Optimal Bounds for Parity-Oblivious Random Access Codes with Applications

André Chailloux[1], Iordanis Kerenidis[2], Srijita Kundu[3], and Jamie Sikora[4]

1 **INRIA, Paris Rocquencourt, SECRET Project Team**
2 **Laboratoire d'Informatique Algorithmique: Fondements et Applications, Université Paris Diderot, Paris, France and Centre for Quantum Technologies, National University of Singapore, Singapore**
3 **Chennai Mathematical Institute, Chennai, India**
4 **Laboratoire d'Informatique Algorithmique: Fondements et Applications, Université Paris Diderot, Paris, France**

Abstract

Random Access Codes is an information task that has been extensively studied and found many applications in quantum information. In this scenario, Alice receives an n-bit string x, and wishes to encode x into a quantum state ρ_x, such that Bob, when receiving the state ρ_x, can choose any bit $i \in [n]$ and recover the input bit x_i with high probability. Here we study a variant called parity-oblivious random acres codes, where we impose the cryptographic property that Bob cannot infer any information about the parity of any subset of bits of the input, apart form the single bits x_i.

We provide the optimal quantum parity-oblivious random access codes and show that they are asymptotically better than the optimal classical ones. For this, we relate such encodings to a non-local game and provide tight bounds for the success probability of the non-local game via semi-definite programming. Our results provide a large non-contextuality inequality violation and resolve the main open question in [22].

1998 ACM Subject Classification E.4 Coding and Information Theory: Data compaction and compression

Keywords and phrases quantum information theory, contextuality, semidefinite programming

Digital Object Identifier 10.4230/LIPIcs.TQC.2014.76

1 Introduction

Quantum Information theory studies how information is encoded in quantum mechanical systems and how it can be transmitted through quantum channels. A main question is whether quantum information is more powerful than classical information. A celebrated result by Holevo [13], shows that quantum information cannot be used to compress classical information. In high level, in order to transmit n uniformly random classical bits, one needs to transmit no less than n quantum bits. This might imply that quantum information is no more powerful than classical information. This however is wrong in many situations. In the model of communication complexity, one can show that transmiting quantum information may result in exponential savings on the communication needed to solve specific problems ([20, 5, 3, 11, 21]).

One specific information task that has been extensively studied in quantum information is the notion of *random access codes* (RACs) [1, 16]. In this scenario, Alice receives an n-bit


9th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC'14).
Editors: Steven T. Flammia and Aram W. Harrow; pp. 76–87

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

string x, drawn from the uniform distribution, and wishes to encode x into a quantum state ρ_x, such that Bob, when receiving the state ρ_x, can choose any bit $i \in [n]$ and recover the input bit x_i with high probability by performing some general quantum operation on ρ_x.

RACs have been used in various situations in quantum information and computation, including in communication complexity, non-locality, extractors and divide-independence cryptography. [4, 14, 19, 10, 15]. Even though this task seems easier than transmitting the entire input string x, it is known that both in the classical and the quantum world, the length of the encoding must be at least $\Omega(n)$ and in fact, there is no gain between classical and quantum encodings [16].

On the other hand, a well-known example of the superiority of quantum information is the example of *dense coding*, or equivalently a RAC of length 1 for uniform inputs of length $n = 2$. In this case, the optimal classical encoding can achieve success probability $3/4$, while there exists a quantum encoding that achieves strictly higher success probability, in fact $\cos^2(\pi/8)$ [8, 23]. An advantage can also be proven for the case of encoding three bits into one qubit, but not for $n \geq 4$ [12].

Nevertheless, a question remained of whether there are variants of random access codes, for which we can have an asymptotically significant advantage in the quantum case. We show that this is indeed the case for the so-called *parity-oblivious* RACs. These are the usual RACs with the extra cryptographic property that the receiver cannot infer any information about the parity of any subset of bits of the input, apart from the single bits x_i.

Random acres codes that are parity-oblivious have been considered before. For example, the dense coding examples for encoding two or three classical bits in one qubit have this property. It is not hard to check, that for the 2-to-1 encoding, Bob's reduced density matrix is exactly the same for the cases where the inputs have parity 0 or 1, in other words, Bob has no information about $x_1 \oplus x_2$. Moreover, Spekkens, Buzacott, Keehn, Toner, and Pryde [22] used parity-oblivious RACs to provide non-contextuality inequalities.

1.1 Our results

In this paper, we provide the optimal quantum parity-oblivious RAC and show that it is asymptotically better than the optimal classical one. We say that an encoding with success probability $\frac{1}{2}(1+\alpha)$ has bias α. More precisely, we prove the following theorem.

