Quantum Random Access Codes with Shared Randomness

Maris Ozols, Laura Mancinska,
Andris Ambainis, Debbie Leung

University of Waterloo, IQC

June 20, 2008

Outline

Introduction

Random access codes (RACs)

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

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

Random access codes (RACs)

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

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

In this talk

1. We will consider only $n \overset{p}{\mapsto} 1$ codes ($m = 1$).
2. We will compare classical and quantum RACs:

Random access codes (RACs)

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

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

In this talk

1. We will consider only $n \overset{p}{\mapsto} 1$ codes ($m = 1$).
2. We will compare classical and quantum RACs:
   - *classical* RAC: Alice encodes n classical bits into 1 classical bit,
   - *quantum* RAC: Alice encodes n classical bits into 1 qubit.

Random access codes (RACs)

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

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

In this talk

1. We will consider only $n \overset{p}{\mapsto} 1$ codes ($m = 1$).
2. We will compare classical and quantum RACs:
   - *classical* RAC: Alice encodes n classical bits into 1 classical bit,
   - *quantum* RAC: Alice encodes n classical bits into 1 qubit.

In quantum case the state collapses after recovery of one bit, so we may loose the other bits.

Classical random access codes with shared randomness

Classical RACs

Classical versus quantum

Let us first consider classical RACs with shared randomness (SR) so that later on we can compare them with quantum RACs with SR.

Classical RACs

Classical versus quantum

Let us first consider classical RACs with shared randomness (SR) so that later on we can compare them with quantum RACs with SR.

Complexity measures

We are interested in the worst case success probability of RAC. However, it is simpler to consider the average case success probability. In the next few slides we will see that there is a way how to switch between these two.

Different kinds of classical RACs

Definition

A *pure classical* $n \mapsto 1$ *RAC* is an ordered tuple $(E, D_1, \ldots, D_n)$ that consists of *encoding function* $E : \{0,1\}^n \mapsto \{0,1\}$ and n *decoding functions* $D_i : \{0,1\} \mapsto \{0,1\}$.

Different kinds of classical RACs

Definition

A *pure classical* $n \mapsto 1$ *RAC* is an ordered tuple $(E, D_1, \ldots, D_n)$ that consists of *encoding function* $E : \{0,1\}^n \mapsto \{0,1\}$ and n *decoding functions* $D_i : \{0,1\} \mapsto \{0,1\}$.

Definition

A *mixed classical* $n \mapsto 1$ *RAC* is an ordered tuple $(P_E, P_{D_1}, \ldots, P_{D_n})$ of probability distributions. P_E is a distribution over encoding functions and P_{D_i} over decoding functions.

Different kinds of classical RACs

Definition

A *pure classical* $n \mapsto 1$ *RAC* is an ordered tuple $(E, D_1, \ldots, D_n)$ that consists of *encoding function* $E : \{0,1\}^n \mapsto \{0,1\}$ and n *decoding functions* $D_i : \{0,1\} \mapsto \{0,1\}$.

Definition

A *classical* $n \mapsto 1$ *RAC with shared randomness* (SR) is a probability distribution over pure classical RACs.

Playing with randomness

Yao's principle

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

The following notations are used:

- f - some function we want to compute,
- $\Pr_{\mu}[\mathcal{D}(x) = f(x)]$ – success probability of deterministic algorithm $\mathcal{D}$ with input x distributed according to μ,
- $\Pr[\mathcal{A}(x) = f(x)]$ – success probability of probabilistic algorithm $\mathcal{A}$ on input x.

Obtaining upper and lower bounds

Upper bound

We can take any input distribution μ_0 that seems to be "hard" for deterministic algorithms and find p such that

$$\max_{\mathcal{D}} \Pr_{\mu_0}[\mathcal{D}(x) = f(x)] \leq p$$

Then according to Yao's principle the worst case success probability of the best probabilistic algorithm is upper bounded by p.

