Constructions of Quantum Random Access Codes

Takashi Imamichi\(^1\) \(*\) \quad Rudy Raymond\(^1\) \(^2\) \(^3\) \(^4\)

\(^1\) Quantum Algorithms and Software Group, IBM Research - Tokyo
\(^2\) Quantum Computing Center, Keio University

Abstract. Quantum Random Access Codes (QRACs) are coding schemes that allow to encode \(n\) bits into \(m\) qubits, for \(n > m\), so that any one of the bits can be extracted with success probability at least \(p > 1/2\). QRAC is one of examples that demonstrate the advantage of quantum communication systems. It is also used in various quantum computation models, such as, quantum finite automata and state learning. Several approaches to derive the construction of QRACs with few qubits have been proposed, but they are mostly not optimal. Here, we investigate the construction of QRACs by heuristics based on semidefinite programming (SDP). The construction allows us to find QRACs on two qubits whose success probabilities are better than those previously known. We also demonstrate the QRACs on the real quantum devices of IBM Q Systems using the open source QISKit.

1 Introduction

Differ from bits that can only exist as one of many possible states, quantum bits (or, qubits) can realize superposition of all possible states. Despite this striking property, Holevo bound states that \(m\) qubits can only be used to faithfully encode \(m\) bits of information. Moreover, there exist communication scenarios where quantum systems do not bring advantages with regards to classical systems [11]. However, when relaxing the faithful restriction, QRACs become examples where quantum schemes are better than their classical counterparts. Namely, when it is allowed to retrieve the partial information about \(n\) bits with some probability \(p > 1/2\), QRACs can encode them with the number of qubits that is half of the bits used in classical random access codes (RACs). \((n, m, p)\)-QRACs exist for any \(n < 2^m\), while their classical counterparts \((n, m, p)\)-RACs exist only for \(n < 2^m\). Some QRACs also offer cryptographic properties known as parity obliviousness [9], which can play important role in cryptography and private information retrieval. Namely, while in RACs every bit can be retrieved with probability at least \(p\), in some properly designed QRACs only a subset of the bits can be extracted.

QRACs were discovered much earlier by [23] but they were popularized by [6] that also showed explicit constructions of \((2,1,1/2+1/(2\sqrt{2}))\)-QRAC. The QRAC for encoding 3 bits of information into 1 qubit was attributed to Chuang whose explicit construction of \((3,1,1/2+1/(2\sqrt{3}))\)-QRAC was shown in [12]. The generic construction of \((O(m), m > 1/2)\)-QRACs with multiple qubits was first introduced by [6], but it was essentially RACs. The first generic construction of \((n, m, p)\)-QRACs for any \(n < 2^m\) was shown in [13]. There are some well-known limitations of QRACs. For example, any \((n, m, p)\)-QRACs must satisfy the so-called Nayak bound [19]: \(m \geq (1-H(p))n\), where \(H(\cdot)\) is the entropy function. Moreover, \(n\) cannot exceed \(2^m-1\) as shown in [12]. Thus, one qubit can only encode at most three bits, and at most fifteen bits by two qubits, and so on.

Very recently [17] shows improved QRACs by better use of the geometry of density matrices and numerical searches. In particular, it shows explicit constructions of \((n,2,p)\)-QRACs for \(7 \leq n \leq 12\) obtained from extensive numerical searches. The \((7, 2, 0.68)\)-QRAC in [17] is better than the \((7, 2, 0.54)\)-QRAC shown in [12], but there is still gap with the upper bound of the success probability implied by the Nayak bound (which is \(\approx 0.81\)). As proved in [17], there is a positive correlation between the success probability of QRACs and their parity obliviousness to conceal the information of other unrevealed bits: the higher the success probabilities, the better its cryptographic properties.

Our Contribution. We propose a heuristic method to construct \((n, m, p)\)-QRACs by utilizing see-saw iterations of semidefinite programming [21]. The heuristic method is based on formulating the encoding-decoding steps of QRACs as (nonconvex) bilinear semidefinite optimization. When either the quantum states (for encoding the bits) or the quantum measurements (for extracting the information of particular bits) are fixed, the formulation reduces to a convex problem of semidefinite programming (SDP). The proposed method allows us to find explicit constructions of QRACs on two qubits that are better than previously known. For example, in addition to better \((n,2,p)\)-QRACs for \(n = 7, 8, 9\), we also find \((3,2,1/2+1/\sqrt{6})\) and \((5,2,0.81)\)-QRACs that were unknown before. For simple cases of one qubit, the SDP formulation can be used to show the optimality of \((2,1,1/2+1/(2\sqrt{2}))\)- and \((3,1,1/2+1/(2\sqrt{3}))\)-QRACs. Combined with the facts that we cannot find \((4,2,p)\)- and \((6,2,p)\)-QRACs with success probabilities better than simply combining two \((2,1,p)\)- or \((3,1,p)\)-QRACs, we conjecture that the success probabilities of \((n,2,p)\)-QRACs satisfy \(p \leq 1/2+1/\sqrt{2^n}\). We also show the experiments of the new two-qubit QRACs on the IBM Q Systems. We hope our proposed method can be used to systematically construct QRACs as communication and computation resources on near-term quantum devices.
2 Related Work

