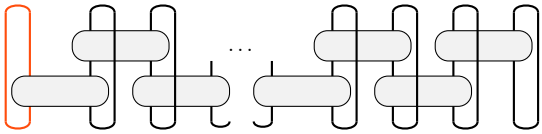
$$t_3(n) \coloneqq \mathrm{Tr}\left[\left(\mathbb{1} \otimes \left(\mathbb{1} + \mathbb{F}_{(2)}\right)^{\otimes n/2-1} \otimes \mathbb{F}\right)\left(4\mathbb{F}_{(2)} - \mathbb{1}\right)^{\otimes n/2}\right] \tag{A.20}$$

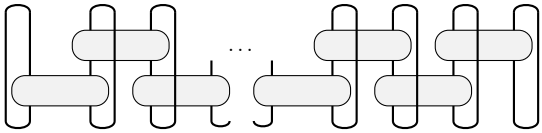
$$= \tag{A.21}$$

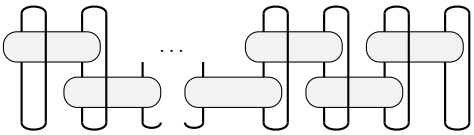
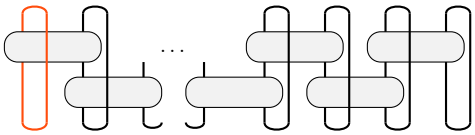


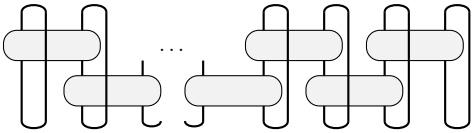
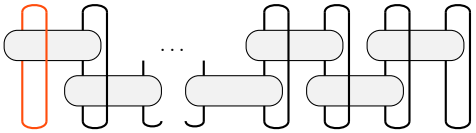
Therefore, we have

$t_1(n) =$ 

$= 8$ 

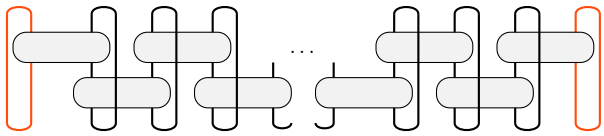
$- 4$ 

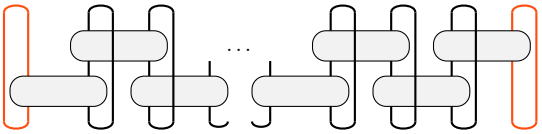
$= 16$  $+ 32$ 

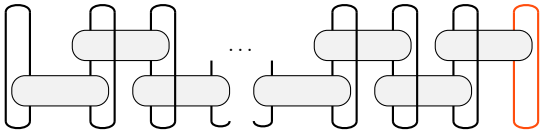
$- 16$  $- 8$ 

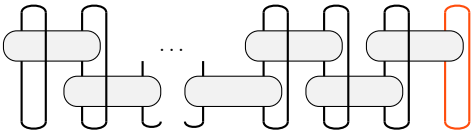
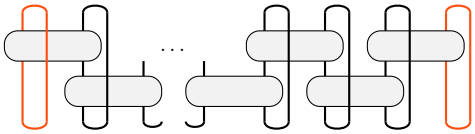
$= 24\, t_3(n-2)\,.$

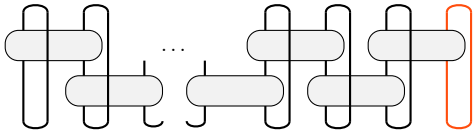
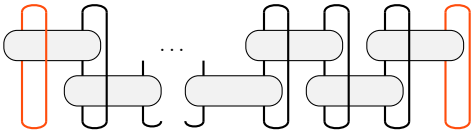
Similarly, for $t_2$ we obtain

$t_2(n) =$ 

$= 16$ 

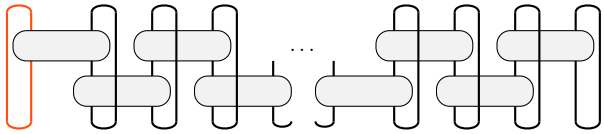
$- 2$ 

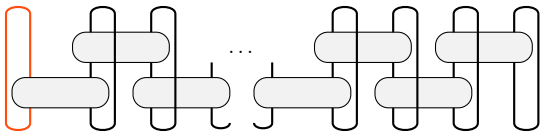
$= 32$  $+ 64$ 

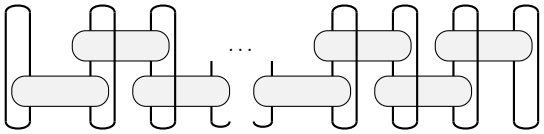
$- 8$  $- 4$ 

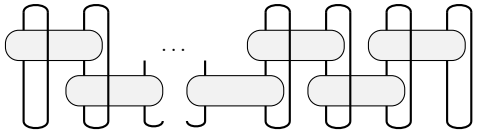
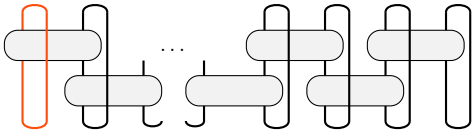
$= 24\, t_3(n-2) + 60\, t_2(n-2)\,.$

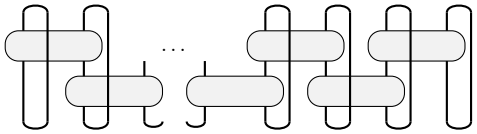
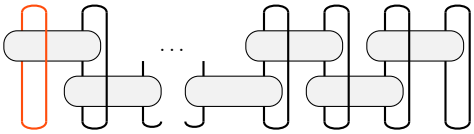
Finally, for $t_3$ a similar calculation yields

$t_3(n) =$ 

$= 16$ 

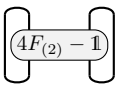
$- 2$ 

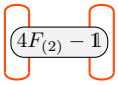
$= 32$  $+ 64$ 

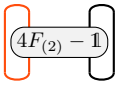
$- 8$  $- 4$ 

$= 24\, t_1(n-2) + 60\, t_3(n-2)\,.$

Moreover,

$t_1(2) =$  $= 0\,,$

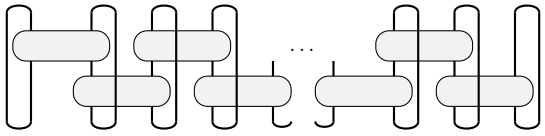
$t_2(2) =$  $= 60\,,$

$t_3(2) =$  $= 24\,.$

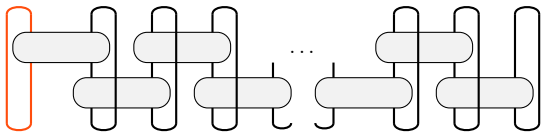
### A.2.2 Proof of relations (6.27) and (6.28)

Recall that, in this case,

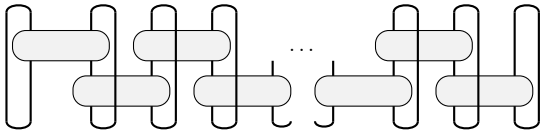
$$t_1(n) \coloneqq \mathrm{Tr}\Big[\Big\{\mathbb{1}_4 \otimes (\mathbb{1} + \mathbb{F}_{(2)})^{\otimes(n/2-1)}\Big\}\Big\{(4\mathbb{F}_{(2)} - \mathbb{1})^{\otimes(n/2-1)} \otimes \mathbb{1}_4\Big\}\Big] \tag{A.22}$$

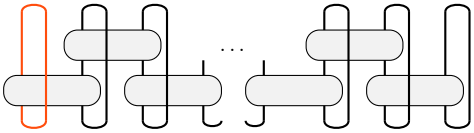
$=$  , (A.23)

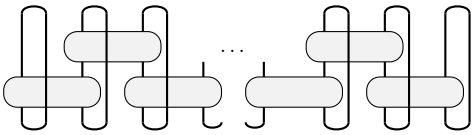
$$t_2(n) \coloneqq \mathrm{Tr}\Big[\Big\{\mathbb{F} \otimes (\mathbb{1} + \mathbb{F}_{(2)})^{\otimes(n/2-1)}\Big\}\Big\{(4\mathbb{F}_{(2)} - \mathbb{1})^{\otimes(n/2-1)} \otimes \mathbb{1}_4\Big\}\Big] \tag{A.24}$$

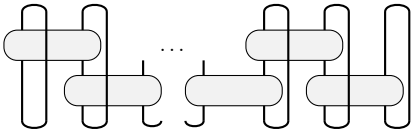
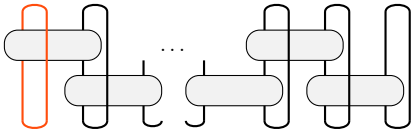
$=$  . (A.25)

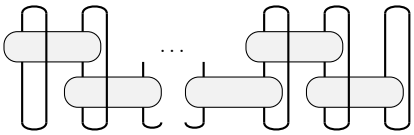
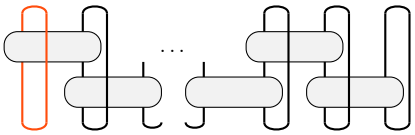
For the first trace we have

$t_1(n) =$ 

$= 8$ 

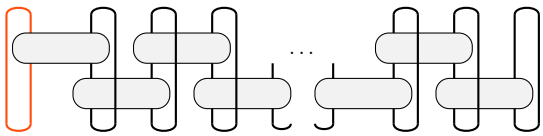
$- 4$ 

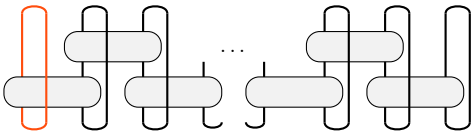
$= 16$  $+ 32$ 

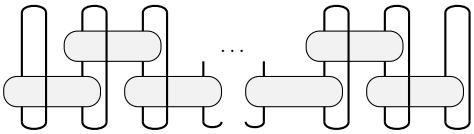
$- 16$  $- 8$ 

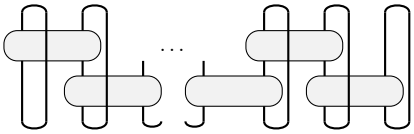
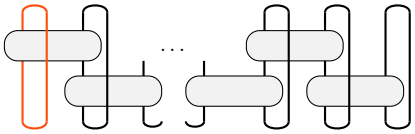
$= 24\, t_2(n-2)\,.$

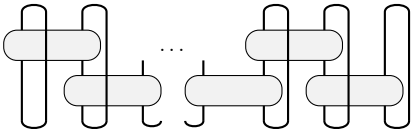
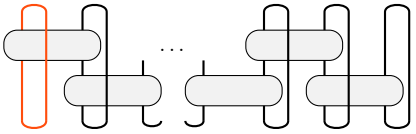
Similarly,

$t_2(n) =$ 

$= 16$ 

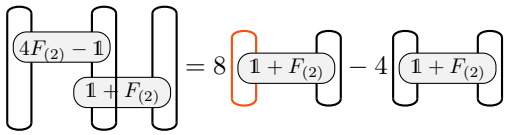
$- 2$ 

$= 32$  $+ 64$ 

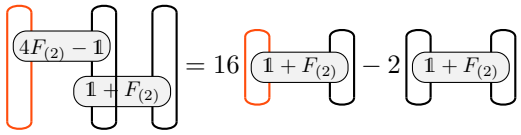
$- 8$  $- 4$ 

$= 24\, t_1(n-2) + 60\, t_2(n-2)\,.$

Moreover,

$t_1(4) =$ 


$= 48\,,$

$t_2(4) =$ 


$= 216\,.$

## A.3 Numeric bounds on the variance

For the construction of the classical shadow, the exact expressions stated in Theorem 26 are required. We here derive simpler (and looser) bounds for controlling the variance.

Let us start with the case relevant for $\mathrm{part}_{\mathrm{BW}}(v) = (n/2)$. Set $a \coloneqq (\sqrt{41}+5)^{1/2}/(5\sqrt{2})$ and $b \coloneqq \mathrm{i}(\sqrt{41}-5)^{1/2}/(5\sqrt{2})$. We have $2 < 1/a < 2.1$, $\frac{1}{1-|b/a|^2} \leq 1.2$ and $\frac{1}{1+|b/a|^2} \geq .89$. Further, since $|b/a| < 1$ and assuming $n \geq 2$ and $n$ even,

$$\frac{1}{\Sigma_{\mathrm{pb}}(n)} = \frac{1}{a^n + b^n} = \frac{1}{a^n}\frac{1}{1+(b/a)^n} \leq \frac{1}{a^n}\frac{1}{1-|b/a|^2} \leq 1.2 \cdot 2.1^n\,, \tag{A.26}$$

and analogously

$$\frac{1}{\Sigma_{\mathrm{pb}}(n)} \geq \frac{1}{a^n}\frac{1}{1+|b/a|^2} \geq 0.8 \cdot 2^n\,. \tag{A.27}$$

In the same way, we can bound $1/\Sigma_{\mathrm{ob}}(n)$. To this end, further set $c = 5(25-3\sqrt{41})/(2\sqrt{41})$ and $d = 5(25+3\sqrt{41})/(2\sqrt{41})$. We have, up to adjusting the phase of $b$,

$$\frac{1}{\Sigma_{\mathrm{ob}}(n)} = \frac{1}{ca^n + db^n} = \frac{1}{ca^n}\frac{1}{1+(d/c)(b/a)^n} \tag{A.28}$$

and, thus, for $n \geq 4$ we have

$$0.3 \cdot 2^n < \frac{1}{ca^n}\frac{1}{1+(d/c)|b/a|^4} \leq \frac{1}{\Sigma_{\mathrm{ob}}(n)} \leq \frac{1}{ca^n}\frac{1}{1-(d/c)|b/a|^4} < 0.6 \cdot 2.1^n. \tag{A.29}$$

Note that Eq. (A.28) goes to $c^{-1}a^{-n} \approx 0.44 \cdot 2.1^n$ for large $n$ as the second fraction becomes 1 asymptotically. Similarly, $\frac{1}{\Sigma_{\mathrm{pb}}(n)}$ asymptotically becomes $a^{-n}$. The deviation from this asymptotic scaling is small already for small $n$. E.g., the relative error of the asymptotic approximation is smaller than $10^{-2}$ for $n \geq 6$. Asymptotically the frame operator elements for periodic and open boundary conditions only differ by a constant factor $c^{-1} \approx 0.44$.

Setting $\Gamma \equiv \frac{1}{c}\frac{1}{1-(d/c)|b/a|^4}$ and $\Delta \equiv \frac{1}{a}$, a bound of the form $1/\Sigma_{\mathrm{ob}}(n) \leq \Gamma\Delta^n$, implies that the variance is dominated by

$$\sigma^2_{\mathrm{BW}} \leq \prod_{l \in \mathrm{part}_{\mathrm{BW}}(v)} \Sigma_{\mathrm{ob}}(2l+2)^{-1} \leq \prod_{l \in \mathrm{part}_{\mathrm{BW}}(v)} (\Gamma\Delta^2)\Delta^{2l} \leq (\Gamma\Delta^2)^{|\,\mathrm{part}_{\mathrm{BW}}(v)|}\Delta^{2\Sigma(\mathrm{part}_{\mathrm{BW}}(v))}, \tag{A.30}$$

where $|\operatorname{part}_{\mathrm{BW}}(v)|$ denotes the length of the tuple $\operatorname{part}_{\mathrm{BW}}(v)$, i.e. the number of parts in the partition, and $\Sigma(\operatorname{part}_{\mathrm{BW}}(v)) \coloneqq \sum_{l\in|\operatorname{part}_{\mathrm{BW}}(v)|} l = |\tilde{v}|$ is the cumulative length of all parts.

Inserting the previous bounds for $\Gamma$ and $\Delta$ (without intermediate rounding), we conclude that

$$\sigma^2_{\mathrm{BW}} \leq 2.2^{|\operatorname{part}_{\mathrm{BW}}(v)|} 4.4^{\Sigma(\operatorname{part}_{\mathrm{BW}}(v))} . \tag{A.31}$$

When comparing to the variance of LC circuits in the case where $\operatorname{part}_{\mathrm{BW}} = (n/2)$ or $(n/2-1)$, we are interested in ensuring that $\Gamma\Delta^n < 3^{|\operatorname{supp}_{\mathrm{LC}}(v)|}$. This is the case when

$$|\operatorname{supp}_{\mathrm{LC}}(v)| \geq n \log_3 \Delta + \log_3 \Gamma , \tag{A.32}$$

which for open and periodic boundary conditions translates to the sufficient condition

$$|\operatorname{supp}_{\mathrm{LC}}(v)| > 0.68n + 0.12 \tag{A.33}$$

(the constant term for open boundary conditions is actually negative).

More generally, Eq. (A.31) is smaller than $3^{|\operatorname{supp}_{\mathrm{LC}}(v)|}$ if

$$|\operatorname{supp}_{\mathrm{LC}}(v)| \geq 0.8|\operatorname{part}_{\mathrm{BW}}(v)| + 1.4\Sigma(\operatorname{part}_{\mathrm{BW}}(v)) . \tag{A.34}$$

# Appendix B

# Additional calculations for bosonic RB

## B.1 Proof of Proposition 39

For convenience, we state again the proposition:

**Proposition 57** (restatement of Proposition 39)**.** *For any $k \in \mathbb{N}$, set $d_{\lambda_k} \equiv \dim \lambda_k$.*

$$d_{\lambda_k} = \left(1 - \frac{k^2}{(k+m-1)^2}\right) (\dim \mathcal{H}_k^m)^2 \ . \tag{B.1}$$

*Proof.* For any irrep $\lambda = (m_1, m_2, \ldots, m_m)$, the following fact holds: [77]

$$\dim \lambda = \prod_{1 \le j < j' \le m} \left(1 + \frac{m_j - m_{j'}}{j' - j}\right) . \tag{B.2}$$

Let us denote the irrep defined in Eq. (10.30) as $\lambda_k = (2k, k, \ldots, k, 0)$. Hence, notice the following facts:

- For $j = 1$ and $j' = 2, \ldots, m-1$ we obtain the contribution $\prod_{j'=2}^{m-1} \left(1 + \frac{k}{j'-1}\right)$.
- For $j = 1$ and $j' = m$ we obtain the contribution $1 + \frac{2k}{m-1}$.
- For $2 \le j < j' \le m-1$ all the products are equal to 1.
- For $2 \le j \le m-1$ and $j' = m$ we obtain the contribution $\prod_{j=2}^{m-1} \left(1 + \frac{k}{m-j}\right)$.