Obtaining upper and lower bounds

Upper bound

We can take any input distribution μ_0 that seems to be "hard" for deterministic algorithms and find p such that

$$\max_{\mathcal{D}} \Pr_{\mu_0}[\mathcal{D}(x) = f(x)] \leq p$$

Then according to Yao's principle the worst case success probability of the best probabilistic algorithm is upper bounded by p.

Lower bound

Any pure RAC with average case success probability p can be turned into a RAC with shared randomness having worst case success probability p by jointly randomizing the input (requires $n + \log n$ shared random bits). Thus we can obtain a lower bound by randomizing any pure RAC.

The “hardest” input distribution

Matching upper and lower bounds

The lower bound was obtained by simulating uniform input distribution. Since any input distribution μ_0 can be used for the upper bound, we can use the uniform distribution as well – then both bounds will match. Hence for pure random access codes uniform input distribution is the “hardest”.

The “hardest” input distribution

Matching upper and lower bounds

The lower bound was obtained by simulating uniform input distribution. Since any input distribution μ_0 can be used for the upper bound, we can use the uniform distribution as well – then both bounds will match. Hence for pure random access codes uniform input distribution is the “hardest”.

Conclusion

Best pure RAC for uniformly distributed input (average success prob.) $\overset{\text{input}}{\underset{\text{randomization}}{\Longrightarrow}}$ Best RAC with SR (worst case success prob.)

Optimal classical RAC

Optimal decoding

Optimal classical RAC

Optimal decoding

- For each bit there are only four possible decoding functions: $D(x) = 0$, $D(x) = 1$, $D(x) = x$, $D(x) = \mathrm{NOT}\, x$.

Optimal classical RAC

Optimal decoding

- For each bit there are only four possible decoding functions: $D(x) = 0$, $D(x) = 1$, $D(x) = x$, $D(x) = \mathrm{NOT}\, x$.
- We cannot make things worse if we *do not* use constant decoding functions 0 and 1 for any bits.

Optimal classical RAC

Optimal decoding

- For each bit there are only four possible decoding functions: $D(x) = 0$, $D(x) = 1$, $D(x) = x$, $D(x) = \mathrm{NOT}\, x$.
- We cannot make things worse if we *do not* use constant decoding functions 0 and 1 for any bits.
- We can always avoid using decoding function $\mathrm{NOT}\, x$ (by negating the input before encoding).

Optimal classical RAC

Optimal decoding

- For each bit there are only four possible decoding functions: $D(x) = 0$, $D(x) = 1$, $D(x) = x$, $D(x) = \mathrm{NOT}\, x$.
- We cannot make things worse if we *do not* use constant decoding functions 0 and 1 for any bits.
- We can always avoid using decoding function $\mathrm{NOT}\, x$ (by negating the input before encoding).

Hence there is an optimal joint strategy such that Bob always replays the received bit no matter which bit is actually asked.

Optimal classical RAC

Optimal decoding

- For each bit there are only four possible decoding functions: $D(x) = 0$, $D(x) = 1$, $D(x) = x$, $D(x) = \mathrm{NOT}\, x$.
- We cannot make things worse if we *do not* use constant decoding functions 0 and 1 for any bits.
- We can always avoid using decoding function $\mathrm{NOT}\, x$ (by negating the input before encoding).

Hence there is an optimal joint strategy such that Bob always replays the received bit no matter which bit is actually asked.

Optimal encoding

Once Alice knows that Bob's decoding function is $D(x) = x$, she simply encodes the majority of all bits.

Exact probability of success

Counting

Let us choose a string from $\{0, 1\}^n$ uniformly at random and mark one bit at a random position.

Exact probability of success

Counting

Let us choose a string from $\{0,1\}^n$ uniformly at random and mark one bit at a random position. What is the probability that the value of the marked bit equals the majority of all bits?