▶ **Theorem 1.** *For any $n \in \mathbb{N}$, the optimal quantum parity-oblivious random access code for inputs of size n, denoted here as* PO-RAC^n*, has bias $\frac{1}{\sqrt{n}}$.*

The main idea of the proof is that quantum encodings can be studied through their relation to non-local games. Such equivalences between encodings and non-local games were previously noted in [17, 7]. A non-local game is a game between two non-communicating parties, who receive some inputs and must produce outputs that satisfy some known predicate. The best-known example is the CHSH game, where the two parties must output bits a and b, whose parity is equal to the logical and of their inputs x and y. The important quantity of such games is the optimal success probability when the two parties are allowed to share an arbitrary entangled state in the beginning of the protocol. In [7], it was shown that certain variants of the CHSH game are equivalent to some variants of quantum RACs and their respective success probabilities are equal.

In order to show an upper bound on the bias of quantum PO-RACs, we first define a weaker variant where only the parities of even-size subsets are hidden, denoted as EPO-RAC^n. An upper bound on the bias of these codes would imply an upper bound on the bias of the general PO-RACs.

Then, we study a natural non-local game which we call the INDEX game and show that EPO-RAC with *average* bias are equivalent to the INDEX game. In other words, the bias of any INDEX game strategy and the *average decoding bias* of an EPO-RAC are equal. In the INDEX^n game (parameterized by n here), Alice receives an n-bit string x, Bob receives an index t, and Alice and Bob are supposed to output bits a and b such that $a \oplus b = x_t$.

▶ **Theorem 2** (Equivalence). *For any $n \in \mathbb{N}$, there exists a quantum* EPO-RAC^n *with* average decoding bias α *if and only if there exists a quantum* INDEX^n *strategy with bias α.*

Last, noting that the INDEX game is an XOR game, i.e. the winning condition depends on the XOR of Alice and Bob's one-bit answers, we use a tight semidefinite programming characterization due to [9] and provide the exact optimal quantum bias.

▶ **Theorem 3** (Optimal INDEX game biases). *For any $n \in \mathbb{N}$, the optimal quantum bias of an* INDEX^n *strategy is $1/\sqrt{n}$ and the optimal classical bias is $\sqrt{\frac{2}{\pi n}}(1 + O(1/n))$.*

Since the *worst case bias* of a quantum PO-RAC is obviously upper bounded by the optimal *average case bias* of a quantum EPO-RAC, Theorems 2 and 3 show that every PO-RAC^n has bias at most $1/\sqrt{n}$. On the other hand, we give an explicit construction of a PO-RAC^n with bias $1/\sqrt{n}$ that uses $\lfloor n/2 \rfloor$ qubits. First, we provide a parity-oblivious encoding where Alice and Bob share $\lfloor n/2 \rfloor$ EPR pairs and then Alice sends one classical bit of communication.

▶ **Theorem 4** (Optimal PO-RAC^n). *For any integer n, there exists a* PO-RAC^n *with bias $1/\sqrt{n}$ that uses $\lfloor n/2 \rfloor$ qubits and 1 classical bit.*

We also remark that even though quantum PO-RAC^n and EPO-RAC^n both share the same optimal bias, the same is not true if we consider *odd-parity-oblivious* encodings where the S-parities are hidden for $|S|$ odd and strictly greater than 1. Consider encoding a six-bit string $(x_1, \ldots, x_6)$ where the first three bits are encoded using the optimal PO-RAC^3, and similarly for the last three bits. It is a straightforward exercise to verify this is odd-parity oblivious with bias $1/\sqrt{3} > 1/\sqrt{6}$.

1.2 Application to non-contextuality

The basic primitives in an operational theory are preparations and measurements. A hidden variable model is *preparation and measurement non-contextual*, if whenever two preparations yield the same statistics for all possible measurements then they have an equivalent representation in the model; and whenever two measurements have the same statistics for all preparations then they have an equivalent representation in the model [22]. Similar to non-locality, a non-contextuality inequality is any inequality on probability distributions that follows from the assumption that there exists a hidden variable model that is preparation or measurement non-contextual.

Spekkens, Buzacott, Keehn, Toner, and Pryde [22] proved the following *non-contextuality inequality* (or NC inequality, for short): In an operational theory that admits a preparation non-contextual hidden variable model, the *average case bias* for any PO-RAC^n is at most $1/n$.

Then, they noted that quantum mechanics violates this non-contextuality (NC) inequality for $n \in \{2, 3\}$, since there exists a quantum parity-oblivious encoding of two and three classical bits into one qubit, with average decoding probability $\frac{1}{2}(1 + \frac{1}{\sqrt{2}})$ and $\frac{1}{2}(1 + \frac{1}{\sqrt{3}})$, respectively [1, 12]. It was left as an open question whether quantum mechanics violates this

NC inequality for larger n. The main difficulty to extend these results for larger input size is that we pose no bound on the dimension of the encoding.

