Classical codes violate the conjectured square-root bound for quantum random access codes

Kangqiao Liu[1,2,*]

[1]*School of Science, Xihua University, Chengdu 610039, China*

[2]*Key Laboratory of High Performance Scientific Computation, Xihua University, Chengdu 610039, China*

Abstract

We consider whether every quantum random access code (QRAC) with density-operator encodings and arbitrary decoding measurements obeys the conjectured bound $p \leq (1 + \sqrt{m/n})/2$, where n classical bits are encoded into m qubits and p is the worst-case success probability. We find that classical random access codes with private randomness, which form a subclass of this QRAC model, violate the bound. We embed these classical codes as QRACs with diagonal encoding states and commuting decoding measurements, and construct pure-state realizations with identical decoding statistics. The achievability theorem of Ambainis, Nayak, Ta-Shma, and Vazirani then yields violations for every fixed $p \in (1/2, 1)$ at sufficiently large input length. The counterexamples span the full open interval between the conjectured and Nayak bounds at each fixed compression rate. A finite-blocklength analysis further yields order-optimal logarithmic qubit scaling for a recovery bias scaling as $\sqrt{\log_2 n/n}$ with a sufficiently large prefactor. These results identify the classical coding rate as the source of the separation and motivate restricted bounds based on quantitative spectral properties of decoding measurements.

I. INTRODUCTION

Wiesner's quantum multiplexing protocol provides the earliest two-to-one instance of the selective-retrieval task underlying quantum random access codes (QRACs) [1]. Ambainis, Nayak, Ta-Shma, and Vazirani (ANTV) introduced the general QRAC model, in which a sender compresses a string into one quantum message from which a receiver can later retrieve any chosen coordinate [2, 3]. Entropic QRAC bounds have supplied space lower bounds for one-way quantum finite automata and, through a quantum reduction, exponential lower bounds for two-query locally decodable codes [4, 5]. Operationally, QRAC decoding probabilities form dimension-constrained prepare-and-measure correlations. This common structure allows observed statistics to certify a minimum Hilbert-space dimension [6, 7] and supports semi-device-independent quantum key distribution and randomness certification [8, 9]. With parity-obliviousness imposed, the same task turns quantum advantage into an operational witness of preparation contextuality [10]. Sharp QRAC success bounds therefore connect asymptotic information rates with finite-dimensional quantum correlations.

* kqliu@xhu.edu.cn

We study the binary worst-case formulation of this task. Let $[n] = \{1, \ldots, n\}$. Following Mančinska and Storgaard [11], an (n, m, p) QRAC encodes each $x \in \{0,1\}^n$ as a density operator ρ_x on a 2^m-dimensional Hilbert space. For every $i \in [n]$, a two-outcome positive operator-valued measure (POVM) $\{D_i^0, D_i^1\}$ is used to decode x_i, and the worst-case success condition is

$$\min_{x\in\{0,1\}^n} \min_{i\in[n]} \mathrm{Tr}\left(\rho_x D_i^{x_i}\right) \geq p, \tag{1}$$

where Tr denotes the trace. Throughout, we consider $1/2 < p < 1$ and $m < n$. This general model permits mixed encoding states and decoding POVMs with mutually commuting effects.

For the shared-randomness model of Ref. [12], Mančinska and Storgaard proved $p \leq 1/2 + \sqrt{2^{m-1}/n}/2$ and confirmed the two-qubit conjecture of Imamichi and Raymond [11, 13]. They asked whether the stronger expression

$$p \leq \frac{1}{2} + \frac{1}{2}\sqrt{\frac{m}{n}} \tag{2}$$

holds for arbitrary (n, m, p) QRACs. The conjectured bound is saturated by repeated concatenations of the optimal $(2, 1)$ and $(3, 1)$ QRACs, and it lies below Nayak's information-theoretic bound [4, 11]. Recent works use the conjectured bound as a reference for finite-size constructions [14, 15]. Kondo *et al.* explicitly record its general validity as open [16].

Prior work establishes the embedding of classical random access codes (RACs) into this general model. Liabøtrø describes classical RACs as QRACs whose encoding states are diagonal in a fixed basis [17]. Lin and de Wolf observe that the asymptotically optimal classical message length is achievable within this diagonal subclass [18]. Kondo *et al.* formulate stochastic classical RACs as diagonal QRACs [16].

This paper constructs counterexamples to Eq. (2) within the general QRAC model. The construction combines this diagonal sector with the ANTV achievability theorem [2, 3]. Let h_2 denote the binary entropy and write $s = 2p - 1$ for the recovery bias. At fixed p, ANTV give classical RACs with private randomness, deterministic decoders, and message length $(1 - h_2(p))n + O(\log_2 n)$ bits. The binary entropy obeys

$$1 - h_2(p) < s^2. \tag{3}$$

The strict gap implies that the embedded ANTV codes violate Eq. (2) for all sufficiently large n. At each fixed compression rate, these codes fill the open interval above Eq. (2) shown in Fig. 1; Nayak's bound $m \geq (1 - h_2(p))n$ [4] supplies its asymptotic upper endpoint.