Using the latter facts, we have

$$d_{\lambda_k} = \frac{2k+m-1}{m-1} \prod_{j=2}^{m-1} \frac{k+m-j}{m-j} \prod_{l=2}^{m-1} \frac{k+l-1}{l-1} \tag{B.3}$$

$$= \frac{2k+m-1}{m-1} \frac{1}{((m-2)!)^2} \prod_{j=2}^{m-1} (k+m-j) \prod_{l=2}^{m-1} (k+l-1) \tag{B.4}$$

$$= \frac{2k+m-1}{m-1}\frac{1}{((m-2)!)^2}\left(\frac{1}{k}(k)_{m-1}\right)^2 \tag{B.5}$$

$$= \frac{1}{k^2}\frac{2k+m-1}{m-1}\left(\frac{(k)_{m-1}}{(m-2)!}\right)^2 \tag{B.6}$$

$$= \frac{1}{k^2}\frac{2k+m-1}{m-1}(m-1)^2\left(\frac{(k)_{m-1}}{(m-1)!}\right)^2 \tag{B.7}$$

$$= \frac{(2k+m-1)(m-1)}{k^2}\left(\frac{(k+m-1)!}{k!(m-1)!}\frac{k}{k+m-1}\right)^2 \tag{B.8}$$

$$= \frac{(2k+m-1)(m-1)}{k^2}\frac{k^2(m-1)}{(k+m-1)^2}\binom{k+m-1}{m-1}^2 \tag{B.9}$$

$$= \frac{(2k+m-1)(m-1)}{(k+m-1)^2}\binom{k+m-1}{m-1}^2 \tag{B.10}$$

$$= \left(1-\frac{k^2}{(k+m-1)^2}\right)(\dim \mathcal{H}_k^m)^2\ . \tag{B.11}$$

In Eq. (B.4) we factorized the denominators and observed that the factors range between 1 and $m-2$. In Eq. (B.5) we introduced the Pochhammer raising factorial symbol, defined as $(a)_k \coloneqq a(a+1)\dots(a+k-1)$ for $a,k\in\mathbb{N}$. In Eq. (B.8) we recognized that, by definition,

$$\frac{(k)_{m-1}}{(m-2)!} = \binom{k+m-2}{m-1} = \frac{(k+m-2)!}{(k-1)!(m-1)!}\cdot\frac{k}{k}\,. \tag{B.12}$$

Finally, rearranging the terms and by symmetry of the binomial coefficient, the assertion follows. □

## B.2 Proof of Lemma 40

In this section, for convenience, we will say that a box in a Young tableau is a $k$-box if it is labeled by $k\in[m]$. Recall that for each $N\in\mathrm{GT}(\tau_n^m)$ we have

$$w_j^{(N)} + w_j^{(\bar{N})} = 0\,,\quad \forall j = 1,\dots m-1\,. \tag{B.13}$$

**Lemma 58** (Restatement of Lemma 40)**.** *Let $\lambda_k$ be an irrep of* $\mathrm{SU}(m)$ *as in Eq.* (10.30) *for any $k\in\mathbb{N}$. Then,*

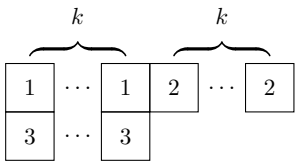
$$\gamma_{\lambda_k}(\mathbf{0}) = \binom{k+m-2}{k}\,. \tag{B.14}$$

*Proof.* From the point of view of Young tableaux, we remark that a state with weight $\mathbf{0}$ implies that in the corresponding Young tableau $T_M$ –where $M\in\mathrm{GT}(\lambda_k)$ satisfies the latter selection rules– all the entries appear the same number of times. Let $\mathrm{SSYT}(\lambda_k)$ be the set of semi-standard Young tableaux of shape $\lambda_k$ and consider the set

$$\mathrm{SSYT}^{(\mathbf{0})}(\lambda_k) \coloneqq \{T \mid T\in\mathrm{SSYT}(\lambda_k) \text{ s.t. } w_i^T = w_{i+1}^T\,\forall i\in[m-1]\}\,. \tag{B.15}$$

It follows that $\gamma_{\lambda_k}(\mathbf{0}) = |\mathrm{SSYT}^{(\mathbf{0})}(\lambda_k)|$ is the inner multiplicity of $\mathbf{0}$ in $\lambda_k$. Clearly, $\gamma(w)=1$ for each weight $w$ in $\mathrm{SU}(2)$, and Eq. (10.54) holds trivially.

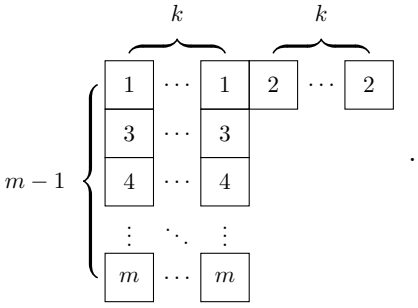
In a similar fashion, counting Young tableaux $T_{\lambda_k}$ for SU(3) is straightforward: any Young tableau $T \in \mathrm{SSYT}^{(\mathbf{0})}(\lambda_k)$ contains the labels $\{1,2,3\}$ exactly $k$ times, with the 1's forced to be placed in the first $k$ boxes of the first row, otherwise $T$ would not be a legal tableau. Then, if we consider a starting Young tableau of the form




(B.16)

all remaining $T \in \mathrm{SSYT}^{(\mathbf{0})}(\lambda_l)$ can be obtained by permuting the last 2-box in the first row with the first 3-box in the second row. The total number of allowed swaps is $k$, which implies $\gamma_{\lambda_k}(\mathbf{0}) = k+1$.

Consider now $m > 3$. As in the previous case, the 1-boxes are fixed to be placed at the beginning of the first row. Suppose the $m$-boxes are all placed in the $m-1$-th row, i.e. we consider




(B.17)

As long as the last row is fixed to contain $m$-boxes only, the total number of such Young tableaux is $\binom{k+m-3}{k}$. Then, we only have to count the remaining allowed configurations of $k$-boxes. For this purpose, observe that the remaining allowed positions for $m$-boxes are only in the first row, and there are $k$ such configurations. Hence, it is enough to count all possible configurations for each placement of $m$-boxes in the first row, which is given by

$$\binom{k-l+m-2}{k-l}, \tag{B.18}$$

where $l$ is the number of free boxes in the first row of the tableau. Therefore, the total number of such configurations is

$$\begin{aligned}\sum_{l=1}^{k}\binom{(k-l)+m-2}{k-l} &= \sum_{j=0}^{k-1}\binom{j+m-2}{j} = \sum_{j=0}^{k-1}\binom{j+m-2}{m-2} \\ &= \binom{k+m-3}{k-1},\end{aligned} \tag{B.19}$$

where we used Fermat's identity

$$\sum_{j=0}^{n}\binom{j+a}{j} = \binom{a+n+1}{n}. \tag{B.20}$$

Therefore, by Pascal's identity, we have

$$\gamma_{\lambda_k}(\mathbf{0}) = \binom{k+m-3}{k} + \binom{k+m-3}{k-1} = \binom{k+m-2}{k}. \tag{B.21}$$

and the proof is complete. □

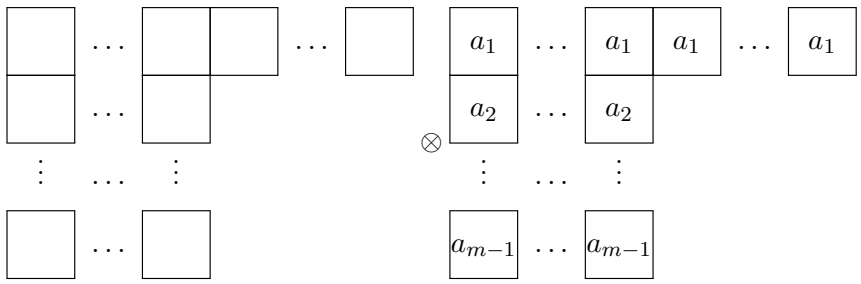
## B.3 Proof of Lemma 47

**Lemma 59** (Restatement of Lemma 47)**.** *Let $\lambda_k$ be a Young diagram as in Eq.* (10.30) *labeling an irrep of* $\mathrm{SU}(m)$, $m \geq 3$. *Then,*

$$\lambda_k \otimes \lambda_k = \bigoplus_{l=0}^{k} \lambda_l^{(l+1)} \oplus \bigoplus_{l=k+1}^{2k} \lambda_l^{(2k-l+1)} \oplus L\,, \tag{B.22}$$

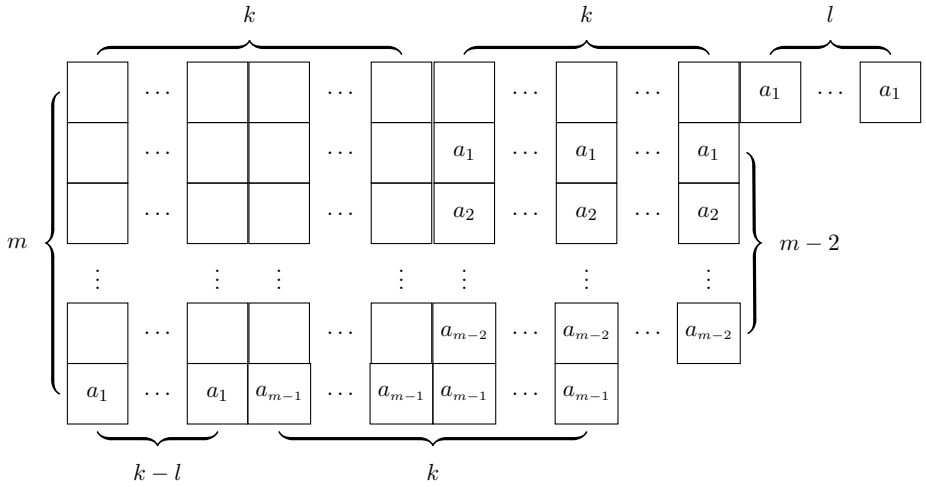
*where $\lambda_0 \equiv \mathbf{1}$, $\lambda_1 \equiv \mathrm{Ad}$, $\lambda_j^{(i)}$ denotes the i-th copy of $\lambda_j$ in $\lambda_l^{\otimes 2}$, and $L$ is a suitable direct sum of irreps which are not of the form $\lambda_l$ for any $l \in \mathbb{N}$.*

*Proof.* Consider for any $k \in \mathbb{N}$ the tensor product

$\lambda_k \otimes \lambda_k =$  . (B.23)

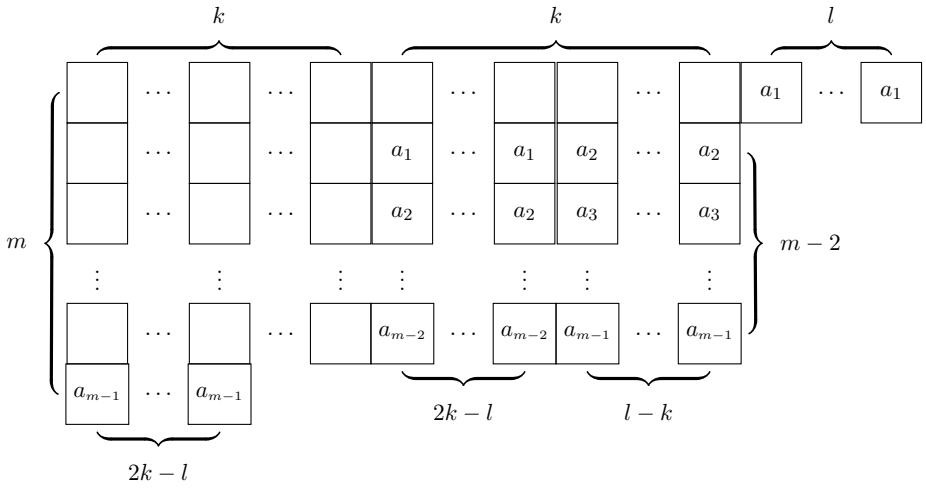

By Littlewood-Richardson's rules, the number of Young diagrams $\lambda_l$ that can be constructed from $\lambda_k^{\otimes 2}$ is determined by all possible allowed configurations we can attach the $a_1$ boxes to the first $\lambda_k$, since the way the remaining $a_i$ boxes, $i = 2, \ldots, m-1$, are attached must follow accordingly. First, notice that only the $a_1$ boxes can be attached to the first row of the first copy of $\lambda_k$ due to the elimination rule. Hence, we have two different 'generating' Young diagrams conditioned by whether $l \leq k$ or $k+1 \leq l \leq 2k$. Suppose $l \leq k$ at first. The $a_1$ boxes are attached to the first copy of $\lambda_k$ as follows: The first $l$ boxes are attached to the first row, the next $k$ boxes are attached to the second row and the remaining $k-l$ boxes are attached to the $m$-th row. Then, all the $a_i$ boxes, for any $i = 2, 3, \ldots, m-2$ are attached to the $i+1$-th row. Finally, the $a_{m-1}$ boxes are attached to the $m$-th row. The

resulting Young diagram is given by




(B.24)

Suppose now $l \geq k+1$. The $a_1$ boxes are attached to the first copy of $\lambda_k$ as follows: The first $l$ boxes are attached to the first row, while the remaining ones are attached to the second row of $\lambda_k$. Then, for the $a_i$ boxes, for any $i = 2, 3, \ldots, m-2$, the first $2k-l$ are attached to the $i$-th row of $\lambda_k$, while the remaining ones are attached to the $i+1$-th row of $\lambda_k$. The first $a_{m-1}$ boxes are attached to the $m-1$-th row of $T_k$ and the remaining ones will form the $m$-th row of the diagram. The resulting Young diagram is




(B.25)

For notation purpose, let us refer to the latter two Young diagrams as the generating Young diagrams.

At this point, we can generate all the remaining copies of $\lambda_l$ in the following way:

1. For any $i = 1, \ldots, m-2$, replace the last $a_i$ box in the $i+1$-th row with an $a_{i+1}$ box.
2. Replace the first $a_{m-1}$ box in the $m$-th row of the diagram with $a_1$.

It follows that the multiplicity of $\lambda_l$ in the decomposition of $\lambda_k^{\otimes 2}$ is determined by the number of $a_1$ boxes in the second row of the generating Young diagram. □

## B.4 Additional details on numerical experiments

Here we provide additional details and plots for the numerical experiment discussed in Fig. 10.1 and the numerical implementation of the filter function (10.63). Computation of the filter function was performed on a MacBook Pro 2020 with Intel Quad-Core i5 (1,4 GHz), 8 GB LPDDR3 (2133 MHz).

The specifics of the simulation are the following: We consider the collision-free input state $|\boldsymbol{n}_0\rangle = |\mathbf{1}_4\rangle \equiv |1111\rangle \in \mathcal{H}_n^4$ and filter onto the $\lambda_k$ irrep for $k = 0, \dots, 4$. Random unitaries $g_j^{(i)} \in \mathrm{SU}(4), i \in [T], j \in [l]$ are drawn from the Haar probability measure according to the procedure described in [286, 287], the sequence lengths considered consisting of $l = 1, \dots, 10$ Haar random unitaries. We assume each gate comes with a probability $1 - p$ of losing a particle on each mode. In particular, we consider experiments with gate independent noise, where $\sqrt{p} = 0.95, 0.975, 0.99$ and simulate a gate dependent noise experiment where the transmittivity $\sqrt{p_j}$ of the $j$-th unitary in the sequence is drawn uniformly at random from the interval $[0.9, 1]$. Concretely, denoting with $\mathcal{L}(g)$ the single-mode lossy channel, this means that the noisy gate is modeled as $\omega_n^m(g) \circ \mathcal{L}(g)^{\otimes m}$ for each gate $g$ in the sequence. Lastly, random Fock states are drawn performing a boson sampling simulation using the Python module Piquasso [288, 289]. Additionally, we collected noiseless samples for evaluation of $\mathbb{E}[f_{\lambda_k}^2]_{\text{ideal}}$ by simply letting $p = 1$. We collect $T = 10000$ sampled pairs $((g_j^{(i)})_{j=1}^l, \boldsymbol{n}^{(i)})$ and store them for post-processing. We remark that the unitaries $g_1^{(i)}, \dots, g_l^{(i)}$ are used to collect exactly one state from the boson sampler, as throughout this work we consider the so-called *single-shot estimator* (10.7) [50].

By post-selecting on the outcome of the boson sampling experiment, we capture the estimation of particle loss rates as described in Section 10.2.3. The results, which employ the indicator filter function (10.11) are shown in Fig. B.1 (the estimator is again the empirical average of the filter function). Since we run simulations under particle loss only, the estimated decay rates are similar to the ones shown in Fig. 10.1.

Next, we evaluate the filter function (10.63) for each sampled pair. Specifically, we compute Clebsch-Gordan coefficients using the SUNRepresentations Julia library [290], which implements Alex's et al. algorithm for the computation of $\mathrm{SU}(m)$ Clebsch-Gordan coefficients [77]. The algorithm can be sketched as follows: For each irrep $\lambda_k$ in $\tau_n^m \otimes \bar{\tau}_n^m$ (or –in the case of the second moment– for each irrep in $\lambda_k^{\otimes 2}$) one shall first find the Clebsch-Gordan coefficients of the highest weight state of $\lambda_k$ (and possibly resolve the ambiguity on the multiplicities by a suitable Gaussian elimination, in the case of $\lambda_k^{\otimes 2}$). Lower weight states are obtained by repeated application of ladder operators. This implies the calculation of all remaining Clebsch-Gordan coefficients by solving linear systems of equations. We remark the computation of Clebsch-Gordan coefficients can be sped up by exploiting the symmetries of the weight spaces under the action of the Weyl group [258] or using analytic expressions for the coefficients $C^M_{N,\bar{N}}$, with $N \in \mathrm{GT}(\tau_n^m), M \in \mathrm{GT}(\lambda_k)$ [150].

Lastly, we analyze the signal form for the irreps $\lambda_0, \dots, \lambda_4$ (we do not include $\lambda_1$ as there is no overlap with the chosen input state). The results are shown in Fig. B.2.

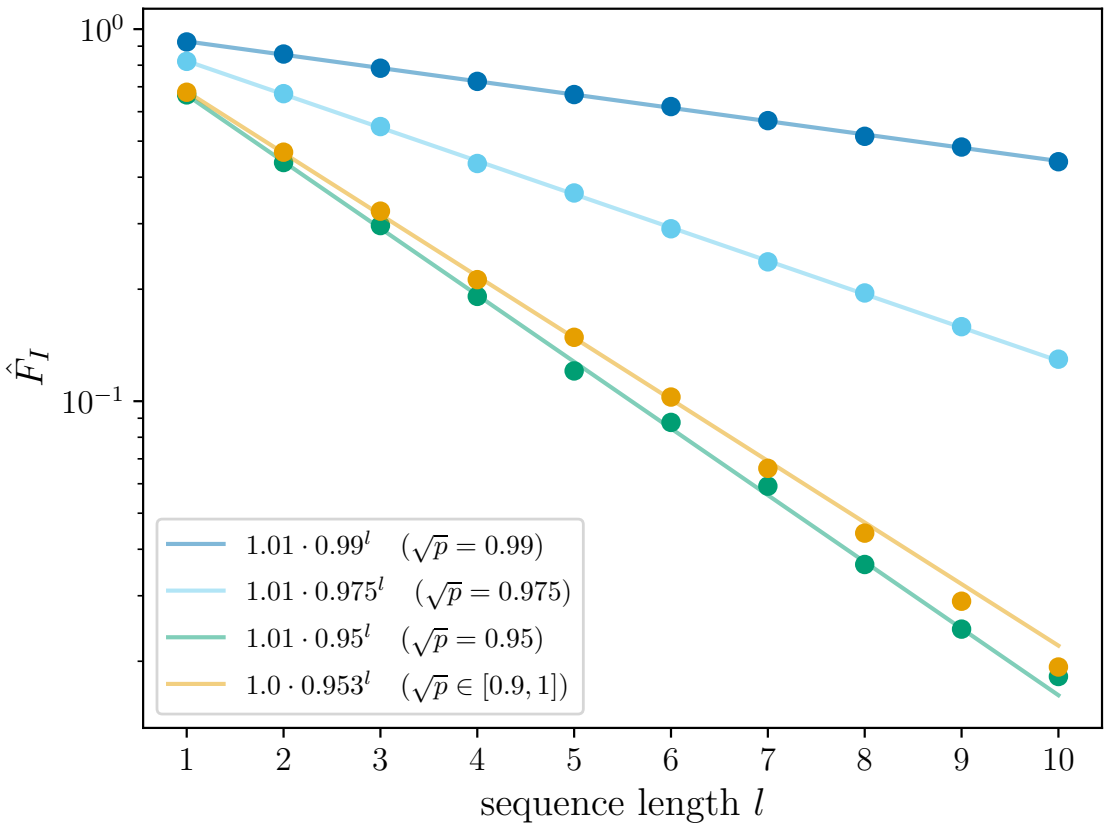



Figure B.1: Passive RB signal with $n = m = k$ and input state $|\mathbf{1}_4\rangle$ using $T = 10000$ samples. The plot shows post-selection on particle loss events under different values of transmittivity.

