

Simple and general bounds on quantum random access codes

Máté Farkas¹, Nikolai Miklin², and Armin Tavakoli³

¹Department of Mathematics, University of York, Heslington, York, YO10 5DD, United Kingdom

²Institute for Quantum-Inspired and Quantum Optimization, Hamburg University of Technology, Germany

³Physics Department and NanoLund, Lund University, Box 118, 22100 Lund, Sweden.

Random access codes are a type of communication task that is widely used in quantum information science. The optimal average success probability that can be achieved through classical strategies is known for any random access code. However, only a few cases are solved exactly for quantum random access codes. In this paper, we provide bounds for the fully general setting of n independent variables, each selected from a d -dimensional classical alphabet and encoded in a D -dimensional quantum system subject to an arbitrary quantum measurement. The bound recovers the exactly known special cases, and we demonstrate numerically that even though the bound is not tight overall, it can still yield a good approximation.

1 Introduction

Quantum random access codes (RACs) are a broadly useful tool in quantum information science. In addition to being studied on their own merit (see e.g. [1, 2, 3, 4, 5, 6, 7, 8]), an incomplete list of their broader relevance includes protocols for quantum contextuality [9], information-theoretic principles for quantum correlations [10], tests of quantum dimension [11, 12], quantum cryptography [13], famous open problems in Hilbert space geometry [14] and certification of measurements [15, 16, 17] and instruments [18, 19]. This widespread use has led to quantum RACs being the focus of many experiments, see e.g. [9, 20, 21, 14, 22, 23, 24]. To prove and maximize the utility of RACs in most of these tasks, it is essential to find optimal quantum RAC strategies, or at least to find relatively tight bounds on the optimal performance. This is because a tight upper bound is necessary e.g. in order to use quantum RACs for certification [25, 26], whereas approximate bounds can lead to applications in e.g. quantum key distribution [13, 27]. Finding such universal bounds is precisely the aim of this work.

Consider a communication scenario in which a sender encodes private data into a message that is sent to a receiver who wants to recover some freely chosen part of the original data set. RACs are a particularly natural class of such tasks. In a RAC, the private data can consist of n independent and uniformly distributed classical variables, $x := \{x_1, x_2, \dots, x_n\}$. Each variable is selected from an alphabet with d distinct symbols, $x_i \in [d] := \{1, 2, \dots, d\}$ for $i = 1, 2, \dots, n$. The data set x is then encoded by the sender,

Máté Farkas: mate.farkas@york.ac.uk

Nikolai Miklin: nikolai.miklin@tuhh.de

Armin Tavakoli: armin.tavakoli@teorfys.lu.se

Alice, into a typically much smaller message whose dimension is D . The message is sent to the receiver, Bob, who privately selects at random which element in the data set he wishes to recover, labeled by $y \in [n]$, and outputs $b \in [d]$ as his guess for the value of the random variable x_y . The average success probability (ASP) of the RAC is hence given by

$$\mathcal{P}_{n,d,D} := \frac{1}{nd^n} \sum_{x \in [d]^n} \sum_{y=1}^n \mathbb{P}[b = x_y | x, y], \quad (1)$$

where, following a common short-hand notation, we used x, y , and x_y as labels of the corresponding random variables' outcomes.

In a classical RAC, the message is represented by a random variable with D possible integer values. The encoding is then represented by any function $E : [d]^n \rightarrow [D]$ and, similarly, the decoding consists of a set of functions $D_y : [D] \rightarrow [d]$. The case in which the message dimension equals the size of the alphabet, i.e., when $D = d$, has been the most studied case so far. The optimal ASP for such protocols was conjectured in [21] and later proven in [28]. In the general case, namely when $D \neq d$, the optimal ASP was recently proven in [29].

In a quantum RAC, the sender encodes the classical data x into a quantum state ρ_x whose Hilbert space dimension is D . The receiver's decoding corresponds to a set of quantum measurements $(M_{b|y})_{b \in [d]}$, for $y \in [n]$, where b denotes the outcome and y denotes the setting. For each y , any D -dimensional positive operator-valued measure (POVM) is a valid decoding operation. Hence, in the quantum RAC, the optimal ASP becomes

$$\mathcal{P}_{n,d,D}^Q := \max_{\rho_x, M_{b|y}} \frac{1}{nd^n} \sum_{x \in [d]^n} \sum_{y=1}^n \text{tr} [\rho_x M_{x_y|y}]. \quad (2)$$

Finding the optimal quantum ASP is, in general, not easy. However, one family of exact results is known. This pertains to the case of $n = 2$ and $D = d$. It was conjectured in [21] and later proven in [26] that

$$\mathcal{P}_{2,d,d}^Q = \frac{1}{2} \left(1 + \frac{1}{\sqrt{d}} \right). \quad (3)$$

This can be achieved by selecting the two decoding measurements as the computational and Fourier bases measurements. The encodings are obtained via the Weyl-Heisenberg group generators as $X^{x_1} Z^{x_2} |\psi\rangle$, where $X = \sum_{k=0}^{d-1} |k+1\rangle\langle k|$ and $Z = \sum_{k=0}^{d-1} e^{\frac{2\pi i}{d}k} |k\rangle\langle k|$, with $|\psi\rangle$ being a uniform superposition of $|0\rangle$ and its Fourier transform [21]. This protocol is also unique, in a weaker self-testing sense: any pair of mutually unbiased bases (MUBs) leads to an optimal strategy, and not all of these are unitarily equivalent to the computational and Fourier bases [26].

One more exact result is known, namely when Alice has three bits and communicates a qubit to Bob. In that case, one has

$$\mathcal{P}_{3,2,2}^Q = \frac{1}{2} \left(1 + \frac{1}{\sqrt{3}} \right). \quad (4)$$

The optimal quantum protocol consists in measuring the three Pauli observables and preparing eight qubit states on the Bloch sphere so that they form a cube [30, 31]. The protocol is known to be unique in a self-testing sense [25].