The analysis establishes a finite-alphabet embedding and an exact classical characterization of QRACs with commuting decoding POVMs. The same decoding statistics admit realizations with diagonal encoding states and with pure encoding states. Strict violations persist in relative open neighborhoods and occur for projective decoding measurements whose effects are noncommuting across every pair of distinct decoding indices. The finite-blocklength analysis also yields counterexamples with logarithmic qubit count in a vanishing-bias regime. Thus the conjectured bound is incompatible with classical RACs with private randomness already included in the general QRAC model.

The remainder of the paper is organized as follows. Section II formulates the classical RAC embedding and characterizes QRAC statistics generated by commuting decoding POVMs. The ANTV rate is applied in Sec. III to obtain the fixed-bias, finite-blocklength, and logarithmic-qubit counterexample families. A compression-rate parametrization in Sec. IV determines the full asymptotic counterexample window. Robustness of the construction under perturbations of states and decoding measurements is established in Sec. V. Section VI illustrates the formal results in the (r, p) plane and through explicit finite-blocklength parameters. Their asymptotic interpretation and relation to current QRAC bounds are developed in Sec. VII. Complete proofs of all formal results and finite-blocklength details are collected in Appendix A.

II. EMBEDDING CLASSICAL RACS

The construction begins with a precise formulation of the classical sector contained in the QRAC model. A stochastic classical RAC with private randomness uses a finite message alphabet $\mathcal{C}$ and assigns a message distribution $P(c|x)$ to each input $x \in \{0,1\}^n$. Given a message c and a requested index $i \in [n]$, the decoder outputs $b \in \{0,1\}$ with probability $q_i(b|c)$, where $q_i(b|c) \geq 0$ and $\sum_{b\in\{0,1\}} q_i(b|c) = 1$. Its worst-case success condition is

$$\sum_{c\in\mathcal{C}} P(c|x)q_i(x_i|c) \geq p, \quad x \in \{0,1\}^n, \quad i \in [n]. \tag{4}$$

The conditional distributions $P(c|x)$ specify the stochastic encoder. A deterministic decoder is given by decoding functions $d_i : \mathcal{C} \to \{0,1\}$ through $q_i(b|c) = \mathbf{1}\{d_i(c) = b\}$, where $\mathbf{1}$ denotes the indicator function.

This setup leads to the embedding and commuting-POVM characterization below.

Proposition 1 (Classical RAC embedding)**.** *Any classical RAC with private randomness on n input bits, finite message alphabet $\mathcal{C}$, and worst-case success at least p yields two $M = \lceil \log_2 |\mathcal{C}| \rceil$-qubit QRAC realizations with the same decoding statistics. One has diagonal encoding states and the other has pure encoding states. Deterministic decoders yield projective decoding measurements. Both realizations violate Eq. (2) whenever*

$$\frac{M}{n} < s^2. \tag{5}$$

Proof sketch. Embedding $P(c|x)$ and $q_i(b|c)$ as diagonal entries of encoding states and POVM effects makes the Born rule reproduce the classical decoding probabilities, with deterministic decoders giving projective decoding measurements through $\{0, 1\}$-valued effect eigenvalues. Replacing $P(c|x)$ by amplitudes $\sqrt{P(c|x)}$ gives the pure-state realization, and Eq. (5) is equivalent to a strict violation of Eq. (2). □

Proposition 2 (Classical characterization of commuting decoding POVMs)**.** *Every (n, M, p) QRAC for which all effects of the decoding POVMs commute has the same decoding statistics as a classical RAC with private randomness and a message alphabet of size at most 2^M.*

Proof sketch. Simultaneous diagonalization turns the diagonal entries of each encoding state into $P(c|x)$ and the effect eigenvalues into $q_i(b|c)$. The resulting classical model reproduces every decoding probability. □

Together, Propositions 1 and 2 characterize the QRAC statistics generated by commuting decoding POVMs as those of classical RACs with private randomness and at most 2^M messages. Equation (5) therefore reduces the counterexample construction in this sector to a classical message-rate comparison.