## B.5 Proof of Lemma 49

**Lemma 60** (Restatement of Lemma 49)**.** *Let $\lambda_k$ be a Young diagram as in Eq.* (10.30) *labeling an irrep of* $\mathrm{SU}(m)$*, $m \geq 3$. Then, for each $k, l \geq 0$,*

$$\lambda_k \otimes \lambda_l = \bigoplus_{j=0}^{\min\{k,l\}} \lambda^{(j+1)}_{|k-l|+j} \oplus \bigoplus_{j=\min\{k,l\}+1}^{k+l} \lambda^{(k+l-j+1)}_{|k-l|+j} \oplus R\,, \tag{B.26}$$

*where $\lambda_0 \equiv \mathbf{1}$, $\lambda_1 \equiv \mathrm{Ad}$, $\lambda^{(i)}_j$ denotes the $i$-th copy of $\lambda_j$ in $\lambda_k \otimes \lambda_l$, and $R$ is a suitable direct sum of irreps which are not of the form $\lambda_l$ for any $l \in \mathbb{N}$.*

*Proof.* Without loss of generality, we can assume that $k > l$. Then, we shall decompose the

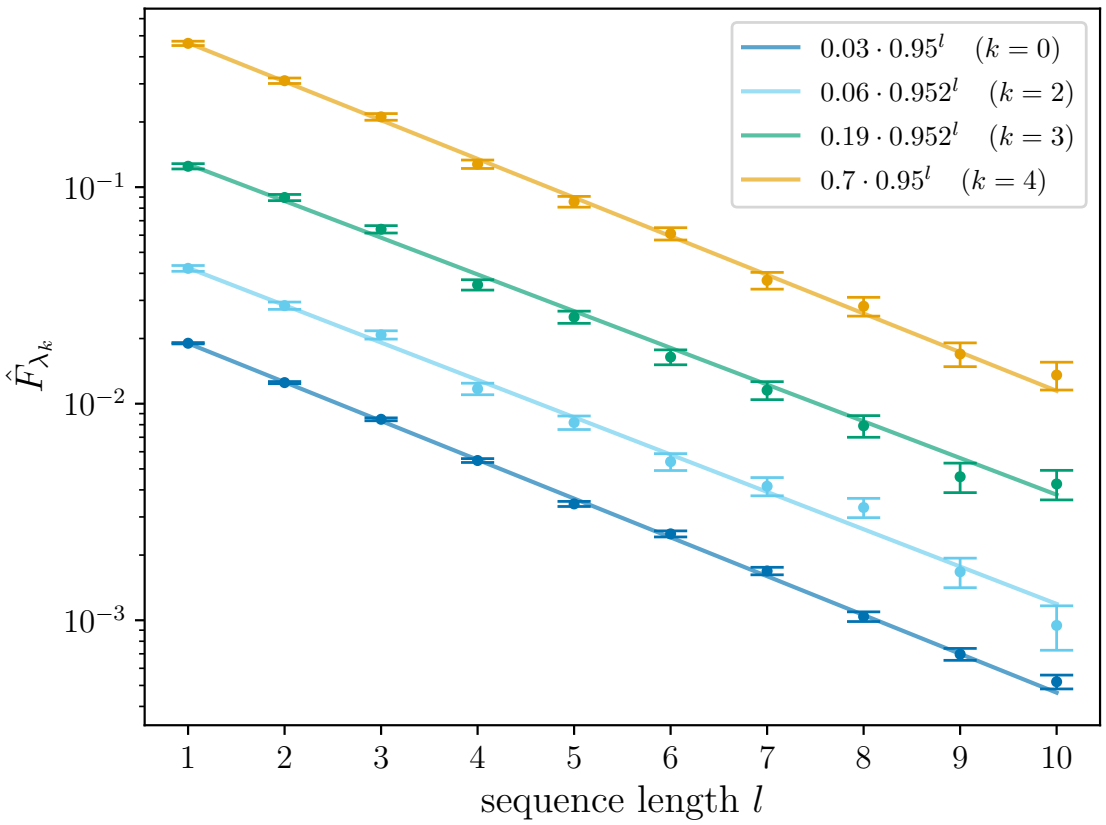
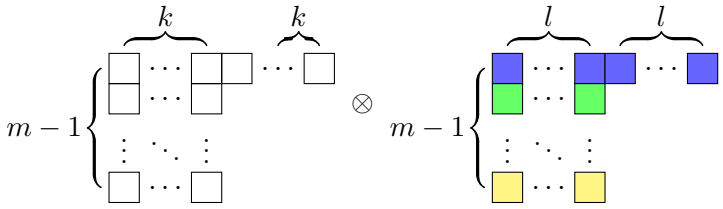



Figure B.2: Passive RB signal in the presence of particles loss with transmittivity $\sqrt{p} = 0.95$, $n = m = k$ and $T = 10000$ samples. The input state is set to $|\mathbf{1}_4\rangle$.

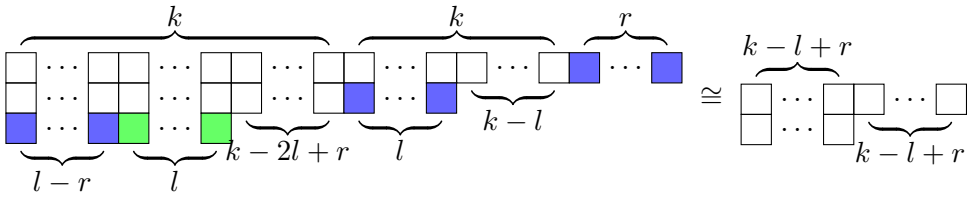
tensor product, C.f. Eq. (10.30)

$$\lambda_k \otimes \lambda_l =$$



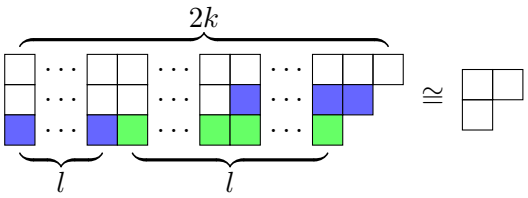

(B.27)

using Littlewood-Richardson's rules. To simplify notation further, let us consider the case $m = 3$, so that the number of rows reduces to 2. Then, as in the proof of Lemma 47, Young diagrams contained in $\lambda_k \otimes \lambda_l$ of shape $\lambda_r$, for some $r$ between $k - l$ and $k$, is obtained either as




(B.28)

or




(B.29)

if $k = l+1$ and $r = 1$. In the latter case, it is clear that the multiplicity of $\lambda_1$ is always 1. In the former, the multiplicity of $\lambda_{k-l+r}$ is determined by the number of swaps between green boxes and blue boxes in the second row, which is determined by the condition $n_b \geq n_g$, where, for each box in the diagram, $n_b$ (respectively, $n_g$) is the number of blue (respectively, green) boxes above and right to it. Hence, the multiplicity of $\lambda_{k-l+r}$ is $r+1$ for each $r$.

Notice that the proof generalizes to the case $m > 3$ straightforwardly, as the allowed positions for yellow boxes is determined by the configuration of blue and green boxes, in complete analogy with Lemma 47. □

## B.6 SPAM constants with distinguishable input states

**Lemma 61.** *For any $k \in [N]$ we have*

$$I_k^{(2)} = \Phi(N_0, N, N^{(1)}, N^{(2)}, L^{(1)}, L^{(2)}) g_k(N_0, N, N^{(1)}, N^{(2)}, M^{(1)}, L^{(1)}, M^{(2)}, L^{(2)}) \,, \tag{B.30}$$

*where* $\Phi(N_0, N, N^{(1)}, N^{(2)}, L^{(1)}, L^{(2)}) = (-1)^{\varphi(N_0)+\varphi(N)+\varphi(N^{(1)})+\varphi(N^{(2)})+\varphi(L^{(1)})+\varphi(L^{(2)})}$ *and*

$$\begin{aligned} g_k = \frac{1}{d_k} \sum_{r,s=0}^{k} \sum_{c=1}^{m_k} \sum_{\substack{M_0, M \in \mathrm{GT}(\lambda_k), \\ M_1, J_1 \in \mathrm{GT}(\lambda_r) \\ M_2, J_2 \in \mathrm{GT}(\lambda_s)}} & C^{M_0}_{N_0, \bar{N}_0} C^{M}_{N, \bar{N}} C^{M_1}_{N^{(1)}, \bar{N^{(1)}}} C^{M_2}_{N^{(2)}, \bar{N^{(2)}}} C^{J_1}_{M^{(1)}, \bar{L^{(1)}}} C^{J_2}_{M^{(2)}, \bar{L^{(2)}}} \\ & \times C^{M, c}_{M_1, M_2} C^{M_0, c}_{J_1, J_2} \,, \end{aligned} \tag{B.31}$$

*where* $g_k \equiv g_k(N_0, N, N^{(1)}, N^{(2)}, M^{(1)}, L^{(1)}, M^{(2)}, L^{(2)})$ *and* $m_k$ *is the multiplicity of* $\lambda_k$ *in* $\lambda_r \otimes \lambda_s$ *for each* $r, s \in [k]$.

*Proof.* Let $A$ be the GT pattern associated with the Fock state $|\boldsymbol{a}\rangle$. By definition, we have

$$\begin{aligned} I_k^{(2)} &= \int dg \, \langle \boldsymbol{n}_0, \boldsymbol{n}_0 | \lambda_k(g)^\dagger | \boldsymbol{n}, \boldsymbol{n} \rangle \langle \boldsymbol{n}^{(1)}, \boldsymbol{n}^{(1)}, \boldsymbol{n}^{(2)}, \boldsymbol{n}^{(2)} | \omega(g)^{\otimes 2} | \boldsymbol{m}^{(1)}, \boldsymbol{l}^{(1)}, \boldsymbol{m}^{(2)}, \boldsymbol{l}^{(2)} \rangle \\ &= \int dg \, \langle N_0, N_0 | \lambda_k(g)^\dagger | N, N \rangle \langle N^{(1)}, N^{(1)}, N^{(2)}, N^{(2)} | \omega(g)^{\otimes 2} | M^{(1)}, L^{(1)}, M^{(2)}, L^{(2)} \rangle \\ &= (-1)^{\varphi(N_0)+\varphi(N)+\varphi(N^{(1)})+\varphi(N^{(2)})+\varphi(L^{(1)})+\varphi(L^{(2)})} \\ &\times \int dg \, \langle N_0, \bar{N}_0 | \lambda_k(g)^\dagger | N, \bar{N} \rangle \langle N^{(1)}, \bar{N}^{(1)}, N^{(2)}, \bar{N}^{(2)} | \omega(g)^{\otimes 2} | M^{(1)}, \bar{L}^{(1)}, M^{(2)}, \bar{L}^{(2)} \rangle \\ &\equiv \Phi(N_0, N, N^{(1)}, N^{(2)}, L^{(1)}, L^{(2)}) g_k(N_0, N, N^{(1)}, N^{(2)}, M^{(1)}, L^{(1)}, M^{(2)}, L^{(2)}) \,, \end{aligned} \tag{B.32}$$

where $\bar{A} = (-1)^{\varphi(A)} A$ is the dual GT pattern of $A$. Consider now the following Clebsch-Gordan decompositions:

$$|N_0, \bar{N}_0\rangle\big|_{\lambda_k} = \sum_{M_0 \in \mathrm{GT}(\lambda_k)} C^{M_0}_{N_0, \bar{N}_0} |M_0\rangle \,, \tag{B.33}$$

$$|N,\bar{N}\rangle\big|_{\lambda_k} = \sum_{M\in \mathrm{GT}(\lambda_k)} C^{M}_{N,\bar{N}} |M\rangle\,, \tag{B.34}$$

$$|N^{(1)},\bar{N}^{(1)}\rangle = \sum_{r_1=0}^{k} \sum_{M_1\in \mathrm{GT}(\lambda_{r_1})} C^{M_1}_{N^{(1)},\bar{N}^{(1)}} |M_1\rangle\,, \tag{B.35}$$

$$|N^{(2)},\bar{N}^{(2)}\rangle = \sum_{r_2=0}^{k} \sum_{M_2\in \mathrm{GT}(\lambda_{r_2})} C^{M_2}_{N^{(2)},\bar{N}^{(2)}} |M_2\rangle\,, \tag{B.36}$$

$$|M^{(1)},\bar{L}^{(1)}\rangle = \sum_{r_3=0}^{k} \sum_{J_1\in \mathrm{GT}(\lambda_{r_3})} C^{J_1}_{M^{(1)},\bar{L}^{(1)}} |J_1\rangle\,, \tag{B.37}$$

$$|M^{(2)},\bar{L}^{(2)}\rangle = \sum_{r_4=0}^{k} \sum_{J_2\in \mathrm{GT}(\lambda_{r_4})} C^{J_2}_{M^{(2)},\bar{L}^{(2)}} |J_2\rangle\,. \tag{B.38}$$

Then,

$$\begin{aligned} g_k &= \sum_{r_1,r_2,r_3,r_4=0}^{k} \sum_{\substack{M_0,M\in \mathrm{GT}(\lambda_k)\\ M_1\in \mathrm{GT}(\lambda_{r_1}),M_2\in \mathrm{GT}(\lambda_{r_2})\\ J_1\in \mathrm{GT}(\lambda_{r_3}),G_2\in \mathrm{GT}(\lambda_{r_4})}} C^{M_0}_{N_0,\bar{N}_0} C^{M}_{N,\bar{N}} C^{M_1}_{N^{(1)},\bar{N}^{(1)}} C^{M_2}_{N^{(2)},\bar{N}^{(2)}} C^{J_1}_{M^{(1)}\bar{L}^{(1)}} C^{J_2}_{M^{(2)},\bar{L}^{(2)}} \\ &\quad\times \int dg\, \langle M_0\,|\lambda_k(g)^\dagger|\,M\rangle \langle M_1,M_2\,|\omega(g)^{\otimes 2}|\,J_1,J_2\rangle \\ &= \sum_{r,s=0}^{k} \sum_{r_1,r_2,r_3,r_4=0}^{k} \sum_{\substack{M_0,M\in \mathrm{GT}(\lambda_k)\\ M_1\in \mathrm{GT}(\lambda_{r_1}),M_2\in \mathrm{GT}(\lambda_{r_2})\\ J_1\in \mathrm{GT}(\lambda_{r_3}),G_2\in \mathrm{GT}(\lambda_{r_4})}} C^{M_0}_{N_0,\bar{N}_0} C^{M}_{N,\bar{N}} C^{M_1}_{N^{(1)},\bar{N}^{(1)}} C^{M_2}_{N^{(2)},\bar{N}^{(2)}} \\ &\quad\times C^{J_1}_{M^{(1)}\bar{L}^{(1)}} C^{J_2}_{M^{(2)},\bar{L}^{(2)}} \\ &\quad\times \int dg\, \langle M_0\,|\lambda_k(g)^\dagger|\,M\rangle \langle M_1,M_2\,|\lambda_r\otimes\lambda_s(g)|\,J_1,J_2\rangle\,, \end{aligned} \tag{B.39}$$

where in the last line we write $\omega^{\otimes 2} = \bigoplus_{r,s=0}^{k} \lambda_r\otimes\lambda s$. Observe that

$$\langle M_1,M_2\,|\lambda_r\otimes\lambda_s(g)|\,J_1,J_2\rangle = \langle M_1\,|\lambda_r(g)|\,J_1\rangle\langle N_2\,|\lambda_s(g)|\,J_2\rangle\,. \tag{B.40}$$

By orthogonality of irreps, this implies that $M_1,J_1\in \mathrm{GT}(\lambda_r)$ and $M_2,J_2\in \mathrm{GT}(\lambda_s)$. Hence,

$$\begin{aligned} g_k &= \sum_{r,s=0}^{k} \sum_{\substack{M_0,M\in \mathrm{GT}(\lambda_k)\\ M_1,J_1\in \mathrm{GT}(\lambda_r)\\ M_2,J_2\in \mathrm{GT}(\lambda_s)}} C^{M_0}_{N_0,\bar{N}_0} C^{M}_{N,\bar{N}} C^{M_1}_{N^{(1)},\bar{N}^{(1)}} C^{M_2}_{N^{(2)},\bar{N}^{(2)}} C^{J_1}_{M^{(1)}\bar{L}^{(1)}} C^{J_2}_{M^{(2)},\bar{L}^{(2)}} \\ &\quad\times \int dg\, \langle M_0\,|\lambda_k(g)^\dagger|\,M\rangle \langle M_1,M_2\,|\lambda_r\otimes\lambda_s(g)|\,J_1,J_2\rangle\,. \end{aligned} \tag{B.41}$$

To compute the integral $\mathcal{I}\equiv\int dg\,\langle M_0\,|\lambda_k(g)^\dagger|\,M\rangle\langle M_1,M_2\,|\lambda_r\otimes\lambda_s(g)|\,J_1,J_2\rangle$ we consider

Lemma 49. Specifically, consider the Clebsch-Gordan decompositions

$$|M_1, M_2\rangle = \sum_{i=0}^{r+s} \sum_{a_1=1}^{m_i} \sum_{R_1 \in \mathrm{GT}(\lambda_i)} C_{M_1,M_2}^{R_1,a_1} |R_1, a_1\rangle\,, \tag{B.42}$$

$$|M_1, M_2\rangle = \sum_{j=0}^{r+s} \sum_{a_2=1}^{m_j} \sum_{R_2 \in \mathrm{GT}(\lambda_j)} C_{J_1,J_2}^{R_2,a_2} |R_2, a_2\rangle \tag{B.43}$$

induced by the decomposition $\lambda_r \otimes \lambda_s = \bigoplus_{h=0}^{r+s} \bigoplus_{c=1}^{m_h} \lambda_h^{(c)}$. Then,

$$\begin{aligned} \mathcal{I} &\equiv \int dg\, \langle M_0 \,|\lambda_k(g)^\dagger|\, M\rangle \langle M_1, M_2 \,|\lambda_r \otimes \lambda_s(g)|\, J_1, J_2\rangle \\ &= \sum_{i,j,h=0}^{r+s} \sum_{a_1=1}^{m_i} \sum_{a_2=1}^{m_j} \sum_{c=1}^{m_h} \sum_{\substack{R_1 \in \mathrm{GT}(\lambda_i) \\ R_2 \in \mathrm{GT}(\lambda_j)}} C_{M_1,M_2}^{R_1,a_1} C_{J_1,J_2}^{R_2,a_2} \\ &\quad \times \int dg\, \langle M_0 \,|\lambda_k(g)^\dagger|\, M\rangle \langle R_1, a_1 \,|\lambda_h^{(c)}(g)|\, R_2, a_2\rangle\,. \end{aligned} \tag{B.44}$$

As before, by orthogonality of irreps, we have $i = j = h$ and $a_1 = a_2 = h$. Hence,

$$\begin{aligned} \mathcal{I} &= \sum_{h=0}^{r+s} \sum_{c=1}^{m_h} \sum_{R_1, R_2 \in \mathrm{GT}(\lambda_h)} C_{M_1,M_2}^{R_1,c} C_{J_1,J_2}^{R_2,c} \int dg\, \langle M_0 \,|\lambda_k(g)^\dagger|\, M\rangle \langle R_1, c \,|\lambda_h^{(c)}(g)|\, R_2, c\rangle \\ &= \frac{1}{d_k} \sum_{c=1}^{m_k} \sum_{R_1, R_2 \in \mathrm{GT}(\lambda_k)} C_{M_1,M_2}^{R_1,c} C_{J_1,J_2}^{R_2,c} \delta_{M_0,R_2} \delta_{M,R_1}\,, \end{aligned} \tag{B.45}$$

where the last line follows from Schur's orthogonality relations. Therefore, Eq. (B.41) becomes

$$\begin{aligned} g_k = \frac{1}{d_k} \sum_{r,s=0}^{k} \sum_{c=1}^{m_k} \sum_{\substack{M_0, M \in \mathrm{GT}(\lambda_k) \\ M_1, J_1 \in \mathrm{GT}(\lambda_r) \\ M_2, J_2 \in \mathrm{GT}(\lambda_s)}} & C_{N_0,\bar{N}_0}^{M_0} C_{N,\bar{N}}^{M} C_{N^{(1)},\bar{N}^{(1)}}^{M_1} C_{N^{(2)},\bar{N}^{(2)}}^{M_2} C_{M^{(1)},\bar{L}^{(1)}}^{J_1} C_{M^{(2)},\bar{L}^{(2)}}^{J_2} \\ \times\, C_{M_1,M_2}^{M,c} & C_{J_1,J_2}^{M_0,c}\,, \end{aligned} \tag{B.46}$$

which completes the proof. □

## B.7 Technical results for passive RB with heterodyne measurements

In this section, we use the shorthand notation

$$\int d^2\boldsymbol{\alpha} \equiv \int d^2\alpha_1 \cdots \int d^2\alpha_m\,, \tag{B.47}$$

where $d^2\alpha_i$ is the complex measure on $\mathbb{C}$. To characterize the frame operator $S = \int d^2\boldsymbol{\alpha} \int dg\, \omega_n^{m\dagger}(g)|E_{\boldsymbol{\alpha}})(E_{\boldsymbol{\alpha}}|\omega_n^m(g)$, consider the following quantity for any $K \in 2\mathbb{N}$:

$$I(\{\boldsymbol{n}_i\}_{i=1}^K) = \frac{1}{\sqrt{\boldsymbol{n}_1!\boldsymbol{n}_2!\ldots\boldsymbol{n}_K!}} \int d^2\boldsymbol{\alpha}\, e^{-K/2|\boldsymbol{\alpha}|^2} \bar{\boldsymbol{\alpha}}^{\boldsymbol{n}_1+\ldots\boldsymbol{n}_{K/2}} \boldsymbol{\alpha}^{\boldsymbol{n}_{K/2+1}+\ldots\boldsymbol{n}_K}\,. \tag{B.48}$$

The latter can be evaluated writing down the integral in polar coordinates and integrating by parts. Specifically, for the single-mode integral, and for any $\eta > 0$, we have

$$\begin{aligned}\int d^2\alpha\, e^{-\eta|\alpha|^2}\alpha^{a+b}\bar{\alpha}^{c+d} &= \int_0^\infty dr\, e^{-\eta r^2} r^{a+b+c+d+1} \int_0^{2\pi} d\theta\, e^{i\theta(a+b-c-d)} \\ &= \pi \left(\frac{a+b+c+d}{2}\right)! \, \eta^{-\frac{a+b+c+d}{2}} \delta_{a+b,c+d}\,.\end{aligned} \tag{B.49}$$

Notice that the expression in parenthesis is a proper factorial due to the $\delta$. This implies

$$I(\{\boldsymbol{n}_i\}_{i=1}^K) = \frac{\pi^m}{(K/2)^n} \frac{(\boldsymbol{n}_1 + \cdots + \boldsymbol{n}_{K/2})!}{\sqrt{\boldsymbol{n}_1! \ldots \boldsymbol{n}_K!}} \delta_{\boldsymbol{n}_1+\cdots+\boldsymbol{n}_{K/2}, \boldsymbol{n}_{K/2+1}+\cdots+\boldsymbol{n}_K}\,. \tag{B.50}$$

where

$$\delta_{\boldsymbol{n}_1+\cdots+\boldsymbol{n}_{K/2}, \boldsymbol{n}_{K/2+1}+\cdots+\boldsymbol{n}_K} = \begin{cases} 1, & \text{if } \sum_{i=1}^{K/2} \boldsymbol{n}_i = \sum_{i=K/2+1}^{K} \boldsymbol{n}_i\,, \\ 0, & \text{otherwise} \end{cases} \tag{B.51}$$

and we used the fact that $|\boldsymbol{n}_i| = n$ for each $i = 1, \ldots K$.

