



Optimal bounds for parity-oblivious random access codes

André Chailloux, Iordanis Kerenidis, Srijita Kundu, Jamie Sikora

► To cite this version:

André Chailloux, Iordanis Kerenidis, Srijita Kundu, Jamie Sikora. Optimal bounds for parity-oblivious random access codes. TQC 2014, May 2014, Singapour, Singapore. 2014. <hal-01094121>

HAL Id: hal-01094121

<https://hal.inria.fr/hal-01094121>

Submitted on 22 Dec 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Optimal bounds for parity-oblivious random access codes

André Chailloux* Iordanis Kerenidis† Srijita Kundu‡ Jamie Sikora§

April 29, 2014

Abstract

Random access coding 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 access 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 from 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 semidefinite programming. We also extend the well-known quantum random access codes for encoding 2 or 3 classical bits into a single qubit. Our results provide a large non-contextuality inequality violation and resolve the main open problem in a work of Spekkens, Buzacott, Keehn, Toner, and Pryde (2009).

*INRIA, Paris Rocquencourt, SECRET Project Team. Email: andre.chailloux@inria.fr.

†Laboratoire d'Informatique Algorithmique: Fondements et Applications, Université Paris Diderot, Paris, France and Centre for Quantum Technologies, National University of Singapore, Singapore. Email: jkeren@liafa.univ-paris-diderot.fr.

‡Chennai Mathematical Institute, Chennai, India. Email: srijita@cmi.ac.in.

§Laboratoire d'Informatique Algorithmique: Fondements et Applications, Université Paris Diderot, Paris, France. Email: jamie.sikora@liafa.univ-paris-diderot.fr.

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 [Hol73], 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 transmitting quantum information may result in exponential savings on the communication needed to solve specific problems ([Raz99, BCWdW01, BJK04, GKK⁺08, RK11]).

One specific information task that has been extensively studied in quantum information is the notion of *random access codes* (RACs) [Nay99, ANTV99, ANTV02]. In this scenario, Alice receives an n -bit 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 device-independent cryptography [BARdW08, INRY07, PZ10, DV10, LPY⁺12]. Even though this task seems easier than transmitting the entire input string x , it is known that the length of quantum encodings must be at least $\Omega(n)$ [Nay99]. In fact, the length of classical encodings can be within a logarithmic additive factor of the quantum encodings [ANTV99].

On the other hand, a well-known example shows the advantages of quantum RACs by using a single qubit to encode two uniformly random classical bits. In this case, the success of correctly decoding either bit is $\cos^2(\pi/8)$ [BBBW83, ANTV99] while the optimal classical encoding can achieve an average success probability of $3/4$. An advantage can also be proven for the case of encoding three classical bits into one qubit as shown by Chuang (see [ANTV02] for details), but not for $n \geq 4$ [HIN⁺06].

Nevertheless, a question remained of whether there are variants of RACs, 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 (denoted here as PO-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.

This cryptographic property means, in particular, that once some information about a bit is learned, then no other information can be extracted about any of the other bits. Such a notion has applications in various areas of cryptography. For example, this is a requirement for a class of classical or quantum protocols known as *symmetric-private information retrieval schemes* (PIR) [GIKM98, KdW04] where one or more servers have a database x , a user chooses an index i and at the end, the user learns x_i but no other bit of x , and i remains hidden. A parity-oblivious RAC satisfies the security conditions of a PIR scheme since the index i remains hidden (the RAC is non-interactive) and the user cannot learn more than one bit of the database.

Random access codes that are parity-oblivious have been considered before. For example, the previously mentioned RACs for encoding two or three classical bits in one qubit have this property. It is not hard to check that for any subset of the inputs of size 2 or greater, Bob's reduced density matrix is exactly the same for the cases where the parity is 0 or 1. In other words, Bob has no information about the parity. These encodings violate a *non-contextuality inequality* developed by Spekkens, Buzacott, Keehn, Toner, and Pryde [SBK⁺09]. This inequality is discussed further in Subsection 1.3.

1.1 Our results

We say that a random access code where every bit can be decoded with success probability at least $\frac{1}{2}(1 + \alpha)$ has *bias* α . The goal is to find quantum parity-oblivious random access codes with optimal bias.

In this paper, we provide optimal bounds on quantum parity-oblivious random access codes and show that they perform asymptotically better than the optimal classical version.