III. COUNTEREXAMPLES FROM THE ANTV RATE

The ANTV achievability theorem supplies the classical message rate required by Eq. (5). Theorem 2.2 of Ref. [2] (see also Theorem 5.2 of Ref. [3]) gives classical RACs with private randomness on n input bits, deterministic decoders, worst-case success at least p, and message length $(1 - h_2(p))n + O(\log_2 n)$ bits. Let k_n denote this bit length. The ANTV construction obeys the finite-blocklength upper bound

$$k_n \leq \lceil (1 - h_2(p))n + 7 \log_2 n \rceil \tag{6}$$

for all sufficiently large n. Proposition 1 embeds the k_n-bit messages into k_n qubits and supplies diagonal-state and pure-state QRAC realizations with the same commuting projective decoding measurements. Combining the ANTV rate with this embedding yields the fixed-bias counterexample family stated next.

Theorem 1 (Fixed-bias counterexamples)**.** *For every fixed p there is an $n_0(p)$ such that, for every $n \geq n_0(p)$, there exists an (n, k_n, p) QRAC with $p > 1/2 + \sqrt{k_n/n}/2$, where $k_n < n$ satisfies Eq. (6).*

Proof sketch. For fixed p, Eq. (3) and $\log_2 n/n \to 0$ eventually give $k_n/n < s^2$. Proposition 1 then yields the counterexample. □

For explicit parameters, this construction yields the following criterion.

Proposition 3 (Finite-blocklength counterexamples)**.** *Let n satisfy $p \leq 1 - 1/n$, and define*

$$K_{p,n} := \lceil (1 - h_2(p))n + 7 \log_2 n \rceil . \tag{7}$$

If $K_{p,n} < ns^2$, there exists an $(n, K_{p,n}, p)$ QRAC that violates Eq. (2).

Proof sketch. The finite-blocklength ANTV construction produces a classical RAC with deterministic decoders whose message alphabet embeds into $K_{p,n}$ bits. Proposition 1 converts it into the claimed QRAC, and the strict rate condition ensures the violation. □

Applying Proposition 3 with a bias that vanishes with n yields the logarithmic-qubit refinement.

Corollary 1 (Logarithmic qubit count)**.** *Let $a = 1 - 1/(2 \ln 2)$, fix $C > 7/a = 25.120896\ldots$, and set the recovery-bias sequence $s_n = \sqrt{C \log_2 n/n}$ and $p_n = (1 + s_n)/2$. For all sufficiently large n, there exists an $(n, K_{p_n,n}, p_n)$ QRAC that violates Eq. (2) with $K_{p_n,n} = \Theta(\log_2 n)$, where Θ denotes asymptotic order.*

Proof sketch. The entropy expansion together with $C > 7/a$ eventually yields $K_{p_n,n} < ns_n^2$, so Proposition 3 applies. The expansion gives $(C/(2 \ln 2) + 7) \log_2 n + o(\log_2 n)$, while Nayak's bound supplies a lower bound of the same asymptotic order. □

The preceding results describe the construction through recovery bias and input length. Reparameterizing the asymptotic family by its compression rate organizes these counterexamples into a region in the (r, p) plane.

IV. RATE-WINDOW FORMULATION

For a fixed asymptotic compression rate $r \in (0,1)$, consider QRAC families satisfying $m/n \to r$. The conjectured bound defines

$$p_{\mathrm{sq}}(r) = \frac{1}{2} + \frac{1}{2}\sqrt{r}. \tag{8}$$

The asymptotic Nayak bound is

$$p_{\mathrm{N}}(r) = h_2^{-1}(1-r), \tag{9}$$

where the inverse is taken on $[1/2, 1]$. Equation (3) gives $p_{\mathrm{sq}}(r) < p_{\mathrm{N}}(r)$ throughout this rate range. The open interval between these curves is

$$p_{\mathrm{sq}}(r) < p < p_{\mathrm{N}}(r). \tag{10}$$

Parameterizing the same ANTV family by r and padding to $\lceil rn \rceil$ yields the following rate-window corollary.

Corollary 2 (Rate window)**.** *Fix $r \in (0,1)$ and p satisfying Eq. (10). Then, for all sufficiently large n, there is an (n, M_n, p) QRAC with*

$$M_n = \lceil rn \rceil \tag{11}$$

and with $p > 1/2 + \sqrt{M_n/n}/2$.

Proof sketch. The upper inequality in Eq. (10) places the ANTV message length below M_n asymptotically and permits padding to M_n bits. The lower inequality gives $M_n/n < s^2$ after rounding, so Proposition 1 yields the stated QRACs. □

The rate-window corollary identifies the full asymptotic counterexample region. The realization structure determines how these strict violations persist under perturbations.

V. STRUCTURAL ORIGIN AND ROBUSTNESS

For an M-qubit embedded realization, the diagonal density operators form a simplex whose 2^M vertices correspond to the computational-basis messages. Each classical message distribution maps to a point in this simplex. Taking square-root amplitudes gives a pure-state

representation with the same computational-basis statistics. For deterministic decoders, each decoding function defines a diagonal projective measurement, so the decoding statistics arise from a one-way classical protocol with messages of at most M bits. The separation from the conjectured bound follows from the achievable rate of classical RACs with private randomness.