Beyond these exact results, a generic bound on the optimal quantum ASP when $d = D = 2$ is known [32] to be

$$\mathcal{P}_{n,2,2}^Q \leq \frac{1}{2} \left(1 + \frac{1}{\sqrt{n}} \right). \quad (5)$$

This was later generalized in [33] to a bound valid for arbitrary tuples (n, d, D) , which reads

$$\mathcal{P}_{n,d,D}^Q \leq \frac{1}{d} + \frac{\sqrt{dD} - 1}{d\sqrt{n}}. \quad (6)$$

Eq. (6) reduces to Eq. (5) when $d = D = 2$ and therefore subsumes that bound. Note that it does not recover the exact family of results in Eq. (3). Other known bounds for quantum RACs rely mainly on relaxation methods based on semidefinite programming (SDP) [34]. These are commonly applied to specific and typically small-scale tuples (n, d, D) , see e.g., [35, 36, 37] for methods and case studies. It is apparent from these studies that SDP techniques scale rather badly with the problem size. It is therefore highly desirable to develop new analytic tools for bounding the quantum ASP for generic tuples (n, d, D) , which is precisely the aim of our work.

In this paper, we present two simple analytical upper bounds on the quantum ASP which apply to the most general setting, namely any tuple (n, d, D) . Our final, combined, bound is given in Corollary 1. It is distinct from the known general bound in Eq. (6). Notably, it recovers the both exact results in Eq. (3) and Eq. (4) as special cases, as well as the bound in Eq. (5). Since our bound is typically not tight, we study its performance through numerical case studies. We demonstrate with examples that it can be a good approximation of the exact value.

2 Bounds on quantum average success probability

Operator norm inequalities have proven to be a useful analytic tool for bounding the quantum ASP of RACs [26]. In order to extend these techniques beyond two measurement settings, we employ the following lemma, which turns out to be highly useful in various ways for obtaining improved analytic bounds for more than two measurement settings.

Lemma 1. *Let A be a trace-zero Hermitian matrix. Then it holds that*

$$\|A\|_\infty \leq \sqrt{\frac{r-1}{r}} \|A\|_F, \quad (7)$$

where r is the rank of A , $\|\cdot\|_\infty$ and $\|\cdot\|_F$ denote the operator and the Frobenius norms, respectively.

Proof. Matrix A has r real eigenvalues which we denote as $\{\lambda_i\}_{i=1}^r$. Since $\text{tr}[A] = 0$, we have that $\sum_{i=1}^r \lambda_i = 0$. Let λ_1 be the largest eigenvalue in the absolute value, which implies that $\|A\|_\infty = |\lambda_1|$. The Frobenius norm can then be lower-bounded as

$$\begin{aligned} \|A\|_F^2 &= \sum_{i=1}^r \lambda_i^2 \geq \lambda_1^2 + \frac{1}{r-1} \left(\sum_{i=2}^r |\lambda_i| \right)^2 \geq \lambda_1^2 + \frac{1}{r-1} \left(\sum_{i=2}^r \lambda_i \right)^2 = \lambda_1^2 + \frac{1}{r-1} (-\lambda_1)^2 \\ &= \frac{r}{r-1} \|A\|_\infty^2. \end{aligned} \quad (8)$$

In the first inequality we used the well-known relation $\|\cdot\|_F \geq \frac{1}{\sqrt{t}} \|\cdot\|_1$, where $\|\cdot\|_1$ is the trace norm and t is the dimension of the relevant operator. In the second inequality

we discarded the absolute values, and in the next step we used the trace-zero condition. Re-arranging the left- and right-hand side returns Eq. (7). $\square$

We now state and prove our first bound on the quantum ASP.

Result 1. *The average success probability of the quantum random access code, in the setting of n -element data set with alphabet size d and message dimension D , is bounded as*

$$\mathcal{P}_{n,d,D}^Q \leq \frac{1}{d} + \frac{D-1}{\sqrt{ndD}}. \quad (9)$$

Proof. We can trivially re-write the quantum ASP in Eq. (2) as

$$\mathcal{P}_{n,d,D}^Q = \frac{1}{nd^n} \sum_x \sum_y \frac{1}{D} \text{tr} [M_{x_y|y}] + \frac{1}{nd^n} \sum_x \text{tr} \left[\rho_x \sum_y \left(M_{x_y|y} - \frac{\mathbb{1}}{D} \text{tr} [M_{x_y|y}] \right) \right], \quad (10)$$

where we omitted writing the maximization and limits of the sums for convenience. In Eq. (10), $\mathbb{1}$ is the identity operator on the D -dimensional Hilbert space in which ρ_x and $M_{b|y}$ are defined. From the normalization, $\sum_{b=1}^d M_{b|y} = \mathbb{1}$, it follows that the first term evaluates to $\frac{1}{d}$. Clearly, the optimal choice of ρ_x corresponds to the eigenvector with the largest eigenvalue of the Hermitian operator $O_x := \sum_y \left(M_{x_y|y} - \frac{\mathbb{1}}{D} \text{tr} [M_{x_y|y}] \right)$. This gives

$$\mathcal{P}_{n,d,D}^Q = \frac{1}{d} + \frac{1}{nd^n} \sum_x \|O_x\|_\infty. \quad (11)$$

