

UC Irvine

Recent Work

Title

Optimal Average Success Probabilities of Binary $(n, n-1)$ and $(n, n-2)$ Quantum Random Access Codes

Permalink

<https://escholarship.org/uc/item/5910g713>

Authors

Tan, Shuo

Jafar, Syed A

Publication Date

2026-10-21

Copyright Information

This work is made available under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives License, available at

<https://creativecommons.org/licenses/by-nc-nd/4.0/>

Optimal Average Success Probabilities of Binary $(n, n - 1)$ and $(n, n - 2)$ Quantum Random Access Codes

Shuo Tan and Syed A. Jafar

Department of Electrical Engineering and Computer Science,
University of California, Irvine, California 92697, USA

A binary (n, m) quantum random access code (QRAC) compresses an n -bit classical string into an m -qubit quantum state, from which a decoder attempts to recover a randomly selected target bit. Of particular interest is the optimal average probability of success, $P_{n,m}^{Q,\text{avg,opt}}$. The square-root expression $\frac{1}{2} + \frac{1}{2}\sqrt{m/n}$ was conjectured to upper-bound this quantity, and recent constructions of $(n, n - 1)$ QRACs by Suzuki and $(n, n - 2)$ QRACs by Akibue et al. meet it exactly. In this work, we prove that these constructions are optimal, thereby determining $P_{n,n-1}^{Q,\text{avg,opt}}$ and $P_{n,n-2}^{Q,\text{avg,opt}}$. The proof uses the local-to-global reconstruction framework of Lin and de Wolf, based on the pretty good measurement (PGM), together with dimensional and positive-semidefinite (PSD) constraints on the induced channel. Based on these constraints, we also derive an efficient linear-programming (LP) converse for general binary (n, m) QRACs. We evaluate this converse in closed form for two infinite parameter families and prove that it is strictly tighter than Akibue et al.'s bound at every point in those families except $(n, m) = (3, 1)$, where the two coincide.

1 Introduction

The fundamental limits of data compression are a central theme in quantum information theory. Holevo's theorem [1] shows that the accessible classical information carried by an m -qubit system is at most m bits, but this global limitation does not fully capture how reliably individual bits of a classical string can be accessed when n bits are compressed into m qubits. Quantum random access codes (QRACs), introduced by Ambainis et al. [2], formalize this tradeoff between compressibility and retrievability. In an (n, m) binary QRAC, a classical string $x \in \{0, 1\}^n$ is encoded into an m -qubit state ρ_x , from which a decoder attempts to recover a randomly selected target bit as reliably as possible. To avoid degenerate cases, we assume throughout that $0 < m < n$. A key performance metric is the optimal average probability of success, $P_{n,m}^{Q,\text{avg,opt}}$.

Beyond this coding interpretation, random access codes (RACs) also provide an operational framework for probing the boundary between quantum and post-quantum nonsignaling correlations. The RAC task underlies the principle of information causality [3], which

Shuo Tan: shuot8@uci.edu

Syed A. Jafar: syed@uci.edu

requires that the sum of the information a receiver can gain about a sender's independent bits not exceed the number of classical bits communicated. This principle recovers Tsirelson's bound for the CHSH inequality and excludes certain stronger-than-quantum nonsignaling correlations [3]. QRACs provide the corresponding prepare-and-measure quantum formulation, with their optimal success probabilities quantifying the limits of selective retrieval from finite-dimensional quantum encodings. Beyond this foundational role, QRAC techniques yield lower bounds in one-way quantum communication complexity [4, 5] and quantum network coding [6], as well as bounds for locally decodable codes [7] and private information retrieval [8]. They also arise in dimension witnessing [9], semi-device-independent cryptography [10–12], high-dimensional communication [13], and self-testing [14]. These foundational and operational connections motivate a precise characterization of $P_{n,m}^{Q,\text{avg,opt}}$.

1.1 Prior work and problem status

While much progress has been made through various bounds and QRAC constructions [2, 14–23], exact characterizations of $P_{n,m}^{Q,\text{avg,opt}}$ were previously known only in a handful of cases. The values for $(n, m) = (2, 1), (3, 1)$ follow from [2, 16]. For $(n, m) = (3, 2), (4, 2), (6, 2)$, the constructions of Imamichi and Raymond [17] meet the $m = 2$ converse of Mančinska and Storgaard [18]. Thus,

$$P_{n,m}^{Q,\text{avg,opt}} = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{m}{n}}, \quad (n, m) \in \{(2, 1), (3, 1), (3, 2), (4, 2), (6, 2)\}. \quad (1)$$

Remarkably, the same form also appears in a numerically conjectured general upper bound noted in [21, 22]:

$$P_{n,m}^{Q,\text{avg,opt}} \stackrel{?}{\leq} \frac{1}{2} + \frac{1}{2}\sqrt{\frac{m}{n}}. \quad (2)$$

It is known that the bound (2) holds if $m \in \{1, 2\}$, because the bound $P_{n,m}^{Q,\text{avg,opt}} \leq \frac{1}{2} + \frac{1}{2}\sqrt{\frac{2^{m-1}}{n}}$ is established in [18], and for $m \in \{1, 2\}$ we have $2^{m-1} = m$.

Although Liu's classical random access code (RAC) counterexamples rule out (2) as a universal upper bound [24], the high-rate cases $m \in \{n-1, n-2\}$ remain of interest because known QRAC constructions attain the square-root value. Specifically the $(n, n-1)$ QRACs constructed by Suzuki in [21], and the $(n, n-2)$ QRACs constructed by Akibue et al. in [22], achieve average success probability $\frac{1}{2} + \frac{1}{2}\sqrt{\frac{m}{n}}$ for $m = n-1$ and $m = n-2$, respectively. Thus, if the conjectured bound (2) can be proved for $m \in \{n-1, n-2\}$, then it would prove the optimality of both constructions, and thus determine the precise values of $P_{n,n-1}^{Q,\text{avg,opt}}$ and $P_{n,n-2}^{Q,\text{avg,opt}}$. Indeed, a proof of (2) for $m \in \{n-1, n-2\}$ is the main contribution of this work.

1.2 Main results and proof idea

Our first result answers this question and determines the optimum for both families:

$$P_{n,m}^{Q,\text{avg,opt}} = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{m}{n}}, \quad m \in \{n-1, n-2\}. \quad (3)$$

Our converse utilizes a translation from local to global reconstruction via pretty good measurement (PGM), that is studied in [20]. The full-string PGM [25, 26] produces an entire candidate string $Y^{\mathfrak{C}, \text{PGM}}$ for the uniform string X encoded by a QRAC $\mathfrak{C}$. Lin and de Wolf in [20, Theorem 2] show that reducing the outcome of the full-string PGM to the

i th bit by summing over the possible outcomes for other bits, induces exactly the one-bit PGM for the i th bit.

Building on this foundation, we find upper and lower bounds on the expected Hamming distance $\Delta^{\mathfrak{C}, \text{PGM}} := \mathbb{E}[d_H(X, Y^{\mathfrak{C}, \text{PGM}})]$. For the upper bound, if a given QRAC $\mathfrak{C}$ has average success probability $P^{\mathfrak{C}}$, then by averaging over one-bit PGMs we show that $\Delta^{\mathfrak{C}, \text{PGM}} \leq \frac{n}{2} \left(1 - (2P^{\mathfrak{C}} - 1)^2\right)$. For the lower bound, based on the full-string PGM we show that when $m \in \{n-1, n-2\}$, then $\Delta^{\mathfrak{C}, \text{PGM}} \geq \frac{n-m}{2}$. Combining these bounds produces the desired proof of (2) with $m \in \{n-1, n-2\}$ for the QRAC $\mathfrak{C}$. Since the bound holds for any (n, m) QRAC $\mathfrak{C}$ with $m \in \{n-1, n-2\}$, it also holds for the optimal average success probability.

This approach extends to general binary (n, m) QRACs through an LP that lower-bounds the PGM distortion. The LP combines the encoding-dimension bound with the full family of Krawtchouk inequalities, including the parity constraint used in the $(n, n-2)$ converse. We show that this LP has the same optimal value as the corresponding Delsarte LP for the minimum average distance of binary codes [27–29]. Applying Mounits’s bounds [28, Theorem 12] then yields closed-form QRAC converses for two infinite parameter families. At $(n, m) = (6, 3)$, the upper bound matches a QRAC construction, determining the exact optimal average success probability.

For comparison, we place the LP converse alongside the general analytic bounds of Nayak [15], Mančinska and Storgaard [18], and Akibue et al. [22]. The resulting curves show that the LP converse and Akibue et al.’s bound are complementary across parameter regimes. On the two closed-form families, however, the comparison can be settled analytically: the LP converse is strictly tighter at every admissible point except $(n, m) = (3, 1)$, where the two bounds coincide.