**Theorem 62.** *Let $\lambda_k$ an irrep of $\tau_n^m \otimes \bar{\tau}_n^m$ as in Eq.* (10.30)*. For a balanced heterodyne measurement setting, the eigenvalues of the frame operator of the filtered RB protocol are given by*

$$s_{\lambda_k} = \frac{\pi^m 2^{-n}}{d_{\lambda_k}} \sum_{\boldsymbol{n}_1, \boldsymbol{n}_2} (-1)^{\varphi(N_1)+\varphi(N_2)} \binom{\boldsymbol{n}_1 + \boldsymbol{n}_2}{\boldsymbol{n}_1} \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N_1,\bar{N}_1} C^M_{N_2,\bar{N}_2}\,, \tag{B.52}$$

*where $N_1, N_2 \in \mathrm{GT}(\tau_n^m)$ are the GT patterns associated with $\boldsymbol{n}_1, \boldsymbol{n}_2$, respectively, and*

$$\binom{\boldsymbol{n}_1 + \boldsymbol{n}_2}{\boldsymbol{n}_2} \equiv \binom{n_{1,1} + n_{2,1}}{n_{2,1}} \cdots \binom{n_{1,m} + n_{2,m}}{n_{2,m}}\,, \tag{B.53}$$

*where $\boldsymbol{n}_i = (n_{i,1}, \ldots, n_{i,m})$.*

*Proof.* For the balanced heterodyne measurement setting the corresponding (ideal) POVM is $\{|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| \equiv E_{\boldsymbol{\alpha}}\}_{\boldsymbol{\alpha}\in\mathbb{C}^m}$, where $|\boldsymbol{\alpha}\rangle = \bigotimes_{i=1}^m |\alpha_i\rangle$ is an $m$ modes coherent state. The associated measurement channel is given by

$$\mathcal{M}(\cdot) \coloneqq \int_{\mathbb{C}^m} d^2\boldsymbol{\alpha}\, \mathrm{Tr}[|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|(\cdot)]\, |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|\,. \tag{B.54}$$

To evaluate Eq. (10.48), we use the multi-mode expansion defined in Eq. (11.16). Moreover, since $P_{\lambda_k}$ is defined onto a subspace of $\mathcal{H}_n^m$, such expansions of the copies of $\boldsymbol{\alpha}$ are truncated. Hence, by Eq. (B.48), we have

$$s_{\lambda_k} = \frac{1}{d_{\lambda_k}} \int d^2\boldsymbol{\alpha}\, \langle\boldsymbol{\alpha}\,| P_{\lambda_k}(|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|)\,|\boldsymbol{\alpha}\rangle \tag{B.55}$$

$$= \frac{1}{d_{\lambda_k}} \sum_{\substack{\boldsymbol{n}_1, \boldsymbol{n}_2 \in \mathcal{H}_n^m \\ \boldsymbol{m}_1, \boldsymbol{m}_2 \in \mathcal{H}_n^m}} I(\boldsymbol{n}_1, \boldsymbol{n}_2, \boldsymbol{m}_1, \boldsymbol{m}_2) \langle \boldsymbol{n}_1\,| P_{\lambda_k}(|\boldsymbol{n}_2\rangle\langle\boldsymbol{m}_2|)\,|\boldsymbol{m}_1\rangle \tag{B.56}$$

$$= \frac{1}{d_{\lambda_k}} \sum_{\substack{\boldsymbol{n}_1,\boldsymbol{n}_2\in\mathcal{H}_n^m \\ \boldsymbol{m}_1,\boldsymbol{m}_2\in\mathcal{H}_n^m}} I(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2)\langle \boldsymbol{n}_1,\boldsymbol{m}_1|P_{\lambda_k}|\boldsymbol{n}_2,\boldsymbol{m}_2\rangle \tag{B.57}$$

$$= \frac{1}{d_{\lambda_k}} \sum_{\substack{\boldsymbol{n}_1,\boldsymbol{n}_2\in\mathcal{H}_n^m \\ \boldsymbol{m}_1,\boldsymbol{m}_2\in\mathcal{H}_n^m}} I(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2)\langle N_1,M_1|P_{\lambda_k}|N_2,M_2\rangle \tag{B.58}$$

$$= \frac{1}{d_{\lambda_k}} \sum_{\substack{\boldsymbol{n}_1,\boldsymbol{n}_2\in\mathcal{H}_n^m \\ \boldsymbol{m}_1,\boldsymbol{m}_2\in\mathcal{H}_n^m}} (-1)^{\varphi(M_1)+\varphi(M_2)} I(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2)\langle N_1,\bar{M}_1|P_{\lambda_k}|N_2,\bar{M}_2\rangle \tag{B.59}$$

$$= \frac{1}{d_{\lambda_k}} \sum_{\substack{\boldsymbol{n}_1,\boldsymbol{n}_2\in\mathcal{H}_n^m \\ \boldsymbol{m}_1,\boldsymbol{m}_2\in\mathcal{H}_n^m}} (-1)^{\varphi(M_1)+\varphi(M_2)} I(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2) \sum_{M\in\mathrm{GT}(\lambda_k)} C^M_{N_1,\bar{M}_1} C^M_{N_2,\bar{M}_2}\,, \tag{B.60}$$

where the phase $\varphi(M)$ is defined in Eq. (3.25) and in the last step we used the definition of $P_{\lambda_k}$, cf. (10.52):

$$\langle N_1,\bar{M}_1|P_{\lambda_k}|N_2,\bar{M}_2\rangle = \sum_{M\in\mathrm{GT}(\lambda_k)} \langle N_1,\bar{M}_1|M\rangle\langle M|N_2,M_2\rangle = \sum_{M\in\mathrm{GT}(\lambda_k)} C^M_{N_1,\bar{M}_1} C^M_{N_2,\bar{M}_2}\,. \tag{B.61}$$

Since $N_1,N_2\in\mathrm{GT}(\tau_n^m)$ and $M_1,M_2\in\mathrm{GT}(\bar{\tau}_n^m)$, selection rules for Clebsch-Gordan coefficients imply $M_1=N_1$ and $M_2=N_2$. Hence,

$$s_{\lambda_k} = \frac{1}{d_{\lambda_k}} \sum_{\boldsymbol{n}_1,\boldsymbol{n}_2\in\mathcal{H}_n^m} (-1)^{\varphi(N_1)+\varphi(N_2)} I(\boldsymbol{n}_1,\boldsymbol{n}_2) \sum_{M\in\mathrm{GT}(\lambda_k)} C^M_{N_1,\bar{N}_1} C^M_{N_2,\bar{N}_2}\,. \tag{B.62}$$

By Eq. (B.50), we have

$$I(\boldsymbol{n}_1,\boldsymbol{n}_2) = \frac{\pi^m}{2^n}\binom{\boldsymbol{n}_1+\boldsymbol{n}_2}{\boldsymbol{n}_1}. \tag{B.63}$$

with

$$\binom{\boldsymbol{n}_1+\boldsymbol{n}_2}{\boldsymbol{n}_2} \equiv \binom{n_{1,1}+n_{2,1}}{n_{2,1}} \cdots \binom{n_{1,m}+n_{2,m}}{n_{2,m}}, \tag{B.64}$$

from which Eq. (B.52) follows. □

**Lemma 63.** *For a heterodyne measurement setting, $\rho=|\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|$ as input state, and an irrep $\lambda_k$ of $\tau_n^m\otimes\bar{\tau}_n^m$, the following holds:*

$$\begin{aligned}\mathbb{E}[f_{\lambda_k}] = \frac{1}{d_{\lambda_k} s_{\lambda_k}} \sum_{M\in\mathrm{GT}(\lambda_k)} |C^M_{N_0,\bar{N}_0}|^2 \sum_{\substack{\boldsymbol{n}_1,\boldsymbol{n}_2\in\mathcal{H}_n^m \\ \boldsymbol{m}_1,\boldsymbol{m}_2\in\mathcal{H}_n^m}} (-1)^{\varphi(M_1)+\varphi(M_2)} I(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2) \\ \times \sum_{S\in\mathrm{GT}(\lambda_k)} C^S_{N_1,\bar{M}_1} C^S_{N_2,\bar{M}_2}\,,\end{aligned} \tag{B.65}$$

*where $|\boldsymbol{n}_0\rangle = |N_0\rangle, |\boldsymbol{n}_1\rangle \equiv |N_1\rangle, |\boldsymbol{n}_2\rangle \equiv |N_2\rangle, |\boldsymbol{m}_1\rangle \equiv |M_1\rangle, |\boldsymbol{m}_1\rangle \equiv |M_1\rangle$, $I$ is as in Eq.* (B.48) *and $\varphi$ is defined in Eq.* (3.25).

*Proof.* As in the proof of Theorem 62, considering the multi-mode expansion of $\boldsymbol{\alpha}$, only the $n$-particle component provides non-trivial contribution to the first moment, since $\omega_n^m$ acts non trivially on $\mathcal{H}_n^m$ only. Recalling Eq. (B.48), it follows

$$\mathbb{E}[f_{\lambda_k}] = \frac{1}{s_{\lambda_k}} \int d^2\boldsymbol{\alpha} \int dg \, \langle \boldsymbol{n}_0 | P_{\lambda_k} \circ \omega_n^m(g)^\dagger(|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|)|\boldsymbol{n}_0\rangle\langle\boldsymbol{\alpha}|\omega_n^m(g)(|\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|)|\boldsymbol{\alpha}\rangle \quad \text{(B.66)}$$

$$= \frac{1}{s_{\lambda_k}} \sum_{\substack{\boldsymbol{n}_1,\boldsymbol{n}_2 \in \mathcal{H}_n^m \\ \boldsymbol{m}_1,\boldsymbol{m}_2 \in \mathcal{H}_n^m}} I(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{m}_1,\boldsymbol{m}_2) \int d^2\boldsymbol{\alpha} \int dg \, \langle \boldsymbol{n}_0 | P_{\lambda_k} \circ \omega_n^m(g)^\dagger(|\boldsymbol{n}_1\rangle\langle\boldsymbol{m}_1|)|\boldsymbol{n}_0\rangle \quad \text{(B.67)}$$

$$\times \langle \boldsymbol{n}_2 | \omega_n^m(g)(|\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|)|\boldsymbol{m}_2\rangle \, . \quad \text{(B.68)}$$

In particular,

$$H \equiv \int d^2\boldsymbol{\alpha} \int dg \, \langle \boldsymbol{n}_0 | P_{\lambda_k} \circ \omega_n^m(g)^\dagger(|\boldsymbol{n}_1\rangle\langle\boldsymbol{m}_1|)|\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_2|\omega_n^m(g)(|\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|)|\boldsymbol{m}_2\rangle \quad \text{(B.69)}$$

$$= \int dg \, \langle \boldsymbol{n}_0, \boldsymbol{n}_0 | P_{\lambda_k} \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger | \boldsymbol{n}_1, \boldsymbol{m}_1\rangle\langle \boldsymbol{n}_2, \boldsymbol{m}_2 | \tau_n^m \otimes \bar{\tau}_n^m(g) | \boldsymbol{n}_0, \boldsymbol{n}_0\rangle \quad \text{(B.70)}$$

$$= \int dg \, \langle N_0, N_0 | P_{\lambda_k} \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger | N_1, M_1\rangle\langle N_2, M_2 | \tau_n^m \otimes \bar{\tau}_n^m(g) | N_0, N_0\rangle \quad \text{(B.71)}$$

$$= (-1)^{\varphi(M_1)+\varphi(M_2)} \int dg \, \langle N_0, \bar{N}_0 | P_{\lambda_k} \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger | N_1, \bar{M}_1\rangle \quad \text{(B.72)}$$

$$\times \langle N_2, \bar{M}_2 | \tau_n^m \otimes \bar{\tau}_n^m(g) | N_0, \bar{N}_0\rangle \quad \text{(B.73)}$$

$$= (-1)^{\varphi(M_1)+\varphi(M_2)} \sum_{M \in \mathrm{GT}(\lambda_k)} C^M_{N_0,\bar{N}_0} \int dg \, \langle M | \lambda_k(g)^\dagger | N_1, \bar{M}_1\rangle \quad \text{(B.74)}$$

$$\times \langle N_2, \bar{M}_2 | \bigoplus_{j=0}^n \lambda_j(g) | N_0, \bar{N}_0\rangle \, . \quad \text{(B.75)}$$

In the last step, we projected $|N_0, \bar{N}_0\rangle$ onto $\lambda_k$ and we used the irrep decomposition of $\tau_n^m \otimes \bar{\tau}_n^m$, see Lemma 38. The latter can be computed by slight modifications of Lemmas 43 and 45. In particular, by orthogonality relations, the integral is non-zero only if $j = k$ and for basis vectors of $\lambda_k$. In other words, it is enough to restrict the Clebsch-Gordan decompositions to the $\lambda_k$-th components:

$$|N_1, \bar{M}_1\rangle\big|_{\lambda_k} = \sum_{S_1 \in \mathrm{GT}(\lambda_k)} C^{S_1}_{N_1,\bar{M}_1} |S_1\rangle \, , \quad \text{(B.76)}$$

$$|N_2, \bar{M}_2\rangle\big|_{\lambda_k} = \sum_{S_2 \in \mathrm{GT}(\lambda_k)} C^{S_2}_{N_2,\bar{M}_2} |S_2\rangle \, , \quad \text{(B.77)}$$

$$|N_0, \bar{N}_0\rangle\big|_{\lambda_k} = \sum_{S_3 \in \mathrm{GT}(\lambda_k)} C^{S_3}_{N_0,\bar{N}_0} |S_3\rangle \, . \quad \text{(B.78)}$$

Therefore, Schur's orthogonality relations (2.10), we have

$$H = \frac{1}{d_{\lambda_k}} (-1)^{\varphi(M_1)+\varphi(M_2)} \sum_{M \in \mathrm{GT}(\lambda_k)} |C^M_{N_0,\bar{N}_0}|^2 \sum_{S \in \mathrm{GT}(\lambda_k)} C^S_{N_1,\bar{M}_1} C^S_{N_2,\bar{M}_2} \quad \text{(B.79)}$$

from which the assertion follows . □

Lastly, we have the following explicit expression for the second moment:

**Theorem 64.** *Consider a passive RB experiment with balanced heterodyne measurement setting, initial Fock state $\rho = |\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|$, and $\lambda$ is an irrep of $\omega_n^m = \tau_n^m(\,\cdot\,)\tau_n^{m\dagger}$. Then, the following holds:*

$$\mathbb{E}[f_{\lambda_k}^2] = \frac{1}{s_{\lambda_k}^2}(-1)^{\varphi(N_0)} \sum_{\substack{\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{n}_3,\\ \boldsymbol{m}_1,\boldsymbol{m}_2,\boldsymbol{m}_3}} (-1)^{\sum_{i=1}^3 \varphi(M_i)} I((\boldsymbol{n}_i)_{i=1}^3(\boldsymbol{m}_i)_{i=1}^3) g_k(\boldsymbol{N},\boldsymbol{M},N_0)\,, \tag{B.80}$$

*where $\boldsymbol{N} \equiv (N_1,N_2,N_3), \boldsymbol{M} \equiv (M_1,M_2,M_3)$, $N_i \equiv N(\boldsymbol{n}_i), M_i \equiv M(\boldsymbol{m}_i)$ are GT patterns associated with $\boldsymbol{n}_i, \boldsymbol{m}_i$, respectively, $I((\boldsymbol{n}_i)_{i=1}^3,(\boldsymbol{m}_i)_{i=1}^3) \equiv I(\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{n}_3,\boldsymbol{m}_1,\boldsymbol{m}_2,\boldsymbol{m}_3)$ is as in Eq.* (B.50) *and*

$$\begin{aligned} g_k(\boldsymbol{N},\boldsymbol{M},N_0) = \sum_{l=0}^{\min\{n,2k\}} \frac{1}{d_{\lambda_k}} \sum_{r=1}^{m_l} \sum_{\substack{M,M'\in \mathrm{GT}(\lambda_k)\\ L,L'\in\mathrm{GT}(\lambda_k)\\ R,R'\in\mathrm{GT}(\lambda_l)}} & C^{M}_{N_0,\bar{N}_0} C^{M'}_{N_0,\bar{N}_0} C^{R,r}_{M,M'} C^{R}_{N_0,\bar{N}_0} C^{R'}_{N_3,\bar{M}_3} C^{L}_{N_1,\bar{M}_1} \\ & \times C^{L'}_{N_2,\bar{M}_2} C^{R',r}_{L,L'}\,. \end{aligned} \tag{B.81}$$

*Proof.* By Eqs. (11.16) and (B.48), we have, for any $\lambda_k$,

$$\mathbb{E}[f_{\lambda_k}^2] = \frac{1}{s_{\lambda_k}^2} \int d^2\boldsymbol{\alpha} \int dg\, \langle \boldsymbol{n}_0 | P_{\lambda_k} \circ \omega_n^m(g)^\dagger(|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|)|\boldsymbol{n}_0\rangle^2 \langle\boldsymbol{\alpha}|\omega_n^m(g)(|\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|)|\boldsymbol{\alpha}\rangle \tag{B.82}$$

$$= \frac{1}{s_{\lambda_k}^2} \sum_{\substack{\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{n}_3\in\mathcal{H}_n^m\\ \boldsymbol{m}_1,\boldsymbol{m}_2,\boldsymbol{m}_3\in\mathcal{H}_n^m}} I((\boldsymbol{n}_i)_{i=1}^3,(\boldsymbol{m}_i)_{i=1}^3) \int dg\, \langle \boldsymbol{n}_0 | P_{\lambda_k} \circ \omega_n^m(g)^\dagger(|\boldsymbol{n}_1\rangle\langle\boldsymbol{m}_1|)|\boldsymbol{n}_0\rangle \tag{B.83}$$

$$\times \langle \boldsymbol{n}_0 | P_{\lambda_k} \circ \omega_n^m(g)^\dagger(|\boldsymbol{n}_2\rangle\langle\boldsymbol{m}_2|)|\boldsymbol{n}_0\rangle \langle\boldsymbol{n}_3|\omega_n^m(g)(|\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|)|\boldsymbol{m}_3\rangle \tag{B.84}$$

$$\equiv \frac{1}{s_{\lambda_k}^2} \sum_{\substack{\boldsymbol{n}_1,\boldsymbol{n}_2,\boldsymbol{n}_3,\\ \boldsymbol{m}_1,\boldsymbol{m}_2,\boldsymbol{m}_3}} I((\boldsymbol{n}_i)_{i=1}^3,(\boldsymbol{m}_i)_{i=1}^3)\, G_k((\boldsymbol{n}_i)_{i=1}^3,(\boldsymbol{m}_i)_{i=1}^3,\boldsymbol{n}_0)\,, \tag{B.85}$$

where

$$\begin{aligned} G_k((\boldsymbol{n}_i)_{i=1}^3,(\boldsymbol{m}_i)_{i=1}^3,\boldsymbol{n}_0) \equiv \int dg\, & \langle \boldsymbol{n}_0 | P_{\lambda_k} \circ \omega_n^m(g)^\dagger(|\boldsymbol{n}_1\rangle\langle\boldsymbol{m}_1|)|\boldsymbol{n}_0\rangle \\ & \times \langle \boldsymbol{n}_0 | P_{\lambda_k} \circ \omega_n^m(g)^\dagger(|\boldsymbol{n}_2\rangle\langle\boldsymbol{m}_2|)|\boldsymbol{n}_0\rangle \langle\boldsymbol{n}_3|\omega_n^m(g)(|\boldsymbol{n}_0\rangle\langle\boldsymbol{n}_0|)|\boldsymbol{m}_3\rangle\,. \end{aligned} \tag{B.86}$$