Notice that by adopting the form (10), we have conveniently ensured that $\text{tr}[O_x] = 0$. Hence, we can now apply Lemma 1 to obtain

$$\mathcal{P}_{n,d,D}^Q \leq \frac{1}{d} + \frac{1}{nd^n} \sqrt{\frac{D-1}{D}} \sum_x \|O_x\|_F \leq \frac{1}{d} + \frac{\sqrt{D-1}}{n\sqrt{Dd^n}} \sqrt{\sum_x \text{tr} [O_x^2]}, \quad (12)$$

where in the second step we used the concavity inequality $\frac{1}{N} \sum_{i=1}^N \sqrt{t_i} \leq \sqrt{\frac{1}{N} \sum_{i=1}^N t_i}$, which holds for any $t_i \geq 0$, $i \in [N]$. Simplifying the expression under the square-root gives

$$\sum_x \text{tr} [O_x^2] = \sum_x \sum_{y,z=1}^n \text{tr} [M_{x_y|y} M_{x_z|z}] - \frac{1}{D} \sum_x \sum_{y,z=1}^n \text{tr} [M_{x_y|y}] \text{tr} [M_{x_z|z}]. \quad (13)$$

The two terms on the right-hand-side of Eq. (13) simplify, respectively, as

$$\begin{aligned} \sum_x \sum_{y,z=1}^n \text{tr} [M_{x_y|y} M_{x_z|z}] &= \sum_y \sum_x \text{tr} [M_{x_y|y}^2] + \sum_{y \neq z} \sum_{x \setminus \{x_y, x_z\}} \sum_{x_y, x_z} \text{tr} [M_{x_y|y} M_{x_z|z}] \\ &= \sum_y \sum_x \text{tr} [M_{x_y|y}^2] + n(n-1)d^{n-2}D, \end{aligned} \quad (14)$$

and

$$\begin{aligned} \frac{1}{D} \sum_x \sum_{y,z=1}^n \text{tr} [M_{x_y|y}] \text{tr} [M_{x_z|z}] &= \frac{1}{D} \sum_y \sum_x \text{tr} [M_{x_y|y}]^2 \\ &\quad + \frac{1}{D} \sum_{y \neq z} \sum_{x \setminus \{x_y, x_z\}} \sum_{x_y} \text{tr} [M_{x_y|y}] \sum_{x_z} \text{tr} [M_{x_z|z}] \\ &\geq \frac{1}{D} \sum_y \sum_x \text{tr} [M_{x_y|y}^2] + n(n-1)d^{n-2}D, \end{aligned} \quad (15)$$

where in the last inequality we used that for $M \geq 0$, we have $\text{tr}[M^2] \leq \text{tr}[M]^2$. In the above two equations, $\sum_{y \neq z}$ denotes the summation over $y \in [n]$ and $z \in [n]$ such that $y \neq z$. Substituting this back into Eq. (13), we obtain

$$\sum_x \text{tr}[O_x^2] \leq \frac{D-1}{D} \sum_y \sum_x \text{tr}[M_{x_y|y}^2] \leq \frac{D-1}{D} \sum_y \sum_{x \setminus \{x_y\}} \sum_{x_y} \text{tr}[M_{x_y|y}] = (D-1)nd^{n-1}, \quad (16)$$

where we used that for an operator $0 \leq M \leq \mathbb{1}$, we have $\text{tr}[M^2] \leq \text{tr}[M]$. Finally, substituting this back into Eq. (12) returns the result in Eq. (9). $\square$

Notice that when $d = D = 2$, we recover the known bound (5). Also, when $d = D$, we recover the previously known bound in Eq. (6). However, for $d = D$ and $n = 2$ the above upper bound coincides with the other known bound (3) only for $d = 2$, and otherwise provides a weaker bound.

We now state and prove the second main result, which is a different general bound on the quantum ASP. This time, it is more relevant for the scaling in d , as it recovers the bound in Eq. (3) as a special case. In this sense, it is complementary to Result 1.

Result 2. *The average success probability of the quantum random access code, in the setting of n -element data set with alphabet size d and message dimension D , is bounded as*

$$\mathcal{P}_{n,d,D}^Q \leq \frac{1}{n} \left(1 + (n-1) \frac{\sqrt{D}}{d} \right). \quad (17)$$

Proof. Our main tool is an operator inequality proved by Popovici and Sebestyén [38]. For a set of n positive semidefinite matrices $\{A_k\}_{k=1}^n$, it holds that

$$\left\| \sum_{k=1}^n A_k \right\|_{\infty} \leq \|\Gamma\|_{\infty}, \quad (18)$$

where Γ is an $n \times n$ matrix with elements $\Gamma_{i,j} := \|\sqrt{A_i} \sqrt{A_j}\|_{\infty}$. Applying this to the quantum ASP we get

$$\mathcal{P}_{n,d,D}^Q = \frac{1}{nd^n} \sum_x \left\| \sum_y M_{x_y|y} \right\|_{\infty} \leq \frac{1}{nd^n} \sum_x \|\Gamma^{(x)}\|_{\infty}, \quad (19)$$

where $\Gamma_{y,z}^{(x)} = \left\| \sqrt{M_{x_y|y}} \sqrt{M_{x_z|z}} \right\|_{\infty}$, for $y, z \in [n]$. Let us now fix the computational basis $\{|y\rangle\}_{y=1}^n$ on $\mathbb{C}^n$, and separate the diagonal and off-diagonal parts of matrices $\Gamma^{(x)}$,

$$\Gamma^{(x)} = \sum_y \left\| M_{x_y|y} \right\|_{\infty} |y\rangle\langle y| + \sum_{z \neq y} \left\| \sqrt{M_{x_y|y}} \sqrt{M_{x_z|z}} \right\|_{\infty} |y\rangle\langle z|, \quad (20)$$

where, as before, $\sum_{y \neq z}$ is the summation over $y \in [n]$ and $z \in [n]$ such that $y \neq z$. Applying the triangle inequality gives

$$\|\Gamma^{(x)}\|_{\infty} \leq \left\| \sum_y \left\| M_{x_y|y} \right\|_{\infty} |y\rangle\langle y| \right\|_{\infty} + \left\| \sum_{y \neq z} \left\| \sqrt{M_{x_y|y}} \sqrt{M_{x_z|z}} \right\|_{\infty} |y\rangle\langle z| \right\|_{\infty}. \quad (21)$$