Theorem 1 (Optimal quantum parity-oblivious random access codes). *For any $n \in \mathbb{N}$, a quantum parity-oblivious random access code of n uniformly random classical bits has bias at most $\frac{1}{\sqrt{n}}$. Moreover, this bound can be achieved using $\lfloor n/2 \rfloor$ qubits and 1 classical bit.*

This is in contrast to the classical setting where the optimal *average-case* bias is provably $1/n$ [SBK⁺09]. We comment further on classical encodings in Subsection 1.2.

The main idea of the proof of the upper bound 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 [OW10, CKS14]. 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. A well-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 . An 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 [CKS14], it was shown that certain variants of the CHSH game are equivalent to some quantum encodings 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 and the bias is *averaged*, i.e., not worst-case. An upper bound on the bias of these encodings would imply an upper bound on the bias of general PO-RACs (since we are relaxing both properties defining PO-RACs).

Then, we study a natural non-local game which we call the INDEX game and show that even-parity-oblivious encodings with *average-case* bias are equivalent to the INDEX game. In other words, any INDEX game strategy with bias α yields an even-parity-oblivious encoding with *average-case* bias α and vice versa. In the INDEX ^{n} game (parameterized by n here), Alice receives an n -bit string s , Bob receives an index $t \in [n]$, and Alice and Bob are supposed to output bits a and b such that $a \oplus b = s_t$.

Theorem 2 (Equivalence). *For any $n \in \mathbb{N}$, there exists a quantum even-parity-oblivious encoding of n uniformly random classical bits with average-case 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 [CSUU08] and provide the exact optimal quantum bias.

Theorem 3 (Optimal quantum INDEX game bias). *For any $n \in \mathbb{N}$, the optimal quantum bias of an INDEX ^{n} strategy is $1/\sqrt{n}$.*

Since the *worst-case* bias of a quantum PO-RAC is obviously upper bounded by the optimal *average-case* bias of a quantum encoding hiding *only* the even parities, Theorems 2 and 3 show that every PO-RAC of n uniformly random classical bits has bias at most $1/\sqrt{n}$.

To prove this upper bound is tight, we give an explicit construction of a PO-RAC of n bits with bias $1/\sqrt{n}$ that uses $\lfloor n/2 \rfloor$ qubits and 1 classical bit. This encoding is based on the notion of *hyperbits* [PW12] and a proof of Tsirelson's theorem [Tsi87].

We remark that parity-oblivious and even-parity-oblivious encodings both share the same worst-case and average-case bias of $1/\sqrt{n}$. However, the same is not true if we consider *odd-parity-oblivious* encodings where the parities are hidden for only odd-size subsets (greater or equal to 3). Consider encoding a six-bit string (x_1, \dots, x_6) where the first three bits are encoded using Chuang’s PO-RAC and similarly for the last three bits. It is a straightforward exercise to verify that this is odd-parity-oblivious and that any bit can be decoded with bias $1/\sqrt{3} > 1/\sqrt{6}$. We leave finding the optimal bounds for odd-parity-oblivious encodings an open problem.

1.2 Remarks on parity-oblivious classical encodings

We can define parity-oblivious classical encodings similar to the quantum case (see Section 2 for rigorous definitions). Moreover, the equivalence stated in Theorem 2 holds in the classical case as well (remarked in Section 3). To prove a tight upper bound on the bias of even-parity-oblivious classical encodings, we provide the following theorem.

Theorem 4 (Optimal classical INDEX game bias). *For any $n \in \mathbb{N}$, the optimal classical bias of an INDEX^n strategy is $\sqrt{\frac{2}{\pi n}}(1 + O(1/n))$.*

This theorem, together with the classical version of the equivalence shows that classical encodings that are even-parity-oblivious have an optimal average-case bias of $\sqrt{\frac{2}{\pi n}}(1 + O(1/n))$. Note that, asymptotically, this value is the same as the quantum value, that is, having a bias of $O(1/\sqrt{n})$. However, differences arise when one considers encodings that also hide the odd parities. Consider the following proposition of Spekkens, Buzacott, Keehn, Toner, and Pryde.

Proposition 1 (Optimal parity-oblivious classical encodings [SBK⁺09]). *For any $n \in \mathbb{N}$, a parity-oblivious classical encoding of n uniformly random classical bits has average-case bias at most $1/n$. Moreover, this bound can be achieved using 1 classical bit.*

Thus, there is a difference between the optimal average-case biases of parity-oblivious and even-parity-oblivious encodings in the classical setting, in contrast to the quantum setting.