Introducing GT patterns, we have

$$G_k((\boldsymbol{n}_i)_{i=1}^3,(\boldsymbol{m}_i)_{i=1}^3,\boldsymbol{n}_0) \equiv G_k(\boldsymbol{N},\boldsymbol{M},N_0)\,, \quad \boldsymbol{N}=(N_1,N_2,N_3)\,,\ \boldsymbol{M}=(M_1,M_2,M_3)\,. \tag{B.87}$$

Then, by Eq. (3.25), the latter assumes the following form:

$$G_k(\boldsymbol{N},\boldsymbol{M},N_0) = \int dg\, \langle N_0,N_0 | P_{\lambda_k} \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger | N_1,M_1\rangle \tag{B.88}$$

$$\times \langle N_0,N_0 | P_{\lambda_k} \tau_n^m \otimes \bar{\tau}_n^m(g)^\dagger | N_2,M_2\rangle \langle N_3,M_3 | \tau_n^m \otimes \bar{\tau}_n^m(g) | N_0,N_0\rangle \tag{B.89}$$

$$= (-1)^{\varphi(N_0)+\sum_{i=1}^{3}\varphi(M_i)} \sum_{M,M'\in \mathrm{GT}(\lambda_k)} C^{M}_{N_0,\bar{N}_0} C^{M'}_{N_0,\bar{N}_0} \tag{B.90}$$

$$\times \int dg\, \langle M, M' \,|\, \lambda_k(g)^{\otimes 2\dagger} \,|\, N_1, \bar{M}_1, N_2, \bar{M}_2\rangle \langle N_3, \bar{M}_3 \,|\, \bigoplus_{j=0}^{n} \lambda_j(g) \,|\, N_0, \bar{N}_0\rangle \tag{B.91}$$

$$\equiv (-1)^{\varphi(N_0)+\sum_{i=1}^{3}\varphi(M_i)} g_k(\boldsymbol{N}, \boldsymbol{M}, N_0)\,. \tag{B.92}$$

We compute the integral

$$g_k(\boldsymbol{N}, \boldsymbol{M}, N_0) \equiv \int dg\, \langle M, M' \,|\, \lambda_k(g)^{\otimes 2\dagger} \,|\, N_1, \bar{M}_1, N_2, \bar{M}_2\rangle \langle N_3, \bar{M}_3 \,|\, \bigoplus_{j=0}^{n} \lambda_j(g) \,|\, N_0, \bar{N}_0\rangle \tag{B.93}$$

as in the proof of Theorem 48: Consider the irrep decomposition of $\lambda_k^{\otimes 2}$ as in Lemma 47. Then, by orthogonality of the matrix coefficients, the non-trivial contributions to the integral come from irreps that appear –with their multiplicities– in both $\omega_n^m$ and $\lambda_k^{\otimes 2}$. This implies

$$g_k(\boldsymbol{N}, \boldsymbol{M}, N_0) = \sum_{l=0}^{\min\{n,2k\}} \sum_{r=1}^{m_l} \int dg\, \langle M, M' \,|\, \lambda_l^{(r)}(g)^{\dagger} \,|\, N_1, \bar{M}_1, N_2, \bar{M}_2\rangle \langle N_3, \bar{M}_3 \,|\, \lambda_l(g) \,|\, N_0, \bar{N}_0\rangle\,. \tag{B.94}$$

Therefore, by the Clebsch-Gordan decompositions

$$|M, M'\rangle = \sum_{R\in \mathrm{GT}(\lambda_l)} C^{R,r}_{M,M'} |R, r\rangle\,, \tag{B.95}$$

$$|N_3, \bar{M}_3\rangle = \sum_{J\in \mathrm{GT}(\lambda_l)} C^{J}_{N_3,\bar{M}_3} |J\rangle\,, \tag{B.96}$$

$$|N_0, \bar{N}_0\rangle = \sum_{J'\in \mathrm{GT}(\lambda_l)} C^{J'}_{N_0,\bar{N}_0} |J'\rangle\,, \tag{B.97}$$

$$|N_1, \bar{M}_1, N_2, \bar{M}_2\rangle = \sum_{L,L'\in \mathrm{GT}(\lambda_k)} C^{L}_{N_1,\bar{M}_1} C^{L'}_{N_2,\bar{M}_2} |L, L'\rangle\,, \tag{B.98}$$

$$|L, L'\rangle = \sum_{R'\in \mathrm{GT}(\lambda_l)} C^{R'r}_{L,L'} |R', r\rangle\,, \tag{B.99}$$

it follows

$$\int dg\, \langle R, r \,|\, \lambda_l^{(r)}(g)^{\dagger} \,|\, R', r\rangle \langle J \,|\, \lambda_l(g) \,|\, J'\rangle = \frac{1}{d_{\lambda_l}} \delta_{R,J'} \delta_{R',J} \tag{B.100}$$

by Schur's orthogonality relations (2.10). Hence,

$$g_k(\boldsymbol{N}, \boldsymbol{M}, N_0) = \sum_{l=0}^{\min\{n,2k\}} \frac{1}{d_{\lambda_k}} \sum_{r=1}^{m_l} \sum_{\substack{M,M'\in \mathrm{GT}(\lambda_k)\\ L,L'\in \mathrm{GT}(\lambda_k)\\ R,R'\in \mathrm{GT}(\lambda_l)}} C^{M}_{N_0,\bar{N}_0} C^{M'}_{N_0,\bar{N}_0} C^{R,r}_{M,M'} C^{R}_{N_0,\bar{N}_0} C^{R'}_{N_3,\bar{M}_3} \tag{B.101}$$

$$\times\, C^{L}_{N_1,\bar{M}_1} C^{L'}_{N_2,\bar{M}_2} C^{R',r}_{L,L'}\,,$$

and the assertion follows from a suitable sorting of all the terms. □

# Bibliography


[1] R. P. Feynman, *Simulating physics with computers*, International Journal of Theoretical Physics **21**, 467 (1982).

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Physical Review Letters **70**, 1895 (1993).

[3] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **26**, 1484 (1997).

[4] L. K. Grover, *A fast quantum mechanical algorithm for database search*, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, 1996) pp. 212–219, arXiv:quant-ph/9605043 [quant-ph] .

[5] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, *Quantum supremacy using a programmable superconducting processor*, Nature **574**, 505 (2019).

[6] R. Acharya, D. A. Abanin, L. Aghababaie-Beni, I. Aleiner, T. I. Andersen, M. Ansmann, F. Arute, K. Arya, A. Asfaw, N. Astrakhantsev, J. Atalaya, R. Babbush, D. Bacon, B. Ballard, J. C. Bardin, J. Bausch, A. Bengtsson, A. Bilmes, S. Blackwell, S. Boixo, G. Bortoli, A. Bourassa, J. Bovaird, L. Brill, M. Broughton, D. A. Browne, B. Buchea, B. B. Buckley, D. A. Buell, T. Burger, B. Burkett, N. Bushnell, A. Cabrera, J. Campero, H.-S. Chang, Y. Chen, Z. Chen, B. Chiaro, D. Chik, C. Chou, J. Claes, A. Y. Cleland, J. Cogan, R. Collins, P. Conner, W. Courtney, A. L. Crook, B. Curtin, S. Das, A. Davies, L. De Lorenzo, D. M. Debroy, S. Demura, M. Devoret, A. Di Paolo, P. Donohoe, I. Drozdov, A. Dunsworth, C. Earle, T. Edlich, A. Eickbusch, A. M. Elbag, M. Elzouka, C. Erickson, L. Faoro, E. Farhi, V. S. Ferreira, L. F. Burgos, E. Forati, A. G. Fowler, B. Foxen, S. Ganjam, G. Garcia, R. Gasca, É. Genois, W. Giang,

C. Gidney, D. Gilboa, R. Gosula, A. G. Dau, D. Graumann, A. Greene, J. A. Gross, S. Habegger, J. Hall, M. C. Hamilton, M. Hansen, M. P. Harrigan, S. D. Harrington, F. J. H. Heras, S. Heslin, P. Heu, O. Higgott, G. Hill, J. Hilton, G. Holland, S. Hong, H.-Y. Huang, A. Huff, W. J. Huggins, L. B. Ioffe, S. V. Isakov, J. Iveland, E. Jeffrey, Z. Jiang, C. Jones, S. Jordan, C. Joshi, P. Juhas, D. Kafri, H. Kang, A. H. Karamlou, K. Kechedzhi, J. Kelly, T. Khaire, T. Khattar, M. Khezri, S. Kim, P. V. Klimov, A. R. Klots, B. Kobrin, P. Kohli, A. N. Korotkov, F. Kostritsa, R. Kothari, B. Kozlovskii, J. M. Kreikebaum, V. D. Kurilovich, N. Lacroix, D. Landhuis, T. Lange-Dei, B. W. Langley, P. Laptev, K.-M. Lau, L. Le Guevel, J. Ledford, J. Lee, K. Lee, Y. D. Lensky, S. Leon, B. J. Lester, W. Y. Li, Y. Li, A. T. Lill, W. Liu, W. P. Livingston, A. Locharla, E. Lucero, D. Lundahl, A. Lunt, S. Madhuk, F. D. Malone, A. Maloney, S. Mandrà, J. Manyika, L. S. Martin, O. Martin, S. Martin, C. Maxfield, J. R. McClean, M. McEwen, S. Meeks, A. Megrant, X. Mi, K. C. Miao, A. Mieszala, R. Molavi, S. Molina, S. Montazeri, A. Morvan, R. Movassagh, W. Mruczkiewicz, O. Naaman, M. Neeley, C. Neill, A. Nersisyan, H. Neven, M. Newman, J. H. Ng, A. Nguyen, M. Nguyen, C.-H. Ni, M. Y. Niu, T. E. O'Brien, W. D. Oliver, A. Opremcak, K. Ottosson, A. Petukhov, A. Pizzuto, J. Platt, R. Potter, O. Pritchard, L. P. Pryadko, C. Quintana, G. Ramachandran, M. J. Reagor, J. Redding, D. M. Rhodes, G. Roberts, E. Rosenberg, E. Rosenfeld, P. Roushan, N. C. Rubin, N. Saei, D. Sank, K. Sankaragomathi, K. J. Satzinger, H. F. Schurkus, C. Schuster, A. W. Senior, M. J. Shearn, A. Shorter, N. Shutty, V. Shvarts, S. Singh, V. Sivak, J. Skruzny, S. Small, V. Smelyanskiy, W. C. Smith, R. D. Somma, S. Springer, G. Sterling, D. Strain, J. Suchard, A. Szasz, A. Sztein, D. Thor, A. Torres, M. M. Torunbalci, A. Vaishnav, J. Vargas, S. Vdovichev, G. Vidal, B. Villalonga, C. V. Heidweiller, S. Waltman, S. X. Wang, B. Ware, K. Weber, T. Weidel, T. White, K. Wong, B. W. K. Woo, C. Xing, Z. J. Yao, P. Yeh, B. Ying, J. Yoo, N. Yosri, G. Young, A. Zalcman, Y. Zhang, N. Zhu, N. Zobrist, and Google Quantum AI and Collaborators, *Quantum error correction below the surface code threshold*, Nature **638**, 920 (2025), arXiv:2408.13687 [quant-ph].

[7] Y. Kim, A. Eddins, S. Anand, K. X. Wei, E. van den Berg, S. Rosenblatt, H. Nayfeh, Y. Wu, M. Zaletel, K. Temme, and A. Kandala, *Evidence for the utility of quantum computing before fault tolerance*, Nature **618**, 500 (2023).

[8] S. Bravyi, A. W. Cross, J. M. Gambetta, D. Maslov, P. Rall, and T. J. Yoder, *High-threshold and low-overhead fault-tolerant quantum memory*, Nature **627**, 778 (2024), arXiv:2308.07915 [quant-ph].

[9] L. Abdurakhimov, J. Adam, H. Ahmad, O. Ahonen, M. Algaba, G. Alonso, V. Bergholm, R. Beriwal, M. Beuerle, C. Bockstiegel, A. Calzona, C. F. Chan, D. Cucurachi, S. Dahl, R. Davletkaliyev, O. Fedorets, A. G. Frieiro, Z. Gao, J. Guldmyr, A. Guthrie, J. Hassel, H. Heimonen, J. Heinsoo, T. Hiltunen, K. Holland, J. Hotari, H. Hsu, A. Huhtala, E. Hyyppä, A. Hämäläinen, J. Ikonen, S. Inel, D. Janzso, T. Jaakkola, M. Jenei, S. Jolin, K. Juliusson, J. Jussila, S. Khalid, S.-G. Kim, M. Koistinen, R. Kokkoniemi, A. Komlev, C. Ockeloen-Korppi, O. Koskinen, J. Kotilahti, T. Kuisma, V. Kukushkin, K. Kumpulainen, I. Kuronen, J. Kylmälä, N. Lamponen, J. Lamprich, A. Landra, M. Leib, T. Li, P. Liebermann, A. Lintunen, W. Liu, J. Luus, F. Marxer, A. M.-v. de Griend, K. Mitra, J. K. Moqadam, J. Mrożek,

H. Mäkynen, J. Mäntylä, T. Naaranoja, F. Nappi, J. Niemi, L. Ortega, M. Palma, M. Papič, M. Partanen, J. Penttilä, A. Plyushch, W. Qiu, A. Rath, K. Repo, T. Riipinen, J. Ritvas, P. F. Romero, J. Ruoho, J. Räbinä, S. Saarinen, I. Sagar, H. Sargsyan, M. Sarsby, N. Savola, M. Savytskyi, V. Selinmaa, P. Smirnov, M. M. Suárez, L. Sundström, S. Słupińska, E. Takala, I. Takmakov, B. Tarasinski, M. Thapa, J. Tiainen, F. Tosto, J. Tuorila, C. Valenzuela, D. Vasey, E. Vehmaanperä, A. Vepsäläinen, A. Vienamo, P. Vesanen, A. Välimaa, J. Wesdorp, N. Wurz, E. Wybo, L. Yang, and A. Yurtalan, *Technology and Performance Benchmarks of IQM's 20-Qubit Quantum Computer* (2024), arXiv:2408.12433 [quant-ph] .

[10] J. M. Pino, J. M. Dreiling, C. Figgatt, J. P. Gaebler, S. A. Moses, M. S. Allman, C. H. Baldwin, M. Foss-Feig, D. Hayes, K. Mayer, C. Ryan-Anderson, and B. Neyenhuis, *Demonstration of the trapped-ion quantum-CCD computer architecture*, Nature **592**, 209 (2021), arXiv:2003.01293 [quant-ph].

[11] C. Ryan-Anderson, J. G. Bohnet, K. Lee, D. Gresh, A. Hankin, J. P. Gaebler, D. Francois, A. Chernoguzov, D. Lucchetti, N. C. Brown, T. M. Gatterman, S. K. Halit, K. Gilmore, J. A. Gerber, B. Neyenhuis, D. Hayes, and R. P. Stutz, *Realization of Real-Time Fault-Tolerant Quantum Error Correction*, Physical Review X **11**, 041058 (2021), arXiv:2107.07505 [quant-ph].

[12] S. A. Moses, C. H. Baldwin, M. S. Allman, R. Ancona, L. Ascarrunz, C. Barnes, J. Bartolotta, B. Bjork, P. Blanchard, M. Bohn, J. G. Bohnet, N. C. Brown, N. Q. Burdick, W. C. Burton, S. L. Campbell, J. P. Campora, C. Carron, J. Chambers, J. W. Chan, Y. H. Chen, A. Chernoguzov, E. Chertkov, J. Colina, J. P. Curtis, R. Daniel, M. DeCross, D. Deen, C. Delaney, J. M. Dreiling, C. T. Ertsgaard, J. Esposito, B. Estey, M. Fabrikant, C. Figgatt, C. Foltz, M. Foss-Feig, D. Francois, J. P. Gaebler, T. M. Gatterman, C. N. Gilbreth, J. Giles, E. Glynn, A. Hall, A. M. Hankin, A. Hansen, D. Hayes, B. Higashi, I. M. Hoffman, B. Horning, J. J. Hout, R. Jacobs, J. Johansen, L. Jones, J. Karcz, T. Klein, P. Lauria, P. Lee, D. Liefer, S. T. Lu, D. Lucchetti, C. Lytle, A. Malm, M. Matheny, B. Mathewson, K. Mayer, D. B. Miller, M. Mills, B. Neyenhuis, L. Nugent, S. Olson, J. Parks, G. N. Price, Z. Price, M. Pugh, A. Ransford, A. P. Reed, C. Roman, M. Rowe, C. Ryan-Anderson, S. Sanders, J. Sedlacek, P. Shevchuk, P. Siegfried, T. Skripka, B. Spaun, R. T. Sprenkle, R. P. Stutz, M. Swallows, R. I. Tobey, A. Tran, T. Tran, E. Vogt, C. Volin, J. Walker, A. M. Zolot, and J. M. Pino, *A Race-Track Trapped-Ion Quantum Processor*, Physical Review X **13**, 041052 (2023), arXiv:2305.03828 [quant-ph].

[13] A. Ransford, M. S. Allman, J. Arkinstall, J. P. Campora, S. F. Cooper, R. D. Delaney, J. M. Dreiling, B. Estey, C. Figgatt, A. Hall, A. A. Husain, A. Isanaka, C. J. Kennedy, N. Kotibhaskar, I. S. Madjarov, K. Mayer, A. R. Milne, A. J. Park, A. P. Reed, R. Ancona, M. P. Andersen, P. Andres-Martinez, W. Angenent, L. Argueta, B. Arkin, L. Ascarrunz, W. Baker, C. Barnes, J. Bartolotta, J. Berg, R. Besand, B. Bjork, M. Blain, P. Blanchard, R. Blume-Kohout, M. Bohn, A. Borgna, D. Y. Botamanenko, R. Boutelle, N. Brown, G. T. Buckingham, N. Q. Burdick, W. C. Burton, V. Carey, C. J. Carron, J. Chambers, J. Children, V. E. Colussi, S. Crepinsek, A. Cureton, J. Davies, D. Davis, M. DeCross, D. Deen, C. Delaney, D. DelVento, B. J. DeSalvo, J. Dominy, R. Duncan, V. Eccles, A. Edgington, N. Erickson, S. Erickson, C. T.