Through our Theorem 1 that provides the optimal bias for PO-RAC^{n}s, we resolve the main open question in [22] and provide a family of non-contextuality inequality violations that grow with the input size n. More precisely, we show an explicit non-contextuality violation of order $\sqrt{n}$.

▶ **Theorem 5.** *For any integer n, there exists an explicit non-contextuality inequality that provides a violation of order $\sqrt{n}$.*

2 Preliminaries

We provide the definitions of the different variants of random access codes that we use and of the non-local game we consider.

2.1 Random Access Codes

▶ **Definition 6** (Random access code)**.** For an integer $n \geq 2$, a quantum *random access code* of n bits, denoted RAC^n, with bias α consists of an encoding map of $x \in \{0,1\}^n$ into quantum states ρ_x together with a sequence of n possible measurements such that the result of the i'th measurement is x_i with probability at least $\frac{1}{2}(1+\alpha)$.

Note that the usual treatment of RACs is to analyze the relationships between n, α, and the encoding dimension (i.e., the dimension of ρ_x). In this paper, we are not concerned with the encoding dimension, but rather the optimal bias when we enforce certain cryptographic properties to RACs. For example, we enforce that Bob remains oblivious of some information about the string x, meaning that he cannot infer any information about it from the encoding. In particular, we consider for each subset S of bits of x the S-parity, which is defined as $\bigoplus_{i\in S} x_i$.

▶ **Definition 7** (Parity-oblivious random access codes)**.** For an integer $n \geq 2$, a quantum *parity-oblivious random access code*, denoted as PO-RAC^n, is a RAC^n with the cryptographic constraint that the receiver is oblivious of every S-parity, for $|S| \geq 2$.

For classical codes, the optimal bias of a PO-RAC^n is known to be $\frac{1}{n}$ (Proposition 1).

In our proofs, we also use a weaker variant of parity-oblivious random access codes, where only the S-parities of even-size remain oblivious.

▶ **Definition 8** (Even-parity-oblivious random access codes)**.** For an integer $n \geq 2$, a quantum *even-parity-oblivious random access code*, denoted as EPO-RAC^n, is a RAC^n with the cryptographic constraint that the receiver is oblivious of every S-parity, for $|S|$ even.

▶ Remark. In the definition of RAC^{n}s, we have that *every bit* is decode with bias α. We have occasion to study EPO-RAC^{n}s with *average case bias* α, that is, the average over all $i \in [n]$ of the decoding probabilities. When we consider average case biases, it is explicitly mentioned, otherwise, worst-case bias is assumed.

2.2 Non-local games

In a non-local game, two non-communicating parties, Alice and Bob, receive some inputs x and y, respectively, and must output a and b, respectively, such that (x, y, a, b) satisfy some specific condition. For example in the CHSH game, the condition is $a \oplus b = x \cdot y$. The goal is

to find the optimal quantum (classical) success probability of satisfying the condition when Alice and Bob are allowed to share some initial quantum state (shared randomness).

We define the following non-local game.

▶ **Definition 9** (Index game). The *Index game*, denoted here as INDEX^n, is the following XOR game:

- Alice's input: Alice receives a random s from the set $S := \{0,1\}^n$.
- Bob's input: Bob receives a random index t from the set $T := [n]$.
- Winning condition: They win if Alice's output bit a and Bob's output bit b satisfy $a \oplus b = s_t$.

The choice of initial resource state and local measurement operators (that depend on the respective inputs) comprise a *strategy*. We say that a strategy has *bias* α if it succeeds with probability $\frac{1}{2}(1+\alpha)$.

Note that our game is similar to the retrieval games studied in [17].

3 Equivalence of EPO-RAC^n decoding and INDEX^n strategies

In this section we prove the equivalence in Theorem 2.

▶ **Theorem 2** (Equivalence). *For any $n \in \mathbb{N}$, there exists a quantum* EPO-RAC^n *with bias α if and only if there exists a quantum* INDEX^n *strategy with bias α.*

3.1 From EPO-RAC^n to INDEX^n

Let us fix an EPO-RAC^n $\{\rho_x\}_{x\in\{0,1\}^n}$ with bias α. Let $\mathcal{B}$ the Hilbert space used for the encoding. Our goal is to construct a strategy for INDEX^n with bias α. For each ρ_x, we fix a purification $|\psi_x\rangle$ of ρ_x in the space $\mathcal{A}\otimes\mathcal{B}$. For $a \in \{0,1\}$, let $\boldsymbol{a}$ be the n-bit string $(a,\ldots,a)$ and $\bar{s}$ is the complement string of s. We define

$$|\Omega_s\rangle = \frac{1}{\sqrt{2}} \sum_{a\in\{0,1\}} |a\rangle_{\mathcal{O}} |\psi_{s\oplus \boldsymbol{a}}\rangle_{\mathcal{AB}} = \frac{1}{\sqrt{2}} \left(|0\rangle|\psi_s\rangle + |1\rangle|\psi_{\bar{s}}\rangle\right) .$$

We would like to show that if Bob has the register $\mathcal{B}$ of the above state, then he has no information about s. Note that his reduced state is the state $\sigma_s = \frac{1}{2}\rho_s + \frac{1}{2}\rho_{\bar{s}}$.