2 QRACs and the Full-String PGM

2.1 Average-case QRAC model

Let $[n] = \{1, \dots, n\}$. A binary (n, m) QRAC $\mathfrak{C}$ is specified as a tuple $(\{\rho_x^{\mathfrak{C}}\}_{x \in \{0,1\}^n}, \{M_{0|i}^{\mathfrak{C}}, M_{1|i}^{\mathfrak{C}}\}_{i \in [n]})$, where $\{\rho_x^{\mathfrak{C}}\}_{x \in \{0,1\}^n}$ is an ensemble of quantum states on a Hilbert space of dimension at most 2^m , and $\{M_{0|i}^{\mathfrak{C}}, M_{1|i}^{\mathfrak{C}}\}$ is a binary positive operator-valued measure (POVM) for decoding the i th bit. The encoder obtains a uniformly random binary string $X \in \{0, 1\}^n$ and maps any realization $X = x = x_1 x_2 \dots x_n$ to the corresponding quantum state $\rho_x^{\mathfrak{C}}$. The decoder is given the encoded quantum state, along with an independently generated uniformly random index $\mathcal{I} \in [n]$. Given $\rho_x^{\mathfrak{C}}$ and the realization $\mathcal{I} = i$, the decoder produces $Y_i^{\mathfrak{C}}$ as the measurement outcome of the POVM $\{M_{0|i}^{\mathfrak{C}}, M_{1|i}^{\mathfrak{C}}\}$ applied to $\rho_x^{\mathfrak{C}}$. Define the coordinate-wise success probability of $\mathfrak{C}$ as

$$\begin{aligned} p_i^{\mathfrak{C}} &:= \mathbb{P}(Y_i^{\mathfrak{C}} = X_i \mid \mathcal{I} = i) \\ &= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \mathbb{P}(Y_i^{\mathfrak{C}} = X_i \mid X = x, \mathcal{I} = i) \\ &= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \text{Tr}(\rho_x^{\mathfrak{C}} M_{x_i|i}^{\mathfrak{C}}), \end{aligned} \tag{4}$$

and the average success probability (ASP) of $\mathfrak{C}$ as

$$P^{\mathfrak{C}} := \frac{1}{n} \sum_{i=1}^n p_i^{\mathfrak{C}}. \tag{5}$$

Define the coordinate-wise success probability of $\mathfrak{C}$, optimized over all POVMs for the i th bit decoding, as

$$p_i^{\mathfrak{C}*} := \max_{\text{POVM:}\{M_{0|i}, M_{1|i}\}} \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \text{Tr}(\rho_x^{\mathfrak{C}} M_{x_i|i}) \quad (6)$$

The *optimal* ASP for the entire class of (n, m) QRACs, $P_{n,m}^{Q,\text{avg,opt}}$ is defined as in [21],

$$P_{n,m}^{Q,\text{avg,opt}} := \max_{\mathfrak{C}} P^{\mathfrak{C}} \quad (7)$$

$$= \max_{\{\rho_x\}, \{M_{b|i}\}} \frac{1}{n 2^n} \sum_{x \in \{0,1\}^n} \sum_{i=1}^n \text{Tr}(\rho_x M_{x_i|i}). \quad (8)$$

2.2 The full-string PGM and Hamming distortion

The full-string PGM is defined from the average state

$$\bar{\rho}^{\mathfrak{C}} := 2^{-n} \sum_{x \in \{0,1\}^n} \rho_x^{\mathfrak{C}} \quad (9)$$

as in [20] with uniform X as follows.

$$Q_y^{\mathfrak{C}} = 2^{-n} (\bar{\rho}^{\mathfrak{C}})^{-1/2} \rho_y^{\mathfrak{C}} (\bar{\rho}^{\mathfrak{C}})^{-1/2}, \quad y \in \{0,1\}^n, \quad (10)$$

where inverse powers are taken on $\text{supp}(\bar{\rho}^{\mathfrak{C}})$ and are zero on the orthogonal complement. Then $\sum_y Q_y^{\mathfrak{C}} = \Pi_{\text{supp}(\bar{\rho}^{\mathfrak{C}})}$ is the orthogonal projection matrix onto $\text{supp}(\bar{\rho}^{\mathfrak{C}})$, and $\{Q_y^{\mathfrak{C}}\}_y$ is a POVM on $\text{supp}(\bar{\rho}^{\mathfrak{C}})$; if desired as a POVM on the whole ambient Hilbert space, it may be completed arbitrarily on $\text{supp}(\bar{\rho}^{\mathfrak{C}})^\perp$. This completion does not affect the probabilities below, because all code states are supported on $\text{supp}(\bar{\rho}^{\mathfrak{C}})$. Let $Y^{\mathfrak{C},\text{PGM}} \in \{0,1\}^n$ denote the PGM output when the input is $X \in \{0,1\}^n$.

For $x, y \in \{0,1\}^n$, write

$$d_H(x, y) = |\{i \in [n] : x_i \neq y_i\}|$$

for their Hamming distance. For the random pair $(X, Y^{\mathfrak{C},\text{PGM}})$, define the PGM distortion by

$$\Delta^{\mathfrak{C},\text{PGM}} := \mathbb{E}[d_H(X, Y^{\mathfrak{C},\text{PGM}})]. \quad (11)$$

The full-string PGM induces a classical channel $T_{xy}^{\mathfrak{C},\text{PGM}}$ with input $x \in \{0,1\}^n$, output $y \in \{0,1\}^n$, and the transition probabilities,

$$T_{xy}^{\mathfrak{C},\text{PGM}} = \mathbb{P}[Y^{\mathfrak{C},\text{PGM}} = y \mid X = x] = \text{Tr}(\rho_x^{\mathfrak{C}} Q_y^{\mathfrak{C}}). \quad (12)$$

3 Main Results

We start with three useful lemmas. The first lemma produces an upper bound on the expected Hamming distance, $\Delta^{\mathfrak{C},\text{PGM}}$, between X and the full-string PGM output Y .

Lemma 1. *For the full-string PGM output $Y^{\mathfrak{C},\text{PGM}}$,*

$$\Delta^{\mathfrak{C},\text{PGM}} \leq \frac{n}{2} \left(1 - (2P^{\mathfrak{C}} - 1)^2\right). \quad (13)$$

Proof. From Lin and de Wolf [20, Proof of Theorem 2], let us recall that reducing the outcome of the full-string PGM to the i th bit by summing over the possible outcomes for other bits, induces exactly the one-bit PGM for the i th bit. Thus, the i th coordinate of the full-string PGM output $Y^{\mathfrak{C}, \text{PGM}}$, namely $Y_i^{\mathfrak{C}, \text{PGM}}$, represents the output of a one-bit PGM for the i th bit from the binary marginal ensemble $\{(1/2, \sigma_{i,0}^{\mathfrak{C}}), (1/2, \sigma_{i,1}^{\mathfrak{C}})\}$, where

$$\sigma_{i,b}^{\mathfrak{C}} := \frac{1}{2^{n-1}} \sum_{x \in \{0,1\}^n: x_i=b} \rho_x^{\mathfrak{C}}, \quad b \in \{0,1\}. \quad (14)$$

This allows us to apply Renes's refined PGM bound [30, Eq. (12)] for a *one-bit* PGM to obtain,

$$\mathbb{P}[Y_i^{\mathfrak{C}, \text{PGM}} = X_i] \geq (p_i^{\mathfrak{C}*})^2 + (1 - p_i^{\mathfrak{C}*})^2 \quad (15)$$

The optimized POVM in (6) is at least as good as choosing the better of the POVM prescribed by $\mathfrak{C}$ and its swapped version, i.e.,

$$p_i^{\mathfrak{C}*} \geq \max\{p_i^{\mathfrak{C}}, 1 - p_i^{\mathfrak{C}}\} \geq 1/2. \quad (16)$$

Recognizing that the function $z^2 + (1 - z)^2$ is increasing for $z \geq 1/2$, we combine (15) and (16) to obtain,

$$\begin{aligned} \mathbb{P}[Y_i^{\mathfrak{C}, \text{PGM}} = X_i] &\geq (\max\{p_i^{\mathfrak{C}}, 1 - p_i^{\mathfrak{C}}\})^2 + (1 - \max\{p_i^{\mathfrak{C}}, 1 - p_i^{\mathfrak{C}}\})^2 \\ &= (p_i^{\mathfrak{C}})^2 + (1 - p_i^{\mathfrak{C}})^2 \end{aligned} \quad (17)$$

$$= (p_i^{\mathfrak{C}})^2 + (1 - p_i^{\mathfrak{C}})^2 \quad (18)$$

which is equivalently expressed as

$$\mathbb{P}[Y_i^{\mathfrak{C}, \text{PGM}} \neq X_i] \leq 2p_i^{\mathfrak{C}}(1 - p_i^{\mathfrak{C}}). \quad (19)$$

Summing over all $i \in [n]$ yields,

$$\begin{aligned} \Delta^{\mathfrak{C}, \text{PGM}} &= \mathbb{E}[d_{\text{H}}(X, Y^{\mathfrak{C}, \text{PGM}})] \\ &= \sum_{i \in [n]} \mathbb{P}[Y_i^{\mathfrak{C}, \text{PGM}} \neq X_i] \end{aligned} \quad (20)$$

$$\leq \sum_{i \in [n]} 2p_i^{\mathfrak{C}}(1 - p_i^{\mathfrak{C}}) \quad (21)$$

$$\leq 2nP^{\mathfrak{C}}(1 - P^{\mathfrak{C}}). \quad (22)$$

Step (22) follows from an application of Jensen's inequality, recognizing that $z(1 - z)$ is a concave function of z . Finally, rearranging the bound $\Delta^{\mathfrak{C}, \text{PGM}} \leq 2nP^{\mathfrak{C}}(1 - P^{\mathfrak{C}})$ yields the desired bound (13). $\square$

The second lemma establishes that the matrix of transition probabilities for the channel $T^{\mathfrak{C}, \text{PGM}}$ defined in (12) is positive semidefinite (PSD).

