Random Access Codes

Laura Mančinska & Māris Ozols

University of Latvia

Our supervisors:
Andris Ambainis & Debbie Leung

Random access codes (RAC)

$n \overset{p}{\mapsto} m$ random access code

- Alice encodes n bits into m and sends them to Bob ($n > m$).
- Bob must be able to restore any of the n initial bits with probability $\geq p$.

Random access codes (RAC)

$n \overset{p}{\mapsto} m$ random access code

- Alice encodes n bits into m and sends them to Bob ($n > m$).
- Bob must be able to restore any of the n initial bits with probability $\geq p$.

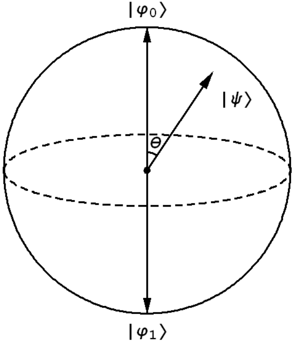
We will look at two kinds of RACs

- **Classical RAC** - Alice encodes n classical bits into 1 classical bit.
- **QRAC** - Alice encodes n classical bits into 1 qubit. After recovery of one bit the quantum state collapses and other bits may be lost.

Bloch sphere

As Bob receives only one qubit we can use Bloch sphere to visualize the states in which Alice encodes different classical bit strings.

$$\Pr[|\psi\rangle \text{ collapses to } |\varphi_0\rangle] = \cos^2\frac{\theta}{2} = \frac{1+\cos\theta}{2}$$



$$|\psi\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix}$$

Previous results on RACs

Pure strategies

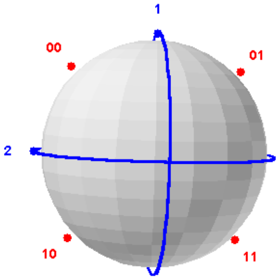
Some specific QRACs are known for the case when only pure strategies are used. That means:

- Alice prepares pure state.
- Bob measures using projective measurements (no POVMs).
- Shared randomness is not allowed.

Known QRACs

$2 \overset{p}{\mapsto} 1$ code

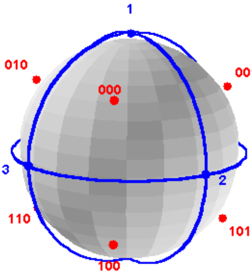
There exists $2 \overset{p}{\mapsto} 1$ code where $p = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$.
This code is optimal. [quant-ph/9804043]



Known QRACs

$3 \overset{p}{\mapsto} 1$ code

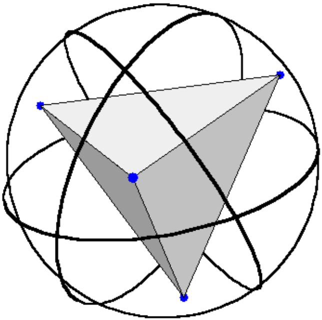
There exists $3 \overset{p}{\mapsto} 1$ code where $p = \frac{1}{2} + \frac{1}{2\sqrt{3}} \approx 0.79$.
This code is optimal. [I.L. Chuang]



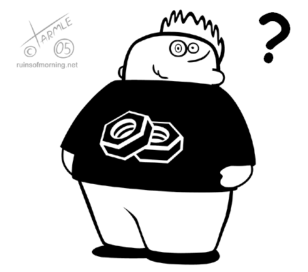
Known QRACs

$4 \overset{p}{\mapsto} 1$ code

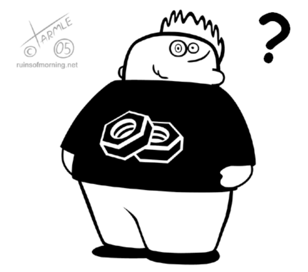
There does not exist $4 \overset{p}{\mapsto} 1$ for $p > \frac{1}{2}$.
Main idea - it is not possible to cut the surface of a sphere into 16 parts with 4 planes. [quant-ph/0604061]



What can we do now?



What can we do now?



Introduce all kinds of randomness (shared randomness will be the most useful).

RACs with shared randomness

Yao's principle

$$\min_{\mu} \max_{D} \Pr_{\mu}[D(x) = f(x)] = \max_{A} \min_{x} \Pr[A(x) = f(x)]$$

- f - some function we want to compute.
- $\Pr_{\mu}[D(x) = f(x)]$ - probability of success when arguments of deterministic algorithm D are distributed according to μ.
- $\Pr[A(x) = f(x)]$ - probability of success of probabilistic algorithm A for argument x.