The first step is to see that Bob has no information about any parity (odd or even) of the string s. For the even parities, note that we started with an EPO-RAC^n encoding and that the strings s and $\bar{s}$ have the same even parities. Hence, Bob has with half probability the state ρ_s from which he cannot get any information about the even parities of s and with half probability the state $\rho_{\bar{s}}$ from which he cannot get any information about the even parities of $\bar{s}$ and consequently s.

For the odd parities: fix an subset $S \subseteq \{1,\ldots,n\}$ of odd size and let $s_S = \oplus_{i\in S} s_i$. Let $M = \{M_0, M_1\}$ be any two outcome POVM. Let $P_b = \{s \in \{0,1\}^n : s_S = b\}$. Each P_b has size 2^{n-1} and $s \in P_b \Leftrightarrow \bar{s} \in P_b$ since S is an odd subset. We have

$$\begin{aligned}\Pr[\text{Bob guesses } s_S \text{ using } M] &= \frac{1}{2^n}\sum_{s\in P_0} tr(M_0\sigma_s) + \sum_{s\in P_1} tr(M_1\sigma_s)\\ &= \frac{1}{2^n}\sum_{s\in P_0} tr(M_0\sigma_s) + \sum_{s\in P_0} tr(M_1\sigma_{\bar{s}})\\ &= \frac{1}{2^n}\sum_{s\in P_0} tr((M_0+M_1)\sigma_s) \qquad \text{using } \forall s, \sigma_s = \sigma_{\bar{s}}\\ &= \frac{1}{2^n}\sum_{s\in P_0} tr(I\sigma_s) = \frac{|P_0|}{2^n} = 1/2\,.\end{aligned}$$

This means that for any measurement M, Bob has probability $1/2$ to guess s_S which means that Bob has no information about this bit.

In the following lemma we prove that if someone has no information about any parity of subsets of bits of a string x, then he has no information about the string x. This is intuitively an obvious statement that we rigorously prove below.

▶ **Lemma 10.** *Let X be the uniform distribution on $x \in \{0,1\}^n$. If Bob has no information about any parity of subsets of bits of x, then he has no information about x.*

Proof. If Bob has some information about x, then the states ρ_x cannot be all the same, which in turn implies that there exists a subset $T \in \{0,1\}^n$ of size 2^{n-1} such that $\rho_T = \frac{1}{2^{n-1}}\sum_{x\in T}\rho_x$ is not equal to $\rho_{\bar{T}} = \frac{1}{2^{n-1}}\sum_{x\in\bar{T}}\rho_x$. This means that there exists a two-outcome measurement that outputs 1 if $x \in T$ and -1 otherwise, with positive bias. We now show for a contradiction that this measurements must also output a parity of some subset with positive bias. Define the function $f : \{0,1\}^n \to \{-1,+1\}$, as the indicator function of T and let b the measurement outcome. Then

$$\mathbb{E}[b\cdot f(x)] > 0\,.$$

By taking the Fourier representation of the function and denoting $x_S = \bigoplus_{i\in S} x_i$ we have

$$\begin{aligned}&\mathbb{E}[b\cdot\sum_S \hat{f}(S)x_S] > 0\,,\\ &\sum_S \hat{f}(S)\mathbb{E}[b\cdot x_S] > 0\,.\end{aligned}$$

Since for the empty set we have $\hat{f}(\emptyset) = \mathbb{E}[f(x)] = 0$, the above implies that there exists a parity S for which $E[b\cdot x_S] > 0$, which is a contradiction. ◀

The above statement means that for each s, we have $Tr_{\mathcal{OA}}|\Omega_s\rangle\langle\Omega_s| = Tr_{\mathcal{OA}}|\Omega_0\rangle\langle\Omega_0|$. In particular, this means that there exist unitaries $\{U_s\}$ acting on $\mathcal{AO}$ such that $(U_s\otimes I)|\Omega_0\rangle = |\Omega_s\rangle$.We use the state $|\psi_0\rangle$ to define the INDEX^n strategy:

- Alice and Bob share the state $|\Omega_0\rangle \in \mathcal{A}\otimes\mathcal{B}$.
- Upon receiving $s \in \{0,1\}^n$, Alice applies U_s on $\mathcal{OA}$ such that Alice and Bob share $|\Omega_s\rangle$. Alice measures register $\mathcal{O}$ in the computational basis and outputs the corresponding a.
- For Alice's input s and output a, Bob has an encoding ρ_x where $x = s\oplus \boldsymbol{a}$. Upon receiving $t \in [n]$, Bob measures $\mathcal{B}$ just as in the EPO-RAC^n to learn x_t. He outputs b equal to his guess.