Exact probability of success

Counting

Let us choose a string from $\{0,1\}^n$ uniformly at random and mark one bit at a random position. What is the probability that the value of the marked bit equals the majority of all bits?

Answer

Exactly:

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

Exact probability of success

Counting

Let us choose a string from $\{0,1\}^n$ uniformly at random and mark one bit at a random position. What is the probability that the value of the marked bit equals the majority of all bits?

Answer

Exactly:

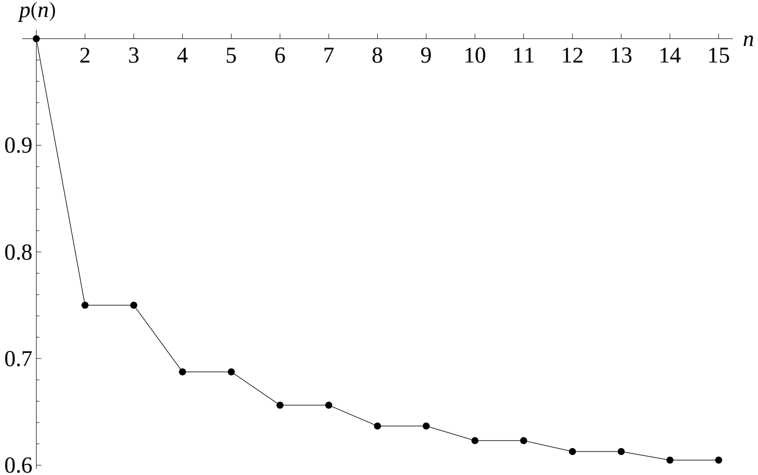
$$p(2m) = p(2m+1) = \frac{1}{2} + \frac{1}{2^{2m+1}}\binom{2m}{m}$$

Using Stirling's approximation:

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

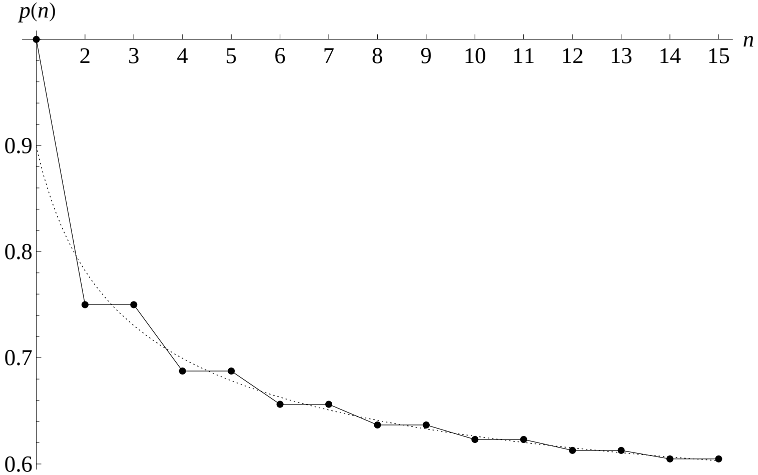
Probability of success

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



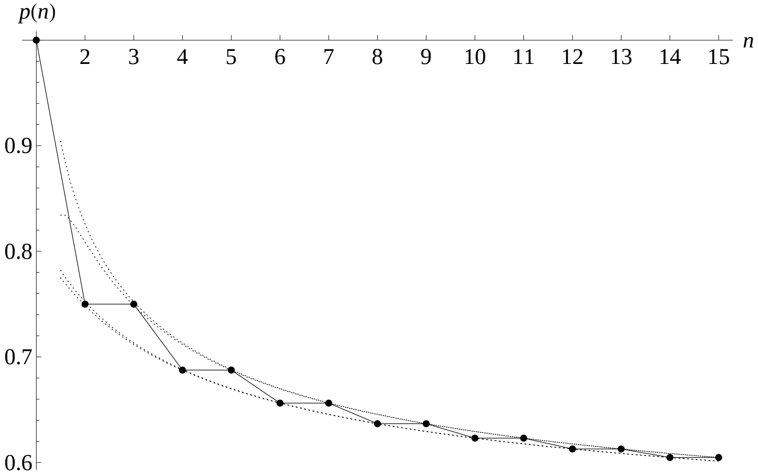
Probability of success

Using Stirling's approximation: $p(n) \approx \frac{1}{2} + 1/\sqrt{2\pi n}$



Probability of success

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



Quantum random access codes with shared randomness

Bloch sphere

Alice encodes a classical bit string into a qubit state and sends it to Bob. We will use the Bloch sphere to visualize these states.

Bloch sphere

Alice encodes a classical bit string into a qubit state and sends it to Bob. We will use the Bloch sphere to visualize these states.

Bloch vector

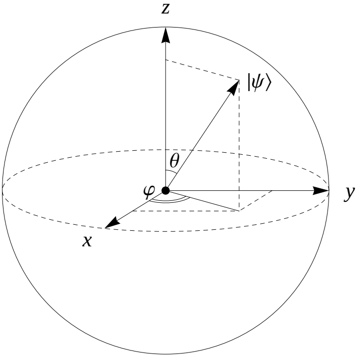
$$|\psi\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} \end{pmatrix}$$

$0 \leq \theta \leq \pi$, $0 \leq \varphi < 2\pi$

Bloch sphere

Alice encodes a classical bit string into a qubit state and sends it to Bob. We will use the Bloch sphere to visualize these states.

Bloch vector



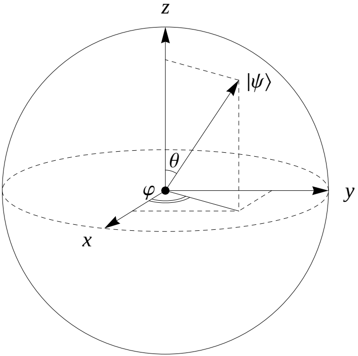
$$|\psi\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} \end{pmatrix}$$

$0 \leq \theta \leq \pi$, $0 \leq \varphi < 2\pi$

Bloch sphere

Alice encodes a classical bit string into a qubit state and sends it to Bob. We will use the Bloch sphere to visualize these states.

Bloch vector



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

$$0 \leq \theta \leq \pi,\ 0 \leq \varphi < 2\pi$$

$$\Updownarrow$$

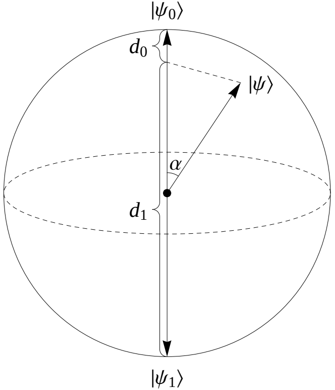
$$\vec{r} = (x, y, z)$$

$$\begin{cases} x = \sin\theta\cos\varphi \\ y = \sin\theta\sin\varphi \\ z = \cos\theta \end{cases}$$

Bloch sphere

Alice encodes a classical bit string into a qubit state and sends it to Bob. We will use the Bloch sphere to visualize these states.

Measurement

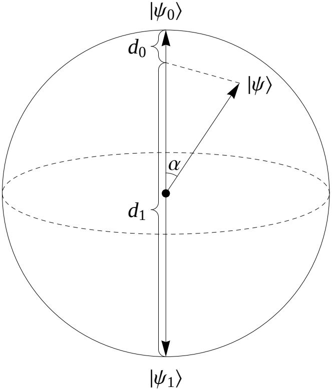


$$|\langle\psi_1|\psi_2\rangle|^2 = \frac{1}{2}(1 + \vec{r}_1 \cdot \vec{r}_2)$$

Bloch sphere

Alice encodes a classical bit string into a qubit state and sends it to Bob. We will use the Bloch sphere to visualize these states.