How to obtain upper and lower bounds?

Upper bound

If we find some distribution μ_0 that seems to be "hard" for all deterministic algorithms and show that

$$\max_D \Pr_{\mu_0}[D(x) = f(x)] = p,$$

then according to Yao's principle we can upper bound the success probability of probabilistic algorithms by p.

How to obtain upper and lower bounds?

Upper bound

If we find some distribution μ_0 that seems to be “hard” for all deterministic algorithms and show that

$$\max_D \Pr_{\mu_0}[D(x) = f(x)] = p,$$

then according to Yao’s principle we can upper bound the success probability of probabilistic algorithms by p.

Lower bound

If we have a deterministic RAC D_0 for which $\Pr_{\mu_0}[D_0(x) = f(x)] = p$, then we can transform it into probabilistic algorithm A_0 for which $\min_x \Pr[A_0(x) = f(x)] = p$. The main idea is to use shared random string in order to simulate uniform distribution.

Optimal classical RAC

According to Yao's principle, we can consider only deterministic strategies. For each bit there are only four possible decoding functions: 0, 1, x, $\mathrm{NOT}\, x$.

Optimal classical RAC

According to Yao's principle, we can consider only deterministic strategies. For each bit there are only four possible decoding functions: 0, 1, x, $\mathrm{NOT}\,x$.

Optimal decoding

There is an optimal classical RAC in such form that:

Optimal classical RAC

According to Yao's principle, we can consider only deterministic strategies. For each bit there are only four possible decoding functions: 0, 1, x, $\mathrm{NOT}\, x$.

Optimal decoding

There is an optimal classical RAC in such form that:

- trivial decoding strategies 0 and 1 are not used for any bits,

Optimal classical RAC

According to Yao's principle, we can consider only deterministic strategies. For each bit there are only four possible decoding functions: 0, 1, x, $\mathrm{NOT}\,x$.

Optimal decoding

There is an optimal classical RAC in such form that:

- trivial decoding strategies 0 and 1 are not used for any bits,
- decoding strategy $\mathrm{NOT}\,x$ is not used for any bit,

Optimal classical RAC

According to Yao's principle, we can consider only deterministic strategies. For each bit there are only four possible decoding functions: 0, 1, x, $\mathrm{NOT}\, x$.

Optimal decoding

There is an optimal classical RAC in such form that:

- trivial decoding strategies 0 and 1 are not used for any bits,
- decoding strategy $\mathrm{NOT}\, x$ is not used for any bit,
- Bob says the received bit no matter which bit is asked.

Optimal classical RAC

According to Yao's principle, we can consider only deterministic strategies. For each bit there are only four possible decoding functions: 0, 1, x, $\mathrm{NOT}\, x$.

Optimal decoding

There is an optimal classical RAC in such form that:

- trivial decoding strategies 0 and 1 are not used for any bits,
- decoding strategy $\mathrm{NOT}\, x$ is not used for any bit,
- Bob says the received bit no matter which bit is asked.

Optimal encoding

Encode the majority of bits.

Exact probability of success

$$p(2m) = \frac{1}{2m \cdot 2^{2m}} \left(2 \sum_{i=m+1}^{2m} \binom{2m}{i} i + \binom{2m}{m} m \right)$$

$$p(2m+1) = \frac{1}{(2m+1) \cdot 2^{2m+1}} \left(2 \sum_{i=m+1}^{2m+1} \binom{2m+1}{i} i \right)$$

Exact probability of success

$$p(2m) = \frac{1}{2m \cdot 2^{2m}} \left(2 \sum_{i=m+1}^{2m} \binom{2m}{i} i + \binom{2m}{m} m \right)$$

$$p(2m+1) = \frac{1}{(2m+1) \cdot 2^{2m+1}} \left(2 \sum_{i=m+1}^{2m+1} \binom{2m+1}{i} i \right)$$

Magic formula

$$\sum_{i=m+1}^{2m} \binom{2m}{i} i = m \cdot 2^{2m-1}$$

Exact probability of success

$$p(2m) = \frac{1}{2m \cdot 2^{2m}} \left(2 \sum_{i=m+1}^{2m} \binom{2m}{i} i + \binom{2m}{m} m \right)$$

$$p(2m+1) = \frac{1}{(2m+1) \cdot 2^{2m+1}} \left(2 \sum_{i=m+1}^{2m+1} \binom{2m+1}{i} i \right)$$