- Alice and Bob win the game if $b = s_t \oplus a = x_t$ meaning that they win the game if and only if Bob correctly guesses x_t.

Since our encoding has bias α, we see that with this INDEX^n strategy, they succeed with probability

$$\frac{1}{n}\sum_{i=1}^{n}\Pr[\text{Bob outputs } a \oplus s_t] = \frac{1}{n}\sum_{i=1}^{n}\Pr[\text{Bob outputs } x_t] = \frac{1}{2}(1+\alpha),$$

as desired. ◀

3.2 From INDEX^n to EPO-RAC^n

Suppose Alice and Bob have a strategy to win the INDEX^n game with bias α with starting state $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$. On input $s \in \{0,1\}^n$, Alice performs her side of the optimal strategy for INDEX^n and has some output a. We have:

$$\frac{1}{n}\sum_{i=1}^{n}\Pr[\text{Bob outputs } a \oplus s_t] = \frac{1}{2}(1+\alpha)\,.$$

Let $\rho_{s,a}$ the state that Bob has when Alice inputs s and outputs a. Let x such that $\forall i, x_i = s_i \oplus a$. When Alice has inputs satisfying $s \oplus \boldsymbol{a} = x$, Bob has the state $\sigma_x = \frac{1}{2}(\rho_{x,0} + \rho_{\bar{x},1})$. We show that $\{\sigma_x\}_x$ is an EPO-RAC^n with average bias α.

1. It's a EPO-RAC^n: for every even parity S, we have $\bigoplus_{i\in S} x_i = \bigoplus_{i\in S}(s_i \oplus a) = \bigoplus_{i\in S} s_i$. Bob has no information about s from non signalling so Bob has no information about $\bigoplus_{i\in S} s_i$.
2. It has average bias α: Alice and Bob win the INDEX^n game with bias α hence

$$\frac{1}{n}\sum_{i=1}^{n}\Pr[\text{Bob outputs } x_t] = \frac{1}{n}\sum_{i=1}^{n}\Pr[\text{Bob outputs } a \oplus s_t] = \frac{1}{2}(1+\alpha)\,.$$

▶ Remark. Note that the above equivalence also holds in the classical setting.

4 On the structure of optimal Index Game strategies

In this section, we prove Theorem 3, below.

▶ **Theorem 11** (Optimal Index Game biases). *For any $n \in \mathbb{N}$, the optimal quantum bias of an* INDEX^n *strategy is $1/\sqrt{n}$ and the optimal classical bias is $\sqrt{\frac{2}{\pi n}}(1 + O(1/n))$.*

4.1 The quantum value

The quantum bias of any XOR game can be found efficiently by solving a semidefinite program (SDP) [9]. Specifically, the quantum bias of the INDEX^n game can be calculated as the optimal value of either SDP below

Primal problem (P)		Dual problem (D)	
supremum:	$\langle B, X\rangle$	infimum:	$\langle e, y\rangle$
subject to:	$\mathrm{diag}(X) = e$,	subject to:	$\mathrm{Diag}(y) \succeq B$,
	$X \succeq 0$,		

where

- $\mathrm{diag}(X)$ is the vector on the diagonal of the square matrix X,
- e is the vector of all ones,
- $\mathrm{Diag}(y)$ is the diagonal matrix with the vector y on the diagonal,
- $B := \frac{1}{2}\begin{bmatrix} 0 & A \\ A^T & 0 \end{bmatrix}$, where $A_{s,t} := \frac{(-1)^{s_t}}{n2^n}$.

For (P), consider the positive semidefinite matrix $X := YY^\top$, where

$$Y := \begin{bmatrix} \sqrt{n}\,2^n A \\ I_T \end{bmatrix}.$$

To show X is feasible in (P), one can check that each diagonal entry of X is equal to 1 from the definition of A above. Note that $\langle B, X\rangle := \sqrt{n}\,2^n\langle A, A\rangle = 1/\sqrt{n}$ proving that the quantum bias is at least $1/\sqrt{n}$ (since the quantum bias is the maximum of $\langle B, X\rangle$ over all feasible X).