Although formulated in the communication setting, QRACs have been extensively used in the theory of quantum computations, such as, the limit of quantum finite automata [6] and quantum state learning [3]. QRACs are applied in quantum communication complexity [15] and used in elaborate coding schemes like network coding [13] and locally decodable codes [22]. It is interesting to notice that QRACs offer quantum advantage approximately twice of their classical counterpart RACs which is similar to superdense coding [8] and quantum teleportation [7]. Namely, QRACs have been used to show that if the success probability is allowed to be only bigger than half, then the number of qubits can be reduced to half of that of the bits in various settings of communication complexity [13]. QRACs have also been applied in quantum non-locality and contextuality [20], cryptography [25], and random number generation [16].

The variants of QRACs using shared entanglement and classical randomness are also popular [5]. In particular, with randomness it is possible to encode any number of bits into a single qubit and the constructions of such QRACs is shown in [5]. QRACs can also exploit d-level quantum systems for d > 2 (i.e., qutrits, qudits, and so on) and interestingly the quantum advantage obtained from such QRACs can be better than the well-known 2-level one [17]. Here, we focus on the original setting of QRACs that does not use shared resources and operates on 2-level quantum systems. Experiments to realize QRACs on few quantum resources were first shown in [20]. The demonstrations of QRACs with one and two qubits described in [12] can also be found at the QISKit tutorial [2].

3 Main Results

We first give the definition of QRACs following [6].

**Definition.** An encoding function of \((n, m, p)\)-QRAC is a function that maps n-bit strings \(x \in \{0, 1\}^n\) to \(m\)-qubit states \(\rho_x\), and a decoding function of the QRAC is the one such that for every \(i \in \{1, 2, \ldots, n\}\) there exists a positive operator-valued measure (POVM) \(E^i = \{E^i_0, E^i_1\}\) such that for all \(x \in \{0, 1\}\) the probability of retrieving its \(i\)-th bit \(x_i\) is at least \(p\), i.e., \(\text{Tr}(E^i_x, \rho_x) \geq p\).

Recall that \(\rho_x\) are positive semidefinite Hermitian matrices whose traces are one. The POVMs also consist of positive semidefinite Hermitian matrices satisfying \(E^0_0 + E^1_1 = I\). In the \((n, m, p)\)-QRACs, both \(\rho_x\) and \(E^0_{(0,1)}\) are \(2^n \times 2^n\) complex matrices. From the definition of QRACs and the properties of quantum states and POVMs, we can derive the following optimization problem that will become the basis to construct QRACs. Notice \(\overline{x_i} = 1 \oplus x_i\), i.e., \(\overline{x_i}\) is the bit-flipped of \(x_i\).

\[
\mathcal{P} = \left\{ \begin{array}{l}
\max_{\{E^i_x, \rho_x\}} \ p \\
\text{subject to} \\
\text{Tr}(E^0_x, \rho_x) \geq p, \quad \forall x \in \{0, 1\}^n \text{ and } \forall i \in [1, n] \\
\text{Tr}(\rho_x) = 1, \quad \forall x \in \{0, 1\}^n \\
E^0_x + E^1_x = I, \quad \forall x \in \{0, 1\}^n \text{ and } \forall i \in [1, n] \\
E^0_x, E^1_x, \rho_x \succeq 0, \quad \forall x \in \{0, 1\}^n \text{ and } \forall i \in [1, n] 
\end{array} \right. 
\]

The above optimization problem \(\mathcal{P}\) is a nonconvex bilinear semidefinite optimization which is NP-hard in general. The number of constraints is \(O(n2^n)\) and therefore can grow quickly with the length of the bitstring \(n\). The optimization problem involves searching \(n\) POVMs and \(2^n\) quantum states for \(n < 2^{2m}\). This is a hard problem for large \(n\). However, \(\mathcal{P}\) can be used to show the optimality of one-qubit QRACs: \(\{2, 1, 1/2 + 1/(2\sqrt{2})\}\) and \(\{3, 1, 1/2 + 1/(2\sqrt{3})\}\)-QRACs are optimal. The proofs follow from geometric arguments that are omitted in this version. The optimality of one-qubit QRACs were already proved in [5] whose bounds also hold for all one-qubit QRACs with shared randomness.