Ertsgaard, B. Evans, T. Evans, M. I. Fabrikant, A. Fischer, C. Foltz, M. Foss-Feig, D. Francois, B. Freyberg, C. Gao, R. Garay, J. Garvin, D. M. Gaudiosi, C. N. Gilbreth, J. Giles, E. Glynn, J. Graves, A. Hansen, D. Hayes, L. Heidemann, B. Higashi, T. Hilbun, J. Hines, A. Hlavaty, K. Hoffman, I. M. Hoffman, C. Holliman, I. Hooper, B. Horning, J. Hostetter, D. Hothem, J. Houlton, J. Hout, R. Hutson, R. T. Jacobs, T. Jacobs, M. Johannsen, J. Johansen, L. Jones, S. Julian, R. Jung, A. Keay, T. Klein, M. Koch, R. Kondo, C. Kong, A. Kosto, A. Lawrence, D. Liefer, M. Lollie, D. Lucchetti, N. K. Lysne, C. Lytle, C. MacPherson, A. Malm, S. Mather, B. Mathewson, D. Maxwell, L. McCaffrey, H. McDougall, R. Mendoza, M. Mills, R. Morrison, L. Narmour, N. Nguyen, L. Nugent, S. Olson, D. Ouellette, J. Parks, Z. Peters, J. Petricka, J. M. Pino, F. Polito, M. Preidl, G. Price, T. Proctor, M. Pugh, N. Ratcliff, D. Raymondson, P. Rhodes, C. Roman, C. Roy, C. Ryan-Anderson, F. B. Sanchez, G. Sangiolo, T. Sawadski, A. Schaffer, P. Schow, J. Sedlacek, H. Semenenko, P. Shevchuk, S. Shore, P. Siegfried, K. Singhal, S. Sivarajah, T. Skripka, L. Sletten, B. Spaun, R. T. Sprenkle, P. Stoufer, M. Tader, S. F. Taylor, T. H. Thompson, R. Tobey, A. Tran, T. Tran, G. Vittorini, C. Volin, J. Walker, S. White, D. Wilson, Q. Wolf, C. Wringe, K. Young, J. Zheng, K. Zuraski, C. H. Baldwin, A. Chernoguzov, J. P. Gaebler, S. J. Sanders, B. Neyenhuis, R. Stutz, and J. G. Bohnet, *Helios: A 98-qubit trapped-ion quantum computer* (2025), arXiv:2511.05465 [quant-ph] .

[14] J. Preskill, *Quantum Computing in the NISQ era and beyond*, Quantum **2**, 79 (2018), arXiv:1801.00862 [quant-ph].

[15] J. Preskill, *Quantum computing 40 years later* (2023), arXiv:2106.10522 [quant-ph] .

[16] R. O'Donnell and J. Wright, *Efficient quantum tomography* (2015), arXiv:1508.01907 [quant-ph] .

[17] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yu, *Sample-optimal tomography of quantum states*, IEEE Transactions on Information Theory **63**, 5628 (2017), arXiv:1508.01797 [quant-ph].

[18] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, *Quantum certification and benchmarking*, Nature Reviews Physics **2**, 382 (2020), arXiv:1910.06343 [quant-ph].

[19] M. Kliesch and I. Roth, *Theory of quantum system certification: A tutorial*, PRX Quantum **2**, 010201 (2021), arXiv:2010.05925.

[20] R. Blume-Kohout, T. Proctor, and K. Young, *Quantum characterization, verification, and validation* (2025), arXiv:2503.16383 [quant-ph] .

[21] Z. Cai, R. Babbush, S. C. Benjamin, S. Endo, W. J. Huggins, Y. Li, J. R. McClean, and T. E. O'Brien, *Quantum Error Mitigation*, Reviews of Modern Physics **95**, 045005 (2023), arXiv:2210.00921 [quant-ph].

[22] P. Cieśliński, S. Imai, J. Dziewior, O. Gühne, L. Knips, W. Laskowski, J. Meinecke, T. Paterek, and T. Vértesi, *Analysing quantum systems with randomised measurements*, Physics Reports **1095**, 1 (2024), arXiv:2307.01251 [quant-ph].

[23] J. J. Wallman and J. Emerson, *Noise tailoring for scalable quantum computation via randomized compiling*, Physical Review A **94**, 052325 (2016).

[24] E. Campbell, *A random compiler for fast Hamiltonian simulation*, Physical Review Letters **123**, 070503 (2019), arXiv:1811.08017 [quant-ph].

[25] A. Hashim, R. K. Naik, A. Morvan, J.-L. Ville, B. Mitchell, J. M. Kreikebaum, M. Davis, E. Smith, C. Iancu, K. P. O'Brien, I. Hincks, J. J. Wallman, J. Emerson, and I. Siddiqi, *Randomized compiling for scalable quantum computing on a noisy superconducting quantum processor*, Physical Review X **11**, 041039 (2021), arXiv:2010.00215 [quant-ph].

[26] A. Elben, J. Yu, G. Zhu, M. Hafezi, F. Pollmann, P. Zoller, and B. Vermersch, *Many-body topological invariants from randomized measurements in synthetic quantum matter*, Science Advances **6**, eaaz3666 (2020), arXiv:1906.05011 [quant-ph].

[27] B. Vermersch, A. Elben, L. M. Sieberer, N. Y. Yao, and P. Zoller, *Probing scrambling using statistical correlations between randomized measurements*, Physical Review X **9**, 021061 (2019), arXiv:1807.09087 [quant-ph].

[28] H.-Y. Huang, M. Broughton, J. Cotler, S. Chen, J. Li, M. Mohseni, H. Neven, R. Babbush, R. Kueng, J. Preskill, and J. R. McClean, *Quantum advantage in learning from experiments*, Science **376**, 1182 (2022), arXiv:2112.00778 [quant-ph].

[29] A. Elben, S. T. Flammia, H.-Y. Huang, R. Kueng, J. Preskill, B. Vermersch, and P. Zoller, *The randomized measurement toolbox*, Nature Reviews Physics **5**, 9 (2023), arXiv:2203.11374 [quant-ph].

[30] S. T. Flammia and Y.-K. Liu, *Direct fidelity estimation from few Pauli measurements*, Physical Review Letters **106**, 230501 (2011), arXiv:1104.4695 [quant-ph].

[31] M. P. da Silva, O. Landon-Cardinal, and D. Poulin, *Practical Characterization of Quantum Devices without Tomography*, Physical Review Letters **107**, 210404 (2011), arXiv:1104.3835 [quant-ph].

[32] S. J. van Enk and C. W. J. Beenakker, *The power of random measurements: Measuring* $\mathrm{Tr}(\rho^n)$ *on single copies of* $\rho$, Physical Review Letters **108**, 110503 (2012), arXiv:1112.1027 [quant-ph].

[33] A. Elben, R. Kueng, H.-Y. Huang, R. van Bijnen, C. Kokail, M. Dalmonte, P. Calabrese, B. Kraus, J. Preskill, P. Zoller, and B. Vermersch, *Mixed-state entanglement from local randomized measurements*, Physical Review Letters **125**, 200501 (2020), arXiv:2007.06305.

[34] D. Gottesman, *The Heisenberg Representation of Quantum Computers*, arXiv:quant-ph/9807006 .

[35] S. Aaronson and D. Gottesman, *Improved Simulation of Stabilizer Circuits*, Physical Review A **70**, 052328 (2004), arXiv:quant-ph/0406196.

[36] M. A. Nielsen, *A simple formula for the average gate fidelity of a quantum dynamical operation*, Physics Letters A **303**, 249 (2002), arXiv:quant-ph/0205035.

[37] D. Gross, K. Audenaert, and J. Eisert, *Evenly distributed unitaries: On the structure of unitary designs*, Journal of Mathematical Physics **48**, 052104 (2007), arXiv:quant-ph/0611002.

[38] Z. Webb, *The Clifford group forms a unitary 3-design*, Quantum Information and Computation **16**, 1379 (2016), arXiv:1510.02769 [quant-ph].

[39] H. Zhu, *Multiqubit clifford groups are unitary 3-designs*, Physical Review A **96**, 062336 (2017), arXiv:1510.02619 [quant-ph].

[40] H. Zhu, R. Kueng, M. Grassl, and D. Gross, *The Clifford group fails gracefully to be a unitary 4-design*, (2016), arXiv:1609.08172 [quant-ph].

[41] D. Gross, S. Nezami, and M. Walter, *Schur–Weyl duality for the Clifford group with applications: Property testing, a robust Hudson theorem, and de Finetti representations*, Communications in Mathematical Physics **385**, 1325 (2021), arXiv:1712.08628 [quant-ph].

[42] A. M. Dalzell, N. Hunter-Jones, and F. G. S. L. Brandão, *Random quantum circuits transform local noise into global white noise* (2021), arXiv:2111.14907 [quant-ph] .

[43] T. Schuster, J. Haferkamp, and H.-Y. Huang, *Random unitaries in extremely low depth*, Science **389**, 92 (2025), arXiv:2407.07754, arXiv:2407.07754 [quant-ph].

[44] J. T. Iosue, K. Sharma, M. J. Gullans, and V. V. Albert, *Continuous-variable quantum state designs: Theory and applications*, Physical Review X **14**, 011013 (2024), arXiv:2211.05127 [quant-ph].

[45] H.-Y. Huang, R. Kueng, and J. Preskill, *Predicting Many Properties of a Quantum System from Very Few Measurements*, Nature Physics **16**, 1050 (2020), arXiv:2002.08953.

[46] M. Paini and A. Kalev, *An approximate description of quantum states*, arXiv:1910.10543 [quant-ph].

[47] J. Emerson, R. Alicki, and K. Życzkowski, *Scalable noise estimation with random unitary operators*, Journal of Optics B: Quantum and Semiclassical Optics **7**, S347 (2005), arXiv:quant-ph/0503243 [quant-ph].

[48] B. Lévi, C. C. López, J. Emerson, and D. G. Cory, *Efficient error characterization in quantum information processing*, Physical Review A **75**, 022314 (2007), arXiv:quant-ph/0608246 [quant-ph].

[49] J. Helsen, I. Roth, E. Onorati, A. H. Werner, and J. Eisert, *General framework for randomized benchmarking*, PRX Quantum **3**, 020357 (2022), arXiv:2010.07974 [quant-ph].

[50] M. Heinrich, M. Kliesch, and I. Roth, *Randomized benchmarking with random quantum circuits* (2023), arXiv:2212.06181 [quant-ph] .

[51] J. Helsen, X. Xue, L. M. K. Vandersypen, and S. Wehner, *A new class of efficient randomized benchmarking protocols*, npj Quantum Information **5**, 1 (2019), arXiv:1806.02048 [quant-ph].

[52] M. Arienzo, M. Heinrich, I. Roth, and M. Kliesch, *Closed-form analytic expressions for shadow estimation with brickwork circuits*, Quantum Information and Computation **23**, 961 (2023), arXiv:2211.09835 [quant-ph].

[53] M. Arienzo, D. Grinko, M. Kliesch, and M. Heinrich, *Bosonic randomized benchmarking with passive transformations*, PRX Quantum **6**, 020305 (2025), arXiv:2408.11111 [quant-ph].

[54] S. Sternberg, *Group theory and physics*, Cambridge University Press (1994).

[55] A. Barut and R. Raczka, *Theory of Group Representations and Applications* (World Scientific, 1986).

[56] G. B. Folland, *Harmonic Analysis in Phase Space*, Annals of Mathematics Studies, Vol. 122 (Princeton University Press, Princeton, New Jersey, 1989).

[57] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. (Cambridge University Press, Cambridge, 2010).

[58] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, *Surface codes: Towards practical large-scale quantum computation*, Physical Review A **86**, 032324 (2012), arXiv:1208.0928 [quant-ph].

[59] Z. Li, H. Zheng, Y. Wang, L. Jiang, Z.-W. Liu, and J. Liu, *SU(d)-Symmetric Random Unitaries: Quantum Scrambling, Error Correction, and Machine Learning*, npj Quantum Information **11**, 158 (2025), arXiv:2309.16556 [quant-ph].

[60] A. Arai, *Analysis on Fock Spaces and Mathematical Theory of Quantum Fields: An Introduction to Mathematical Analysis of Quantum Fields* (Wolrd Scientific, 2018).

[61] E. Bannai, Y. Nakata, T. Okuda, and D. Zhao, *Explicit construction of exact unitary designs* (2020), arXiv:2009.11170 [math] .

[62] T. Giordano, D. Kerr, N. C. Phillips, and A. Toms, *Crossed Products of $C^*$-Algebras, Topological Dynamics, and Classification*, edited by F. Perera, Advanced Courses in Mathematics – CRM Barcelona (Birkhäuser, Cham, Switzerland, 2018).

[63] G. B. Folland, *A Course in Abstract Harmonic Analysis*, 2nd ed., Textbooks in Mathematics (CRC Press, Boca Raton, Florida, 2016).

[64] E. Kaniuth and K. F. Taylor, *Induced Representations of Locally Compact Groups*, Cambridge Tracts in Mathematics (Cambridge University Press, Cambridge, 2012).

[65] A. W. Knapp, *Lie Groups Beyond an Introduction* (Birkhäuser Boston, Boston, MA, 1996).

[66] B. C. Hall, *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*, Graduate Texts in Mathematics, Vol. 222 (Springer International Publishing, Cham, 2015).

[67] W. Gowers, *Generalizations of Fourier analysis, and how to apply them*, Bulletin of the American Mathematical Society **54**, 1 (2016).

[68] V. S. Varadarajan, *Geometry of Quantum Theory: Second Edition*, 2nd ed. (Springer-Verlag, New York, 1968).

[69] W. Fulton and J. Harris, *Representation Theory*, Graduate Texts in Mathematics, Vol. 129 (Springer, New York, NY, 2004).

[70] L. C. Biedenharn, *On the Representations of the Semisimple Lie Groups. I. The Explicit Construction of Invariants for the Unimodular Unitary Group in N Dimensions*, Journal of Mathematical Physics **4**, 436 (2004).

[71] G. E. Baird and L. C. Biedenharn, *On the Representations of the Semisimple Lie Groups. II*, Journal of Mathematical Physics **4**, 1449 (2004).

[72] G. E. Baird and L. C. Biedenharn, *On the representations of the semisimple lie groups. III. The explicit conjugation operation for* $\mathrm{SU}_n$, Journal of Mathematical Physics **5**, 1723 (1964).

[73] R. M. Delaney and B. Gruber, *Inner and Restriction Multiplicity for Classical Groups*, Journal of Mathematical Physics **10**, 252 (1969).

[74] A. Alex, *Non-Abelian Symmetries in the Numerical Renormalization Group*, Ph.D. thesis, Ludwig-Maximilians-Universität Münich (2009).

[75] W. Fulton, *Young Tableaux: With Applications to Representation Theory and Geometry*, London Mathematical Society Student Texts (Cambridge University Press, Cambridge, 1996).

[76] P. Di Francesco, P. Mathieu, and D. Sénéchal, *Conformal Field Theory*, Graduate Texts in Contemporary Physics (Springer, New York, NY, 1997).

[77] A. Alex, M. Kalus, A. Huckleberry, and J. von Delft, *A numerical algorithm for the explicit calculation of SU(N) and SL*$(n, \mathbb{C})$ *Clebsch–Gordan coefficients*, Journal of Mathematical Physics **52**, 023507 (2011), arXiv:1009.0437 [quant-ph].

[78] M. Mathur, I. Raychowdhury, and R. Anishetty, *SU(N) irreducible Schwinger bosons*, Journal of Mathematical Physics **51**, 093504 (2010), arXiv:1003.5487 [math-ph].

[79] M. Mathur, I. Raychowdhury, and T. P. Sreeraj, *Invariants, projection operators and SU(N)×SU(N) irreducible Schwinger bosons*, Journal of Mathematical Physics **52**, 113505 (2011), arXiv:1108.5246 [math-ph].

[80] J. F. Cornwell, *Group Theory in Physics*, Vol. 1 (Academic Press, 1984).

[81] J. F. Cornwell, *Group Theory in Physics*, Vol. 2 (Academic Press, 1984).

[82] R. Goodman and N. R. Wallach, *Symmetry, Representations, and Invariants*, Graduate Texts in Mathematics, Vol. 255 (Springer, New York, NY, 2009).

[83] B. Collins and P. Sniady, *Integration with respect to the Haar measure on unitary, orthogonal and symplectic group*, Communications in Mathematical Physics **264**, 773 (2006), arXiv:math-ph/0402073.

[84] A. A. Mele, *Introduction to Haar measure tools in quantum information: A beginner's tutorial*, Quantum **8**, 1340 (2024), arXiv:2307.08956 [quant-ph].

[85] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, and D. G. Cory, *Pseudo-random unitary operators for quantum information processing*, Science **302**, 2098 (2003), arXiv:quant-ph/0410087 [quant-ph].

[86] A. J. Scott, *Tight informationally complete quantum measurements*, Journal of Physics A: Mathematical and General **39**, 13507 (2006), arXiv:quant-ph/0604049 [quant-ph].

[87] J. Kovačević and A. Chebira, *An introduction to frames*, Foundations and Trends in Signal Processing **2**, 1 (2008).

[88] S. F. D. Waldron, *An Introduction to Finite Tight Frames* (Springer, New York, NY, 2018).

[89] F. C. Perez, V. G. Avella, and D. Goyeneche, *Mutually unbiased frames*, Quantum **6**, 851 (2022), arXiv:2110.08293 [quant-ph].

[90] M. Heinrich, *On stabiliser techniques and their application to simulation and certification of quantum devices*, Ph.D. thesis, Universität zu Köln (2021).

[91] G. M. D'Ariano, M. G. A. Paris, and M. F. Sacchi, *Quantum Tomography*, arXiv:quant-ph/0302028 (2003), arXiv:quant-ph/0302028.

[92] S. T. Flammia, D. Gross, Y.-K. Liu, and J. Eisert, *Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators*, New Journal of Physics **14**, 095022 (2012), arXiv:1205.2300 [quant-ph].

[93] S. Aaronson, *Shadow Tomography of Quantum States*, (2018), arXiv:1711.01053 [quant-ph].

[94] R. King, D. Gosset, R. Kothari, and R. Babbush, *Triply efficient shadow tomography*, PRX Quantum **6**, 010336 (2025), arXiv:2404.19211 [quant-ph].

[95] W. J. Huggins, J. R. McClean, N. C. Rubin, Z. Jiang, N. Wiebe, and R. Babbush, *Unbiasing fermionic quantum Monte Carlo with a quantum computer*, Nature **603**, 416 (2022), arXiv:2106.16235 [quant-ph].

[96] K. Wan, W. J. Huggins, J. Lee, and R. Babbush, *Matchgate Shadows for Fermionic Quantum Simulation*, Communications in Mathematical Physics **404**, 629 (2023), arXiv:2207.13723 [quant-ph].

[97] B. Wu and D. E. Koh, *Error-mitigated fermionic classical shadows on noisy quantum devices*, npj Quantum Information **10**, 39 (2024), arXiv:2310.12726 [quant-ph].

[98] Y. Wang, I. Avdic, and D. A. Mazziotti, *Shadow ansatz for the many-fermion wave function in scalable molecular simulations on quantum computing devices*, Physical Review A **112**, 022432 (2025), arXiv:2408.11026 [quant-ph].

[99] A. Zhao, N. C. Rubin, and A. Miyake, *Fermionic partial tomography via classical shadows*, Physical Review Letters **127**, 110504 (2021), arXiv:2010.16094 [quant-ph].

[100] J. Helsen, M. Ioannou, J. Kitzinger, E. Onorati, A. H. Werner, J. Eisert, and I. Roth, *Shadow estimation of gate-set properties from random sequences*, Nature Communications **14**, 5039 (2023), arXiv:2110.13178 [quant-ph].

[101] A. Acharya, S. Saha, and A. M. Sengupta, *Informationally complete POVM-based shadow tomography* (2021), arXiv:2105.05992 [quant-ph] .

[102] B. Moran, S. Howard, and D. Cochran, in *Excursions in Harmonic Analysis, Volume 2*, Applied and Numerical Harmonic Analysis, edited by T. D. Andrews, R. Balan, J. J. Benedetto, W. Czaja, and K. A. Okoudjou (Birkhäuser Boston, Boston, Massachusetts, 2013) pp. 49–64, arXiv:1111.1450 [math.FA] .

[103] F. Sauvage and M. Larocca, *Classical shadows with symmetries* (2024), arXiv:2408.05279 [quant-ph] .

[104] M. R. Jerrum, L. G. Valiant, and V. V. Vazirani, *Random generation of combinatorial structures from a uniform distribution*, Theoretical Computer Science **43**, 169 (1986).

[105] K. Bu, D. E. Koh, R. J. Garcia, and A. Jaffe, *Classical shadows with Pauli-invariant unitary ensembles*, npj Quantum Information **10**, 6 (2024), arXiv:2202.03272 [quant-ph].

[106] C. Bertoni, J. Haferkamp, M. Hinsche, M. Ioannou, J. Eisert, and H. Pashayan, *Shallow Shadows: Expectation estimation using low-depth random Clifford circuits*, Physical Review Letters **133**, 020602 (2024), arXiv:2209.12924 [cond-mat, physics:quant-ph].