For (D), let $y := \begin{bmatrix} u\,e_S \\ v\,e_T \end{bmatrix}$ where $u, v > 0$ and e_S and e_T are the vectors of all ones indexed by entries in S and T, respectively. Then

$$\mathrm{Diag}(y) \succeq B \iff \begin{bmatrix} uI_S & -\frac{1}{2}A \\ -\frac{1}{2}A^T & vI_T \end{bmatrix} \succeq 0 \iff uvI_T \succeq \frac{1}{4}A^\top A = \frac{1}{4n^2 2^n} I_T.$$

From above, if we set $v := \frac{1}{2n\sqrt{n}}$ and $u := \frac{1}{2\sqrt{n}2^n}$, then y is feasible in (D). Since $\langle e, y\rangle = 2^n u + nv = \frac{1}{\sqrt{n}}$, we know the quantum bias is at most $1/\sqrt{n}$ (since the quantum bias is equal to the minimum of $\langle e, y\rangle$ over all feasible y).

Therefore, the quantum bias is exactly $1/\sqrt{n}$, as required.

4.2 The classical value

We can assume without loss of generality that Alice and Bob's strategies are deterministic. Define $b \in \{0,1\}^n$ as the string of potential answers Bob gives where b_t is the bit that Bob outputs on input $t \in [n]$. Now let us examine Alice's strategy. For a fixed input s, if she outputs 0, they win the game with probability $\frac{1}{n}|b \oplus s|_H$, where $|x|_H$ denotes the Hamming weight of a string $x \in \{0,1\}^n$. If she outputs 1, they win the game with probability $\frac{1}{n}|b \oplus \overline{s}|_H = n - \frac{1}{n}|b \oplus s|_H$. This means that they win the game with probability at most

$$\begin{aligned} \mathop{\mathbb{E}}_{s\in\{0,1\}^n}\left[\frac{1}{n}\max\{|b\oplus s|_H, n - \frac{1}{n}|b\oplus s|_H\}\right] &= \frac{1}{n}\mathop{\mathbb{E}}_{s}\left[\frac{n}{2} + \left|\frac{n}{2} - |b\oplus s|_H\right|\right] \\ &= \frac{1}{2} + \frac{1}{n}\mathop{\mathbb{E}}_{s}\left[\left|\frac{n}{2} - |b\oplus s|_H\right|\right]. \end{aligned}$$

The quantity $\mathbb{E}_s[|n/2 - |b \oplus s|_H|]$ corresponds to the expected deviation that the uniform binomial distribution has from the average. This is a well studied quantity and we know that

$$\mathop{\mathbb{E}}_{s}\left[\left|\frac{n}{2} - |b\oplus s|_H\right|\right] = \frac{2}{\sqrt{\pi}}\frac{\Gamma(n+1/2)}{\Gamma(n)} = \sqrt{\frac{2n}{\pi}}\left(1 + O\left(\frac{1}{n}\right)\right).$$

Therefore, any strategy has success probability bounded above by

$$\frac{1}{2} + \frac{1}{n}\mathop{\mathbb{E}}_{s}\left[\left|\frac{n}{2} - |b\oplus s|_H\right|\right] = \frac{1}{2} + \sqrt{\frac{2}{\pi n}}\left(1 + O\left(\frac{1}{n}\right)\right).$$

Now, consider the following strategy: Alice outputs a which equals the majority of s, and Bob outputs 0. This strategy has success probability precisely

$$\frac{1}{2} + \frac{1}{n}\mathop{\mathbb{E}}_{s}\left[\left|\frac{n}{2} - |b \oplus s|_H\right|\right]$$

which is optimal.

5 A construction of a quantum PO-RAC^n with optimal bias

In this section we give an explicit construction of an quantum PO-RAC^n with optimal bias.

▶ **Theorem 12** (Optimal PO-RAC^n)**.** *For any integer $n \geq 2$, there exists a* PO-RAC^n *with bias $1/\sqrt{n}$ that uses $\lfloor n/2 \rfloor$ qubits and 1 classical bit.*

Our construction builds upon the well-known RACs for sending 2 (resp. 3) bits with bias $1/\sqrt{2}$ (resp. $1/\sqrt{3}$) [24, 2, 12]. These are the vertices from the corners of a square inscribed in an equatorial plane in the Bloch sphere, and the corners of a cube inscribed in the Bloch sphere, respectively. To generalize this idea to an n-cube inscribed in an n-dimensional sphere, we use the intuition of *hyperbits* which is a way to visualize such unit vectors in a quantum mechanical setting. A full discussion of hyperbits and their equivalence to certain quantum protocols is beyond the scope of this paper, but we refer the interested reader to the work of Pawlowski and Winter [18].

5.1 The construction

Our construction is very similar to the proof of Tsirelson's theorem [23]. We start by recursively defining the observables $G_{n,1}, \ldots, G_{n,n}$ which are used to define the actions of Alice and Bob in the PO-RAC^n.