Proposition 4 (Robustness)**.** *Let ρ_x, $x \in \{0,1\}^n$, be the encoding states of an (n, M, p) QRAC, and let D_i^b, $i \in [n]$ and $b \in \{0,1\}$, be its decoding POVM effects. Define its gap by $\delta := p - 1/2 - \sqrt{M/n}/2$ and assume $\delta > 0$. Every family of valid encoding states $\widetilde{\rho}_x$ and decoding POVM effects $\widetilde{D}_i^b$ on the same 2^M-dimensional Hilbert space satisfying*

$$\max_{x,i,b} \left[\frac{1}{2} \left\| \widetilde{\rho}_x - \rho_x \right\|_1 + \left\| \widetilde{D}_i^b - D_i^b \right\|_\infty \right] < \delta \tag{12}$$

also violates Eq. (2), where $\|\cdot\|_1$ and $\|\cdot\|_\infty$ denote the trace norm and operator norm. If all D_i^b are nontrivial projectors and $n \geq 2$, every operator-norm neighborhood of these decoding measurements contains projective decoding measurements satisfying $\|[\widetilde{D}_i^b, \widetilde{D}_j^{b'}]\|_\infty > 0$ for all $i \neq j$ and $b, b' \in \{0,1\}$. The projective decoding measurements obtained by embedding the ANTV codes satisfy this nontriviality condition.

Proof sketch. Trace-distance and operator-norm continuity preserve the strict success gap under Eq. (12). Worst-case success makes every ANTV decoding function attain both output values, and independent small unitary conjugations of nontrivial projectors avoid the finite union of real-analytic commutator zero sets. □

Each embedded pure-state ANTV realization therefore lies in a relative open subset of valid state-POVM tuples that violate Eq. (2), and every operator-norm neighborhood of its decoding measurements contains a projective tuple whose effects are noncommuting across every pair of distinct decoding indices.

The formal results admit direct illustrations in the (r, p) plane and at finite blocklength.

VI. EXAMPLES AND PARAMETER-SPACE ILLUSTRATION

Figure 1 displays the full open rate window of Corollary 2. Its markers correspond to the finite-blocklength guarantees from Proposition 3 listed in Table I.