1.3 Large non-contextuality inequality violations

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 [SBK⁺09]. 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 [SBK⁺09] proved the following *non-contextuality inequality* (or NC inequality, for short).

Proposition 2 (Non-contextuality inequality [SBK⁺09]). *In any operational theory that admits a preparation non-contextual hidden variable model, the average-case bias for any parity-oblivious encoding is at most $1/n$.*

Then, they showed that quantum mechanics violates this NC inequality for $n \in \{2, 3\}$, by noting the previously mentioned parity-oblivious quantum encodings of two and three classical bits into one qubit with respective average-case biases of $\frac{1}{\sqrt{2}}$ and $\frac{1}{\sqrt{3}}$. It was left as an open question whether quantum mechanics violates this NC inequality for $n \geq 4$.

Through our analysis, we have shown that the optimal average-case bias for quantum parity-oblivious encodings is $1/\sqrt{n}$, thus resolving their main open question. This provides a family of NC inequality violations that grow with the input size n .

Note, that if there 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 with winning probability at least $1/2 + \delta_2$, then we can obtain a violation of order δ_2/δ_1 (see [BRSdW12] for details). Hence, to quantify the violation of this NC inequality, we consider the ratio of the optimal average-case bias of quantum parity-oblivious encodings and that of any operational theory admitting a preparation non-contextual hidden variable model. More precisely, we show an explicit non-contextuality inequality violation of order \sqrt{n} .

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

Note that other large non-contextuality inequality violations have been found, see for example the work of Vidick and Wehner [VW11].

2 Preliminaries and notation

For two matrices X and Y of the same size, we use $\langle X, Y \rangle$ to denote the trace inner product $\text{Tr}(X^*Y)$.

Next, we provide the definitions of the quantum and classical encodings and of the non-local games we consider.

2.1 Quantum and classical encodings and random access codes

Definition 1 (Quantum encodings with worst-case and average-case biases). *A quantum encoding of a string $x \in \{0, 1\}^n$ is a set of quantum states $\{\rho_x : x \in \{0, 1\}^n\}$ along with a decoding procedure i.e., for each i , a two-outcome measurement $\{M_0^i, M_1^i\} : i \in [n]\}$ for learning the individual bits of x .*

We say the encoding has worst-case bias α if

$$\Pr[\text{correctly decoding } x_i] = \langle M_{x_i}^i, \rho_x \rangle \geq \frac{1}{2}(1 + \alpha), \text{ for all } x \in \{0, 1\}^n, i \in [n].$$

We say the encoding has average-case bias α if

$$\mathbb{E}_{x \sim \mu(\{0, 1\}^n)} \mathbb{E}_{i \sim \mu([n])} \Pr[\text{correctly decoding } x_i] = \frac{1}{2}(1 + \alpha),$$

where μ is the uniform probability distribution.

Definition 2 (Classical encodings with worst-case and average-case biases). *A classical encoding of a string $x \in \{0, 1\}^n$ is a set of strings $\{e(x, r) : x \in \{0, 1\}^n, r \in \{0, 1\}^m\}$ where r corresponds to private randomness; along with a decoding procedure, i.e., for each i , a function f_i for learning the individual bits of x .*

We say the encoding has worst-case bias α if

$$\Pr[\text{correctly decoding } x_i] = \Pr[f_i(e(x, r)) = x_i] \geq \frac{1}{2}(1 + \alpha), \text{ for all } x \in \{0, 1\}^n, i \in [n],$$

where the probabilities are taken over all the random coins r . We say the encoding has average-case bias α if

$$\mathbb{E}_{x \sim \mu(\{0,1\}^n)} \mathbb{E}_{i \sim \mu([n])} \Pr[\text{correctly decoding } x_i] = \mathbb{E}_{x \sim \mu(\{0,1\}^n)} \mathbb{E}_{i \sim \mu([n])} \Pr[f_i(e(x, r)) = x_i] = \frac{1}{2}(1 + \alpha),$$

where μ is the uniform probability distribution.

Note that we can define average-case biases over non-uniform distributions. However, we have only the need for uniform probability distributions in this paper.

In this paper, we are concerned with quantum encodings which enforce certain cryptographic properties. For example, we enforce that the encoding *hides* some information about the encoded string x . By information being *hidden*, we mean that there exists no measurement which yields a correct guess with probability greater than that of randomly guessing. In particular, we consider the case for which certain parities of the encoded string are hidden.