For $n = 2$ and $n = 3$, we define

$$G_{2,1} := X, \quad G_{2,2} := Y \qquad \text{and} \qquad G_{3,1} := X, \quad G_{3,1} := Y, \quad G_{3,3} := Z.$$

We use the $n = 3$ observables as a base case for a recursive formula: for n even, we define

$$G_{n,i} := G_{n-1,i} \otimes X, \quad \text{for} \quad i \in \{1, \ldots, n-1\}, \qquad \text{and} \qquad G_{n,n} = \mathbb{I} \otimes Y$$

and for n odd, we define

$$G_{n,i} := G_{n-2,i} \otimes X, \quad \text{for} \quad i \in \{1, \ldots, n-2\}, \quad G_{n,n-1} = \mathbb{I} \otimes Y, \quad \text{and} \quad G_{n,n} = \mathbb{I} \otimes Z.$$

Note that these act on $\lfloor n/2 \rfloor$ qubits, have eigenvalues ± 1, and satisfy the anti-commutation relation

$$\{G_{n,i}, G_{n,j}\} = 2\delta_{i,j}\mathbb{I}.$$

Define the following operators for $x \in \{0,1\}^n$ and $t \in [n]$:

$$A_x := \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} G_i \qquad \text{and} \qquad B_t := G_t^{\top}.$$

Note that $A_x^2 = \mathbb{I}$, for all $x \, in \{0,1\}^n$, and $B_t^2 = \mathbb{I}$, for all $t \in [n]$, so each have ± 1 eigenvalues.

The PO-RAC^n protocol is defined below.

- Encoding states: Alice chooses a uniformly random $x \in \{0,1\}^n$, creates $\lfloor n/2 \rfloor$ EPR pairs, and measures the first "halves" with the observable A_x to get an outcome $a \in \{-1,+1\}$. She sends the second "halves" and a to Bob. Bob now has a quantum state encoding the string x.
- Decoding procedure: If Bob wishes to learn x_t, he measures his EPR halves with the observable B_t to get an outcome $b \in \{-1,+1\}$. He computes $c = ab$ and outputs 0 if $c = +1$, and 1 otherwise.

In the next two lemmas, we show that the bias of this RAC^n is $\frac{1}{\sqrt{n}}$ and that it is parity-oblivious, thereby proving Theorem 4.

▶ **Lemma 13.** *This* RAC^n *has bias* $1/\sqrt{n}$.

Proof. We can assume at the beginning of the protocol, Alice and Bob share the maximally entangled state

$$|\psi\rangle := \frac{1}{\sqrt{2^{\lfloor \frac{n}{2} \rfloor}}} \sum_{j=1}^{2^{\lfloor \frac{n}{2} \rfloor}} |j\rangle_{\mathcal{A}} |j\rangle_{\mathcal{B}}.$$

The expectation value of the observable $C = A_x \otimes B_t$ in this state is given by:

$$\langle C \rangle = \langle \psi | A_x \otimes B_t | \psi \rangle = \frac{1}{\sqrt{n}} \frac{1}{2^{\lfloor \frac{n}{2} \rfloor}} \sum_{i=1}^{n} (-1)^{x_i} \underbrace{\sum_{j,k=1}^{2^{\lfloor \frac{n}{2} \rfloor}} \langle j|_{\mathcal{A}} \langle j|_{\mathcal{B}} G_i \otimes G_t^{\top} |k\rangle_{\mathcal{A}} |k\rangle_{\mathcal{B}}}_{=2^{\lfloor \frac{n}{2} \rfloor} \delta_{i,t}} = \frac{(-1)^{x_t}}{\sqrt{n}}.$$

where the third equality is derived from the anti-commutation relation.
Now, $\langle C \rangle = \Pr[c = +1] - \Pr[c = -1] = \langle \psi | A_x \otimes B_t | \psi \rangle$, so

$$\Pr[\text{Bob outputs } 0] = \Pr[c = +1] = \frac{1}{2}\left[1 + \frac{(-1)^{x_t}}{\sqrt{n}}\right]$$

$$\Pr[\text{Bob outputs } 1] = \Pr[c = -1] = \frac{1}{2}\left[1 - \frac{(-1)^{x_t}}{\sqrt{n}}\right]$$

implying

$$\Pr[\text{Bob outputs } x_t] = \frac{1}{2}\left(1 + \frac{1}{\sqrt{n}}\right),$$

as desired. ◀

▶ **Lemma 14.** *This* RAC^n *is parity-oblivious.*

Proof. Protocols involving shared entanglement and sending one bit of classical information have limited guessing probabilities for functions such as parity, as shown in [18]. In particular, it can be been shown that the biases of learning $\bigoplus_{i \in S} x_i$, denoted here as α_S, satisfy

$$\sum_{S \subseteq \{0,1\}^n \setminus \text{Empty Set}} \alpha_S^2 \leq 1.$$

For our protocol,

$$\sum_{S:|S|=1} \alpha_S^2 = n \cdot \left(\frac{1}{\sqrt{n}}\right)^2 = 1$$

implying $\alpha_S = 0$ for all S of size 2 or greater, implying it is parity-oblivious. ◀

