Quantum Random Access Codes with Shared Randomness

Andris Ambainis, Debbie Leung,
Laura Mancinska, Maris Ozols

Introduction

Consider the following communication method: the sender encodes n classical bits into m qubits and sends them to the receiver who performs a certain measurement depending on which of the initial bits must be recovered. This procedure is called $n \overset{p}{\mapsto} m$ *quantum random access code* (QRAC) where $p > 1/2$ is its worst case success probability. *Classical random access code* is defined similarly, except the information is encoded into m *classical* bits.

We extend these models by allowing both parties to cooperate using *shared randomness* (SR). However, we consider only the case $m = 1$, i.e., n bits are encoded in 1 qubit or 1 bit, respectively.

Motivation

Originally quantum random access codes have been studied in the context of quantum finite automata [1, 2]. However, they also have applications in quantum communication [4, 5, 6]. More recently results on quantum random access codes have been applied also for quantum state learning [7]. We hope that our results will extend the possible range of applications of quantum random access codes in different branches of quantum information theory.

Prior work

It is known that $2 \overset{0.85}{\longmapsto} 1$ and $3 \overset{0.79}{\longmapsto} 1$ QRACs (with no classical counterparts) exist [1]. The Bloch sphere representation of these codes is shown in Fig. 1. In the first case a string of two classical bits is encoded in a state corresponding to one of the four vertices of a square. Similarly, for three classical bits one uses the vertices of a cube. The optimal success probability is obtained by using the largest square (or cube) that can be inscribed in the Bloch sphere. For a particular choice of encodings shown in Fig. 1 one has to measure along the coordinate axis to recover the encoded classical bits (x, y, and z axis correspond to the first, second, and third bit, respectively).

However, it has been shown that $4 \overset{p}{\mapsto} 1$ QRAC with $p > 1/2$ is not possible [3]. The proof essentially is based on the observation that the surface of the Bloch sphere cannot be cut into 16 pieces by four planes that pass through its center (these planes correspond to the four measurements).

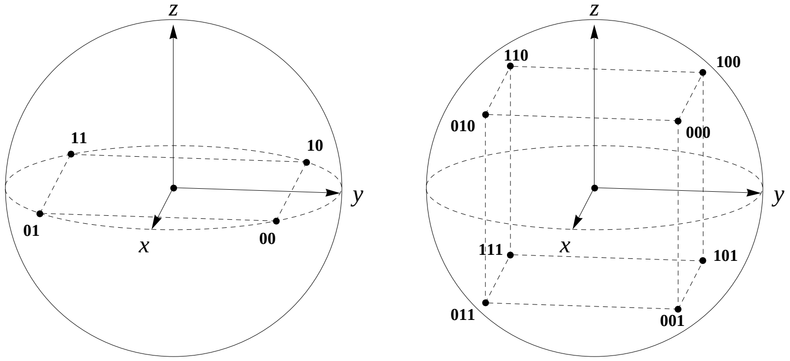

Figure 1: Bloch sphere representation of encodings for 2 ↦ 1 and 3 ↦ 1 QRACs.

It is also known that $n \overset{p}{\mapsto} m$ QRACs with $m > 1$ do not provide a good compression. In particular, given n and p, the following lower bound holds [1, 2]:

$$m \geq \bigl(1 - H(p)\bigr)n, \tag{1}$$

where $H(p) = -p \log p - (1-p)\log(1-p)$ is the binary entropy function.

Yao's principle

We extend the conventional model of random access codes with *shared randomness* (SR) that is accessible to both parties. For both classical and quantum RACs with SR we are interested in the *worst case* success probability. However, it is simpler to consider the *average case* success probability of a (deterministic) RACs *without* SR.