Definition 3 (*S*-parities). For a string $x \in \{0, 1\}^n$ and subset $S \subseteq [n]$, we define its *S*-parity as $x_S := \bigoplus_{i \in S} x_i$.

In the definition above, we usually only care about subsets of size 2 or greater, but we have occasion to consider the singleton sets as well.

Definition 4 (Parity-oblivious and even-parity oblivious encodings). We say a quantum encoding is parity-oblivious if it has the cryptographic constraint that every *S*-parity is hidden, that is,

$$\mathbb{E}_{x \sim \mu(\{0,1\}^n)} \Pr[\text{correctly decoding } x_S] = \frac{1}{2}, \text{ for all } S \subseteq [n], |S| \geq 2.$$

An even-parity-oblivious quantum encoding is a quantum encoding such that every *S*-parity is hidden when $|S|$ is even.

In this paper, we examine quantum encodings with varying notions of bias and parity-obliviousness. However, we are primarily concerned with bounding the bias of *parity-oblivious random access codes*, defined below.

Definition 5 (Parity-oblivious random access codes). A quantum parity-oblivious random access code of n uniformly random classical bits, denoted here as PO-RACⁿ, with bias α is a parity-oblivious quantum encoding with worst-case bias α .

Note that the above definition includes the most stringent of both properties. However, as the analysis in this paper shows, the optimal bias for PO-RACⁿs is equal to the optimal *average-case* bias for quantum encodings that are even-parity-oblivious. Thus, our definition of PO-RACⁿ is not too demanding.

Note that the usual treatment of RACs is to analyze the relationships between n , α , and the dimension of the encoding. Here, we are not concerned with the encoding dimension, but rather the ability to achieve parity-obliviousness.

2.2 Non-local games

In a non-local game, two non-communicating parties, Alice and Bob, receive some inputs s and t , respectively, and must output a and b , respectively, such that (s, t, a, b) satisfy some specific condition. For example in the CHSH game, the condition is $a \oplus b = s \cdot t$. 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 6 (INDEX game). *The INDEXⁿ game, parameterized by n here, 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

$$\mathbb{E}_{s \sim \mu(\{0,1\}^n)} \mathbb{E}_{t \sim \mu([n])} \Pr[\text{Alice's output } a \text{ and Bob's output } b \text{ satisfy } a \oplus b = s_t] = \frac{1}{2}(1 + \alpha).$$

The INDEX game turns out to be equivalent to the Retrieval game studied in [OW10] which is defined similarly except the first bit of Alice's input is always 0 (otherwise the other $n - 1$ bits are chosen independently and uniformly at random). To see the equivalence, notice that in the INDEX game Alice can take her input $s \in \{0, 1\}^n$, define $s' = \mathbf{m} \oplus s$, where m fixes the specific bit to a specific value, play the Retrieval game strategy with input s' to generate a' , and then output $a := a' \oplus m$ (Bob plays the same strategy). Thus, any strategy for the Retrieval game with bias α yields a strategy for the INDEX game with bias α as well. We further remark that the quantum bias of the Retrieval game is shown to be $1/\sqrt{n}$ in [OW10] through the use of uncertainty relations. Using this result, and the equivalence to the INDEX game, we have another proof that the quantum bias of the INDEX game is $1/\sqrt{n}$.

3 Equivalence of even-parity-oblivious encodings and INDEXⁿ strategies

In this section we prove the equivalence in Theorem 2, reproduced below.

Theorem 2 (Equivalence). *For any $n \in \mathbb{N}$, there exists a quantum even-parity-oblivious encoding of n uniformly random classical bits with average-case bias α if and only if there exists a quantum INDEXⁿ strategy with bias α .*

3.1 From encodings to INDEX strategies

Let us fix an even-parity-oblivious encoding $\{\rho_x : x \in \{0, 1\}^n\}$ with average-case bias α . Let \mathcal{B} be the Hilbert space used for the encoding. Our goal is to construct a strategy for INDEXⁿ 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 \mathbf{a} be the n -bit string (a, \dots, a) and \bar{s} be the bit-wise complement of a string s . Define the following state

$$|\Omega_s\rangle = \frac{1}{\sqrt{2}} \sum_{a \in \{0,1\}} |a\rangle_{\mathcal{O}} |\psi_{s \oplus \mathbf{a}}\rangle_{\mathcal{AB}} = \frac{1}{\sqrt{2}} |0\rangle |\psi_s\rangle + \frac{1}{\sqrt{2}} |1\rangle |\psi_{\bar{s}}\rangle,$$

where \mathcal{O} is a qubit register containing the value of a . 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 $\sigma_s = \frac{1}{2}\rho_s + \frac{1}{2}\rho_{\bar{s}}$.