From \(\mathcal{P}\) we can obtain two convex optimization sub problems: one when the POVMs are fixed, and the other when the quantum states are fixed. Let us denote the former by \(\mathcal{P}_1\) and the latter by \(\mathcal{P}_2\). Both \(\mathcal{P}_1\) and \(\mathcal{P}_2\) are semidefinite programming (SDP) that can be solved efficiently by standard SDP solvers, such as, SDPA [24] that we use to construct QRACs. The semidefinite programming is already useful to find QRACs with fixed measurements. For example, we can observe that the POVMs of one-qubit QRACs are mutually unbiased bases (MUB) in Hilbert space \(\mathbb{C}^2\) (see [10] for more details on MUB). We expect the POVMs of multi-qubit QRACs are MUB or have similar property. In such cases, we can construct the QRACs by using MUB as the fixed POVMs and find the optimal states by \(\mathcal{P}_1\). Say, the five sets of MUB in Hilbert space \(\mathbb{C}^2\) can be used to find \((5, 2, p)\)-QRACs, which are different from simply combining two one-qubit QRACs.

However, we find that fixing MUB as POVMs and using \(\mathcal{P}_1\) to construct \((3, 2, p)\)- and \((5, 2, p)\)-QRACs do not result in optimal QRACs. Instead, the following heuristic method that performs see-saw iterations of solving \(\mathcal{P}_1\) and \(\mathcal{P}_2\) starting from random POVMs can lead to better QRACs (as detailed later). The proposed heuristic to construct (local) optimal multi-qubit QRACs is as follow: (i) choose POVMs at random, (ii) solve the sub problem \(\mathcal{P}_1\) with the fixed POVMs to obtain optimal quantum states, and (iii) solve the sub problem \(\mathcal{P}_2\) with the fixed quantum states to obtain optimal POVMs, and return to (ii). The iterations are repeated for several times (pre determined or terminated when the optimal solution does not improve after several iterations). There are many alternatives to choose POVMs at (i), and we obtain random bases generated according to techniques to generate random quantum states from parameters described in [14]. We should note that although there is no guarantee to obtain global optimal, similar see-saw iterations of SDPs have been successfully applied to similar bilinear optimization problems, such as finding maximum violations.
of Bell inequality and its variants [18], or finding MUB for d-level QRACs with averaged success probabilities [4].

Although the proposed heuristic method returns numerical solutions, by analyzing them we can obtain the following analytical solution of the new $(3, 2, 1/2 + 1/\sqrt{6})$-QRAC as below.

**Theorem 1** There exists a $(3, 2, 1/2 + 1/\sqrt{6})$-QRAC.

**Proof.** The pure quantum states for encoding the bit-string $x_1x_2x_3$, i.e., $|\psi_{x_1x_2x_3}\rangle$, are as follows:

$$|\psi_{000}\rangle = |00\rangle, |\psi_{001}\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |10\rangle),$$

$$|\psi_{010}\rangle = \frac{1}{\sqrt{3}}(|00\rangle - |01\rangle + |11\rangle), |\psi_{011}\rangle = |01\rangle,$$

$$|\psi_{100}\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |10\rangle + |11\rangle), |\psi_{101}\rangle = |10\rangle,$$

$$|\psi_{110}\rangle = |11\rangle, |\psi_{111}\rangle = \frac{1}{\sqrt{3}}(|01\rangle - |10\rangle + |11\rangle).$$

The POVMs for decoding the $i$-th bit to be 0 are projective measurements in the basis $\{|\phi^1_i\rangle, |\phi^2_i\rangle\}$ (which is denoted as $E^i_0$). Namely, the $i$-th bit is 0 if either $|\phi^1_i\rangle$ or $|\phi^2_i\rangle$ is observed from measuring the encoding state (otherwise, the $i$-th bit is 1). Letting $p = 1/2 + 1/\sqrt{6}$, $E^i_0$ are given as follows:

$$E^1_0 = \{\sqrt{p}|00\rangle + \sqrt{\frac{1-p}{2}}(|10\rangle + |11\rangle),$$

$$-\sqrt{p}|01\rangle + \sqrt{\frac{1-p}{2}}(|00\rangle + |11\rangle)\},$$

$$E^2_0 = \{-\sqrt{p}|00\rangle + \sqrt{\frac{1-p}{2}}(|01\rangle + |11\rangle),$$

$$\sqrt{p}|10\rangle + \sqrt{\frac{1-p}{2}}(|01\rangle + |11\rangle)\},$$

$$E^3_0 = \{-\sqrt{p}|00\rangle + \sqrt{\frac{1-p}{2}}(|01\rangle + |10\rangle),$$

$$\sqrt{p}|11\rangle + \sqrt{\frac{1-p}{2}}(|01\rangle + |10\rangle)\}.$$
References