Let $\mathcal{S}$ be a classical (or quantum) $n \mapsto 1$ RAC with SR and $\mathcal{S}(x,i)$ be a stochastic variable that represents the outcome of $\mathcal{S}$ when $x \in \{0,1\}^n$ is encoded and the ith bit is recovered, where $i \in \{1,\dots,n\}$. Then the worst case success probability of the optimal RAC with SR is given by

$$\max_{\mathcal{S}} \min_{x,i} \Pr[\mathcal{S}(x,i) = x_i]. \tag{2}$$

However, if we fix some distribution μ over the input set $\{0,1\}^n \times \{1,\dots,n\}$, then the expected success probability of a classical (or quantum) $n \mapsto 1$ RAC $\mathcal{P}$ *without* SR is given by $\Pr_\mu[\mathcal{P}(x,i) = x_i]$. If the "hardest" input distribution is chosen as μ, then the expected success probability of the best RAC without SR for this distribution is

$$\min_{\mu} \max_{\mathcal{P}} \Pr_\mu[\mathcal{P}(x,i) = x_i]. \tag{3}$$

Yao's principle states that the quantities given in (2) and (3) are equal [8]:

$$\max_{\mathcal{S}} \min_{x,i} \Pr[\mathcal{S}(x,i) = x_i] = \min_{\mu} \max_{\mathcal{P}} \Pr_\mu[\mathcal{P}(x,i) = x_i]. \tag{4}$$

Note that both parties can randomize the input (x, i) by XORing it with the random string they share. In this way we show that the "hardest" input distribution for classical (and quantum) RACs is the uniform distribution over $\{0,1\}^n \times \{1, \ldots, n\}$.

Thus Yao's principle implies that the worst case success probability of a classical (or quantum) RAC with SR is the same as the average success probability of a classical (or quantum) RAC without SR on uniformly distributed input. In addition we show that for quantum RACs with SR without loss of generality we can consider only projective measurements, instead of the more general POVM measurements.

Quantum lower bound

We show that $n \overset{p}{\mapsto} 1$ QRAC with $p > 1/2$ is possible for any $n \geq 1$ if SR is allowed. In particular, we show that there exists $n \overset{p}{\mapsto} 1$ QRAC with SR such that

$$p \geq \frac{1}{2} + \sqrt{\frac{2}{3\pi n}}. \tag{5}$$

This lower bound is obtained by choosing the direction for each of the n projective measurements uniformly at random. The plot of (5) is shown on Fig. 2.

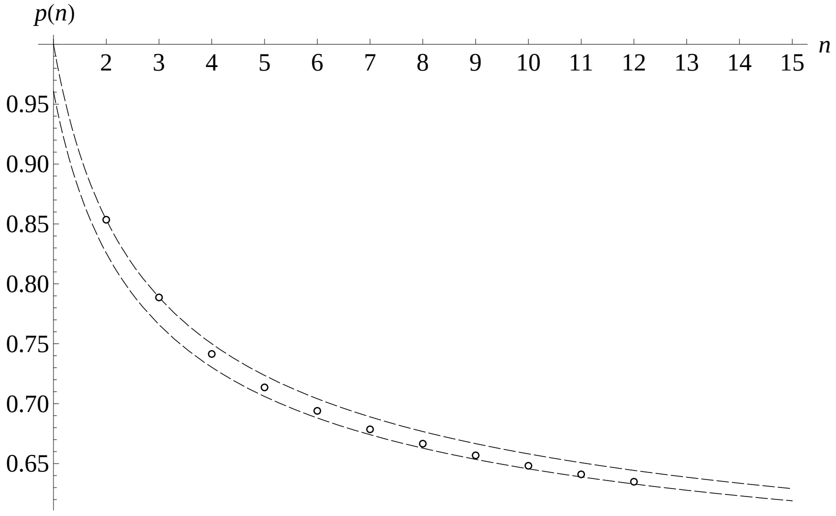

Figure 2: Success probabilities $p(n)$ of $n \mapsto 1$ QRACs with SR for several small values of n. Upper bound (6) and lower bound (5) correspond to dashed lines.