Magic formula

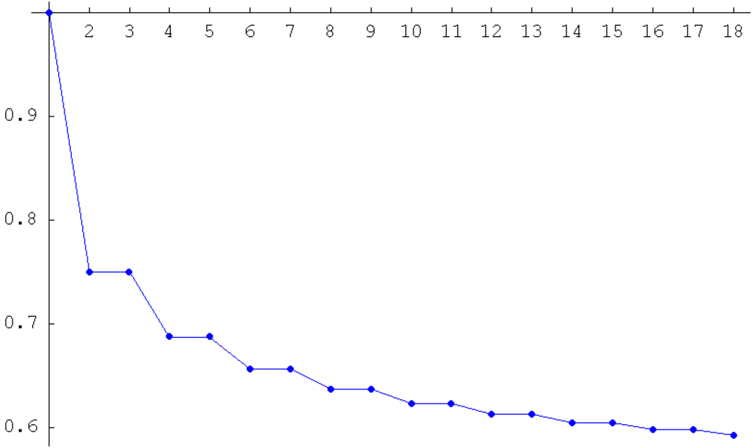
$$\sum_{i=m+1}^{2m} \binom{2m}{i} i = m \cdot 2^{2m-1}$$

Final formula

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

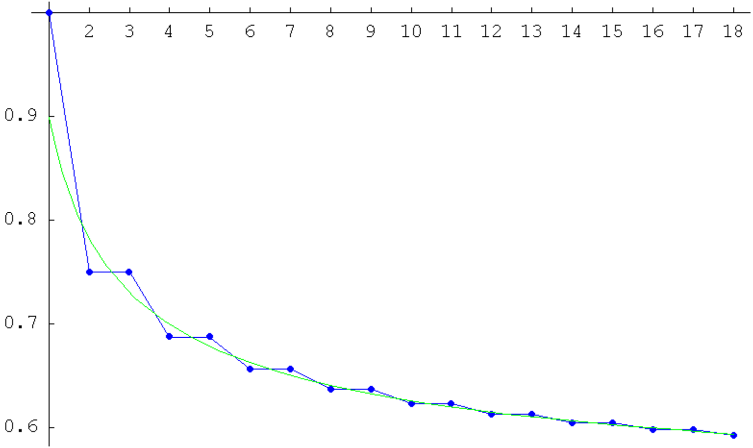
Bounds for the probability of success

Exact probability $p(2m) = p(2m+1) = \frac{1}{2} + \binom{2m}{m}/2^{2m+1}$.



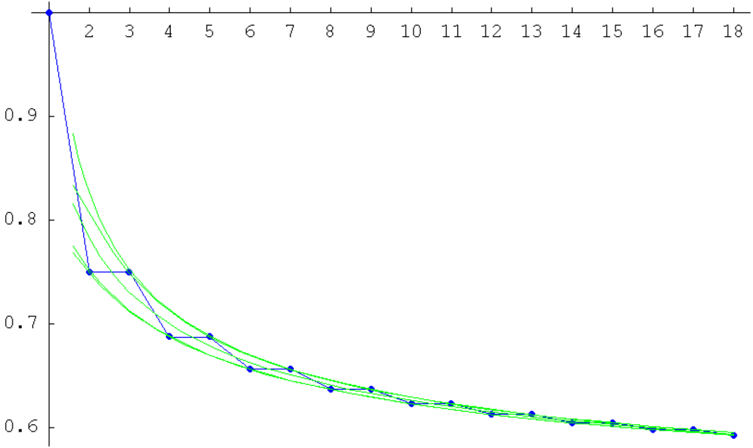
Bounds for the probability of success

Using Stirling's approximation we get $p(n) = \frac{1}{2} + 1/\sqrt{2\pi n}$.



Bounds for the probability of success

Using inequalities $\sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n}}$.