The completeness condition of POVMs implies $\|M_{b|y}\|_\infty \leq 1$ for all $b \in [d], y \in [n]$, which when applied to the first term above bounds it by 1. Substituting the above into the right-hand-side of Eq. (19), we arrive at

$$\mathcal{P}_{n,d,D}^Q \leq \frac{1}{n} + \frac{1}{nd^n} \sum_x \left\| \sum_{y \neq z} \left\| \sqrt{M_{x_y|y}} \sqrt{M_{x_z|z}} \right\|_\infty |y\rangle\langle z| \right\|_\infty. \quad (22)$$

Notice now that the operators $\sum_{y \neq z} \left\| \sqrt{M_{x_y|y}} \sqrt{M_{x_z|z}} \right\|_\infty |y\rangle\langle z|$ are Hermitian and trace-zero. Hence we can apply Lemma 1 to bound the operator norm by the Frobenius norm. This gives

$$\begin{aligned} \mathcal{P}_{n,d,D}^Q &\leq \frac{1}{n} + \frac{\sqrt{n-1}}{n\sqrt{nd^n}} \sum_x \left\| \sum_{y \neq z} \left\| \sqrt{M_{x_y|y}} \sqrt{M_{x_z|z}} \right\|_\infty |y\rangle\langle z| \right\|_F \\ &= \frac{1}{n} + \frac{\sqrt{n-1}}{n\sqrt{nd^n}} \sum_x \sqrt{\sum_{y \neq z} \left\| \sqrt{M_{x_y|y}} \sqrt{M_{x_z|z}} \right\|_\infty^2}. \end{aligned} \quad (23)$$

Bounding the operator norm by the Frobenius norm again, but this time without the trace-zero condition, and therefore without the rank pre-factor, and then using the concavity of the square-root function as well as the completeness condition, we get

$$\begin{aligned} \mathcal{P}_{n,d,D}^Q &\leq \frac{1}{n} + \frac{\sqrt{n-1}}{n\sqrt{nd^n}} \sum_x \sqrt{\sum_{y \neq z} \left\| \sqrt{M_{x_y|y}} \sqrt{M_{x_z|z}} \right\|_F^2} \\ &= \frac{1}{n} + \frac{\sqrt{n-1}}{n\sqrt{nd^n}} \sum_x \sqrt{\sum_{y \neq z} \text{tr} [M_{x_y|y} M_{x_z|z}]} \\ &\leq \frac{1}{n} + \frac{\sqrt{n-1}}{n\sqrt{n}\sqrt{d^n}} \sqrt{\sum_{y \neq z} \sum_{x \in \{x_y, x_z\}} \sum_{x_y} \sum_{x_z} \text{tr} [M_{x_y|y} M_{x_z|z}]} = \frac{1}{n} + (n-1) \frac{\sqrt{D}}{nd}, \end{aligned} \quad (24)$$

which is the final result. $\square$

Combining the bounds in Result 1 and Result 2, the our final bound on the quantum ASP becomes simply the smallest of the two, which is summarized by the following Corollary.

Corollary 1. *The average success probability of the quantum random access code, in the setting of n -element data set with alphabet size d and message dimension D , is bounded as*

$$\mathcal{P}_{n,d,D}^Q \leq \min \left\{ \frac{1}{d} + \frac{D-1}{\sqrt{ndD}}, \frac{1}{n} \left(1 + (n-1) \frac{\sqrt{D}}{d} \right) \right\}. \quad (25)$$

In particular, for the case $D = d = n$, the two expressions are identical. For the case $D = d$ and $n \geq d$, we have that

$$\mathcal{P}_{n,d,d}^Q \leq \frac{1}{d} \left(1 + \frac{d-1}{\sqrt{n}} \right), \quad (26)$$

which corresponds to the first bound in Eq. (25), and for $D = d$ and $n \leq d$, we have that

$$\mathcal{P}_{n,d,d}^Q \leq \frac{1}{n} \left(1 + \frac{n-1}{\sqrt{d}} \right), \quad (27)$$

which corresponds to the second bound in Eq. (25).

When applied to the special cases of $(n, 2, 2)$ and $(2, d, d)$, the bound in Corollary 1 reduces to the previously known bounds in Eq. (5) and Eq. (3). The bound in Corollary 1 and the other known generic bound, given in Eq. (6), admit no strict hierarchy. That is, there exist tuples (n, d, D) for which one of the bounds performs better than the other. For instance, when $D = d$ and $n \geq d$, the two bounds are identical, while for $n \leq d \leq D$, Corollary 1 provides a tighter bound. This is also the case when $D < d$. On the other hand, for $D > d$ and a sufficiently large n , Eq. (6) is a tighter bound. In general, the best known bound can be easily determined for each particular case.

It is worth mentioning that Results 1 and 2 can be extended to explicitly account for a noisy communication channel between Alice and Bob. If we denote by Λ the quantum channel used by the parties for communication, then a more accurate formula for the optimal ASP becomes

$$\tilde{\mathcal{P}}_{n,d,D}^Q := \max_{\rho_x, M_{b|y}} \frac{1}{nd^n} \sum_{x \in [d]^n} \sum_{y=1}^n \text{tr} [\Lambda(\rho_x) M_{x_y|y}]. \quad (28)$$

Clearly, since $\Lambda(\rho_x)$ are again quantum states, the bounds from Corollary 1 also apply for $\tilde{\mathcal{P}}_{n,d,D}^Q$ in Eq. (28). However, as recently shown in Ref. [8], noisy communication channel can make the maximally attainable ASP significantly lower.