Lemma 2. *The matrix $T^{\mathfrak{C}, \text{PGM}}$ is positive semidefinite.*

Proof. Define

$$A_x^{\mathfrak{C}} := (\bar{\rho}^{\mathfrak{C}})^{-1/4} \rho_x^{\mathfrak{C}} (\bar{\rho}^{\mathfrak{C}})^{-1/4} \quad (23)$$

and note that the cyclicity of trace implies

$$T_{xy}^{\mathfrak{C}, \text{PGM}} = \text{Tr}(\rho_x^{\mathfrak{C}} Q_y^{\mathfrak{C}}) \quad (24)$$

$$= \text{Tr}(\rho_x^{\mathfrak{C}} 2^{-n} (\bar{\rho}^{\mathfrak{C}})^{-1/2} \rho_y^{\mathfrak{C}} (\bar{\rho}^{\mathfrak{C}})^{-1/2}) \quad (25)$$

$$= 2^{-n} \text{Tr}(A_x^{\mathfrak{C}} A_y^{\mathfrak{C}}) \quad (26)$$

Thus, $T_{xy}^{\mathfrak{C}, \text{PGM}} = 2^{-n} \text{Tr}(A_x^{\mathfrak{C}} A_y^{\mathfrak{C}})$ is a real symmetric Gram matrix in the Hilbert-Schmidt inner product, which makes it positive semidefinite. $\square$

The third lemma bounds the probability that the Hamming distance between X and the full-string PGM output is odd, essentially by showing that for any n -bit random strings X and Y , if the matrix representation of their joint probability mass function is positive semidefinite, then the Hamming distance between X and Y is not more likely to be odd than it is to be even.

Lemma 3. *We have the following bound,*

$$\mathbb{P}[d_H(X, Y^{\mathfrak{C}, \text{PGM}}) \text{ is odd}] \leq \frac{1}{2}. \quad (27)$$

Proof. Let $s : \{0, 1\}^n \rightarrow \{-1, 1\}$ be defined by $s(x) = (-1)^{|x|}$, where $|x|$ denotes the Hamming weight of x . Using the fact established in Lemma 2, i.e., $T^{\mathfrak{C}, \text{PGM}} \succeq 0$, we have

$$0 \leq 2^{-n} \sum_{x, y} s(x) T_{xy}^{\mathfrak{C}, \text{PGM}} s(y) \quad (28)$$

$$= 2^{-n} \sum_{x, y} s(x) \mathbb{P}[Y^{\mathfrak{C}, \text{PGM}} = y \mid X = x] s(y) \quad (29)$$

$$= \sum_{x, y} s(x) \mathbb{P}[Y^{\mathfrak{C}, \text{PGM}} = y, X = x] s(y) \quad (30)$$

$$= \mathbb{E}[s(X) s(Y^{\mathfrak{C}, \text{PGM}})] \quad (31)$$

$$= \mathbb{E}[(-1)^{|X| + |Y^{\mathfrak{C}, \text{PGM}}|}] \quad (32)$$

$$= \mathbb{E}[(-1)^{d_H(X, Y^{\mathfrak{C}, \text{PGM}})}] \quad (33)$$

$$= \mathbb{P}[d_H(X, Y^{\mathfrak{C}, \text{PGM}}) \text{ is even}] - \mathbb{P}[d_H(X, Y^{\mathfrak{C}, \text{PGM}}) \text{ is odd}] \quad (34)$$

$$= 1 - 2\mathbb{P}[d_H(X, Y^{\mathfrak{C}, \text{PGM}}) \text{ is odd}] \quad (35)$$

Step (29) follows from (12). Step (30) follows from the uniform distribution on X . Step (33) follows from the fact that $(|x| + |y|) \bmod 2$ is equal to $d_H(x, y) \bmod 2$. Rearranging (35) yields the desired bound (27). $\square$

Main Result.— Our main result appears in the following theorem.

Theorem 1. *For $m \in \{n-1, n-2\}$, every binary (n, m) QRAC $\mathfrak{C}$ has average success probability bounded as*

$$P^{\mathfrak{C}} \leq \frac{1}{2} + \frac{1}{2} \sqrt{\frac{m}{n}}. \quad (36)$$

Consequently Eq. (2) holds for $P_{n,m}^{Q, \text{avg}, \text{opt}}$.

Proof. By relabeling the two outcomes of each coordinate POVM if necessary, we may assume without loss of generality that $p_i^{\mathfrak{C}} \geq 1/2$ for all i . This is because relabeling leaves the encoding ensemble, and hence the full-string PGM channel and $\Delta^{\mathfrak{C},\text{PGM}} = \mathbb{E}[d_{\text{H}}(X, Y^{\mathfrak{C},\text{PGM}})]$, unchanged, while it can only increase the ASP.

It will be useful to recall Nayak's result in [15, Theorem 2.4, Part 2] which directly implies that $\mathbb{P}[Y = X] \leq 2^{m-n}$ if $Y \in \{0, 1\}^n$ is obtained by making *any* measurement (not restricted to PGM) of an m -qubit encoding of a uniform $X \in \{0, 1\}^n$. In particular, this implies

$$\mathbb{P}[Y^{\mathfrak{C},\text{PGM}} = X] \leq 2^{m-n}. \quad (37)$$

Case 1: For $m = n - 1$ we have,

$$\Delta^{\mathfrak{C},\text{PGM}} = \sum_{i \in [n]} \mathbb{P}[Y_i^{\mathfrak{C},\text{PGM}} \neq X_i] \quad (38)$$

$$\geq \mathbb{P}[Y^{\mathfrak{C},\text{PGM}} \neq X] \quad (39)$$

$$\geq 1/2 \quad (40)$$

Step (40) follows by applying (37) with $m = n - 1$.

Case 2: Now consider $m = n - 2$. For compact notation let us define $q_0 := \mathbb{P}[d_{\text{H}}(X, Y^{\mathfrak{C},\text{PGM}}) = 0]$ and $q_{\text{odd}} := \mathbb{P}[d_{\text{H}}(X, Y^{\mathfrak{C},\text{PGM}}) \text{ is odd}]$.

$$\Delta^{\mathfrak{C},\text{PGM}} = \mathbb{E}[d_{\text{H}}(X, Y^{\mathfrak{C},\text{PGM}})] \quad (41)$$

$$\geq \mathbb{P}[d_{\text{H}}(X, Y^{\mathfrak{C},\text{PGM}}) \text{ is odd}] \quad (42)$$

$$+ 2\mathbb{P}[d_{\text{H}}(X, Y^{\mathfrak{C},\text{PGM}}) \text{ is nonzero and even}]$$

$$= q_{\text{odd}} + 2(1 - q_0 - q_{\text{odd}}) \quad (43)$$

$$= 2 - 2q_0 - q_{\text{odd}} \quad (44)$$

$$\geq 2 - 2(1/4) - (1/2) \quad (45)$$

$$= 1 \quad (46)$$

Step (42) uses the fact that odd values of the Hamming distance must be at least one, and nonzero even values of the Hamming distance must be at least 2. Step (45) applies the bound $q_0 \leq 1/4$ which follows from (37) for $m = n - 2$, and the bound $q_{\text{odd}} \leq 1/2$ which follows from Lemma 3.

Thus $\Delta^{\mathfrak{C},\text{PGM}} \geq (n - m)/2$ in both cases. Applying Lemma 1 and substituting this into (13) yields

$$\frac{n - m}{2} \leq \frac{n}{2} (1 - (2P^{\mathfrak{C}} - 1)^2) \quad (47)$$

$$\implies n(2P^{\mathfrak{C}} - 1)^2 \leq m. \quad (48)$$

Since $P^{\mathfrak{C}} = \frac{1}{n} \sum_{i=1}^n p_i^{\mathfrak{C}} \geq 1/2$ as assumed without loss of generality, for $m \in \{n - 1, n - 2\}$ we obtain the desired bound

$$P^{\mathfrak{C}} \leq \frac{1}{2} + \frac{1}{2} \sqrt{\frac{m}{n}}. \quad (49)$$

□

The exact values of $P_{n,m}^{Q,\text{avg,opt}}$ for $m \in \{n - 1, n - 2\}$ now follow as a corollary.

Corollary 1. For $m \in \{n-1, n-2\}$,

$$P_{n,m}^{Q,\text{avg,opt}} = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{m}{n}}. \quad (50)$$

Proof. The upper bound follows by Theorem 1. For $m = n-1$, Suzuki's $(n, n-1)$ construction achieves the right-hand side [21]. For $m = n-2$ the $(n, n-2)$ construction of Akibue et al. achieves the right-hand side [22]. $\square$

4 An LP Extension

The $(n, n-1)$ and $(n, n-2)$ converses above used only the bound $q_0 \leq 2^{m-n}$ and the parity bound $q_{\text{odd}} \leq 1/2$. For a general binary (n, m) QRAC, we retain the full family of PSD constraints at the Hamming-distance distribution level, reducing the original matrix problem to an LP with $n+1$ variables and only $O(n)$ constraints. We then show that the diagonal-mass constraint is saturated at every optimal solution, which is the key to transforming the LP into the Delsarte LP. This identification allows existing analytic results for the Delsarte LP to be transferred directly to QRAC converses, thereby building a bridge between QRAC analysis and established classical coding theory.

4.1 The PSD structure of the PGM-induced joint probability matrix

The three lemmas above and the dimension bound underlying (37) do not require the encoding dimension to be a power of two. We therefore allow an encoding system of dimension at most a positive integer D ; the m -qubit setting corresponds to $D = 2^m$.

Write $N := 2^n$ and define the joint probability matrix of the uniform input and the full-string PGM output by

$$J_{xy}^{\mathfrak{C},\text{PGM}} := \mathbb{P}[X = x, Y^{\mathfrak{C},\text{PGM}} = y] = \frac{1}{N} T_{xy}^{\mathfrak{C},\text{PGM}}, \quad x, y \in \{0, 1\}^n. \quad (51)$$

Writing $J := J^{\mathfrak{C},\text{PGM}} = N^{-1} T^{\mathfrak{C},\text{PGM}}$, we obtain directly from the channel definition (12), Lemma 2, and the dimension bound above that

$$J_{xy} \geq 0, \quad J = J^T, \quad J \succeq 0, \quad (52)$$

$$J\mathbf{1} = \frac{1}{N}\mathbf{1}, \quad \text{Tr } J \leq \frac{D}{N}. \quad (53)$$

We next use these matrix constraints to derive an LP for the Hamming-distance distribution.