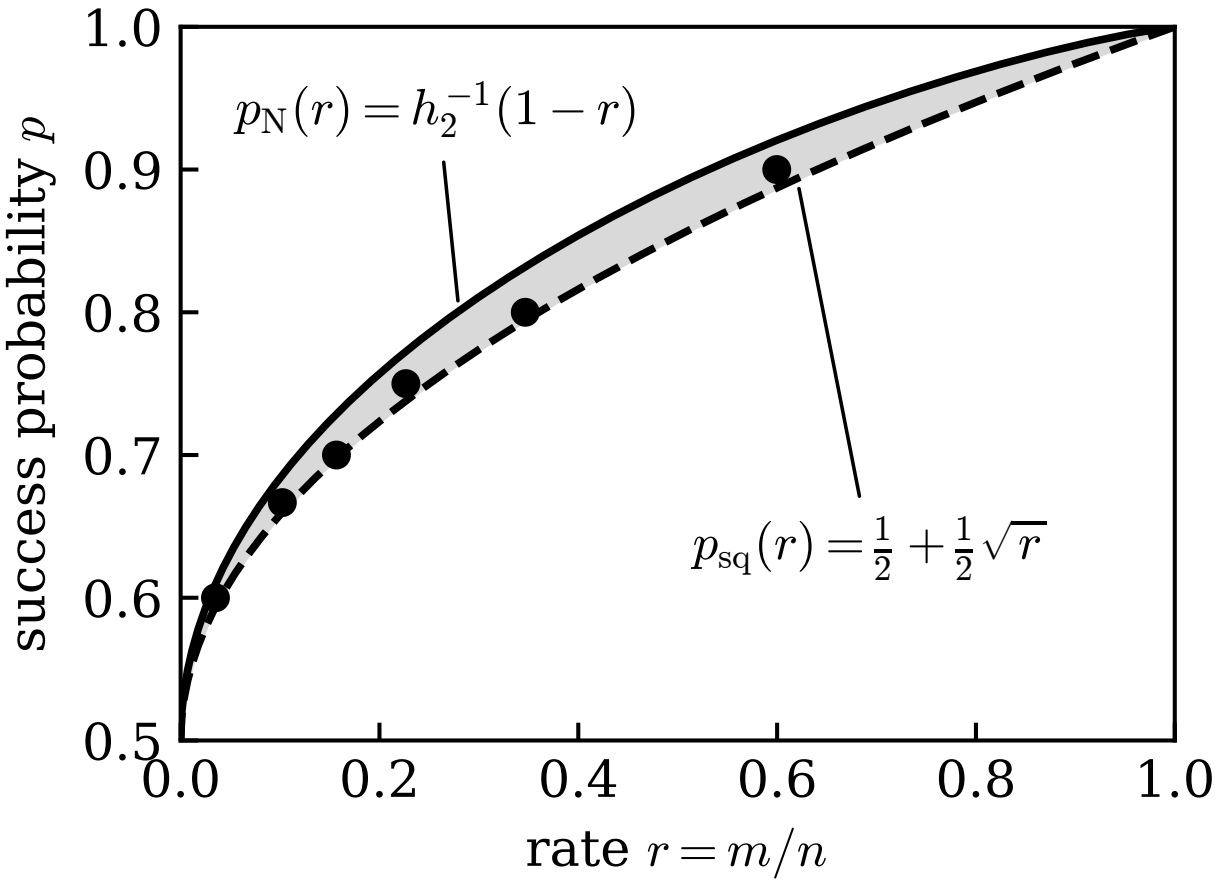

FIG. 1. Counterexamples fill the asymptotic interval between the conjectured and Nayak bounds. For every rate r and every p in the shaded open window, $(n, \lceil rn \rceil, p)$ QRACs exist for all sufficiently large n by Corollary 2. The dashed and solid curves show $p_{\mathrm{sq}}(r)$ and $p_{\mathrm{N}}(r)$, respectively. Markers show the parameter values of Table I.

A representative finite-blocklength example illustrates the guarantee of Proposition 3. For $p = 3/4$ and $n = 4096$, Eq. (7) gives

$$\begin{aligned} m = K_{3/4,4096} &= \lceil (1 - h_2(3/4))4096 + 7\log_2 4096 \rceil \\ &= 858. \end{aligned} \tag{13}$$

At this success probability, $s = 1/2$. The hypotheses of Proposition 3 hold because $3/4 \leq 1 - 1/4096$ and $858 < 4096s^2 = 1024$. The proposition therefore gives a $(4096, 858, 3/4)$ QRAC with

$$p_{\mathrm{sq}}(858/4096) = 0.7288409143\ldots < \frac{3}{4}. \tag{14}$$

Table I extends this calculation to six additional parameter choices.

TABLE I. Finite-blocklength QRAC existence guarantees from Proposition 3. Each row sets $m = K_{p,n}$ and lists the gap above $p_{\mathrm{sq}}(m/n)$.

p	n	m	$p - p_{\mathrm{sq}}(m/n)$
0.6000	16384	574	0.006413
2/3	4096	419	0.006749
0.7000	2048	321	0.002049
0.7500	2048	464	0.012007
0.8000	1024	355	0.005602
0.9000	1024	614	0.012828

VII. DISCUSSION AND CONCLUSION

The combined achievability and converse results determine the asymptotic meaning of the two curves in Fig. 1. At every fixed rate r, the ANTV construction approaches $p_{\mathrm{N}}(r)$ from below, and Nayak's bound supplies the matching converse. The entropy curve $p_{\mathrm{N}}(r)$ therefore gives the asymptotic supremum of the worst-case success probability in the unrestricted QRAC model. The square-root curve $p_{\mathrm{sq}}(r)$ is attained by several structured families and lies strictly inside the feasible region at every fixed rate. Thus the general density-operator model is governed asymptotically by the entropy rate of its embedded classical message sector.

The realizations identify structural features that preserve this separation. For the paired realizations of Proposition 1, the diagonal mixed states and pure states have identical decoding statistics and the same embedded classical message rate. Proposition 4 places projective decoding measurements with noncommuting effects across every pair of distinct decoding indices in every operator-norm neighborhood of the commuting realization. The success gap is stable under perturbations that change the measurement commutators. Measurement incompatibility is known to be necessary for quantum advantage over classical RAC strategies under an average-success comparison [19]. Relevant quantitative parameters include decoder spectra, measurement overlaps, and the minimum classical message-alphabet size required to reproduce the decoding statistics. This interpretation complements the spectral formulation of Akibue *et al.*, whose finite-size bounds and equality conditions are expressed through decoding-measurement geometry [15].

The high-rate constructions of Suzuki and Kondo *et al.* show that the square-root value is attained within specified families. Suzuki establishes average-case saturation for $(n, n-1)$ QRACs [14]. Tan and Jafar prove the conjectured average-success upper bound for the $(n, n-1)$ and $(n, n-2)$ cases [20]. Kondo *et al.* recover related high-rate QRACs and develop geometric characterizations of classical RACs under average- and worst-case criteria [16]. The rate-window corollary places these high-rate results in a broader parameter space, where classical RACs with private randomness reach every fixed-rate point below the entropy boundary. The finite-parameter classical-quantum gaps reported by Kondo *et al.* and the present asymptotic classical achievability together show that RAC-QRAC comparisons depend on the scaling regime and success criterion.