6 Large non-contextuality inequality violations

Spekkens et al. [22] constructed a family of non-contextuality inequalities from the notion of parity-oblivious random access codes. More precisely, they showed that

▶ Proposition 1 ([22], NC inequality). In any operational theory that admits a preparation non-contextual hidden variable model, the *average case bias* for any PO-RAC^n is at most $1/n$.

In order to quantify the violation of this NC inequality, we consider the ratio of the average case bias of quantum PO-RAC^n and PO-RAC^n of any operational theory that admits a preparation non-contextual hidden variable model.

Note, that if three exists a game for which the winning probability of any classical strategy cannot deviate from $1/2$ by more than δ_1 and, moreover, there is a quantum strategy obtaining winning probability at least $1/2 + \delta_2$, then we can obtain a violation of order δ_2/δ_1 (see [6] for details).

Then, Theorem 5 is a direct consequence of Proposition 1 and our Theorem 1.

▶ **Theorem 15.** *For any $n \in \mathbb{N}$, there exists an explicit non-contextuality inequality that provides a violation of order $\sqrt{n}$.*

References

1 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 31st Annual ACM Symposium on Theory of Computing*, pages 376 – 383, 1999.

2 A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and quantum finite automata. *Journal of the ACM*, 49(4):496–511, 2002.

3 Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of 36th ACM STOC*, pages 128–137, 2004.

4 Avraham Ben-Aroya, Oded Regev, and Ronald de Wolf. A hypercontractive inequality for matrix-valued functions with applications to quantum computing and ldcs. In *FOCS'08*, pages 477–486, 2008.

5 H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87:167902, Sep 2001.

6 Harry Buhrman, Oded Regev, Giannicola Scarpa, and Ronald de Wolf. Near-optimal and explicit bell inequality violations. *Theory of Computing*, 8(27):623–645, 2012.

7 A. Chailloux, I. Kerenidis, and J. Sikora. Strong connections between quantum encodings, non-locality and quantum cryptography. *PRA, to appear.*, 2014.

8 J. Clauser, M. Horne, A. Shimony, and R. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

9 R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay. Perfect parallel repetition theroem for quantum XOR proof systems. *Computational Complexity*, 17(2):282–299, 2008.

10 Anindya De and Thomas Vidick. Near-optimal extractors against quantum storage. In *STOC'10*, pages 161–170, 2010.

11 D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM J. Comput.*, 38(5):1695–1708, 2008.

12 M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. 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(8):129, 2006.

13 A. Holevo. Some estimates of the information transmitted by quantum communication channels. *Problemy Peredachi Informatsii*, 9:3–11, 1973.

14 Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita. Unbounded-error one-way classical and quantum communication complexity. In *ICALP'07*, pages 110–121, 2007.

15 Hong-Wei Li, Marcin Pawłowski, Zhen-Qiang Yin, Guang-Can Guo, and Zheng-Fu Han. Semi-device-independent randomness certification using $n \to 1$ quantum random access codes. *Phys. Rev. A*, 85:052308, May 2012.

16 A. Nayak. Optimal lower bounds for quantum automata and random access codes. *Proceedings of 40th IEEE Symposium on Foundations of Computer Science*, 0:369–376, 1999.

17 J. Oppenheim and S. Wehner. The uncertainty principle determines the non-locality of quantum mechanics. *Science*, 330:6007:1072–1074, 2010.

18 M. Pawlowski and A. Winter. From qubits to hyperbits. *Phys. Rev. A*, 85:022331, 2012.

19 Marcin Pawłowski and Marek Żukowski. Entanglement-assisted random access codes. *Phys. Rev. A*, 81:042326, Apr 2010.

20 Ran Raz. Exponential separation of quantum and classical communication complexity. In *Proc. 31st Annual ACM Symposium on Theory of Computing*, pages 358–367, New York, NY, USA, 1999. ACM.

21 O. Regev and B. Klartag. Quantum one-way communication can be exponentially stronger than classical communication. In *STOC'11*, pages 31–40, 2011.

22 R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde. Preparation contextuality powers parity-oblivious multiplexing. *Physical Review Letters*, 102:010401, 2009.

23 B. Tsirelson. Quantum analogues of the bell inequalities: The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36:557–570, 1987.

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