4.2 From the joint probability matrix to a distance LP

For a joint probability matrix J indexed by $\{0, 1\}^n \times \{0, 1\}^n$, define its Hamming-distance distribution by

$$q_k(J) := \sum_{\substack{x, y \in \{0, 1\}^n \\ d_H(x, y) = k}} J_{xy}, \quad 0 \leq k \leq n.$$

For $J = J^{\mathfrak{C},\text{PGM}}$, the vector $q(J) = (q_0(J), \dots, q_n(J))$ is the probability distribution of $d_H(X, Y^{\mathfrak{C},\text{PGM}})$. In particular,

$$q_k(J) \geq 0, \quad \sum_{k=0}^n q_k(J) = 1, \quad q_0(J) = \text{Tr } J,$$

and

$$\Delta^{\mathfrak{C}, \text{PGM}} = \sum_{k=0}^n k q_k(J).$$

We next extract from $J \succeq 0$ a family of inequalities that depends only on the distance distribution $q(J)$. For $S \subseteq [n]$, define the binary character

$$\chi_S(x) := (-1)^{\sum_{i \in S} x_i}, \quad x \in \{0, 1\}^n,$$

and view χ_S as a vector indexed by $\{0, 1\}^n$. Since $J \succeq 0$, for every $S \subseteq [n]$,

$$\begin{aligned} \chi_S^\top J \chi_S &= \sum_{x, y \in \{0, 1\}^n} \chi_S(x) \chi_S(y) J_{xy} \\ &= \sum_{x, y \in \{0, 1\}^n} (-1)^{\sum_{i \in S} (x_i \oplus y_i)} J_{xy} \geq 0. \end{aligned} \tag{54}$$

The fixed-distance averages of these characters are described by the binary Krawtchouk polynomials. For $0 \leq j, k \leq n$, define the degree- j binary Krawtchouk polynomial [31] as follows:

$$K_j^{(n)}(k) := \sum_{\ell=0}^j (-1)^\ell \binom{k}{\ell} \binom{n-k}{j-\ell}, \tag{55}$$

We use the normalized form

$$\kappa_j^{(n)}(k) := \frac{K_j^{(n)}(k)}{\binom{n}{j}}, \tag{56}$$

for which $\kappa_j^{(n)}(0) = 1$.

To see directly why these polynomials arise, fix $j \in \{1, \dots, n\}$ and suppose that $d_H(x, y) = k$. The vector $x \oplus y$ then has exactly k nonzero coordinates. If a set $S \subseteq [n]$ of size j contains exactly ℓ of these coordinates, then $(-1)^{\sum_{i \in S} (x_i \oplus y_i)} = (-1)^\ell$. There are $\binom{k}{\ell} \binom{n-k}{j-\ell}$ such sets S . Therefore,

$$\begin{aligned} \frac{1}{\binom{n}{j}} \sum_{\substack{S \subseteq [n] \\ |S|=j}} (-1)^{\sum_{i \in S} (x_i \oplus y_i)} &= \frac{1}{\binom{n}{j}} \sum_{\ell=0}^j (-1)^\ell \binom{k}{\ell} \binom{n-k}{j-\ell} \\ &= \frac{K_j^{(n)}(k)}{\binom{n}{j}} = \kappa_j^{(n)}(k). \end{aligned} \tag{57}$$

Thus, $\kappa_j^{(n)}(k)$ is precisely the average of all binary characters χ_S with $|S| = j$, evaluated on a pair of strings at Hamming distance k .

Averaging (54) over all $\binom{n}{j}$ subsets S of size j , and then using (57), gives

$$\begin{aligned} 0 &\leq \frac{1}{\binom{n}{j}} \sum_{\substack{S \subseteq [n] \\ |S|=j}} \chi_S^\top J \chi_S \\ &= \sum_{x, y \in \{0, 1\}^n} J_{xy} \kappa_j^{(n)}(d_H(x, y)) \\ &= \sum_{k=0}^n q_k(J) \kappa_j^{(n)}(k), \quad 1 \leq j \leq n. \end{aligned} \tag{58}$$

We refer to (58) as the normalized Krawtchouk inequalities. They are the consequences of $J \succeq 0$ that remain after J is reduced to its Hamming-distance distribution.

The case $j = 0$ provides no additional constraint, since $\kappa_0^{(n)}(k) = 1$ and $\sum_{k=0}^n q_k(J) = 1$. At the other extreme, when $j = n$, $K_n^{(n)}(k) = (-1)^k$. Hence (58) reduces to $\sum_{k=0}^n (-1)^k q_k(J) \geq 0$, which is precisely the parity inequality used in Lemma 3.

Motivated by these necessary conditions, define

$$\Delta_{\text{LP}}(n, D) := \min_{q_0, \dots, q_n} \sum_{k=0}^n k q_k \quad (59)$$

subject to

$$\begin{aligned} q_k &\geq 0, & 0 \leq k \leq n, \\ \sum_{k=0}^n q_k &= 1, & q_0 \leq \frac{D}{2^n}, \end{aligned} \quad (60)$$

$$\sum_{k=0}^n q_k \kappa_j^{(n)}(k) \geq 0, \quad 1 \leq j \leq n. \quad (61)$$

Thus, $\Delta_{\text{LP}}(n, D)$ is the minimum mean Hamming distance permitted by the relaxation consisting of the diagonal-mass constraint and the normalized Krawtchouk inequalities.

For a positive integer D , let $P_n^{Q, \text{avg}, \text{opt}}(D)$ denote the optimum in (8) when the encoding states act on a Hilbert space of dimension at most D . In particular,

$$P_n^{Q, \text{avg}, \text{opt}}(2^m) = P_{n, m}^{Q, \text{avg}, \text{opt}}.$$

Consequently, any uniform lower bound on the PGM distortion gives an upper bound on the optimal ASP. More precisely, suppose $L \in [0, n/2]$ satisfies

$$\Delta^{\mathfrak{C}, \text{PGM}} \geq L \quad (62)$$

for every binary QRAC $\mathfrak{C}$ whose encoding dimension is at most D . Combining this bound with Lemma 1 gives

$$|2P^{\mathfrak{C}} - 1| \leq \sqrt{1 - \frac{2L}{n}}$$

for every such $\mathfrak{C}$. Maximizing over all such QRACs therefore gives

$$P_n^{Q, \text{avg}, \text{opt}}(D) \leq \frac{1}{2} \left(1 + \sqrt{1 - \frac{2L}{n}} \right). \quad (63)$$

Since the right-hand side of (63) is decreasing in L , a stronger uniform lower bound on the PGM distortion yields a stronger QRAC converse.

Theorem 2. *Every binary QRAC $\mathfrak{C}$ whose encoding dimension is at most D satisfies*

$$\Delta^{\mathfrak{C}, \text{PGM}} \geq \Delta_{\text{LP}}(n, D). \quad (64)$$

Consequently,

$$P_n^{Q, \text{avg}, \text{opt}}(D) \leq \frac{1}{2} \left(1 + \sqrt{1 - \frac{2\Delta_{\text{LP}}(n, D)}{n}} \right). \quad (65)$$

Proof. For $J = J^{\mathfrak{C}, \text{PGM}}$, the preceding derivation shows that its distance distribution $q(J)$ satisfies (61). Moreover,

$$q_0(J) = \text{Tr } J \leq \frac{D}{2^n},$$

so $q(J)$ also satisfies (60). It is therefore feasible for the LP (59), and its objective value is

$$\sum_{k=0}^n k q_k(J) = \Delta^{\mathfrak{C}, \text{PGM}}.$$

By the definition of the minimum,

$$\Delta^{\mathfrak{C}, \text{PGM}} \geq \Delta_{\text{LP}}(n, D),$$

which proves (64). Equation (65) then follows from (63) with $L = \Delta_{\text{LP}}(n, D)$. $\square$

In particular, $\Delta_{\text{LP}}(n, 2^{n-1}) = 1/2$ and $\Delta_{\text{LP}}(n, 2^{n-2}) = 1$, so Theorem 2 recovers the high-rate converses of Theorem 1.

4.3 Identification with the Delsarte LP

For fixed length n and code size M , the classical minimum-average-distance problem asks for the smallest possible average Hamming distance between two independently and uniformly chosen codewords of a binary code $C \subseteq \{0, 1\}^n$ with $|C| = M$ [27]. The Delsarte distance-distribution LP approach relaxes this problem by optimizing over distance distributions subject to the corresponding Krawtchouk inequalities [27, 31]. This is directly comparable with the QRAC distance LP in (59)–(61), which has the same distance objective and the same Krawtchouk inequalities.

To make this comparison explicit, let $C \subseteq \{0, 1\}^n$ be a binary code with $|C| = M$, and let U, V be independently and uniformly distributed over C . Following [29], define the distance distribution of C by

$$\pi_k(C) := \mathbb{P}[d_H(U, V) = k] = \frac{1}{M^2} |\{(u, v) \in C^2 : d_H(u, v) = k\}|, \quad 0 \leq k \leq n. \quad (66)$$

Then $\pi_k(C) \geq 0$, $\sum_{k=0}^n \pi_k(C) = 1$, $\pi_0(C) = \frac{1}{M}$. According to [29], the distance distribution satisfies the Krawtchouk inequalities, $\sum_{k=0}^n \pi_k(C) K_j^{(n)}(k) \geq 0$. Since $K_j^{(n)}(k) = \binom{n}{j} \kappa_j^{(n)}(k)$, this is equivalently $\sum_{k=0}^n \pi_k(C) \kappa_j^{(n)}(k) \geq 0$, $1 \leq j \leq n$.