Success criterion also connects the present results to general QRAC bounds. Farkas, Miklin, and Tavakoli bound average success for arbitrary input alphabet and Hilbert-space dimension [21]. Every worst-case guarantee obtained here is also an average-case guarantee, so the embedded ANTV codes provide explicit feasible points for that broader optimization problem. Their framework constrains average-case performance at finite dimension. The present construction supplies asymptotically tight achievable worst-case rates in the binary setting.

The counterexample families have $m \to \infty$, with the logarithmic construction showing that growth of the embedded classical message space already produces a separation at $m = \Theta(\log_2 n)$. Existing fixed-m theorems and finite small-block constructions retain their stated parameter domains. Natural restricted formulations may combine fixed-m regimes with quantitative spectral regularity of the decoding measurements. Identifying quantitative conditions that contain the known square-root-saturating families and control the embedded classical rate remains a structural question. Within the standard density-operator model, the asymptotic worst-case boundary is $p_{\mathrm{N}}(r)$, and robust counterexamples occur throughout the open region above $p_{\mathrm{sq}}(r)$.

Appendix A: Detailed proofs

Proof of Proposition 1. The choice $M = \lceil \log_2 |\mathcal{C}| \rceil$ permits an injection of $\mathcal{C}$ into the computational basis. Let I denote the identity operator and define

$$\Pi_\perp = I - \sum_{c \in \mathcal{C}} |c\rangle\langle c|, \tag{A1}$$

where $\Pi_\perp$ projects onto the unused basis states. Define

$$\rho_x = \sum_{c \in \mathcal{C}} P(c|x)|c\rangle\langle c|, \tag{A2}$$

$$D_i^b = \sum_{c \in \mathcal{C}} q_i(b|c)|c\rangle\langle c| + \mathbf{1}\{b = 0\}\Pi_\perp, \quad b \in \{0, 1\}. \tag{A3}$$

Each ρ_x is positive semidefinite and has unit trace. The normalization of $q_i(b|c)$ gives

$$D_i^0 + D_i^1 = \sum_{c \in \mathcal{C}} |c\rangle\langle c| + \Pi_\perp = I. \tag{A4}$$

The coefficients of the basis projectors lie in $[0, 1]$, so $0 \leq D_i^b \leq I$. All POVM effects are diagonal and hence commute. Direct evaluation gives

$$\mathrm{Tr}(\rho_x D_i^{x_i}) = \sum_{c \in \mathcal{C}} P(c|x) q_i(x_i|c). \tag{A5}$$

For a deterministic decoder, every coefficient in Eq. (A3) lies in $\{0, 1\}$. The two effects are then complementary orthogonal projectors. Define

$$|\psi_x\rangle = \sum_{c \in \mathcal{C}} \sqrt{P(c|x)}|c\rangle \tag{A6}$$

The vectors are normalized, and diagonality gives

$$\langle\psi_x|D_i^{x_i}|\psi_x\rangle = \sum_{c \in \mathcal{C}} P(c|x) q_i(x_i|c). \tag{A7}$$

Thus the realizations with diagonal encoding states and pure encoding states have the same decoding statistics. Finally, Eq. (5) is equivalent to $1/2 + \sqrt{M/n}/2 < p$. □

Proof of Proposition 2. The commuting Hermitian effects admit a common orthonormal eigenbasis $\{|c\rangle\}_{c=1}^{2^M}$. In this basis, define

$$P(c|x) = \langle c|\rho_x|c\rangle, \qquad q_i(b|c) = \langle c|D_i^b|c\rangle. \tag{A8}$$

Positivity and normalization of the states make $P(\cdot|x)$ a probability distribution. The POVM relations make $q_i(\cdot|c)$ a probability distribution. Since each D_i^b is diagonal in the common basis,

$$\mathrm{Tr}(\rho_x D_i^b) = \sum_{c=1}^{2^M} P(c|x) q_i(b|c), \tag{A9}$$

which reproduces all decoding probabilities with a classical message alphabet of size 2^M. □

Derivation of Eq. (3). Since $s \in (0,1)$, the binary entropy deficit has the convergent expansion

$$1 - h_2\left(\frac{1+s}{2}\right) = \frac{1}{\ln 2} \sum_{j=1}^{\infty} \frac{s^{2j}}{(2j-1)(2j)}. \tag{A10}$$