The simplest type of noisy communication channel to consider is the depolarizing channel, whose action on an operator X can be described as $\Lambda(X) = (1 - \eta)X + \eta \frac{\text{tr}[X]\mathbb{1}}{D}$, where $\eta \in [0, 1]$ is the depolarizing parameter. Plugging this formula into Eq. (28) lets us deduce straightforwardly that in this case $\tilde{\mathcal{P}}_{n,d,D}^Q = (1 - \eta)\mathcal{P}_{n,d,D}^Q + \frac{\eta}{d}$, where $\mathcal{P}_{n,d,D}^Q$ is the optimal ASP from Eq. (2). Other types of noisy channels, e.g., dephasing channel, are less straightforward to account for, and, in our opinion, adapting Results 1 and 2 to such cases deserves a separate study. However, we can lay out a general strategy that can be followed. Since in our proofs we eliminate the states from the optimization and only optimize over the POVM effects $M_{x_y|y}$, it is meaningful to move to the Heisenberg picture and consider the dual of the noise channel. That is, use the defining relation for the dual channel

$$\text{tr} [\Lambda(\rho_x) M_{x_y|y}] = \text{tr} [\rho_x \Lambda^\dagger(M_{x_y|y})], \quad (29)$$

and optimize over POVM elements under the fixed dual channel $\Lambda^\dagger$. In this way, one can potentially use tighter bounds in the proofs of Results 1 and 2, depending on the nature of the map Λ . As an example, in Eq. (16) we use the inequality $\text{tr} [M_{x_y|y}^2] \leq \text{tr} [M_{x_y|y}]$, which is only tight for projectors. The image of the dual of noisy channels are not projections in most cases. As such, given an explicit description of the channel, the above inequality can likely be tightened.

3 Numerical case studies

In this section, we present numerical bounds on the quantum ASP for some families of RACs in order to benchmark our analytic bounds. We present both lower bounds to see the possible gap between our analytic results and the actual optimal ASP, and upper bounds to prove that in some cases our bounds can be improved. Our codes generating the numerical data (apart from those taken from Ref. [37]) can be found in our open-access repository [39].

We use the *seesaw* SDP algorithms to derive lower bounds on the quantum ASP. Note that the ASP (2) is linear in both ρ_x and in $M_{b|y}$. Consequently, for a fixed POVM

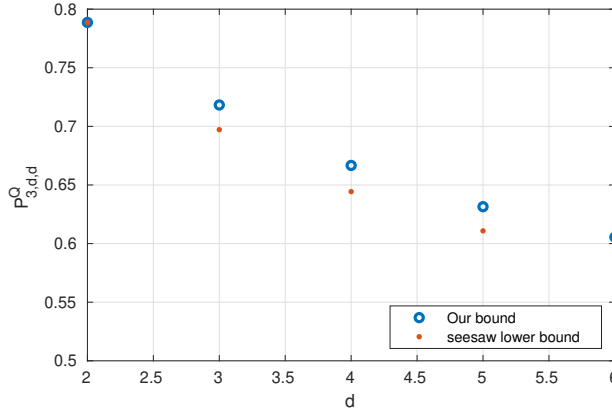


Figure 1: The upper bound from Corollary 1 and a seesaw lower bound on ASP for $n = 3$ and $d = D$ with respect to the dimension D of the quantum system.

operators $M_{b|y}$, optimizing the ASP over the set of ρ_x is an SDP. Similarly, for a fixed set of ρ_x , optimizing the ASP over $M_{b|y}$ is again an SDP. The seesaw algorithm starts with a randomly selected set of ρ_x , and finds the optimal $M_{b|y}$ for that set as the solution of an SDP. Then $M_{b|y}$ found in the first iteration are fixed, and the optimal ρ_x for this set of POVMs are found via an SDP. This process is iterated until the value of the ASP converges to a locally optimal value up to some error threshold. This method is not guaranteed to find a global maximum, but every set of ρ_x and $M_{b|y}$ found by this algorithm provide a valid lower bound on the ASP.

The performance of the seesaw algorithm is highly dependent on the initialization, i.e., on the randomly selected ρ_x . To obtain the lower bounds in this paper, in our numerical calculations we sample random pure states ρ_x uniformly (with respect to the Haar measure) and repeat the algorithm a fixed number of times. Since there is no guarantee that the produced estimate is unbiased, one cannot determine a sufficient number of random initialization of the seesaw algorithm. Nevertheless, by observing the distribution of the local optima produced by the seesaw algorithm for a number of random initializations, one can judge about optimality of the produced lower bounds.

Since the case of $n = 3$ and $d = D$ has been the focus of study for some time [14] and this family is unsolved apart from $d = 2$, in Fig. 1 we compare lower bounds from seesaw techniques with our analytic bound from Corollary 1, which correspond to Eq. (27) because we have $n \leq d$, for values $d \in \{3, 4, 5, 6\}$. We also include the point for $d = 2$, for which the seesaw algorithm finds the known optimal ASP. This plot demonstrates that our bound is possibly not tight for these values of d , but the gap between the lower bound from the seesaw algorithm and our upper bound is seemingly not too large. That is, our upper bounds provide a reasonable approximation of the optimal quantum ASP from above.

The smallest unsolved case of quantum RAC is $n = d = D = 3$, for which the best lower bound, both analytically and numerically, is given by performing measurements in three MUBs, and choosing the corresponding optimal states [14, 40]. This gives the lower bound $\mathcal{P}_{3,3,3}^Q \gtrsim 0.6971$, and our analytic upper bound is $\mathcal{P}_{3,3,3}^Q \leq \frac{1}{2} \left(1 + \frac{2}{\sqrt{3}}\right) \approx 0.7182$, according to Eq. (27). In order to test the tightness of our analytic upper bound, we numerically computed upper bounds on $\mathcal{P}_{3,3,3}^Q$ using SDP techniques, in particular using the QDimSum package [41] to implement the techniques described in [35, 36]. Note that this technique,

as implemented in [41], assumes that the measurements used are projective. While there is no evidence that projective measurements are not optimal for the $n = d = D = 3$ case, the upper bounds provided by this technique may be lower than the actual maximum.

