Quantum Random Access Codes with Shared Randomness

Andris Ambainis, Debbie Leung, Laura Mancinska, Maris Ozols

University of Waterloo & Institute for Quantum Computing

Random Access Codes

Random access code (RAC) stands for encoding n bits into m and be able to recover any one of the initial bits with probability at least p. Such code is characterized by symbol "$n \overset{p}{\mapsto} m$". We consider only the case when $m = 1$.

Classical and Quantum RACs

Classical RACs: There are two parties – Alice and Bob. Alice is asked to encode some classical n-bit string into 1 *bit* and send this bit to Bob. We want Bob to be able to recover any one of the n initial bits with high success probability.

Quantum RACs (QRACs): Alice must encode her classical n-bit message into 1 *qubit* and send it to Bob. He performs some measurement on the received qubit to extract the required bit (the measurement that is used depends on which bit is needed).

Known RACs

There are $2 \overset{0.85}{\longmapsto} 1$ and $3 \overset{0.79}{\longmapsto} 1$ QRACs (with no classical counterparts) [1], and $4 \overset{p}{\mapsto} 1$ QRAC with $p > 1/2$ is not possible [2].

Shared Randomness

We allow both parties to cooperate – Alice and Bob can use *shared randomness* (SR) to agree on which strategy to use.

Optimal Classical RAC with SR

Using *Yao's principle* we argue that the following classical $n \overset{p}{\mapsto} 1$ RAC with shared randomness 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 success probability p of this code an show that asymptotically

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

Quantum Lower Bound

If shared randomness is allowed, then $n \overset{p}{\mapsto} 1$ QRAC with SR and $p > 1/2$ exists for any $n \geq 1$. In particular, we show that

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

by choosing each of the n projective measurements *uniformly at random*. This is better than the optimal classical RAC with SR.

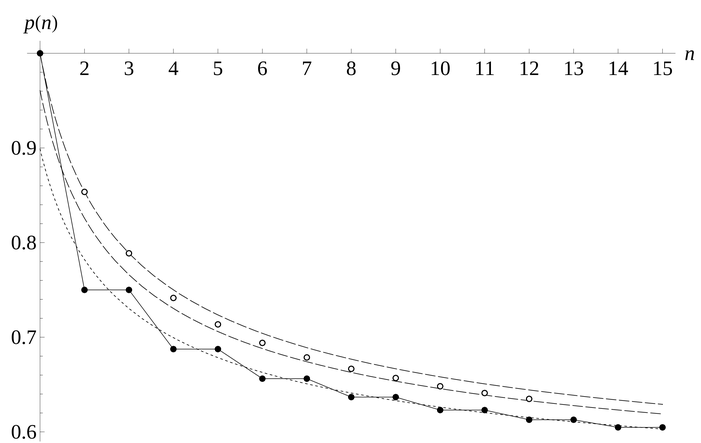
Quantum Upper Bound

It is *not* possible to reliably encode arbitrary many classical bits into 1 qubit using QRACs. For any $n \overset{p}{\mapsto} 1$ QRAC with SR

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

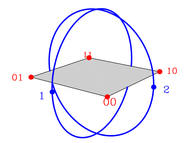
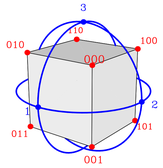
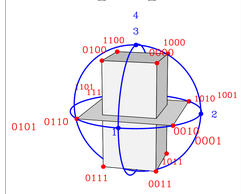
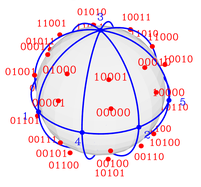
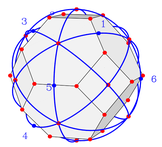
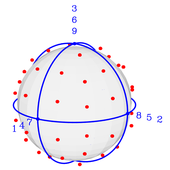
This upper bound is obtained using a generalization of the *parallelogram identity*. The known $2 \overset{0.85}{\longmapsto} 1$ and $3 \overset{0.79}{\longmapsto} 1$ QRACs match this upper bound, since the measurements are performed along directions that are orthogonal in the Bloch sphere.

Comparison of Classical and Quantum RACs with SR

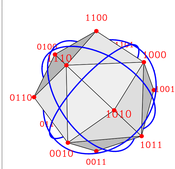
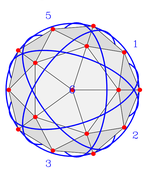
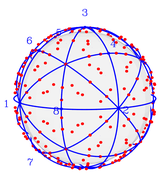
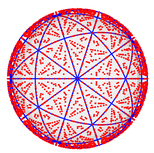


Success probabilities of classical and quantum RACs with SR. Black dots correspond to optimal classical RAC with SR and dotted line shows the asymptotic behavior. Circles correspond to numerical QRACs with SR and dashed lines to quantum upper and lower bounds, respectively.

Numerical QRACs

$2 \overset{p}{\mapsto} 1$  $p \approx 0.8535533906$	$3 \overset{p}{\mapsto} 1$  $p \approx 0.7886751346$	$4 \overset{p}{\mapsto} 1$  $p \approx 0.7414814566$
$5 \overset{p}{\mapsto} 1$  $p \approx 0.7135779205$	$6 \overset{p}{\mapsto} 1$  $p \approx 0.6940463870$	$9 \overset{p}{\mapsto} 1$  $p \approx 0.6568927813$

Symmetric QRACs

$4 \overset{p}{\mapsto} 1$  $p \approx 0.7332531755$	$6 \overset{p}{\mapsto} 1$  $p \approx 0.6940418856$	$9 \overset{p}{\mapsto} 1$  $p \approx 0.6563927998$	$15 \overset{p}{\mapsto} 1$  $p \approx 0.6201829084$

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