The coefficient sum satisfies

$$\frac{1}{\ln 2} \sum_{j=1}^{\infty} \frac{1}{(2j-1)(2j)} = 1, \tag{A11}$$

because $[(2j-1)(2j)]^{-1} = (2j-1)^{-1} - (2j)^{-1}$ and the resulting series sums to $\ln 2$. In this range, every s^{2j} is at most s^2, and the inequality is strict for $j \geq 2$. Equations (A10) and (A11) therefore give

$$1 - h_2\left(\frac{1+s}{2}\right) < s^2. \tag{A12}$$

Since $p = (1+s)/2$, this yields Eq. (3). □

Proof of Theorem 1. For fixed p, define

$$\Delta_p := s^2 - [1 - h_2(p)] > 0, \tag{A13}$$

where positivity follows from Eq. (3). Since $(7\log_2 n + 1)/n \to 0$, it is smaller than Δ_p for all sufficiently large n. In this range, the ANTV classical RAC exists with the length in Eq. (6) and satisfies

$$\frac{k_n}{n} \leq 1 - h_2(p) + \frac{7\log_2 n + 1}{n} < s^2 < 1. \tag{A14}$$

Proposition 1 yields the claimed QRAC and the strict violation of Eq. (2). □

Proof of Proposition 3. For $p \leq 1 - 1/n$, the finite-blocklength ANTV construction uses a covering-code index of at most $(1-h_2(p))n + 4\log_2 n$ bits and an index for n^3 permutation-mask pairs of length $3\log_2 n$. The total message length is therefore at most $(1 - h_2(p))n + 7\log_2 n$ bits. The decoders are deterministic. A Chernoff bound of e^{-2n} applies to each pair (x, i), and the union bound over the $n2^n$ pairs gives total failure probability at most $n2^n e^{-2n} < 1$

for every positive integer n. Hence a fixed family of permutation-mask pairs attains the required worst-case success.

Consequently, the message alphabet obeys

$$\lceil \log_2 |\mathcal{C}| \rceil \leq K_{p,n}. \tag{A15}$$

Padding to $K_{p,n}$ bits preserves the decoding statistics. Under $K_{p,n} < ns^2$, Proposition 1 gives the claimed QRAC and the strict violation of Eq. (2). □

Proof of Corollary 1. Equation (A10) gives

$$\Delta_{p_n} := s_n^2 - [1 - h_2(p_n)] = aC\frac{\log_2 n}{n} + O\left(\frac{(\log_2 n)^2}{n^2}\right). \tag{A16}$$

Since $aC > 7$, $n\Delta_{p_n} - 7\log_2 n \to \infty$, which gives $K_{p_n,n} < ns_n^2$ for all sufficiently large n. In the same range, $p_n \leq 1 - 1/n$, so Proposition 3 gives the stated QRAC. The expansion

$$1 - h_2(p_n) = \frac{s_n^2}{2\ln 2} + O(s_n^4) \tag{A17}$$

yields

$$K_{p_n,n} = \left(\frac{C}{2\ln 2} + 7\right)\log_2 n + o(\log_2 n). \tag{A18}$$

For any QRAC with success p_n, Nayak's bound [4] gives

$$m \geq [1 - h_2(p_n)]n = \left(\frac{C}{2\ln 2} + o(1)\right)\log_2 n. \tag{A19}$$

The construction and lower bound establish order-optimal logarithmic qubit scaling at this bias. □

Proof of Corollary 2. The condition $p < h_2^{-1}(1 - r)$ is equivalent to $1 - h_2(p) < r$. The ANTV length k_n in Eq. (6) is therefore at most M_n for all sufficiently large n. Padding each classical message with $M_n - k_n$ fixed zero bits and applying Proposition 1 gives an (n, M_n, p) QRAC. The lower inequality in Eq. (10) gives $r < s^2$. Hence $M_n/n < s^2$ for all sufficiently large n, and the padded QRAC violates Eq. (2) at the exact qubit count M_n. □

Proof of Proposition 4. For $0 \leq \widetilde{D}_i^b \leq I$, the trace-distance and operator-norm bounds give

$$\begin{aligned}\mathrm{Tr}(\widetilde{\rho}_x \widetilde{D}_i^{x_i}) \geq\ & \mathrm{Tr}(\rho_x D_i^{x_i}) - \frac{1}{2}\|\widetilde{\rho}_x - \rho_x\|_1 \\ & - \|\widetilde{D}_i^{x_i} - D_i^{x_i}\|_\infty.\end{aligned} \tag{A20}$$

Equation (12) therefore preserves a success probability greater than $p - \delta = 1/2 + \sqrt{M/n}/2$.