Loosely speaking, the method [35] relies on *moment matrices* indexed by monomials of the operators ρ_x and $M_{b|y}$. The more monomials are used for building the moment matrix, the tighter the upper bound, leading to a *hierarchy* of upper bounds. On level 1 of the hierarchy, only order-1 monomials are used, that is, the monomials $\{\mathbb{1}\} \cup \{\rho_x\}_x \cup \{M_{b|y}\}_{b,y}$. On level 2, all order-2 monomials are used, that is, the monomials

$$\{\mathbb{1}\} \cup \{\rho_x\}_x \cup \{M_{b|y}\}_{b,y} \cup \{\rho_x \rho_{x'}\}_{x,x'} \cup \{M_{b|y} M_{b'|y'}\}_{b,y,b',y'} \cup \{\rho_x M_{b|y}\}_{x,b,y}. \quad (30)$$

One can also define “intermediate” levels, for example, the level “ $1 + \rho M$ ”, using the monomials

$$\{\mathbb{1}\} \cup \{\rho_x\}_x \cup \{M_{b|y}\}_{b,y} \cup \{\rho_x M_{b|y}\}_{x,b,y}. \quad (31)$$

Using this notation, the upper bounds we found for the various levels of the SDP hierarchy for $\mathcal{P}_{3,3,3}^Q$ are given in Table 1.

Level	Upper bound on $\mathcal{P}_{3,3,3}^Q$
1	0.7182
$1 + \rho M$	0.6989
2	0.6989
$2 + MMM$	0.6989
$2 + \rho MM$	0.69855
$2 + MMM + \rho MM$	0.69853

Table 1: Numerical upper bounds on $\mathcal{P}_{3,3,3}^Q$ using the QDimSum package [41] for different levels of the hierarchy.

Note that our analytic bound is recovered, up to the solver precision, for level 1 of the hierarchy. Then, various consecutive levels yield the same upper bound, which, interestingly, corresponds to the hypothetical case of measuring in three orthonormal bases $\{|e_j\rangle\}$, $\{|f_j\rangle\}$ and $\{|g_j\rangle\}$ on $\mathbb{C}^3$ that form a set of MUBs with the triple products

$$\langle e_j | f_k \rangle \langle f_k | g_l \rangle \langle g_l | e_j \rangle + \langle e_j | g_l \rangle \langle g_l | f_k \rangle \langle f_k | e_j \rangle \quad (32)$$

being uniform, even though such bases are known not to exist [40]. Note that these triple products are naturally related to Bargmann invariants [42]. Adding certain order-3 monomials, such as ρMM and MMM , makes the upper bound tighter, with our current best numerical upper bound being $\mathcal{P}_{3,3,3}^Q \lesssim 0.69853$, which shows that there is still room for an improvement when deriving analytic upper bounds.

We also compare our analytical bounds to other recently developed SDP techniques [37]. In particular, a special case of the bounds developed in [37] corresponds to upper bounds on $\mathcal{P}_{3,3,D}^Q$. Importantly, these do not assume that the measurements are projective. In Figure 2 we plot the seesaw lower bound, our analytical upper bound, and the upper bound from Ref. [37] on $\mathcal{P}_{3,3,D}^Q$ for $D \in \{2, 3, \dots, 10\}$. These numerical results show that our bound is not tight for this family of RACs apart from the $D = 2$ case, where our analytical upper bound is actually tighter than the one obtained in Ref. [37].

Lastly, we compare our analytical upper bounds with seesaw lower bounds in the $n = 3$ case for various different values for d and D in Table 2. While our bound is potentially not tight apart from the $d = D = 2$ case, it provides a good approximation of the quantum optimal ASP for generic values of d and D .

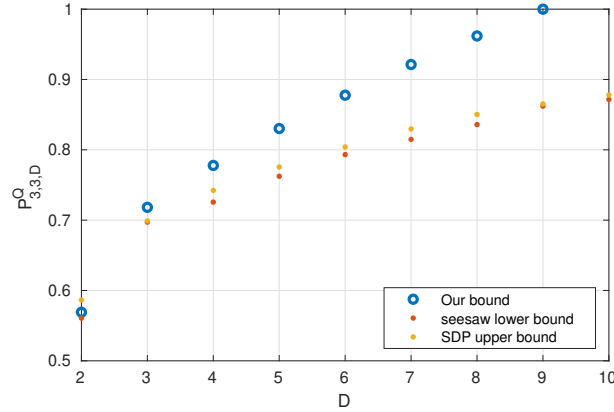


Figure 2: The upper bound from Corollary 1, the upper bound from the SDP hierarchy of Ref. [37], and a seesaw lower bound on ASP for $n = 3$, $d = 3$ with respect to the dimension D of the quantum system.

(d, D)	Seesaw lower bound	Our upper bound
(2,2)	0.78868	0.78868
(2,3)	0.80794*	0.91068
(2,4)	0.90825	1
(3,2)	0.56066	0.56904
(3,3)	0.69715	0.71823
(3,4)	0.72567	0.77778
(3,5)	0.76241	0.83024
(4,2)	0.43697	0.45412
(4,3)	0.47525	0.58333
(4,4)	0.64434	0.66667
(4,5)	0.66331*	0.70601

Table 2: Lower bounds on $\mathcal{P}_{3,d,D}^Q$ for various values of (d, D) from the seesaw method and the upper bound from Corollary 1. The presented estimates for the lower bound are the maximal obtained values of ASP for 100 runs of the seesaw algorithm with random initial states. *The cases (2,3) and (4,5) appear to be special in a way that the seesaw algorithm often finds other local minima, which is not the case for other cases in this table.