The first step is to see that Bob has no information about any parity of s (not even of the values of the singleton bits). Fix an arbitrary, non-empty subset S . The reduced state Bob has for $s_S = b$ is given by

$$\sigma_S^b := \begin{cases} \rho_S^b & \text{if } |S| \text{ even,} \\ \frac{1}{2}\rho_S^0 + \frac{1}{2}\rho_S^1 & \text{if } |S| \text{ odd,} \end{cases}$$

where $\rho_S^b := \frac{1}{2^{n-1}} \sum_{s: s_S=b} \rho_s$. This shows that if $|S|$ is odd, then $\sigma_S^0 = \sigma_S^1$. If $|S|$ is even (and nonzero), we have $\rho_S^0 = \rho_S^1$ since the even parities of the encoding $\{\rho_x : x \in \{0, 1\}^n\}$ are hidden (when chosen uniformly at random). Hence, we have $\sigma_S^0 = \sigma_S^1$. This means that for any nonempty subset S and measurement M , Bob has a maximum probability of $1/2$ of successfully guessing s_S .

In the following lemma, we prove that if an encoding reveals no information about the parity of any subset, then the encoding reveals no information about the string. This is intuitively an obvious statement that we rigorously prove below.

Lemma 1. *If an encoding $\{\sigma_s : s \in \{0, 1\}^n\}$ satisfies $\mathbb{E}_{s \sim \mu(\{0, 1\}^n)} \Pr[\text{learn } s_S] = \frac{1}{2}$, for every subset $S \subseteq [n] \setminus \emptyset$, then $\sigma_s = \sigma_{s'}$ for all $s, s' \in \{0, 1\}^n$.*

Proof. Suppose for a contradiction that there exists $s, s' \in \{0, 1\}^n$ such that $\sigma_s \neq \sigma_{s'}$. Then there exists a subset $T \in \{0, 1\}^n$ of size 2^{n-1} such that $\sigma_T = \frac{1}{2^{n-1}} \sum_{s \in T} \sigma_s$ is not equal to $\sigma_{\bar{T}} = \frac{1}{2^{n-1}} \sum_{s \in \bar{T}} \sigma_s$, see footnote¹. This means that there exists a two-outcome measurement that outputs 1 if $s \in T$ and -1 otherwise, with positive bias. We now show for a contradiction that this measurement must also output a parity of some nonempty subset with positive bias. Define the function $f : \{0, 1\}^n \rightarrow \{-1, +1\}$, as the indicator function of T and let b be the measurement outcome. Then

$$\mathbb{E}_{s \sim \mu(\{0, 1\}^n)} [b \cdot f(s)] > 0.$$

By taking the Fourier representation of the function, we have

$$\mathbb{E}_{s \sim \mu(\{0, 1\}^n)} [b \cdot f(s)] = \mathbb{E}_{s \sim \mu(\{0, 1\}^n)} \left[b \cdot \sum_{S \subseteq [n]} \hat{f}(S) (-1)^{s_S} \right] = \sum_{S \subseteq [n]} \hat{f}(S) \mathbb{E}_{s \sim \mu(\{0, 1\}^n)} [b \cdot (-1)^{s_S}] > 0.$$

Note that $\hat{f}(\emptyset) = \mathbb{E}[f(s)] = 0$, implying that there exists a non-empty subset S for which

$$\mathbb{E}_{s \sim \mu(\{0, 1\}^n)} [b \cdot (-1)^{s_S}] \neq 0,$$

which is a contradiction. □

The above statement means that for each s , we have $\text{Tr}_{\mathcal{O}\mathcal{A}} |\Omega_s\rangle\langle\Omega_s| = \text{Tr}_{\mathcal{O}\mathcal{A}} |\Omega_0\rangle\langle\Omega_0|$. In particular, this means that for any $s \in \{0, 1\}^n$ there exists a unitary U_s acting on $\mathcal{O}\mathcal{A}$ such that $(U_s \otimes I) |\Omega_0\rangle = |\Omega_s\rangle$. We use the state $|\Omega_0\rangle$ to define the INDEXⁿ strategy:

- Alice and Bob share the state $|\Omega_0\rangle \in \mathcal{A} \otimes \mathcal{B}$.