For each $i \neq j$, define the real-analytic map

$$\mathcal{F}_{ij}(U_1, \ldots, U_n) = [U_i D_i^0 U_i^\dagger, U_j D_j^0 U_j^\dagger] \tag{A21}$$

on the product unitary group. For any two nontrivial projectors Γ and Λ, a unitary V can be chosen such that $[\Gamma, V\Lambda V^\dagger] \neq 0$. Thus each $\mathcal{F}_{ij}$ takes a nonzero value. The product unitary group is connected, and the zero set of each $\mathcal{F}_{ij}$ is a proper real-analytic subset with empty interior. These zero sets are closed, so their finite union also has empty interior. Every neighborhood of the identity tuple therefore contains a unitary tuple outside this union. Continuity of unitary conjugation places the resulting tuple of decoding measurements in any prescribed operator-norm neighborhood of the original tuple. Setting $\widetilde{D}_i^b = U_i D_i^b U_i^\dagger$ gives the stated commutator condition. Since $D_i^1 = I - D_i^0$, complementary binary effects change each commutator only by a sign.

For the embedded ANTV codes, fix $i \in [n]$ and $b \in \{0, 1\}$, and choose an input x with $x_i = b$. The positive worst-case success probability implies $P(c|x) > 0$ for some message c satisfying $d_i(c) = b$. Hence every decoding function d_i attains both output values on $\mathcal{C}$. Under the embedding of Proposition 1, both complementary projectors D_i^0 and D_i^1 consequently have ranks between 1 and $2^M - 1$. □

---

[1] S. Wiesner, Conjugate coding, SIGACT News **15**, 78–88 (1983).

[2] A. Ambainis, A. Nayak, A. Ta-Shma, and U. 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*, STOC '99 (Association for Computing Machinery, New York, NY, USA, 1999) p. 376–383.

[3] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, Dense quantum coding and quantum finite automata, J. ACM **49**, 496–511 (2002).

[4] A. Nayak, Optimal lower bounds for quantum automata and random access codes, in *Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, FOCS '99 (IEEE Computer Society, USA, 1999) p. 369.

[5] I. Kerenidis and R. de Wolf, Exponential lower bound for 2-query locally decodable codes via

a quantum argument, Journal of Computer and System Sciences **69**, 395 (2004), special Issue on STOC 2003.

[6] S. Wehner, M. Christandl, and A. C. Doherty, Lower bound on the dimension of a quantum system given measured data, Phys. Rev. A **78**, 062112 (2008).

[7] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Device-independent tests of classical and quantum dimensions, Phys. Rev. Lett. **105**, 230501 (2010).

[8] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302(R) (2011).

[9] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Semi-device-independent randomness certification using $n \to 1$ quantum random access codes, Phys. Rev. A **85**, 052308 (2012).

[10] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, Preparation contextuality powers parity-oblivious multiplexing, Phys. Rev. Lett. **102**, 010401 (2009).

[11] L. Mančinska and S. A. L. Storgaard, The geometry of bloch space in the context of quantum random access codes, Quantum Information Processing **21**, 143 (2022).

[12] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, Quantum random access codes with shared randomness (2009), arXiv:0810.2937 [quant-ph].

[13] T. Imamichi and R. Raymond, Constructions of quantum random access codes, in *Asian Quantum Information Symposium (AQIS)*, Vol. 66 (2018).

[14] T. Suzuki, Analytical construction of $(n, n-1)$-quantum random access codes saturating the conjectured bound, Phys. Rev. A **114**, 012441 (2026).

[15] S. Akibue, R. Raymond, S. Tamaki, and K. Teramoto, Measurement geometry for quantum random access codes: Beyond Nayak bound and toward optimality (2026), arXiv:2606.12700 [quant-ph].

[16] R. Kondo, Y. Sato, H. Yano, Y. Maeda, K. Ito, and N. Yamamoto, Random access codes: Explicit constructions, optimality, and classical-quantum gaps (2026), arXiv:2604.21274 [quant-ph].

[17] O. Liabøtrø, Improved classical and quantum random access codes, Phys. Rev. A **95**, 052315 (2017).

[18] H.-H. Lin and R. de Wolf, Getting almost all the bits from a quantum random access code (2025), arXiv:2506.01903 [quant-ph].

[19] Carmeli, Claudio, Heinosaari, Teiko, and Toigo, Alessandro, Quantum random access codes and incompatibility of measurements, EPL **130**, 50001 (2020).

[20] S. Tan and S. A. Jafar, Optimal average success probabilities of binary $(n, n-1)$ and $(n, n-2)$ quantum random access codes via a proof of the corresponding conjectured bound (2026), arXiv:2607.10414 [quant-ph].

[21] M. Farkas, N. Miklin, and A. Tavakoli, Simple and general bounds on quantum random access codes, Quantum **9**, 1643 (2025).