Motivated by these necessary conditions, call a vector $\pi = (\pi_0, \dots, \pi_n)$ a *formal distance distribution of size M* if

$$\begin{aligned} \pi_k &\geq 0, & 0 \leq k \leq n, \\ \sum_{k=0}^n \pi_k &= 1, & \pi_0 = \frac{1}{M}, \\ \sum_{k=0}^n \pi_k \kappa_j^{(n)}(k) &\geq 0, & 1 \leq j \leq n. \end{aligned} \quad (67)$$

The Delsarte LP retains these linear constraints while dropping the requirement that π be realized by an actual binary code. Its minimum-average-distance value is

$$\Delta_{\text{Del}}(n, M) := \min_{\pi} \sum_{k=0}^n k \pi_k, \quad (68)$$

where the minimum is over all π satisfying (67).

Now set $D = 2^m$, $M = 2^{n-m}$. Then $\frac{D}{2^n} = \frac{1}{M}$. Comparing (67) with the QRAC constraints (60)–(61), all constraints agree term by term except at zero distance: the Delsarte LP requires $\pi_0 = \frac{1}{M}$, whereas the QRAC distance LP only imposes $q_0 \leq \frac{1}{M}$. The following proposition shows that this inequality is saturated at every optimal solution. Consequently, on the saturated face $q_0 = 1/M$, the two LPs coincide under the variable identification $\pi_k = q_k$, $0 \leq k \leq n$.

Proposition 1 (Identification with the Delsarte LP). *For $0 \leq m \leq n$ and $M := 2^{n-m}$,*

$$\Delta_{\text{LP}}(n, 2^m) = \Delta_{\text{Del}}(n, M). \quad (69)$$

Proof. Since $D = 2^m$, the diagonal-mass constraint is $q_0 \leq 1/M$. Suppose that a feasible q satisfies $q_0 < 1/M$. Let

$$e_0 := (1, 0, \dots, 0), \quad \theta := \frac{1/M - q_0}{1 - q_0}, \quad \tilde{q} := (1 - \theta)q + \theta e_0.$$

Because $q_0 < 1/M \leq 1$, we have $0 < \theta \leq 1$. Hence $\tilde{q}$ is a probability distribution with $\tilde{q}_0 = 1/M$. Moreover, since $\kappa_j^{(n)}(0) = 1$,

$$\sum_{k=0}^n \tilde{q}_k \kappa_j^{(n)}(k) = (1 - \theta) \sum_{k=0}^n q_k \kappa_j^{(n)}(k) + \theta \geq 0, \quad 1 \leq j \leq n.$$

Thus $\tilde{q}$ remains feasible. Since $q_0 < 1$, we have $\sum_{k=1}^n q_k > 0$, and consequently $\sum_{k=0}^n k q_k > 0$. Therefore,

$$\sum_{k=0}^n k \tilde{q}_k = (1 - \theta) \sum_{k=0}^n k q_k < \sum_{k=0}^n k q_k.$$

No feasible point with $q_0 < 1/M$ can therefore be optimal. Hence every optimal solution of the QRAC distance LP satisfies $q_0 = \frac{1}{M}$.

On this saturated face, the QRAC constraints (60)–(61) coincide exactly with (67) under the identity $\pi_k = q_k$, $0 \leq k \leq n$. Their objectives coincide as well:

$$\sum_{k=0}^n k q_k = \sum_{k=0}^n k \pi_k.$$

Thus restricting the QRAC distance LP to its saturated face does not change its optimal value and yields precisely the probability-normalized Delsarte LP. This proves (69). $\square$

Proposition 1 identifies the two distance-distribution LP relaxations. Thus, an evaluation of $\Delta_{\text{Del}}(n, M)$ gives $\Delta_{\text{LP}}(n, 2^m)$ and, through Theorem 2, yields a converse for binary QRACs.

4.4 Two closed-form families

Write $m = n - r$, so that the effective size is $M = 2^r$. The choices $n = 2^r - 1$ and $n = 2^r - 2$ give $M = n + 1$ and $M = n + 2$, respectively. In both cases, Proposition 1 reduces the evaluation of the QRAC distance LP to the corresponding Delsarte minimum-average-distance LP. A lower bound follows by specializing an LP bound of Mounits [28, Theorem 12], and we then show that it is attained by an explicit formal distance distribution supported on distances 0, 1, 2. This gives the following exact LP values.

Theorem 3. Let $m = n - r$ and $D = 2^m$.

1. If $r \geq 2$ and $n = 2^r - 1$, then

$$\Delta_{\text{LP}}(n, D) = \frac{2n}{n+3}, \quad (70)$$

$$P_{n, n-r}^{Q, \text{avg}, \text{opt}} \leq \frac{1}{2} \left(1 + \sqrt{\frac{n-1}{n+3}} \right). \quad (71)$$

2. If $r \geq 3$ and $n = 2^r - 2$, then

$$\Delta_{\text{LP}}(n, D) = \frac{2n}{n+2}, \quad (72)$$

$$P_{n, n-r}^{Q, \text{avg}, \text{opt}} \leq \frac{1}{2} \left(1 + \sqrt{\frac{n-2}{n+2}} \right). \quad (73)$$

Proof. Write $n = 2^r - c$, $c \in \{1, 2\}$, so that $M = 2^r = n + c$. Since $D = 2^m$ and $m = n - r$, Proposition 1 gives $\Delta_{\text{LP}}(n, D) = \Delta_{\text{Del}}(n, M)$. It therefore suffices to evaluate the corresponding Delsarte LP.

We first establish the lower bound. For any π satisfying (67), define its unnormalized Krawtchouk transform by $B_j := \sum_{k=0}^n \pi_k K_j^{(n)}(k)$, $0 \leq j \leq n$. Since $K_j^{(n)}(k) = \binom{n}{j} \kappa_j^{(n)}(k)$, the normalized Krawtchouk inequalities in (67) imply that $B_j \geq 0$. Moreover, $B_0 = 1$, and, since $K_1^{(n)}(k) = n - 2k$, $B_1 = n - 2 \sum_{k=0}^n k \pi_k$. Equivalently,

$$\sum_{k=0}^n k \pi_k = \frac{n - B_1}{2}. \quad (74)$$

The dual-polynomial criterion of Mounits [28, Theorem 9 and Corollary 2] uses a polynomial $\alpha(x) = \sum_{j=0}^n \alpha_j K_j^{(n)}(x)$ satisfying $\alpha_1 = 1$, $\alpha_j \geq 0$ ($2 \leq j \leq n$), $\alpha(k) \leq 0$ ($1 \leq k \leq n$). For every π satisfying (67), these conditions give

$$\alpha_0 + B_1 \leq \sum_{j=0}^n \alpha_j B_j = \sum_{k=0}^n \pi_k \alpha(k) \leq \pi_0 \alpha(0) = \frac{\alpha(0)}{M}. \quad (75)$$

Combining this with (74) yields

$$\sum_{k=0}^n k \pi_k \geq \frac{1}{2} \left(n + \alpha_0 - \frac{\alpha(0)}{M} \right).$$

In particular, this argument uses only the formal Delsarte constraints and does not require π to be realized by an actual binary code.

According to the dual polynomials constructed in Mounits [28, Theorem 12], we have $\alpha(0) = 2(n+1)$ and $\alpha_0 = \frac{6(n+1)}{n+3} - n$ for $c = 1$, whereas $\alpha(0) = 2n$ and $\alpha_0 = \frac{6n}{n+2} - n$ for $c = 2$. Substituting these parameters into the general bound yields

$$\Delta_{\text{Del}}(n, M) \geq \begin{cases} \frac{3(n+1)}{n+3} - \frac{n+1}{M}, & c = 1, \\ \frac{3n}{n+2} - \frac{n}{M}, & c = 2. \end{cases} \quad (76)$$

Since $M = n + c$, this simplifies directly to

$$\Delta_{\text{Del}}(n, M) \geq \frac{2n}{n + 4 - c}. \quad (77)$$

To show that this LP lower bound is tight, set $q_k = 0$ for $k \geq 3$ and define

$$(q_0, q_1, q_2) = \begin{cases} \left(\frac{1}{n+1}, \frac{4n}{(n+1)(n+3)}, \frac{n(n-1)}{(n+1)(n+3)} \right), & c = 1, \\ \left(\frac{1}{n+2}, \frac{2}{n+2}, \frac{n-1}{n+2} \right), & c = 2. \end{cases}$$

In either case, the entries are nonnegative,

$$q_0 = \frac{1}{M}, \quad \sum_{k=0}^n q_k = 1.$$

Using

$$\kappa_j^{(n)}(0) = 1, \quad \kappa_j^{(n)}(1) = \frac{n-2j}{n}, \quad \kappa_j^{(n)}(2) = \frac{(n-2j)^2 - n}{n(n-1)},$$

a direct substitution gives

$$\sum_{k=0}^n q_k \kappa_j^{(n)}(k) = \frac{(n-2j+2-c)(n-2j+4-c)}{(n+2-c)(n+4-c)}, \quad 0 \leq j \leq n.$$

For every integer $j \in \{0, \dots, n\}$, the two numerator factors are adjacent even integers and hence cannot have opposite nonzero signs. Their product is therefore nonnegative. Since the denominator is strictly positive, all normalized Krawtchouk inequalities are satisfied. Thus q is feasible for the Delsarte LP.