¹To see this, take any subset $T \in \{0, 1\}^n$ of size 2^{n-1} . If $\sigma_T = \sigma_{\bar{T}}$, then we can find $s \in T$ and $s' \in \bar{T}$ such that $\sigma_s \neq \sigma_{s'}$, since all the σ_i are not equal. We consider the subset T' where we add $\{s'\}$ and remove $\{s\}$ from T . We obtain $\sigma_{T'} \neq \sigma_{\bar{T}'}$.

- Upon receiving $s \in \{0, 1\}^n$, Alice applies U_s on $\mathcal{O}\mathcal{A}$ such that Alice and Bob share $|\Omega_s\rangle$. Alice measures register \mathcal{O} in the computational basis and outputs the measurement outcome a .
- For Alice's input s and output a , Bob has an encoding ρ_x where $x := s \oplus a$ occurs uniformly at random. Upon receiving $t \in [n]$, Bob measures \mathcal{B} just as in the encoding 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 the encoding has bias α , we see that with this INDEXⁿ strategy, they succeed with probability

$$\begin{aligned}
& \mathbb{E}_{s \sim \mu(\{0,1\}^n)} \mathbb{E}_{t \sim \mu([n])} \Pr[\text{Alice's output } a \text{ and Bob's output } b \text{ satisfy } a \oplus b = s_t] \\
&= \mathbb{E}_{x \sim \mu(\{0,1\}^n)} \mathbb{E}_{t \sim \mu([n])} \Pr[\text{Bob learns } x_t \text{ from the } \{\rho_x : x \in \{0, 1\}^n\} \text{ encoding}] \\
&= \frac{1}{2}(1 + \alpha),
\end{aligned}$$

as desired.

3.2 From INDEX strategies to encodings

Suppose Alice and Bob have a strategy to win the INDEXⁿ game with bias α with starting state $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$. On input $s \in \{0, 1\}^n$, Alice performs on her side the corresponding measurement which generates her outcome a . Let $\rho_{s,a}$ be the state that Bob has when Alice has input s and outputs a . Define $x := s \oplus a$ and let σ_x be Bob's encoding of x (a weighted sum of $\rho_{x,0}$ and $\rho_{x,\bar{0}}$ with the weights given by the corresponding probabilities). We show that $\{\sigma_x : x \in \{0, 1\}^n\}$ is an even-parity-oblivious encoding with average-case bias α .

1. First, it hides the even parities: each even parity of x is equal to an even parity of s , which is hidden from the no-signalling principle.
2. Second, Alice and Bob win the INDEXⁿ game with bias α hence,

$$\frac{1}{2}(1 + \alpha) = \mathbb{E}_{s \sim \mu(\{0,1\}^n)} \mathbb{E}_{t \sim \mu([n])} \Pr[\text{Bob learns } s_t \oplus a] = \mathbb{E}_{x \sim \mu(\{0,1\}^n)} \mathbb{E}_{t \sim \mu([n])} \Pr[\text{Bob learns } x_t],$$

as desired.

Remark The above equivalence also holds in the classical setting.

4 On the structure of optimal INDEX game strategies

In this section, we prove Theorems 3 and 4, reproduced below.

Theorem 3 (Optimal quantum INDEX game bias). *For any $n \in \mathbb{N}$, the optimal quantum bias of an INDEXⁿ strategy is $1/\sqrt{n}$.*

Theorem 4 (Optimal classical INDEX game bias). *For any $n \in \mathbb{N}$, the optimal classical bias of an INDEXⁿ strategy 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) [CSUU08]. The optimization takes place over a matrix indexed by $s \in S$ and $t \in T$ with each entry corresponding to the expectation of the measurement outcome of a fixed game strategy. Such a matrix of inner products can be written as a positive semidefinite matrix and the expectation (or bias) of the game strategy is then an inner product of this matrix and one containing the information of the XOR game.