4 Conclusions

In this paper, we derive a universal analytic upper bound on the average success probability of quantum random access codes. We consider the most general case of RACs with n independent variables from a d -dimensional alphabet encoded into a D -dimensional quantum system, for arbitrary n, d and D . Our bounds recover known families of upper bounds for the case of $d = D$ and $n = 2$, which is known to be tight [26], and the $d = D = 2$ case, which is known to be tight for $n = 2$ and 3 [32]. In the general case, our bounds are not tight, although numerical evidence suggests that they provide reasonably good approximations of the actual quantum maximum. For the interesting case of $n = d = 3$, we show numerically that our upper bounds can be improved, and that the question whether MUBs measurements are optimal for this case is still unresolved. We believe that our bounds,

in combination with that obtained in [33], will be useful for the analytical treatment of problems where RACs are used as a tool for benchmarking quantum information protocols.

Apart from benchmarking, approximate bounds on ASP of RACs are useful for analyzing semi-device-independent quantum key distribution (QKD) protocols [13]. As discussed in [13], the security of some common QKD protocols, such as BB84 [43], cannot be guaranteed if the devices used for quantum communication are not characterized. To alleviate this issue, we can use protocols based on dimension witnesses—such as RACs—which provide security without a full characterization. For the case of RACs, the amount of distillable key only depends on the ASP and not on a full characterization of the devices [44].

Note that both of our bounds in Result 1 and 2 rely on pairwise properties of the measurements. In particular, both of these bounds at some point involve Hilbert-Schmidt inner products of measurement effects, and are, in principle, maximized when these inner products are uniform as both bounds use the concavity of the square root function. This would imply that if MUBs are indeed optimal for RACs, then *any* set of MUBs should give rise to the optimal ASP, as all sets of MUBs satisfy the above trace uniformity condition. It is known, however, that not all sets of MUBs give rise to the same ASP when $n = 3$ [14, 40]. This implies that either MUBs are not optimal for RACs in the general case, or that new upper bounds relying on more than pairwise properties of measurements are needed to prove optimality.

A potential new avenue for obtaining improved analytic upper bounds is highlighted by the relatively strong performance of the numerical techniques in Ref. [37]. While these bounds are numerical, they are based on well-established SDP hierarchy techniques. Therefore, analysing the dual SDP hierarchy induced by that in Ref. [37] is a promising direction for deriving analytic bounds stronger than those presented in this work.

Acknowledgements

We thank Marcin Pawłowski for the years of insightful discussions about the subject of this paper. We thank Julio de Vicente for a valuable feedback. A.T. is supported by the Knut and Alice Wallenberg Foundation through the Wallenberg Center for Quantum Technology (WACQT) and the Swedish Research Council under Contract No. 2023-03498. This research was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation), project number 441423094, and the Fujitsu Germany GmbH as part of the endowed professorship “Quantum Inspired and Quantum Optimization”.

References

- [1] Ashwin Nayak. “Optimal lower bounds for quantum automata and random access codes”. In 40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039). Pages 369–376. (1999).
- [2] Masahito Hayashi, Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita. “(4,1)-quantum random access coding does not exist—one qubit is not enough to recover one of four bits”. *New Journal of Physics* **8**, 129 (2006).
- [3] Marcin Pawłowski and Marek Żukowski. “Entanglement-assisted random access codes”. *Phys. Rev. A* **81**, 042326 (2010).
- [4] Armin Tavakoli, Breno Marques, Marcin Pawłowski, and Mohamed Bourennane. “Spatial versus sequential correlations for random access coding”. *Phys. Rev. A* **93**, 032336 (2016).

- [5] Ola Liabøtrø. “Improved classical and quantum random access codes”. *Phys. Rev. A* **95**, 052315 (2017).
- [6] João F. Doriguello and Ashley Montanaro. “Quantum Random Access Codes for Boolean Functions”. *Quantum* **5**, 402 (2021).
- [7] Rui-Heng Miao, Zhao-Di Liu, Yong-Nan Sun, Chen-Xi Ning, Chuan-Feng Li, and Guang-Can Guo. “High-dimensional multi-input quantum random access codes and mutually unbiased bases”. *Phys. Rev. A* **106**, 042418 (2022).
- [8] Rafael A. da Silva and Breno Marques. “Semidefinite-programming-based optimization of quantum random access codes over noisy channels”. *Phys. Rev. A* **107**, 042433 (2023).
- [9] Robert W. Spekkens, D. H. Buzacott, A. J. Keehn, Ben Toner, and G. J. Pryde. “Preparation contextuality powers parity-oblivious multiplexing”. *Phys. Rev. Lett.* **102**, 010401 (2009).
- [10] Marcin Pawłowski, Tomasz Paterek, Dagomir Kaszlikowski, Valerio Scarani, Andreas Winter, and Marek Żukowski. “Information causality as a physical principle”. *Nature* **461**, 1101–1104 (2009).
- [11] Nicolas Brunner, Miguel Navascués, and Tamás Vértesi. “Dimension witnesses and quantum state discrimination”. *Phys. Rev. Lett.* **110**, 150501 (2013).
- [12] Armin Tavakoli, Jef Pauwels, Erik Woodhead, and Stefano Pironio. “Correlations in entanglement-assisted prepare-and-measure scenarios”. *PRX Quantum* **2**, 040357 (2021).
- [13] Marcin Pawłowski and Nicolas Brunner. “Semi-device-independent security of one-way quantum key distribution”. *Phys. Rev. A* **84**, 010302 (2011).
- [14] Edgar A. Aguilar, Jakub J. Borkala, Piotr Mironowicz, and Marcin Pawłowski. “Connections between mutually unbiased bases and quantum random access codes”. *Phys. Rev. Lett.* **121**, 050501 (2018).
- [15] Piotr Mironowicz and Marcin Pawłowski. “Experimentally feasible semi-device-independent certification of four-outcome positive-operator-valued measurements”. *Phys. Rev. A* **100**, 030301 (2019).
- [16] Armin Tavakoli, Massimiliano Smania, Tamás Vértesi, Nicolas Brunner, and Mohamed Bourennane. “Self-testing nonprojective quantum measurements in prepare-and-measure experiments”. *Science Advances* **6**, eaaw6664 (2020).
- [17] Claudio Carmeli, Teiko Heinosaari, and Alessandro Toigo. “Quantum random access codes and incompatibility of measurements”. *Europhysics Letters* **130**, 50001 (2020).
- [18] Karthik Mohan, Armin Tavakoli, and Nicolas Brunner. “Sequential random access codes and self-testing of quantum measurement instruments”. *New Journal of Physics* **21**, 083034 (2019).
- [19] Nikolai Miklin, Jakub J. Borkala, and Marcin Pawłowski. “Semi-device-independent self-testing of unsharp measurements”. *Phys. Rev. Res.* **2**, 033014 (2020).
- [20] Sadiq Muhammad, Armin Tavakoli, Maciej Kuran, Marcin Pawłowski, Marek Żukowski, and Mohamed Bourennane. “Quantum bidding in bridge”. *Phys. Rev. X* **4**, 021047 (2014).
- [21] Armin Tavakoli, Alley Hameedi, Breno Marques, and Mohamed Bourennane. “Quantum random access codes using single d -level systems”. *Phys. Rev. Lett.* **114**, 170502 (2015).