Its objective value is

$$\sum_{k=0}^n k q_k = q_1 + 2q_2 = \frac{2n}{n+4-c}.$$

Together with (77), this proves

$$\Delta_{\text{Del}}(n, M) = \frac{2n}{n+4-c}.$$

Proposition 1 now gives

$$\Delta_{\text{LP}}(n, D) = \frac{2n}{n+4-c}.$$

Finally, Theorem 2 yields

$$\begin{aligned} P_{n, n-r}^{Q, \text{avg}, \text{opt}} &\leq \frac{1}{2} \left(1 + \sqrt{1 - \frac{2}{n} \frac{2n}{n+4-c}} \right) \\ &= \frac{1}{2} \left(1 + \sqrt{\frac{n-c}{n+4-c}} \right). \end{aligned}$$

Taking $c = 1$ and $c = 2$ gives (71) and (73), respectively. $\square$

For $n = 2^r - c$ with $c \in \{1, 2\}$, classical $(n, n - r)$ RAC constructions based on binary Hamming codes achieve an ASP of $1 - \frac{1}{n+2-c}$ [23, 32]. Because the set of QRACs naturally subsumes all classical RACs [23], this achievable classical ASP serves as an immediate lower bound for $P_{n,n-r}^{Q,\text{avg,opt}}$. Combining this with the analytic upper bound of Theorem 3 gives

$$1 - \frac{1}{n+2-c} \leq P_{n,n-r}^{Q,\text{avg,opt}} \leq \frac{1}{2} \left(1 + \sqrt{\frac{n-c}{n+4-c}} \right). \quad (78)$$

Therefore, quantum resources can improve upon these optimal classical constructions by at most $O(n^{-2})$. For $r = 3$ and $c = 2$, the upper bound is exactly attained by a QRAC, yielding the optimal $(6, 3)$ value below.

4.5 An exact consequence: the $(6, 3)$ QRAC

Corollary 2. *The optimal average success probability of a binary $(6, 3)$ QRAC is*

$$P_{6,3}^{Q,\text{avg,opt}} = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \right). \quad (79)$$

Proof. Setting $r = 3$ in Theorem 3 gives $n = 6$ and $m = 3$, and hence

$$P_{6,3}^{Q,\text{avg,opt}} \leq \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \right).$$

For achievability, partition the six input bits into three pairs and encode each pair using the $(2, 1)$ QRAC of Ambainis et al. [2, Lemma 3.1]. The tensor product of the three one-qubit encodings recovers every target bit with probability $\cos^2(\frac{\pi}{8}) = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \right)$, which attains the upper bound. $\square$

4.6 Comparison with general analytic converses

We finally compare the LP converse with the general analytic converses. In our notation, Nayak's entropy bound [15] and the bound of Mančinska and Storgaard [18] are

$$B_N(n, m) := h_2^{-1} \left(1 - \frac{m}{n} \right), \quad B_{MS}(n, m) := \min \left\{ 1, \frac{1}{2} \left(1 + \sqrt{\frac{2^{m-1}}{n}} \right) \right\}, \quad (80)$$

where $h_2(p) := -p \log_2 p - (1-p) \log_2 (1-p)$ and the inverse is taken on $[1/2, 1]$. The finite-size refinement of the Nayak bound due to Akibue et al. [22, Theorem 2] is

$$B_A(n, m) := \frac{1}{2} \left[1 + \frac{1}{n} \inf_{\ell \in \mathbb{Z}_{\geq 1}} \left(\frac{2^m}{2^{n+1}} \sum_{k=0}^n \binom{n}{k} (n-2k)^{2\ell} \right)^{1/(2\ell)} \right]. \quad (81)$$

The choice $\ell = 1$ gives B_{MS} before truncation at one, so the optimization in (81) subsumes that bound. We write the LP converse as

$$B_{LP}(n, m) := \frac{1}{2} \left(1 + \sqrt{1 - \frac{2\Delta_{LP}(n, 2^m)}{n}} \right). \quad (82)$$

For the two closed-form families, the comparison with Akibue et al.'s bound can be settled analytically.

Proposition 2 (Comparison with Akibue et al.’s bound). *Let $m = n - r$. If either $n = 2^r - 1$ with $r \geq 2$ or $n = 2^r - 2$ with $r \geq 3$, then*

$$B_{\text{LP}}(n, m) \leq B_{\text{A}}(n, m),$$

with equality if and only if $(n, m) = (3, 1)$.

The proof is deferred to Appendix A. Proposition 2 shows that the closed-form LP converses are strictly tighter than Akibue et al.’s bound throughout both families, with equality only at $(n, m) = (3, 1)$.

Outside the two closed-form families, neither bound dominates globally. To illustrate their complementary regimes, we compare the bounds over three slices of the (n, m) plane: fixed n , fixed m , and fixed redundancy $n - m$. These respectively vary the coding rate at fixed input length, increase the input length at a fixed qubit budget, and approach the high-rate regime while $n - m$ remains fixed. In each figure, the upper panel shows these bounds, while the lower panel plots $B_{\text{A}} - B_{\text{LP}}$; positive values indicate that the LP converse is tighter. The binary specializations of de Vicente [33] and Farkas et al. [19] are omitted because they are no stronger than B_{MS} .

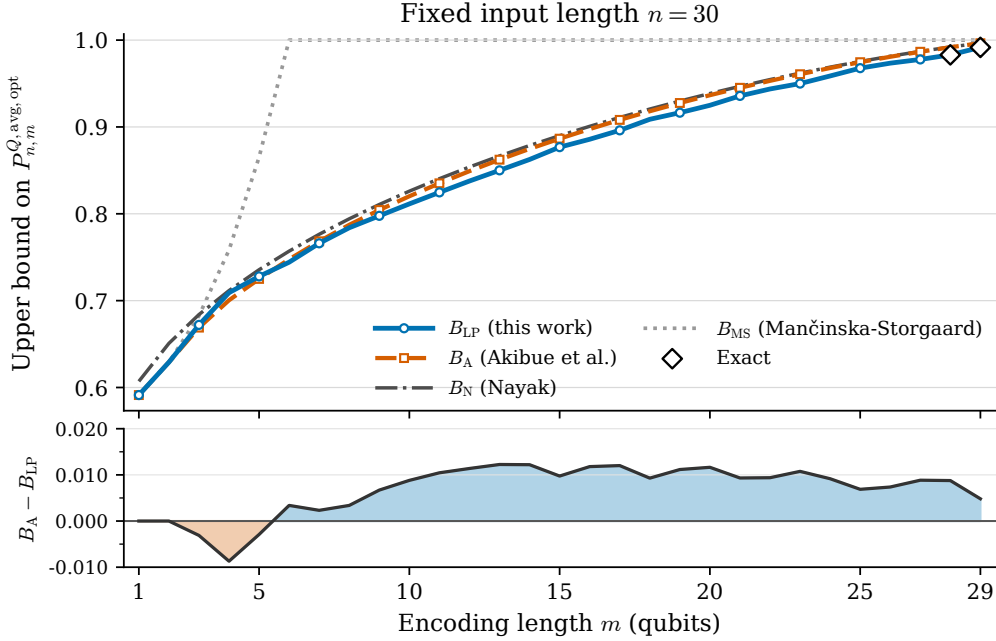


Figure 1: Comparison of converse bounds on $P_{30,m}^{Q,\text{avg},\text{opt}}$ for $1 \leq m < 30$. The lower panel shows $B_{\text{A}} - B_{\text{LP}}$. The diamonds at $m \in \{28, 29\}$ mark the exact values from Corollary 1.

For fixed input length $n = 30$, Akibue et al.’s bound is tighter for $3 \leq m \leq 5$, while the LP converse is tighter for $6 \leq m < 30$ and is tight at $m \in \{28, 29\}$.

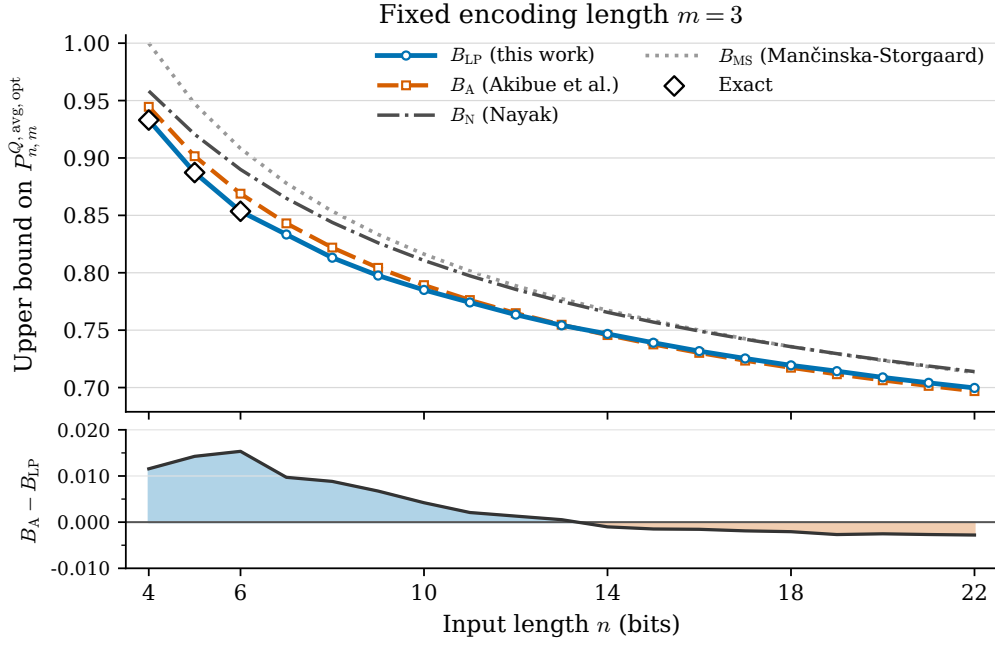


Figure 2: Comparison of converse bounds on $P_{n,3}^{Q,avg,opt}$ for $4 \leq n \leq 22$. The lower panel shows $B_A - B_{LP}$. The diamonds at $n \in \{4, 5, 6\}$ mark the exact values from Corollary 1 and Corollary 2.

For a fixed three-qubit encoding ($m = 3$), the ordering reverses as n grows: the LP converse is tighter for $4 \leq n \leq 13$, whereas Akibue et al.'s bound is tighter for $14 \leq n \leq 22$. The LP converse is tight at $n \in \{4, 5, 6\}$.