Explicit constructions

There are QRACs with SR that have higher success probability than (5). We give explicit constructions of such codes for several small values of n (success probabilities of these QRACs is shown in Fig. 2). An example for $n = 6$ is shown in Fig 3. Blue dots indicate the measurement directions, blue circles are orthogonal to these directions and correspond to states with equiprobable outcomes, but red dots show the states used for encoding.

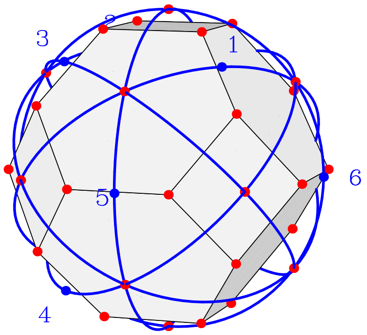

Figure 3: Bloch sphere representation of the $6 \mapsto 1$ QRAC with SR.

Quantum upper bound

It is not possible to reliably encode arbitrary many classical bits into 1 qubit using QRACs with SR. Indeed, we show that for any $n \overset{p}{\mapsto} 1$ QRAC with SR

$$p \leq \frac{1}{2} + \frac{1}{2\sqrt{n}} \tag{6}$$

(p approaches $1/2$ as n increases). This upper bound is obtained using a generalization of the parallelogram identity and is also shown on Fig. 2. The known $2 \overset{0.85}{\longmapsto} 1$ and $3 \overset{0.79}{\longmapsto} 1$ QRACs match this upper bound, since the measurements are performed along directions that are orthogonal in the Bloch sphere.

Classical random access codes with SR

We also study the classical counterpart of this model where n bits are encoded into 1 bit instead of 1 qubit and SR is used. We use Yao's principle to argue that the following classical $n \mapsto 1$ RAC with SR is optimal:

1. Alice XORs the input string with n random bits she shares with Bob, computes the majority and sends it to Bob.

2. If the ith bit is asked, Bob outputs the ith bit of the shared random string XORed with the received bit.

We use a combinatorial argument to compute the worst case success probability $p(n)$ of this code exactly. It turns out to be equal for $n = 2m$ and $n = 2m + 1$. In particular, we get

$$p(2m) = p(2m+1) = \frac{1}{2} + \frac{1}{2^{2m+1}}\binom{2m}{m}. \tag{7}$$

This function is shown in Fig. 4. Asymptotically we get

$$p \approx \frac{1}{2} + \frac{1}{\sqrt{2\pi n}}, \tag{8}$$

which is less than in the quantum case (see Fig. 5 for comparison of classical and quantum RACs).

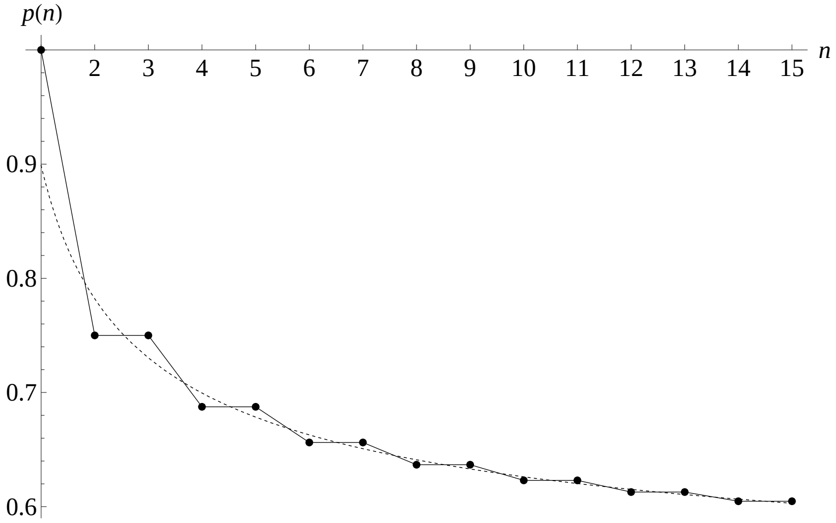

Figure 4: Exact probability of success $p(n)$ for optimal $n \mapsto 1$ classical RAC (solid line) and its approximate value (dotted line). These probabilities are given by equations (7) and (8), respectively.