- [22] Giulio Foletto, Luca Calderaro, Giuseppe Vallone, and Paolo Villoresi. “Experimental demonstration of sequential quantum random access codes”. *Phys. Rev. Res.* **2**, 033205 (2020).
- [23] Hammad Anwer, Sadiq Muhammad, Walid Cherifi, Nikolai Miklin, Armin Tavakoli, and Mohamed Bourennane. “Experimental characterization of unsharp qubit observables and sequential measurement incompatibility via quantum random access codes”. *Phys. Rev. Lett.* **125**, 080403 (2020).
- [24] Ya Xiao, Xin-Hong Han, Xuan Fan, Hui-Chao Qu, and Yong-Jian Gu. “Widening the sharpness modulation region of an entanglement-assisted sequential quantum random access code: Theory, experiment, and application”. *Phys. Rev. Res.* **3**, 023081 (2021).
- [25] Armin Tavakoli, Jędrzej Kaniewski, Tamás Vértesi, Denis Rosset, and Nicolas Brunner. “Self-testing quantum states and measurements in the prepare-and-measure scenario”. *Phys. Rev. A* **98**, 062307 (2018).
- [26] Máté Farkas and Jędrzej Kaniewski. “Self-testing mutually unbiased bases in the prepare-and-measure scenario”. *Phys. Rev. A* **99**, 032316 (2019).
- [27] Erik Woodhead and Stefano Pironio. “Secrecy in prepare-and-measure clauser-horne-shimony-holt tests with a qubit bound”. *Phys. Rev. Lett.* **115**, 150501 (2015).
- [28] Andris Ambainis, Dmitry Kravchenko, Sk Sazim, Joonwoo Bae, and Ashutosh Rai. “Quantum advantages in $(n, d) \mapsto 1$ random access codes”. *New Journal of Physics* **26**, 123023 (2024).
- [29] Debashis Saha, Debarshi Das, Arun Kumar Das, Bihalan Bhattacharya, and A. S. Majumdar. “Measurement incompatibility and quantum advantage in communication”. *Phys. Rev. A* **107**, 062210 (2023).
- [30] Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, and Umesh Vazirani. “Dense quantum coding and a lower bound for 1-way quantum automata”. In Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing. Page 376–383. STOC ’99 New York, NY, USA (1999). Association for Computing Machinery.
- [31] Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, and Umesh Vazirani. “Dense quantum coding and quantum finite automata”. *J. ACM* **49**, 496–511 (2002).
- [32] Andris Ambainis, Debbie Leung, Laura Mancinska, and Maris Ozols. “Quantum random access codes with shared randomness” (2009). [arXiv:0810.2937](https://arxiv.org/abs/0810.2937).
- [33] Julio I de Vicente. “A general bound for the dimension of quantum behaviours in the prepare-and-measure scenario”. *Journal of Physics A: Mathematical and Theoretical* **52**, 095304 (2019).
- [34] Armin Tavakoli, Alejandro Pozas-Kerstjens, Peter Brown, and Mateus Araújo. “Semidefinite programming relaxations for quantum correlations”. *Rev. Mod. Phys.* **96**, 045006 (2024).
- [35] Miguel Navascués, Adrien Feix, Mateus Araújo, and Tamás Vértesi. “Characterizing finite-dimensional quantum behavior”. *Phys. Rev. A* **92**, 042117 (2015).
- [36] Armin Tavakoli, Denis Rosset, and Marc-Olivier Renou. “Enabling computation of correlation bounds for finite-dimensional quantum systems via symmetrization”. *Phys. Rev. Lett.* **122**, 070501 (2019).
- [37] Jef Pauwels, Stefano Pironio, Erik Woodhead, and Armin Tavakoli. “Almost qudits in the prepare-and-measure scenario”. *Phys. Rev. Lett.* **129**, 250504 (2022).

- [38] Dan Popovici and Zoltán Sebestyén. “Norm estimations for finite sums of positive operators”. *Journal of Operator Theory* **56**, 3–15 (2006). url: <http://www.jstor.org/stable/24715730>.
- [39] “On-line repository: https://github.com/nikolai-miklin/qrac_bounds”.
- [40] Máté Farkas. “ n -fold unbiased bases: an extension of the MUB condition” (2017). [arXiv:1706.04446](https://arxiv.org/abs/1706.04446).
- [41] “Qdimsum package: <https://denisrosset.github.io/qdimsum/>”.
- [42] Dariusz Chruściński and Andrzej Jamiolkowski. “Geometric phases in classical and quantum mechanics”. *Birkhäuser Boston*. (2004).
- [43] Charles H. Bennett and Gilles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. *Theoretical Computer Science* **560**, 7–11 (2014).
- [44] Imre Csiszár and János Körner. “Broadcast channels with confidential messages”. *IEEE Transactions on Information Theory* **24**, 339–348 (1978).