[107] A. Roy and A. J. Scott, *Unitary designs and codes*, Designs, Codes and Cryptography **53**, 13 (2009), arXiv:0809.3813 [quant-ph].

[108] H.-Y. Hu, S. Choi, and Y.-Z. You, *Classical shadow tomography with locally scrambled quantum dynamics*, Physical Review Research **5**, 023027 (2023), arXiv:2107.04817 [quant-ph].

[109] A. A. Akhtar, H.-Y. Hu, and Y.-Z. You, *Scalable and flexible classical shadow tomography with tensor networks*, Quantum **7**, 1026 (2023), arXiv:2209.02093 [quant-ph].

[110] R. König and J. A. Smolin, *How to efficiently select an arbitrary Clifford group element*, Journal of Mathematical Physics **55**, 122202 (2014), arXiv:1406.2170 [quant-ph].

[111] S. Bravyi and D. Maslov, *Hadamard-Free Circuits Expose the Structure of the Clifford Group*, IEEE Transactions on Information Theory **67**, 4546 (2021), arXiv:2003.09412 [quant-ph].

[112] M. Ippoliti, Y. Li, T. Rakovszky, and V. Khemani, *Operator relaxation and the optimal depth of classical shadows*, Physical Review Letters **130**, 230403 (2023), arXiv:2212.11963 [quant-ph].

[113] T. Zhang, J. Sun, X.-X. Fang, X.-M. Zhang, X. Yuan, and H. Lu, *Experimental quantum state measurement with classical shadows*, Physical Review Letters **127**, 200501 (2021), arXiv:2008.05234 [quant-ph].

[114] G. Struchalin, Ya. A. Zagorovskii, E. Kovlakov, S. Straupe, and S. Kulik, *Experimental Estimation of Quantum State Properties from Classical Shadows*, PRX Quantum **2**, 010307 (2021), arXiv:2008.05234 [quant-ph].

[115] S. Chen, W. Yu, P. Zeng, and S. T. Flammia, *Robust shadow estimation*, PRX Quantum **2**, 030348 (2021), arXiv:2011.09636.

[116] D. E. Koh and S. Grewal, *Classical shadows with noise*, Quantum **6**, 776 (2022), arXiv:2011.11580 [quant-ph].

[117] R. Brieger, M. Heinrich, I. Roth, and M. Kliesch, *Stability of classical shadows under gate-dependent noise*, Physical Review Letters **134**, 090801 (2025), arXiv:2310.19947 [quant-ph].

[118] C. Dankert, *Efficient Simulation of Random Quantum States and Operators*, Master's thesis, University of Waterloo (2005), arXiv:quant-ph/0512217 [quant-ph] .

[119] A. V. Oppenheim, R. W. Schafer, and J. R. Buck, *Discrete-Time Signal Processing*, 2nd ed. (Prentice Hall, Upper Saddle River, NJ, 1999).

[120] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, *Local random quantum circuits are approximate polynomial-designs*, Communications in Mathematical Physics **346**, 397–434 (2016), arXiv:1208.0692 [quant-ph].

[121] The mpmath development team, *mpmath: a Python Library for Arbitrary-Precision Floating-Point Arithmetic, Version 1.3.0* (2023).

[122] Y. Alexeev, V. S. Batista, N. Bauman, L. Bertels, D. Claudino, R. Dutta, L. Gagliardi, S. Godwin, N. Govind, M. Head-Gordon, M. Hermes, K. Kowalski, A. Li, C. Liu, J. Liu, P. Liu, J. M. García-Lastra, D. Mejía-Rodríguez, K. Mueller, M. Otten, B. Peng, M. Raugus, M. Reiher, P. Rigor, W. Shaw, M. van Schilfgaarde, T. Vegge, Y. Zhang, M. Zheng, and L. Zhu, *A perspective on quantum computing applications in quantum chemistry using 25–100 logical qubits* (2025), arXiv:2506.19337 [quant-ph] .

[123] P. Deglmann, A. Schäfer, and C. Lennartz, *Application of quantum calculations in the chemical industry—An overview*, International Journal of Quantum Chemistry **115**, 107 (2015).

[124] A. Heifetz, ed., *Quantum Mechanics in Drug Discovery*, Methods in Molecular Biology, Vol. 2114 (Springer US, New York, NY, 2020).

[125] A. Van der Ven, Z. Deng, S. Banerjee, and S. P. Ong, *Rechargeable alkali-ion battery materials: Theory and computation*, Chemical Reviews **120**, 6977 (2020).

[126] N. S. Blunt, J. Camps, O. Crawford, R. Izsák, S. Leontica, A. Mirani, A. E. Moylett, S. A. Scivier, C. Sünderhauf, P. Schopf, J. M. Taylor, and N. Holzmann, *Perspective on the current state-of-the-art of quantum computing for drug discovery applications*, Journal of Chemical Theory and Computation **18**, 7001 (2022).

[127] V. Lordi and J. M. Nichol, *Advances and opportunities in materials science for scalable quantum computing*, MRS Bulletin **46**, 589 (2021).

[128] Y. Cao, J. Romero, and A. Aspuru-Guzik, *Potential of quantum computing for drug discovery*, IBM Journal of Research and Development **62**, 6:1 (2018).

[129] D. A. Mazziotti, *First-order semidefinite programming for the two-electron treatment of many-electron atoms and molecules*, ESAIM: Mathematical Modelling and Numerical Analysis **41**, 249 (2007).

[130] I. Peschel and V. Eisler, *Reduced density matrices and entanglement entropy in free lattice models*, Journal of Physics A: Mathematical and Theoretical **42**, 504003 (2009).

[131] A. E. DePrince III, *Variational determination of the two-electron reduced density matrix: A tutorial review* (2023), arXiv:2310.10746 [physics.chem-ph] .

[132] A. J. Coleman, *Structure of Fermion Density Matrices*, Reviews of Modern Physics **35**, 668 (1963).

[133] D. A. Mazziotti, *Two-electron reduced density matrix as the basic variable in many-electron quantum chemistry and physics*, Chemical Reviews **112**, 244 (2012).

[134] H. R. Fredheim and S. Kvaal, *Reduced Density Matrix Functional Theory And A Reduced Formulation Of Density Functional Theory* (2026), arXiv:2510.12242 [math-ph] .

[135] E. Knill, *Fermionic Linear Optics and Matchgates* (2001), arXiv:quant-ph/0108033 .

[136] S. Bravyi, *Lagrangian representation for fermionic linear optics* (2004), arXiv:quant-ph/0404180 .

[137] J. Helsen, S. Nezami, M. Reagor, and M. Walter, *Matchgate benchmarking: Scalable benchmarking of a continuous family of many-qubit gates*, Quantum **6**, 657 (2022), arXiv:2011.13048 [quant-ph].

[138] A. A. Mele and Y. Herasymenko, *Efficient learning of quantum states prepared with few fermionic non-gaussian gates*, PRX Quantum **6**, 010319 (2025), arXiv:2402.18665 [quant-ph].

[139] B. M. Terhal and D. P. DiVincenzo, *Classical simulation of noninteracting-fermion quantum circuits* (2001), arXiv:quant-ph/0108010 .

[140] M. Ishikawa and M. Wakayama, *Applications of minor summation formula iii, Plücker relations, lattice paths and Pfaffian identities* (2005), arXiv:math/0312358 .

[141] V. Heyraud, H. Chomet, and J. Tilly, *Unified framework for matchgate classical shadows*, npj Quantum Information **11**, 65 (2025), arXiv:2409.03836 [quant-ph].

[142] G. H. Low, *Classical shadows of fermions with particle number symmetry* (2024), arXiv:2208.08964 [quant-ph] .

[143] M. Reiher, N. Wiebe, K. M. Svore, D. Wecker, and M. Troyer, *Elucidating reaction mechanisms on quantum computers*, Proceedings of the National Academy of Sciences of the United States of America **114**, 7555 (2017).

[144] R. Babbush, C. Gidney, D. W. Berry, N. Wiebe, J. McClean, A. Paler, A. Fowler, and H. Neven, *Encoding electronic spectra in quantum circuits with linear T complexity*, Physical Review X **8**, 041015 (2018), arXiv:1805.03662 [quant-ph].

[145] G. H. Low and N. Wiebe, *Hamiltonian simulation in the interaction picture* (2018), arXiv:1805.00675 [quant-ph] .

[146] J. Wilkens, M. Ioannou, E. Derbyshire, J. Eisert, D. Hangleiter, I. Roth, and J. Haferkamp, *Benchmarking bosonic and fermionic dynamics* (2024), arXiv:2408.11105 .

[147] G.-L. R. Anselmetti, D. Wierichs, C. Gogolin, and R. M. Parrish, *Local, expressive, quantum-number-preserving VQE ansätze for fermionic systems*, New Journal of Physics **23**, 113010 (2021), arXiv:2104.05695 [quant-ph].

[148] A. Zhao and A. Miyake, *Group-theoretic error mitigation enabled by classical shadows and symmetries*, npj Quantum Information **10**, 57 (2024), arXiv:2310.03071 [quant-ph].

[149] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press, Boca Raton, 2017).

[150] N. J. Vilenkin and A. U. Klimyk, *Representation of Lie Groups and Special Functions: Volume 3: Classical and Quantum Groups and Special Functions* (Springer Science & Business Media).

[151] N. Vilenkin and A. Klimyk, *Representation of Lie Groups and Special Functions*, Vol. 1: Simplest Lie Groups, Special Functions and Integral Transforms (Springer, 1993) part of the book series: Mathematics and its Applications.

[152] N. Vilenkin and A. Klimyk, *Representation of Lie Groups and Special Functions*, Vol. 2: Class I Representations, Special Functions, and Integral Transforms (Springer, 1993) part of the book series: Mathematics and its Applications.

[153] J. Paldus, *Matrix elements of unitary group generators in many-fermion correlation problem. I. tensorial approaches*, Journal of Mathematical Chemistry **59**, 1 (2021).

[154] J. Paldus, *Matrix elements of unitary group generators in many-fermion correlation problem. II. graphical methods of spin algebras*, Journal of Mathematical Chemistry **59**, 37 (2021).

[155] J. Paldus, *Matrix elements of unitary group generators in many-fermion correlation problem. III. green-gould approach*, Journal of Mathematical Chemistry **59**, 72 (2021).

[156] F. Di Colandrea, A. Babazadeh, A. Dauphin, P. Massignan, L. Marrucci, and F. Cardano, *Ultra-long quantum walks via spin–orbit photonics*, Optica **10**, 324 (2023).

[157] F. Di Colandrea, T. Jaouni, J. Grace, D. Paneru, M. Arienzo, A. D'Errico, and E. Karimi, *Engineering qubit dynamics in open systems with photonic synthetic lattices*, Physical Review Research **7**, 023236 (2025), arXiv:2412.04701 [quant-ph].

[158] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, *Continuous-variable quantum key distribution system: Past, present, and future*, Applied Physics Reviews **11**, 011318 (2024), arXiv:2310.04831 [quant-ph].

[159] R. Schnabel, *Squeezed states of light and their applications in laser interferometers*, Physics Reports **684**, 1 (2017), arXiv:1611.03986 [quant-ph].

[160] E. Knill, R. Laflamme, and G. J. Milburn, *A scheme for efficient quantum computation with linear optics*, Nature **409**, 46 (2001), arXiv:quant-ph/0006088 [quant-ph].

[161] M. Koashi, T. Yamamoto, and N. Imoto, *Probabilistic manipulation of entangled photons*, Physical Review A **63**, 030301 (2001), arXiv:quant-ph/0102141 [quant-ph].

[162] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, *Linear optical quantum computing with photonic qubits*, Reviews of Modern Physics **79**, 135 (2007), arXiv:quant-ph/0512071 [quant-ph].

[163] T. Rudolph, *Why i am optimistic about the silicon-photonic route to quantum computing*, APL Photonics **2**, 030901 (2017), arXiv:1607.08535 [quant-ph].

[164] S.-H. Tan and P. P. Rohde, *The resurgence of the linear optics quantum interferometer: Recent advances and applications*, Reviews in Physics **4**, 100030 (2019), arXiv:1805.11827 [quant-ph].

[165] PsiQuantum team, *A manufacturable platform for photonic quantum computing*, Nature **641**, 876 (2025), arXiv:2404.17570 [quant-ph].

[166] V. V. Albert, in *Proceedings of the International School of Physics "Enrico Fermi"*, Vol. 209 (IOS Press, 2025) pp. 79–107, arXiv:2211.05714 [quant-ph] .

[167] B. Q. Baragiola, G. Pantaleoni, R. N. Alexander, A. Karanjai, and N. C. Menicucci, *All-Gaussian universality and fault tolerance with the Gottesman-Kitaev-Preskill code*, Physical Review Letters **123**, 200502 (2019), arXiv:1903.00012 [quant-ph].

[168] D. Gottesman, A. Kitaev, and J. Preskill, *Encoding a qubit in an oscillator*, Physical Review A **64**, 012310 (2001), arXiv:quant-ph/0008040 [quant-ph].

[169] R. Raussendorf and H. J. Briegel, *A one-way quantum computer*, Physical Review Letters **86**, 5188 (2001), arXiv:quant-ph/0010033 [quant-ph].

[170] R. Raussendorf, D. E. Browne, and H. J. Briegel, *Measurement-based quantum computation on cluster states*, Physical Review A **68**, 022312 (2003), arXiv:quant-ph/0301052 [quant-ph].

[171] R. Jozsa, *An introduction to measurement based quantum computation* (2005), arXiv:quant-ph/0508124 .

[172] M. V. Larsen, X. Guo, C. R. Breum, J. S. Neergaard-Nielsen, and U. L. Andersen, *Deterministic generation of a two-dimensional cluster state*, Science **366**, 369–372 (2019), arXiv:1906.08709 [physics, physics:quant-ph].

[173] M. V. Larsen, X. Guo, C. R. Breum, J. S. Neergaard-Nielsen, and U. L. Andersen, *Deterministic multi-mode gates on a scalable photonic quantum computing platform*, Nature Physics **17**, 1018 (2021), arXiv:2010.14422 [quant-ph].

[174] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, *Silica-on-Silicon Waveguide Quantum Circuits*, Science **320**, 646 (2008), arXiv:0802.0136 [quant-ph].

[175] J. P. Sprengers, A. Gaggero, D. Sahin, S. Jahanmirinejad, G. Frucci, F. Mattioli, R. Leoni, J. Beetz, M. Lermer, M. Kamp, S. Höfling, R. Sanjines, and A. Fiore, *Waveguide superconducting single-photon detectors for integrated quantum photonic circuits*, Applied Physics Letters **99**, 181110 (2011), arXiv:1108.5107 [quant-ph].

[176] J. W. Silverstone, D. Bonneau, K. Ohira, N. Suzuki, H. Yoshida, N. Iizuka, M. Ezaki, C. M. Natarajan, M. G. Tanner, R. H. Hadfield, V. Zwiller, G. D. Marshall, J. G. Rarity, J. L. O'Brien, and M. G. Thompson, *On-chip quantum interference between silicon photon-pair sources*, Nature Photonics **8**, 104 (2014), arXiv:1304.1490 [quant-ph].

[177] T. Meany, M. Gräfe, R. Heilmann, A. Perez-Leija, S. Gross, M. J. Steel, M. J. Withford, and A. Szameit, *Laser written circuits for quantum photonics*, Laser & Photonics Reviews **9**, 363 (2015).

[178] D. Ruiz, J. Guillaud, A. Leverrier, M. Mirrahimi, and C. Vuillot, *LDPC-cat codes for low-overhead quantum computing in 2D*, Nature Communications **16**, 1040 (2025), arXiv:2401.09541 [quant-ph].

[179] J. E. Bourassa, R. N. Alexander, M. Vasmer, A. Patil, I. Tzitrin, T. Matsuura, D. Su, B. Q. Baragiola, S. Guha, G. Dauphinais, K. K. Sabapathy, N. C. Menicucci, and I. Dhand, *Blueprint for a Scalable Photonic Fault-Tolerant Quantum Computer*, Quantum **5**, 392 (2021), arXiv:2010.02905 [quant-ph].

[180] S. Aaronson and A. Arkhipov, *The computational complexity of linear optics*, in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing*, STOC '11 (Association for Computing Machinery, New York, NY, USA, 2011) p. 333–342, arXiv:1011.3245 [quant-ph] .

[181] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, *Gaussian Boson Sampling*, Physical Review Letters **119**, 170501 (2017), arxiv:1612.01199 [quant-ph].

[182] L. Chakhmakhchyan and N. J. Cerf, *Boson sampling with Gaussian measurements*, Physical Review A **96**, 032326 (2017), arXiv:1705.05299 [quant-ph].

[183] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, *Quantum*

*computational advantage using photons*, Science **370**, 1460 (2020), arXiv:2012.01625 [cond-mat, physics:physics, physics:quant-ph].

[184] H.-S. Zhong, Y.-H. Deng, J. Qin, H. Wang, M.-C. Chen, L.-C. Peng, Y.-H. Luo, D. Wu, S.-Q. Gong, H. Su, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, J. J. Renema, C.-Y. Lu, and J.-W. Pan, *Phase-programmable gaussian boson sampling using stimulated squeezed light*, Physical Review Letters **127**, 180502 (2021).

[185] L. S. Madsen, F. Laudenbach, M. F. Askarani, F. Rortais, T. Vincent, J. F. F. Bulmer, F. M. Miatto, L. Neuhaus, L. G. Helt, M. J. Collins, A. E. Lita, T. Gerrits, S. W. Nam, V. D. Vaidya, M. Menotti, I. Dhand, Z. Vernon, N. Quesada, and J. Lavoie, *Quantum computational advantage with a programmable photonic processor*, Nature **606**, 75 (2022).

[186] A. I. Lvovsky and M. G. Raymer, *Continuous-variable optical quantum state tomography*, Reviews of Modern Physics **81**, 299 (2009), arXiv:quant-ph/0511044.

[187] K. Sharma and M. M. Wilde, *Characterizing the performance of continuous-variable Gaussian quantum gates*, Physical Review Research **2**, 013126 (2020), arXiv:1810.12335 [quant-ph].

[188] Y.-D. Wu, G. Bai, G. Chiribella, and N. Liu, *Efficient Verification of Continuous-Variable Quantum States and Devices without Assuming Identical and Independent Operations*, Physical Review Letters **126**, 240503 (2021).

[189] L. Bittel, F. A. Mele, J. Eisert, and A. A. Mele, *Energy-independent tomography of Gaussian states* (2025), arXiv:2508.14979 [quant-ph] .

[190] C. C. López, A. Bendersky, J. P. Paz, and D. G. Cory, *Progress toward scalable tomography of quantum maps using twirling-based methods and information hierarchies*, Physical Review A **81**, 062113 (2010), arXiv:1003.2444 [quant-ph].

[191] C. T. Schmiegelow, A. Bendersky, M. A. Larotonda, and J. P. Paz, *Selective and Efficient Quantum Process Tomography without Ancilla*, Physical Review Letters **107**, 100502 (2011), arXiv:1002.4436 [quant-ph].

[192] A. Bendersky and J. P. Paz, *Selective and efficient quantum state tomography and its application to quantum process tomography*, Physical Review A **87**, 012122 (2013), arXiv:1808.01258 [quant-ph].

[193] R. Namiki, *Schmidt-number benchmarks for continuous-variable quantum devices*, Physical Review A **93**, 052336 (2016), arXiv:1511.03321 [quant-ph].

[194] J. B. Altepeter, D. Branning, E. Jeffrey, T. C. Wei, P. G. Kwiat, R. T. Thew, J. L. O'Brien, M. A. Nielsen, and A. G. White, *Ancilla-assisted quantum process tomography*, Physical Review Letters **90**, 193601 (2003), arXiv:quant-ph/0303038 [quant-ph].

[195] G. Bai and G. Chiribella, *Test One to Test Many: A Unified Approach to Quantum Benchmarks*, Physical Review Letters **120**, 150502 (2018), arXiv:2409.03836 [quant-ph].

[196] R. Blume-Kohout and P. S. Turner, *The curious nonexistence of gaussian 2-designs*, Communications in Mathematical Physics **326** (2014), arXiv:1110.1042 [quant-ph].

[197] Q. Zhuang, T. Schuster, B. Yoshida, and N. Y. Yao, *Scrambling and Complexity in Phase Space*, Physical Review A **99**, 062334 (2019), arXiv:1902.04076.