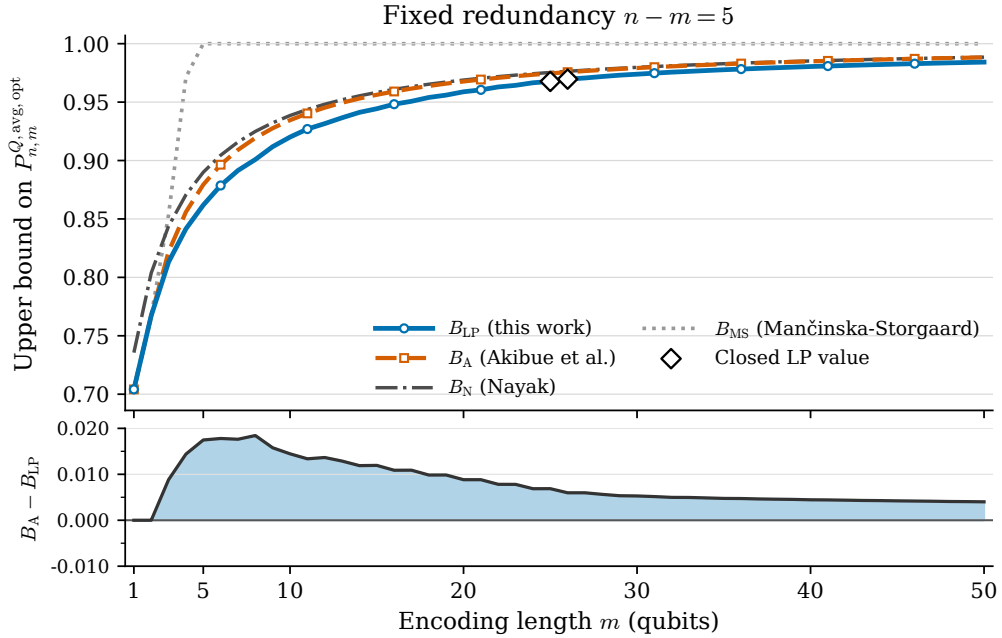


Figure 3: Comparison of converse bounds on $P_{m+5,m}^{Q,avg,opt}$ along the fixed-redundancy slice $n - m = 5$, for $1 \leq m \leq 50$. The lower panel shows $B_A - B_{LP}$. The diamonds at $m = 25$ and $m = 26$ mark the closed-form LP converse values at $(n, m) = (30, 25)$ and $(31, 26)$ from Theorem 3.

Along the fixed-redundancy slice $n - m = 5$, the LP converse is strictly tighter at

every displayed point with $3 \leq m \leq 50$, including the two closed-form points $m = 25$ and $m = 26$.

5 Discussion

In this paper, we determined the exact values of the optimal average success probability for binary $(n, n-1)$ and $(n, n-2)$ QRACs. The converse is driven by the PSD structure of the joint probability matrix of the uniform input X and the full-string PGM output $Y^{\mathfrak{c}, \text{PGM}}$, together with the encoding-dimension bound on its trace. Although Theorem 1 is stated for dimensions $D = 2^m$, the argument itself does not require D to be a power of two. For example, if $n = 4$ and $D = 6$, then the trace bound in (53) and Lemma 3 give $q_0 \leq 6/16$ and $q_{\text{odd}} \leq 1/2$, respectively. The odd-even decomposition in the proof of Theorem 1 therefore yields $\Delta^{\mathfrak{c}, \text{PGM}} \geq 3/4$, and Eq. (63) with $L = 3/4$ yields $P_4^{Q, \text{avg}, \text{opt}}(6) \leq \frac{1}{2} \left(1 + \sqrt{\frac{5}{8}}\right)$. This is strictly smaller than $\frac{1}{2} \left(1 + \sqrt{\log_2(6)/4}\right)$, obtained by formally replacing m with $\log_2 D$ in the square-root expression. Thus, even near the high-rate regime, direct logarithmic interpolation in the encoding dimension need not be tight.

The same trace and PSD constraints also yield the LP converse for general binary (n, m) QRACs. After restricting the distance LP to its saturated face and setting the effective size $M = 2^{n-m}$, Proposition 1 identifies the resulting face of the QRAC distance LP with the Delsarte minimum-average-distance LP. This yields the two closed-form families in Theorem 3. On both families, the resulting analytic bound is strictly tighter than that of Akibue et al., except at $(3, 1)$, where the two coincide; it also determines the exact value at $(6, 3)$. Outside these families, the two bounds are complementary. More broadly, these closed-form families represent only two instances enabled by the Delsarte identification; indeed, a much broader class of converses can be unlocked through this bridge, highlighting the rich potential of leveraging classical coding theory to establish sharper analytical bounds for QRACs.

The present LP retains the diagonal-mass constraint and the full distance-level content of $J \succeq 0$, but it does not characterize which feasible distance distributions can actually arise from a QRAC. Incorporating this missing realizability structure may lead to stronger converses. The resulting optimization, however, would generally be semidefinite or nonlinear rather than linear, making it less amenable to closed-form analysis.

Acknowledgements

The authors acknowledge the use of OpenAI’s ChatGPT (GPT-5.5) as a research assistant during the development of this work.

The authors independently formulated the research objectives and proposed the key LP formulation for the QRAC converse. ChatGPT assisted with intermediate calculations, identifying the connection between the resulting LP and the Delsarte minimum-average-distance LP in classical coding theory, generating simulation code, and developing and drafting proofs presented in the appendix.

All AI-assisted calculations, code, derivations, and mathematical proofs were independently verified, revised, and approved by the authors, who take full responsibility for the correctness and content of the manuscript.

A Proof of the Comparison with Akibue et al.'s Bound

Proof of Proposition 2. Write $n = 2^r - c$ with $c \in \{1, 2\}$ and set $b := \frac{n-c}{n+4-c}$. Let $S_n = \varepsilon_1 + \dots + \varepsilon_n$, where $\varepsilon_1, \dots, \varepsilon_n$ are independent random variables with $\mathbb{P}(\varepsilon_i = +1) = \mathbb{P}(\varepsilon_i = -1) = \frac{1}{2}$. Since $\sum_{k=0}^n \binom{n}{k} (n-2k)^{2\ell} = 2^n \mathbb{E}[S_n^{2\ell}]$, Eq. (81) and Theorem 3 give

$$2B_A(n, n-r) - 1 = \sqrt{b} \inf_{\ell \geq 1} F_\ell^{1/(2\ell)},$$

$$2B_{LP}(n, n-r) - 1 = \sqrt{b},$$

where

$$F_\ell := \frac{2^{n-r-1} \mathbb{E}[S_n^{2\ell}]}{n^{2\ell} b^\ell}.$$

Thus the desired comparison is equivalent to showing $\inf_{\ell \geq 1} F_\ell^{1/(2\ell)} \geq 1$, with equality only at the endpoint. For the non-endpoint cases, we first establish $F_\ell > 1$ for each $\ell \geq 1$; the passage to a strict infimum is justified at the end of the proof.

For $(c, r) = (1, 2)$, we have $n = 3$ and $b = 1/3$, so

$$F_\ell = \frac{3^\ell + 3^{1-\ell}}{4} \geq 1,$$

with equality at $\ell = 1$. This proves the endpoint equality. Henceforth assume $(c, r) \neq (1, 2)$; then $r \geq 3$. Set

$$L := 3 \cdot 2^{r-3} = \frac{3(n+c)}{8}, \quad K := L - 1.$$

We use complementary estimates for $1 \leq \ell \leq K$ and $\ell \geq L$.

Moderate values of ℓ . For $1 \leq \ell \leq K$, retain from the expansion of $S_n^{2\ell}$ the terms in which ℓ distinct indices each occur twice. This gives

$$F_\ell \geq C_\ell := \frac{2^{n-r-1} (n)_\ell (2\ell-1)!!}{n^{2\ell} b^\ell}, \quad \frac{C_{\ell+1}}{C_\ell} = \frac{(n-\ell)(2\ell+1)}{n^2 b},$$

where $(n)_\ell = n(n-1) \dots (n-\ell+1)$. For $n \geq 14$, the function $t \mapsto (n-t)(2t+1)$ is increasing on $[0, 3n/8]$, and hence, for $1 \leq \ell < K$,

$$(n-\ell)(2\ell+1) < \frac{15n^2}{32} + \frac{5n}{8} < n^2 \frac{n-2}{n+2} \leq n^2 b.$$

The same conclusion follows directly from the ratio formula for $n \in \{6, 7\}$. Therefore $C_\ell \geq C_K$ for $1 \leq \ell \leq K$.

Let $\alpha := K/n < 3/8$. The elementary sum–integral comparisons

$$\sum_{j=0}^{K-1} \log \left(1 - \frac{j}{n} \right) \geq n \int_0^\alpha \log(1-t) dt, \quad \sum_{j=1}^K \log \left(\frac{2j-1}{n} \right) \geq \int_0^K \log \left(\frac{2t}{n} \right) dt$$

yield, using $2^r = n + c$ and $b < 1$,

$$\log C_K \geq nh(\alpha) - \log(2(n+c)),$$

where

$$h(\alpha) := \log 2 - (1-\alpha) \log(1-\alpha) + \alpha \log(2\alpha) - 2\alpha.$$

Since $h'(\alpha) = \log(2\alpha(1-\alpha)) < 0$ on $(0, 3/8]$ and $h(3/8) > 1/10$,

$$C_K > \frac{e^{n/10}}{2(n+c)} > 1 \quad (n \geq 62).$$

For the remaining admissible lengths $n \in \{6, 7, 14, 15, 30, 31\}$, direct evaluation gives $C_K \geq 10/9$. Consequently,

$$F_\ell > 1, \quad 1 \leq \ell \leq K.$$

Large values of ℓ . The two extreme nonzero levels satisfy

$$\mathbb{P}(|S_n| = n) = 2^{1-n}, \quad \mathbb{P}(|S_n| = n-2) = n2^{1-n}.$$

Retaining only these levels gives

$$F_\ell \geq E_\ell := \frac{x^\ell + ny^\ell}{n+c}, \quad x := \frac{1}{b}, \quad y := \frac{a}{b}, \quad a := \left(1 - \frac{2}{n}\right)^2.$$

A direct calculation gives

$$E_{\ell+1} \geq E_\ell \iff a^\ell \leq \frac{1-b}{n(b-a)} = \begin{cases} \frac{n}{2n-3}, & c=1, \\ \frac{n}{n-2}, & c=2. \end{cases}$$

For $c=1$,

$$a^L < e^{-4L/n} < e^{-3/2} < \frac{1}{2} < \frac{n}{2n-3},$$

whereas for $c=2$ the threshold $n/(n-2)$ is larger than one. Thus E_ℓ is nondecreasing for $\ell \geq L$.