Additional details

More details can be found in `arXiv:0810.2937v2`.

Supplementary materials are available on-line at
`http://home.lanet.lv/~sd20008/racs`

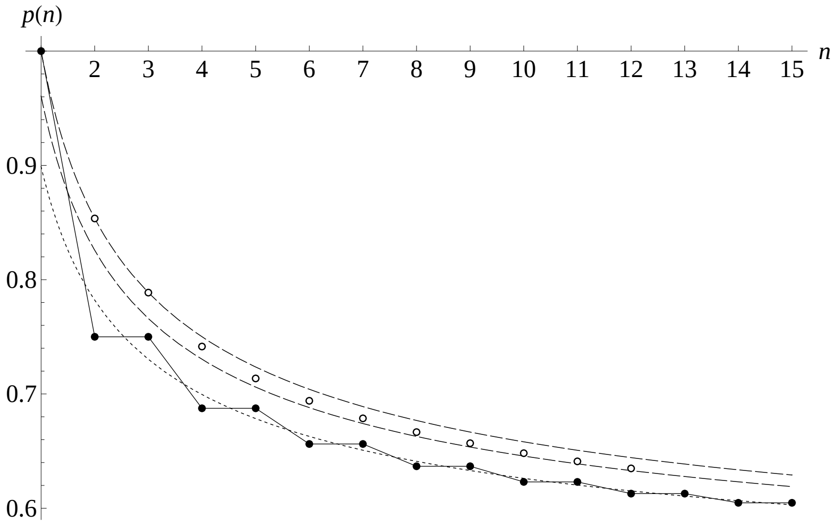

Figure 5: Comparison of success probabilities of classical and quantum RACs from Figs. 4 and 2, respectively. Black dots correspond to optimal classical RAC and dotted line shows the asymptotic behavior. Circles correspond to numerical QRACs and dashed lines to quantum upper and lower bounds, respectively.

References

[1] Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, Umesh Vazirani, "Dense Quantum Coding and Quantum Finite Automata," *Journal of the ACM*, vol. 49, no. 4, pp. 496–511, 2002. arXiv:quant-ph/9804043v2

[2] Ashwin Nayak, "Optimal lower bounds for quantum automata and random access codes," Proceedings of 40th IEEE symposium on Foundations of Computer Science (FOCS'99), pp. 369–376, 1999. arXiv:quant-ph/9904093v3

[3] Masahito Hayashi, Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, Shigeru Yamashita, "(4, 1)-Quantum Random Access Coding Does Not Exist," *New J. Phys.*, vol. 8, 129, 2006. arXiv:quant-ph/0604061v1

[4] Hartmut Klauck, "Lower bounds for quantum communication complexity," Proceedings of 42nd IEEE symposium on Foundations of Computer Science (FOCS'01), pp. 288, 2001. arXiv:quant-ph/0106160v3

[5] Iordanis Kerenidis, Ronald de Wolf, "Exponential Lower Bound for 2-Query Locally Decodable Codes via a Quantum Argument," *J. Comput. Syst. Sci.*, vol. 69, 3, pp. 395–420, 2004. arXiv:quant-ph/0208062v2

[6] Scott Aaronson, "Limitations of Quantum Advice and One-Way Communication," Proceedings of 19th Annual IEEE Conference on Computational Complexity (CCC'04), pp. 320–332, 2004. arXiv:quant-ph/0402095v4

[7] Scott Aaronson, "The Learnability of Quantum States", *Proc. Roy. Soc. London Ser. A*, vol. 463, no. 2088, pp. 3089–3114, 2007. `arXiv:quant-ph/0608142v3`

[8] Yao A.C., "Probabilistic computations: towards a unified measure of complexity," Proceedings 18th Annual IEEE Symposium on Foundations of Computer Science, October 1977, 222–227.