Optimal quantum encoding

Let $\vec{v}_i$ be the measurement for the i-th bit and $\vec{r}_x$ be the encoding of string $x \in \{0,1\}^n$. The average success probability is given by

$$p = \frac{1}{2^n n} \sum_{x \in \{0,1\}^n} \sum_{i=1}^{n} \frac{1 + (-1)^{x_i} \vec{v}_i \cdot \vec{r}_x}{2}.$$

In order to maximize the average probability, we must consider

$$\max_{\{\vec{v}_i\},\{\vec{r}_x\}} \sum_{x \in \{0,1\}^n} \vec{r}_x \sum_{i=1}^{n} (-1)^{x_i} \vec{v}_i = \max_{\{\vec{v}_i\}} \sum_{x \in \{0,1\}^n} \left\| \sum_{i=1}^{n} (-1)^{x_i} \vec{v}_i \right\|.$$

For given measurements $\vec{v}_i$ the optimal encoding for string x is unit vector in direction $\sum_{i=1}^{n} (-1)^{x_i} \vec{v}_i$.
If $\forall i,j : \vec{v}_i = \vec{v}_j$ we get optimal classical encoding.

Upper bound for QRACs

Using the inequality of arithmetic and geometric means $\sqrt{a \cdot b} \leq \frac{a+b}{2}$ we can estimate the square of the previous sum from above:

$$\left(\sum_{x \in \{0,1\}^n} \left\| \sum_{i=1}^{n} (-1)^{x_i} \vec{v}_i \right\| \right)^2 \leq n \cdot 2^{2n}$$

and afterwards easily gain upper bound for average success probability:

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

Lower bound for QRACs

Suppose that in each round Alice and Bob use the shared random string to agree on some random measurements $\vec{v}_i$ and the corresponding optimal encoding vectors $\vec{r}_x$. To find the average success probability we must consider this expectation

$$\mathop{E}_{\{\vec{v}_i\}}\left(\sum_{x\in\{0,1\}^n}\left\|\sum_{i=1}^{n}(-1)^{x_i}\vec{v}_i\right\|\right) = 2^n \cdot \mathop{E}_{\{\vec{v}_i\}}\left(\left\|\sum_{i=1}^{n}\vec{v}_i\right\|\right).$$

This problem is equivalent to problem of finding the average distance traveled after n unit steps where the direction of each step is chosen at random.

Random walk

Chandrasekhar gives the probability density to arrive at point $\vec{R}$ after performing $n \gg 1$ steps of random walk:

$$W(\vec{R}) = \left(\frac{3}{2\pi n}\right)^{3/2} e^{-3\left\|\vec{R}\right\|^2/2n}.$$

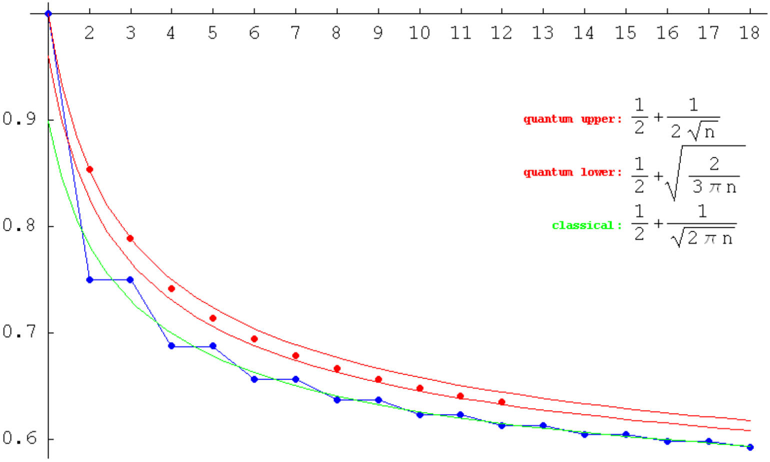
Therefore the average distance traveled will be:

$$\int_0^\infty 4\pi R^2 \cdot R \cdot W(R) \cdot dR = 2\sqrt{\frac{2n}{3\pi}}.$$

It gives the expected success probability if measurements are chosen at random:

$$p(n) = \frac{1}{2} + \sqrt{\frac{2}{3\pi n}}.$$

All bounds


2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
0.9
0.8
0.7
0.6
quantum upper: $\frac{1}{2}+\frac{1}{2\sqrt{n}}$
quantum lower: $\frac{1}{2}+\sqrt{\frac{2}{3\pi n}}$
classical: $\frac{1}{2}+\frac{1}{\sqrt{2\pi n}}$

Some QRACs obtained by numerical optimization

http://home.lanet.lv/∼sd20008/RAC/RACs.htm

Thanks

Great thanks goes to Andris and Debbie!