It remains to verify $E_L > 1$. Write $x = 1+u$ and $y = 1-z$. The inequalities

$$\log(1+u) \geq \frac{2u}{2+u}, \quad (1-z)^L \geq 1-Lz$$

imply

$$(n+c)E_L \geq \exp\left(\frac{2Lu}{2+u}\right) + n(1-Lz).$$

If $c=1$, then

$$u = \frac{4}{n-1}, \quad z = \frac{4(2n-3)}{n^2(n-1)}, \quad \frac{2Lu}{2+u} = \frac{3}{2},$$

and

$$nLz = \frac{3}{2}g_n, \quad g_n := \frac{(2n-3)(n+1)}{n(n-1)} < \frac{21}{10}.$$

Since $e^{3/2} > 67/16 > 83/20 > 1 + \frac{3}{2}g_n$, we obtain $(n+1)E_L > n+1$. If $c=2$, then

$$u = \frac{4}{n-2}, \quad z = \frac{4}{n^2}, \quad q := \frac{2Lu}{2+u} = \frac{3(n+2)}{2n} > \frac{3}{2},$$

and $nLz = q$. Hence

$$(n+2)E_L \geq e^q + n - q > n+2,$$

where the last inequality follows from $e^q > 1 + q + q^2/2 > 2 + q$. Therefore,

$$F_\ell > 1, \quad \ell \geq L.$$

The two regimes show that $F_\ell^{1/(2\ell)} > 1$ for every $\ell \geq 1$. Moreover,

$$F_\ell^{1/(2\ell)} = \frac{2^{(n-r-1)/(2\ell)} \|S_n\|_{2\ell}}{\sqrt{b} n} \rightarrow \frac{1}{\sqrt{b}} > 1,$$

because $\|S_n\|_{2\ell} \rightarrow \|S_n\|_\infty = n$. The tail is therefore bounded away from one, while only finitely many smaller values of ℓ remain. Hence

$$\inf_{\ell \geq 1} F_\ell^{1/(2\ell)} > 1.$$

Combining this with the normalized identities at the beginning of the proof gives the strict inequality in all non-endpoint cases. $\square$

References

- [1] Alexander S. Holevo. “Bounds for the quantity of information transmitted by a quantum communication channel”. *Problems of Information Transmission* **9**, 177–183 (1973).
- [2] 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*. Pages 376–383. ACM (1999).
- [3] Marcin Pawłowski, Tomasz Paterek, Dagomir Kaszlikowski, Valerio Scarani, Andreas Winter, and Marek Żukowski. “Information causality as a physical principle”. *Nature* **461**, 1101–1104 (2009).
- [4] Hartmut Klauck. “On quantum and probabilistic communication: Las Vegas and one-way protocols”. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*. Pages 644–651. ACM (2000).
- [5] Scott Aaronson. “Limitations of quantum advice and one-way communication”. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*. Pages 320–332. IEEE (2004). [arXiv:quant-ph/0402095](#).
- [6] Masahito Hayashi, Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita. “Quantum network coding”. In *STACS 2007. Volume 4393 of Lecture Notes in Computer Science*, pages 610–621. Springer (2007).
- [7] Iordanis Kerenidis and Ronald de Wolf. “Exponential lower bound for 2-query locally decodable codes via a quantum argument”. *Journal of Computer and System Sciences* **69**, 395–420 (2004).
- [8] Stephanie Wehner and Ronald de Wolf. “Improved lower bounds for locally decodable codes and private information retrieval”. In *Automata, Languages and Programming. Volume 3580 of Lecture Notes in Computer Science*, pages 1424–1436. Springer (2005). [arXiv:quant-ph/0403140](#).
- [9] Nicolas Brunner, Miguel Navascués, and Tamás Vértesi. “Dimension witnesses and quantum state discrimination”. *Physical Review Letters* **110**, 150501 (2013).
- [10] Marcin Pawłowski and Nicolas Brunner. “Semi-device-independent security of one-way quantum key distribution”. *Physical Review A* **84**, 010302 (2011).
- [11] Hong-Wei Li, Zhen-Qiang Yin, Yu-Chun Wu, Xu-Bo Zou, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. “Semi-device-independent random-number expansion without entanglement”. *Physical Review A* **84**, 034301 (2011).
- [12] Hong-Wei Li, Marcin Pawłowski, Zhen-Qiang Yin, Guang-Can Guo, and Zheng-Fu Han. “Semi-device-independent randomness certification using $n \rightarrow 1$ quantum random access codes”. *Physical Review A* **85**, 052308 (2012).
- [13] Armin Tavakoli, Alley Hameedi, Breno Marques, and Mohamed Bourennane. “Quantum random access codes using single d -level systems”. *Physical Review Letters* **114**, 170502 (2015). [arXiv:1504.08105](#).
- [14] Máté Farkas and Jędrzej Kaniewski. “Self-testing mutually unbiased bases in the prepare-and-measure scenario”. *Physical Review A* **99**, 032316 (2019). [arXiv:1803.00363](#).

- [15] Ashwin Nayak. “Optimal lower bounds for quantum automata and random access codes”. In Proceedings of the 40th Annual Symposium on Foundations of Computer Science. Pages 369–376. IEEE (1999).
- [16] Andris Ambainis, Debbie Leung, Laura Mančinska, and Maris Ozols. “Quantum random access codes with shared randomness” (2008). [arXiv:0810.2937](#).
- [17] Takashi Imamichi and Rudy Raymond. “Constructions of quantum random access codes”. In Proceedings of the 18th Asian Quantum Information Science Conference. (2018). url: [ibm.com](#).
- [18] Laura Mančinska and Sigurd A. L. Storgaard. “The geometry of Bloch space in the context of quantum random access codes”. *Quantum Information Processing* **21**, 143 (2022). [arXiv:2106.00155](#).
- [19] Máté Farkas, Nikolai Miklin, and Armin Tavakoli. “Simple and general bounds on quantum random access codes”. *Quantum* **9**, 1643 (2025). [arXiv:2312.14142](#).
- [20] Han-Hsuan Lin and Ronald de Wolf. “Getting almost all the bits from a quantum random access code” (2025). [arXiv:2506.01903](#).
- [21] Takayuki Suzuki. “Analytical construction of $(n, n-1)$ quantum random access codes saturating the conjectured bound”. *Physical Review A* **114**, 012441 (2026). [arXiv:2601.19190](#).
- [22] Seiseki Akibue, Rudy Raymond, Suguru Tamaki, and Kosei Teramoto. “Measurement geometry for quantum random access codes: Beyond Nayak bound and toward optimality” (2026). [arXiv:2606.12700](#).
- [23] Ruho Kondo, Yuki Sato, Hiroshi Yano, Yota Maeda, Kosuke Ito, and Naoki Yamamoto. “Random access codes: Explicit constructions, optimality, and classical–quantum gaps” (2026). [arXiv:2604.21274](#).
- [24] Kangqiao Liu. “Classical codes violate the conjectured square-root bound for quantum random access codes” (2026). [arXiv:2607.15617](#).
- [25] Paul Hausladen and William K. Wootters. “A “pretty good” measurement for distinguishing quantum states”. *Journal of Modern Optics* **41**, 2385–2390 (1994).
- [26] Paul Hausladen, Richard Jozsa, Benjamin Schumacher, Michael Westmoreland, and William K. Wootters. “Classical information capacity of a quantum channel”. *Physical Review A* **54**, 1869–1876 (1996).
- [27] Fang-Wei Fu, Victor K. Wei, and Raymond W. Yeung. “On the minimum average distance of binary codes: Linear programming approach”. *Discrete Applied Mathematics* **111**, 263–281 (2001).
- [28] Benjamin Mounits. “Lower bounds on the minimum average distance of binary codes”. *Discrete Mathematics* **308**, 6241–6253 (2008). [arXiv:0706.3295](#).
- [29] Lei Yu and Vincent Y. F. Tan. “An improved linear programming bound on the average distance of a binary code” (2019). [arXiv:1910.09416](#).
- [30] Joseph M. Renes. “Better bounds on optimal measurement and entanglement recovery, with applications to uncertainty and monogamy relations”. *Physical Review A* **96**, 042328 (2017). [arXiv:1707.01114](#).
- [31] Philippe Delsarte. “An algebraic approach to the association schemes of coding theory”. Pages 1–97. Number 10 in Philips Research Reports Supplements. Philips Research Laboratories. (1973). url: <https://hdl.handle.net/2078.1/205698>.
- [32] F. Jessie MacWilliams and Neil J. A. Sloane. “The theory of error-correcting codes”. Volume 16 of North-Holland Mathematical Library. North-Holland. Amsterdam (1977).
- [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). [arXiv:1809.02414](#).