Specifically, the quantum bias of the INDEXⁿ 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: $\text{diag}(X) = e$ | subject to: $\text{Diag}(y) \succeq B$ |
| $X \succeq 0$ | |

where

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

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 $u, v > 0$ (determined later) and e_S and e_T are the vectors of all ones indexed by entries in S and T , respectively. Then

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

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 1, they win the game with probability

$$\mathbb{E}_{t \sim \mu(\{[n]\})} \Pr[b_t \neq s_t] = \frac{1}{n} |b \oplus s|_H,$$

where $|x|_H$ denotes the Hamming weight of a string $x \in \{0, 1\}^n$. If she outputs 0, they win the game with probability

$$\mathbb{E}_{t \sim \mu(\{[n]\})} \Pr[b_t = s_t] = 1 - \frac{1}{n} |b \oplus s|_H.$$

Since their strategies are deterministic, Alice should output the maximum of these two, so

$$\max \left\{ \frac{1}{n} |b \oplus s|_H, 1 - \frac{1}{n} |b \oplus s|_H \right\} = \frac{1}{2} + \left| \frac{1}{2} - \frac{1}{n} |b \oplus s|_H \right| = \frac{1}{2} + \frac{1}{2} \cdot \frac{2}{n} \left| \frac{n}{2} - |b \oplus s|_H \right|.$$

Therefore, the classical bias is precisely $\frac{2}{n} \mathbb{E}_{s \sim \mu(\{0,1\}^n)} \left| \frac{n}{2} - |b \oplus s|_H \right|$. The quantity $\mathbb{E}_{s \sim \mu(\{0,1\}^n)} \left| \frac{n}{2} - |b \oplus s|_H \right|$ corresponds to the mean deviation of the uniform binomial distribution. This is a well studied quantity and we know that

$$\mathbb{E}_{s \sim \mu(\{0,1\}^n)} \left[\left| \frac{n}{2} - |b \oplus s|_H \right| \right] = \sqrt{\frac{n}{2\pi}} \left(1 + O\left(\frac{1}{n}\right) \right).$$

Therefore, the classical bias is $\frac{2}{n} \sqrt{\frac{n}{2\pi}} \left(1 + O\left(\frac{1}{n}\right) \right) = \sqrt{\frac{2}{\pi n}} \left(1 + O\left(\frac{1}{n}\right) \right)$, as desired.

5 A construction of a quantum PO-RACⁿ with optimal bias

In this section, we give an explicit construction of a quantum PO-RACⁿ with optimal bias.

Lemma 2 (Optimal PO-RACⁿ). *For any $n \in \mathbb{N}$, there exists a PO-RACⁿ with bias $1/\sqrt{n}$ that uses $\lfloor n/2 \rfloor$ qubits and 1 classical bit.*

Our construction builds upon the previously mentioned RACs for sending 2 (resp. 3) classical bits with bias $1/\sqrt{2}$ (resp. $1/\sqrt{3}$). 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 Pawłowski and Winter [PW12].

We note that, after the publication of this paper, we became aware that a similar encoding had been previously discovered by Wehner [Weh08], but remained unpublished.

5.1 The construction

Note Lemma 2 is trivially true for $n = 1$ as the encoding can just be the bit itself. For the rest of the construction, we assume $n \geq 2$.

Our construction is very similar to a proof of Tsirelson's theorem [Tsi87]. We start by recursively defining the observables $G_{n,1}, \dots, G_{n,n}$, for $n \geq 2$, which are used to define the actions of Alice and Bob in the PO-RAC n . For $n = 2$ and $n = 3$, we define

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

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

$$\begin{aligned} n \text{ even} : \quad & G_{n,i} := G_{n-1,i} \otimes X, \quad \text{for } i \in \{1, \dots, n-1\}, & G_{n,n} &= I \otimes Y, \\ n \text{ odd} : \quad & G_{n,i} := G_{n-2,i} \otimes X, \quad \text{for } i \in \{1, \dots, n-2\}, & G_{n,n-1} &= I \otimes Y, \quad G_{n,n} = I \otimes Z. \end{aligned}$$

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

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

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

$$A_x := \frac{1}{\sqrt{n}} \sum_{i=1}^n (-1)^{x_i} G_{n,i} \quad \text{and} \quad B_t := G_{n,t}^\top.$$

Note that $A_x^2 = I$, for all $x \in \{0, 1\}^n$, and $B_t^2 = I$, 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 worst-case bias of this encoding is $\frac{1}{\sqrt{n}}$ and that it is parity-oblivious, thereby proving Lemma 2.

