Quantum Random Access Codes with Shared Randomness

Andris Ambainis, Debbie Leung,
Laura Mancinska, Maris Ozols

We consider a communication method, where the sender encodes n classical bits into 1 qubit and sends it to the receiver who performs a certain measurement depending on which of the initial bits must be recovered. This procedure is called $n \overset{p}{\mapsto} 1$ quantum random access code (QRAC) where $p > 1/2$ is its worst case success probability. It is known that $2 \overset{0.85}{\longmapsto} 1$ and $3 \overset{0.79}{\longmapsto} 1$ QRACs (with no classical counterparts) exist [1] and that $4 \overset{p}{\mapsto} 1$ QRAC with $p > 1/2$ is not possible [2].

We extend this model with shared randomness (SR) that is accessible to both parties. Then $n \overset{p}{\mapsto} 1$ QRAC with SR and $p > 1/2$ exists for any $n \geq 1$. In particular, we show that

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

This lower bound is obtained by choosing the direction for each of the n projective measurements uniformly at random.

There are QRACs with SR that have higher success probability than (1). We give explicit constructions of such codes for several small values of n. An example for $n = 6$ is shown in Fig 1. 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.

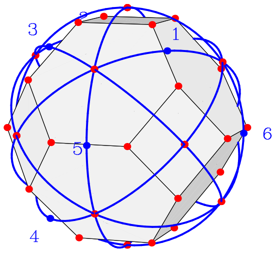

Figure 1: Bloch sphere representation of the $6 \mapsto 1$ QRAC with SR.

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

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

(p approaches 1/2 as n increases). This upper bound is obtained using a generalization of the parallelogram identity. 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.

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 of this code and show that asymptotically

$$p \approx \frac{1}{2} + \frac{1}{\sqrt{2\pi n}}, \tag{3}$$

which is less than in the quantum case.

More details can be found in arXiv:0810.2937v2.

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

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] 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