[198] R. M. S. Farias and L. Aolita, *Certification of continuous-variable gates using average channel-fidelity witnesses*, Quantum Science and Technology **6**, 035014 (2021), arXiv:1812.01968.

[199] S. T. Merkel, E. J. Pritchett, and B. H. Fong, *Randomized benchmarking as convolution: Fourier analysis of gate dependent errors*, Quantum **5**, 581 (2021), arXiv:1804.05951 [quant-ph].

[200] L. Kong, *A framework for randomized benchmarking over compact groups* (2021), arXiv:2111.10357 [quant-ph] .

[201] C. Dankert, R. Cleve, J. Emerson, and E. Livine, *Exact and approximate unitary 2-designs and their application to fidelity estimation*, Physical Review A **80**, 012304 (2009), arXiv:quant-ph/0606161 [quant-ph].

[202] J. Emerson, M. Silva, O. Moussa, C. Ryan, M. Laforest, J. Baugh, D. G. Cory, and R. Laflamme, *Symmetrised Characterisation of Noisy Quantum Processes*, Science **317**, 1893 (2007), arXiv:0707.0685 [quant-ph].

[203] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Randomized benchmarking of quantum gates*, Physical Review A **77**, 012307 (2008), arXiv:0707.0963 [quant-ph].

[204] E. Magesan, J. M. Gambetta, and J. Emerson, *Scalable and Robust Randomized Benchmarking of Quantum Processes*, Physical Review Letters **106**, 180504 (2011), arXiv:1009.3639 [quant-ph].

[205] E. Magesan, J. M. Gambetta, B. R. Johnson, C. A. Ryan, J. M. Chow, S. T. Merkel, M. P. da Silva, G. A. Keefe, M. B. Rothwell, T. A. Ohki, M. B. Ketchen, and M. Steffen, *Efficient Measurement of Quantum Gate Error by Interleaved Randomized Benchmarking*, Physical Review Letters **109**, 080505 (2012), arXiv:1203.4550 [quant-ph].

[206] T. Proctor, K. Rudinger, K. Young, M. Sarovar, and R. Blume-Kohout, *What randomized benchmarking actually measures*, Physical Review Letters **119**, 130502 (2017), arXiv:1702.01853 [quant-ph].

[207] J. J. Wallman, *Randomized benchmarking with gate-dependent noise*, Quantum **2**, 47 (2018), arXiv:1703.09835 [quant-ph].

[208] R. Harper, I. Hincks, C. Ferrie, S. T. Flammia, and J. J. Wallman, *Statistical analysis of randomized benchmarking*, Physical Review A **99**, 052350 (2019), arXiv:1901.00535 [quant-ph].

[209] T. Proctor, S. Seritan, K. Rudinger, E. Nielsen, R. Blume-Kohout, and K. Young, *Scalable randomized benchmarking of quantum computers using mirror circuits*, Physical Review Letters **129**, 150502 (2022), arXiv:2112.09853 [quant-ph].

[210] R. Harper and S. T. Flammia, *Estimating the fidelity of T gates using standard interleaved randomized benchmarking*, Quantum Science and Technology **2**, 015008 (2017), arXiv:1608.02943 [quant-ph].

[211] E. Onorati, A. H. Werner, and J. Eisert, *Randomized benchmarking for individual quantum gates*, Physical Review Letters **123**, 060501 (2019), arXiv:1811.11775.

[212] S. Sheldon, L. S. Bishop, E. Magesan, S. Filipp, J. M. Chow, and J. M. Gambetta, *Characterizing errors on qubit operations via iterative randomized benchmarking*, Physical Review A **93**, 012301 (2016), arXiv:1504.06597 [quant-ph].

[213] A. Erhard, J. J. Wallman, L. Postler, M. Meth, R. Stricker, E. A. Martinez, P. Schindler, T. Monz, J. Emerson, and R. Blatt, *Characterizing large-scale quantum computers via cycle benchmarking*, Nature Communications **10**, 5347 (2019), arXiv:1902.08543.

[214] T. J. Proctor, A. Carignan-Dugas, K. Rudinger, E. Nielsen, R. Blume-Kohout, and K. Young, *Direct randomized benchmarking for multiqubit devices*, Physical Review Letters **123**, 030503 (2019), arXiv:1807.07975 [quant-ph].

[215] J. J. Wallman, C. Granade, R. Harper, and S. T. Flammia, *Estimating the Coherence of Noise*, New Journal of Physics **17**, 113020 (2015), arXiv:1503.07865 [quant-ph].

[216] J. J. Wallman, M. Barnhill, and J. Emerson, *Robust characterization of leakage errors*, New Journal of Physics **18**, 043021 (2016), arXiv:1412.4126 [quant-ph].

[217] C. J. Wood and J. M. Gambetta, *Quantification and Characterization of Leakage Errors*, Physical Review A **97**, 032306 (2018), arXiv:1704.03081 [quant-ph].

[218] Y.-H. Chen and C. H. Baldwin, *Randomized benchmarking with leakage errors*, Physical Review Research **7**, 043065 (2025), arXiv:2502.00154 [quant-ph].

[219] D. S. França and A.-L. Hashagen, *Approximate Randomized Benchmarking for Finite Groups*, Journal of Physics A: Mathematical and Theoretical **51**, 395302 (2018), arXiv:1803.03621.

[220] J. Helsen, M. Ioannou, J. Kitzinger, E. Onorati, A. H. Werner, J. Eisert, and I. Roth, *Shadow estimation of gate-set properties from random sequences*, Nature Communications **14** (2023), arXiv:2110.13178 [quant-ph].

[221] A. W. Knapp, *Basic Algebra*, Cornerstones (Birkhäuser, Boston, MA, 2006).

[222] J. J. Wallman, *Randomized benchmarking with gate-dependent noise*, Quantum **2**, 47 (2018), arXiv:1703.09835 [quant-ph].

[223] J. M. Hokanson, *Numerically Stable and Statistically Efficient Algorithms for Large Scale Exponential Fitting*, Ph.D. thesis, Rice University (2013).

[224] S. T. Flammia and J. J. Wallman, *Efficient estimation of Pauli channels*, ACM Transactions on Quantum Computing **1**, 1 (2020), arXiv:1907.12976.

[225] A. Carignan-Dugas, J. J. Wallman, and J. Emerson, *Characterizing universal gate sets via dihedral benchmarking*, Physical Review A **92**, 060302 (2015), arXiv:1508.06312 [quant-ph].

[226] G. W. Stewart and J.-g. Sun, *Matrix Perturbation Theory* (Elsevier Science, 1990).

[227] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).

[228] C. H. Valahu, T. Navickas, M. J. Biercuk, and T. R. Tan, *Benchmarking bosonic modes for quantum information with randomized displacements*, PRX Quantum **5**, 040337 (2024), arxiv:2405.15237 [quant-ph].

[229] Y. Liu, M. Otten, R. Bassirianjahromi, L. Jiang, and B. Fefferman, *Benchmarking near-term quantum computers via random circuit sampling* (2022), arXiv:2105.05232 [quant-ph] .

[230] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, *Characterizing Quantum Supremacy in Near-Term Devices*, Nature Physics **14**, 595 (2018), arXiv:1608.00263.

[231] X. Liu, C. Guo, Y. Liu, Y. Yang, J. Song, J. Gao, Z. Wang, W. Wu, D. Peng, P. Zhao, F. Li, H.-L. Huang, H. Fu, and D. Chen, *Redefining the Quantum Supremacy Baseline With a New Generation Sunway Supercomputer*, (2021), arXiv:2111.01066 [quant-ph].

[232] D. Hangleiter and J. Eisert, *Computational advantage of quantum random sampling*, Reviews of Modern Physics **95**, 035001 (2023), arXiv:2206.04079 [quant-ph].

[233] G. Adesso, S. Ragy, and A. R. Lee, *Continuous variable quantum information: Gaussian states and beyond*, Open Systems and Information Dynamics **21**, 1440001 (2014), arXiv:1401.4679 [quant-ph].

[234] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian States in Quantum Information*, Napoli Series on Physics and Astrophysics (Bibliopolis, 2005) arXiv:quant-ph/0503237 [quant-ph] .

[235] J. B. Brask, *Gaussian states and operations: A quick reference* (2021), arXiv:2102.05748 [quant-ph] .

[236] Arvind, B. Dutta, N. Mukunda, and R. Simon, *The real symplectic groups in quantum mechanics and optics*, Pramana **45**, 471 (1995), arXiv:quant-ph/9509002 [quant-ph].

[237] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, *Experimental realization of any discrete unitary operator*, Physical Review Letters **73**, 58 (1994).

[238] J. Carolan, C. Harrold, C. Sparrow, E. Martín-López, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G. D. Marshall, M. G. Thompson, J. C. F. Matthews, T. Hashimoto, J. L. O'Brien, and A. Laing, *Universal linear optics*, Science **349**, 711 (2015), arXiv:1505.01182 [quant-ph].

[239] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley, *Optimal design for universal multiport interferometers*, Optica **3**, 1460 (2016), arXiv:1603.08788 [quant-ph].

[240] H. de Guise, O. Di Matteo, and L. L. Sanchez-Soto, *Simple factorization of unitary transformations*, Physical Review A **97**, 022328 (2018), arXiv:1708.00735 [quant-ph].

[241] P. Aniello, C. Lupo, and M. Napolitano, *Exploring Representation Theory of Unitary Groups via Linear Optical Passive Devices*, Open Systems and Information Dynamics **13**, 415 (2006).

[242] F. Marsili, D. Bitauld, A. Gaggero, S. Jahanmirinejad, R. Leoni, F. Mattioli, and A. Fiore, *Physics and application of photon number resolving detectors based on superconducting parallel nanowires*, New Journal of Physics **11**, 045022 (2009), arXiv:0902.4824 [quant-ph].

[243] J. Provazník, L. Lachman, R. Filip, and P. Marek, *Benchmarking photon number resolving detectors*, Optics Express **28**, 14839 (2020), arXiv:2005.02093 [quant-ph].

[244] R. Nehra and K. V. Jacob, *Characterizing quantum detectors by Wigner functions* (2019), arXiv:1909.10628 [quant-ph] .

[245] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Gaussian Quantum Information*, Reviews of Modern Physics **84**, 621 (2012), arXiv:1110.3234.

[246] A. S. Holevo, *Structure of a general quantum gaussian observable*, Proceedings of the Steklov Institute of Mathematics **313**, 70–77 (2021).

[247] M. Cooper, L. J. Wright, C. Söller, and B. J. Smith, *Experimental generation of multi-photon Fock states*, Optics Express **21**, 5309 (2013), arXiv:1212.4412 [quant-ph].

[248] A. I. Lvovsky, P. Grangier, A. Ourjoumtsev, V. Parigi, M. Sasaki, and R. Tualle-Brouri, *Production and applications of non-Gaussian quantum states of light* (2020), arXiv:2006.16985 [physics, physics:quant-ph] .

[249] M. Walschaers, *Non-gaussian quantum states and where to find them*, PRX Quantum **2**, 030204 (2021), arXiv:2104.12596 [quant-ph].

[250] S. Scheel, *Permanents in linear optical networks* (2004), arXiv:quant-ph/0406127 .

[251] I. Dhand, B. C. Sanders, and H. de Guise, *Algorithms for SU(n) boson realizations and D-functions*, Journal of Mathematical Physics **56**, 111705 (2015), arXiv:1507.06274 [quant-ph].

[252] U. Chabaud, T. Douce, D. Markham, P. van Loock, E. Kashefi, and G. Ferrini, *Continuous-Variable Sampling from Photon-Added or Photon-Subtracted Squeezed States*, Physical Review A **96**, 062307 (2017), arXiv:1707.09245 [quant-ph].

[253] J. Marshall and N. Anand, *Simulation of quantum optics by coherent state decomposition*, Optica Quantum **1**, 78 (2023), arXiv:2305.17099 [quant-ph].

[254] J. E. Bourassa, N. Quesada, I. Tzitrin, A. Száva, T. Isacsson, J. Izaac, K. K. Sabapathy, G. Dauphinais, and I. Dhand, *Fast simulation of bosonic qubits via Gaussian functions in phase space*, PRX Quantum **2**, 040315 (2021), arXiv:2103.05530 [quant-ph].

[255] S. Rahimi-Keshari, T. C. Ralph, and C. M. Caves, *Sufficient Conditions for Efficient Classical Simulation of Quantum Optics*, Physical Review X **6**, 021039 (2016), arXiv:1511.06526 [quant-ph].

[256] N. Heurtel, S. Mansfield, J. Senellart, and B. Valiron, *Strong simulation of linear optical processes*, Computer Physics Communications **291**, 108848 (2023), arXiv:2206.10549 [quant-ph].

[257] W. Roga and M. Takeoka, *Classical simulation of boson sampling with sparse output*, Scientific Reports **10**, 14739 (2020), arXiv:1904.05494 [quant-ph].

[258] A. Alex, L. Everding, P. Littelmann, and J. von Delft, *SU(N) Clebsch-Gordan coefficients and non-Abelian symmetries*, in *APS March Meeting Abstracts*, Vol. 2012 (2012) pp. W26–011.

[259] H. J. Ryser, *Combinatorial mathematics*, Vol. 14 (American Mathematical Soc., 1963).

[260] A. Nijenhuis and H. S. Wilf, *Combinatorial algorithms: for computers and calculators*, 2nd ed. (Academic Press, Inc., 1978).

[261] P. Aniello, C. Lupo, and M. Napolitano, *Exploring Representation Theory of Unitary Groups via Linear Optical Passive Devices*, Open Systems and Information Dynamics **13**, 415 (2006).

[262] M. Bentivegna, N. Spagnolo, C. Vitelli, F. Flamini, N. Viggianiello, L. Latmiral, P. Mataloni, D. J. Brod, E. F. Galvão, A. Crespi, R. Ramponi, R. Osellame, and F. Sciarrino, *Experimental Scattershot Boson Sampling*, Science Advances **1** (2015), arXiv:1505.03708 [quant-ph].

[263] Y. Benoist and J.-F. Quint, *Random Walks on Reductive Groups* (Springer International Publishing, Cham, 2016).

[264] B. Bekka, P. de la Harpe, and A. Valette, *Kazhdan's Property (T)*, New Mathematical Monographs (Cambridge University Press, Cambridge, 2008).

[265] R. Howe, *Perspectives on Invariant Theory: Schur Duality, Multiplicity-free Actions and beyond*, Israel Mathematical Conference Proceedings **8** (1995).

[266] R. Howe, in *Harmonic Analysis and Group Representation*, C.I.M.E. Summer Schools, edited by A. F. Talamanca (Springer, Berlin, Heidelberg, 2011) pp. 224–331.

[267] V. S. Shchesnovich, *Partial indistinguishability theory for multiphoton experiments in multiport devices*, Physical Review A **91**, 013844 (2015), arXiv:1410.1506 [quant-ph].

[268] H. Ollivier, S. E. Thomas, S. C. Wein, I. M. de Buy Wenniger, N. Coste, J. C. Loredo, N. Somaschi, A. Harouri, A. Lemaitre, I. Sagnes, L. Lanco, C. Simon, C. Anton, O. Krebs, and P. Senellart, *Hong-Ou-Mandel Interference with Imperfect Single Photon Sources*, Physical Review Letters **126**, 063602 (2021), arXiv:2005.01743 [quant-ph].

[269] M. Tillmann, S.-H. Tan, S. E. Stoeckl, B. C. Sanders, H. de Guise, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, *Generalized Multiphoton Quantum Interference*, Physical Review X **5**, 041015 (2015), arXiv:1403.3433 [quant-ph].

[270] J. Shi and T. Byrnes, *Effect of partial distinguishability on quantum supremacy in Gaussian Boson sampling*, npj Quantum Information **8**, 54 (2022).

[271] M. Englbrecht, T. Kraft, C. Dittel, A. Buchleitner, G. Giedke, and B. Kraus, *Indistinguishability of identical bosons from a quantum information theory perspective*, Physical Review Letters **132**, 050201 (2024), arXiv:2307.06626 [quant-ph].

[272] E. Annoni and S. C. Wein, *Incoherent behavior of partially distinguishable photons* (2025), arXiv:2502.05047 [quant-ph] .

[273] S. Kimmel, M. P. da Silva, C. A. Ryan, B. R. Johnson, and T. Ohki, *Robust Extraction of Tomographic Information via Randomized Benchmarking*, Physical Review X **4**, 011050 (2014), arXiv:1306.2348.

[274] I. Roth, R. Kueng, S. Kimmel, Y.-K. Liu, D. Gross, J. Eisert, and M. Kliesch, *Recovering quantum gates from few average gate fidelities*, Physical Review Letters **121**, 170502 (2018), arXiv:1803.00572 [quant-ph].

[275] R. T. Sutherland, A. C. Hughes, J. P. Marceaux, H. M. Knaack, C. M. Löschnauer, and R. Srinivas, *Subspace Leakage Error Randomized Benchmarking of Mølmer-Sørensen Gates* (2025), arXiv:2510.09508 [quant-ph] .

[276] J. J. Renema, A. Menssen, W. R. Clements, G. Triginer, W. S. Kolthammer, and I. A. Walmsley, *Efficient Classical Algorithm for Boson Sampling with Partially Distinguishable Photons*, Physical Review Letters **120**, 220502 (2018), arXiv:1707.02793 [quant-ph].

[277] J. J. Renema, *Simulability of partially distinguishable superposition and Gaussian boson sampling*, Physical Review A **101**, 063840 (2020), arXiv:1911.10112 [quant-ph].

[278] S. N. van den Hoven, E. Kanis, and J. J. Renema, *Efficient classical algorithm for simulating boson sampling with heterogeneous partial distinguishability*, Physical Review A **111**, 052448 (2025), arXiv:2406.17682 [quant-ph].

[279] A. E. Moylett and P. S. Turner, *Quantum simulation of partially distinguishable boson sampling*, Physical Review A **97**, 062329 (2018), arXiv:1803.03657 [quant-ph].

[280] Y.-R. Fan, C.-Z. Yuan, R.-M. Zhang, S. Shen, P. Wu, H.-Q. Wang, H. Li, G.-W. Deng, H.-Z. Song, L.-X. You, Z. Wang, Y. Wang, G.-C. Guo, and Q. Zhou, *Effect of dispersion on indistinguishability between single-photon wave packets*, Photonics Research **9**, 1134 (2021), arXiv:1911.10112 [quant-ph].

[281] J. Osca and J. Vala, *Implementation of photon partial distinguishability in a quantum optical circuit simulation*, Computer Physics Communications **289**, 108773 (2023), arXiv:2208.03250 [quant-ph].

[282] J. Saied, J. Marshall, N. Anand, S. Grabbe, and E. G. Rieffel, *Advancing Quantum Networking: Some Tools and Protocols for Ideal and Noisy Photonic Systems*, in *Quantum Computing, Communication, and Simulation IV* (2024) p. 121, arXiv:2403.02515 [quant-ph] .

[283] M. Reed and B. Simon, *Functional Analysis*, Vol. 1 (Academic Press, 1980).

[284] G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, *Informationally complete measurements and groups representation*, Journal of Optics B: Quantum and Semiclassical Optics **6**, S487 (2004), arXiv:quant-ph/0310013.

[285] L. Everding, *Calculation of Clebsch-Gordan coefficients via Weyl group symmetry* (Ludwig–Maximilians–Universitaet, Muenchen, 2011).

[286] F. Mezzadri, *How to generate random matrices from the classical compact groups*, (2006), arXiv:math-ph/0609050.

[287] M. Ozols, *How to generate a random unitary matrix* (2009).

[288] Á. Kaposi, Z. Kolarovszki, T. Kozsik, Z. Zimborás, and P. Rakyta, *Polynomial speedup in Torontonian calculation by a scalable recursive algorithm* (2022), arXiv:2109.04528 [quant-ph] .

[289] Z. Kolarovszki, T. Rybotycki, P. Rakyta, Á. Kaposi, B. Poór, S. Jóczik, D. T. R. Nagy, H. Varga, K. H. El-Safty, G. Morse, M. Oszmaniec, T. Kozsik, and Z. Zimborás, *Piquasso: A photonic quantum computer simulation software platform*, Quantum **9**, 1708 (2025), arXiv:2403.04006 [quant-ph].

[290] L. Devos, `https://github.com/QuantumKitHub/SUNRepresentations.jl`.