Lemma 3. *In the encoding above, Bob can learn x_t with bias $1/\sqrt{n}$, for any $x \in \{0, 1\}^n$, $t \in [n]$.*

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:

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

²We note here that the choice of these observables is not unique and there are applications in the literature that use slightly different observables. However, this particular choice reduces the encoding dimension by one qubit when n is odd. For example, for $n = 3$ our encoding uses $\lfloor n/2 \rfloor = 1$ qubit (as opposed to two) just as in the well-known quantum encoding of three classical bits into one qubit.

where the third equality is derived from the anti-commutation relation. We can write

$$\langle C \rangle = \Pr[c = +1] - \Pr[c = -1] = \langle \psi | A_x \otimes B_t | \psi \rangle$$

implying

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

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

proving that

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

as desired. \square

Lemma 4. *In the encoding above, the parity of any subset of size 2 or greater is hidden.*

Proof. Protocols involving shared entanglement and sending one classical bit have limited guessing probabilities for functions such as parity [PW12]. In particular, it can be shown that the biases α_S of learning x_S satisfy

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

In the encoding above, we have

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

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

Acknowledgements

This research was supported by the French National Research Agency, through CRYQ (ANR-09-JCJC-0067) and by the European Union through the ERC project QCC.

References

- [ANTV99] 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.
- [ANTV02] 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.
- [BARdW08] A. Ben-Aroya, O. Regev, and R. de Wolf. A hypercontractive inequality for matrix-valued functions with applications to quantum computing and LDCs. In *FOCS*, pages 477–486, 2008.

- [BBBW83] C. Bennett, G. Brassard, S. Breidbard, and S. Wiesner. Quantum cryptography, or unforgeable subway tokens. In *Advances in Cryptology CRYPTO 1982*, pages 267–275, 1983.
- [BCWdW01] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87:167902, Sep 2001.
- [BJK04] 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.
- [BRSdW12] H. Buhrman, O. Regev, G. Scarpa, and R. de Wolf. Near-optimal and explicit Bell inequality violations. *Theory of Computing*, 8(27):623–645, 2012.
- [CHSH69] 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.
- [CKS14] A. Chailloux, I. Kerenidis, and J. Sikora. Strong connections between quantum encodings, non-locality and quantum cryptography. *Physical Review A*, 89:022334, 2014.
- [CSUU08] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay. Perfect parallel repetition theorem for quantum XOR proof systems. *Computational Complexity*, 17(2):282–299, 2008.
- [DV10] A. De and T. Vidick. Near-optimal extractors against quantum storage. In *STOC*, pages 161–170, 2010.
- [GIKM98] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin. Protecting data privacy in private information retrieval schemes. In *JCSS*, pages 151–160. ACM Press, 1998.
- [GKK⁺08] 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.
- [HIN⁺06] 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.
- [Hol73] A. Holevo. Some estimates of the information transmitted by quantum communication channels. *Problemy Peredachi Informatsii*, 9:3–11, 1973.
- [INRY07] K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita. Unbounded-error one-way classical and quantum communication complexity. In *ICALP*, pages 110–121, 2007.
- [KdW04] I. Kerenidis and R. de Wolf. Quantum symmetrically-private information retrieval. *Information Processing Letters*, 90(3):109–114, 2004.
- [LPY⁺12] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han. Semi-device-independent randomness certification using $n \rightarrow 1$ quantum random access codes. *Phys. Rev. A*, 85:052308, May 2012.
- [Nay99] 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.

- [OW10] J. Oppenheim and S. Wehner. The uncertainty principle determines the non-locality of quantum mechanics. *Science*, 330:6007:1072–1074, 2010.
- [PW12] M. Pawłowski and A. Winter. From qubits to hyperbits. *Phys. Rev. A*, 85:022331, 2012.
- [PZ10] M. Pawłowski and M. Żukowski. Entanglement-assisted random access codes. *Phys. Rev. A*, 81:042326, Apr 2010.
- [Raz99] R. 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.
- [RK11] O. Regev and B. Klartag. Quantum one-way communication can be exponentially stronger than classical communication. In *STOC*, pages 31–40, 2011.
- [SBK⁺09] 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.
- [Tsi87] B. Tsirelson. Quantum analogues of the Bell inequalities: The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36:557–570, 1987.
- [VW11] T. Vidick and S. Wehner. Does ignorance of the whole imply ignorance of the parts? *Physical Review Letters*, 107:030402, 2011.
- [Weh08] S. Wehner. Unpublished note, 2008.