Measurement



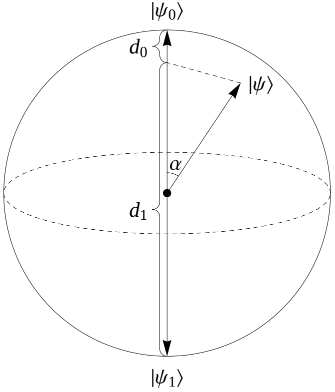
$$|\langle\psi_1|\psi_2\rangle|^2 = \frac{1}{2}(1 + \vec{r}_1 \cdot \vec{r}_2)$$

$\Pr[|\psi_0\rangle$ given $|\psi\rangle]$

Bloch sphere

Alice encodes a classical bit string into a qubit state and sends it to Bob. We will use the Bloch sphere to visualize these states.

Measurement



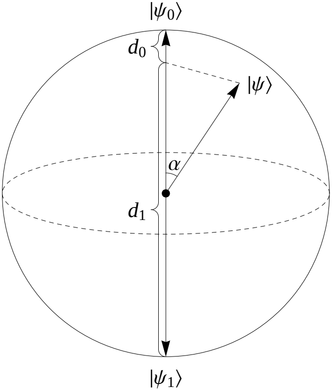
$$|\langle\psi_1|\psi_2\rangle|^2 = \frac{1}{2}(1 + \vec{r}_1 \cdot \vec{r}_2)$$

$$\Pr[|\psi_0\rangle \text{ given } |\psi\rangle] = |\langle\psi_0|\psi\rangle|^2$$

Bloch sphere

Alice encodes a classical bit string into a qubit state and sends it to Bob. We will use the Bloch sphere to visualize these states.

Measurement



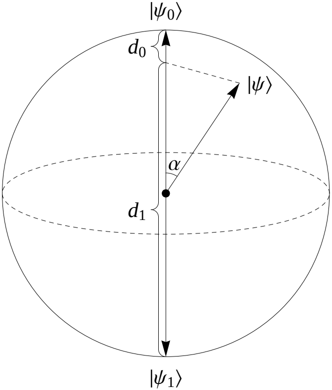
$$|\langle\psi_1|\psi_2\rangle|^2 = \frac{1}{2}(1 + \vec{r}_1 \cdot \vec{r}_2)$$

$$\begin{aligned}\Pr[|\psi_0\rangle \text{ given } |\psi\rangle] &= |\langle\psi_0|\psi\rangle|^2 \\ &= \frac{1+\cos\alpha}{2}\end{aligned}$$

Bloch sphere

Alice encodes a classical bit string into a qubit state and sends it to Bob. We will use the Bloch sphere to visualize these states.

Measurement



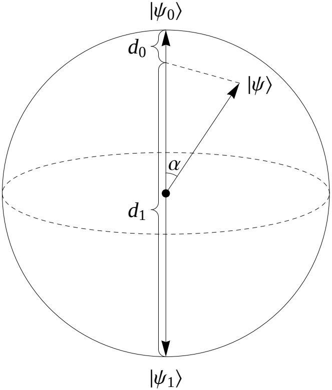
$$|\langle\psi_1|\psi_2\rangle|^2 = \frac{1}{2}(1 + \vec{r}_1 \cdot \vec{r}_2)$$

$$\begin{aligned}\Pr[|\psi_0\rangle \text{ given } |\psi\rangle] &= |\langle\psi_0|\psi\rangle|^2 \\ &= \frac{1+\cos\alpha}{2} = \frac{d_1}{2}\end{aligned}$$

Bloch sphere

Alice encodes a classical bit string into a qubit state and sends it to Bob. We will use the Bloch sphere to visualize these states.

Measurement



$$|\langle\psi_1|\psi_2\rangle|^2 = \frac{1}{2}(1 + \vec{r}_1 \cdot \vec{r}_2)$$

$$\Pr[|\psi_0\rangle \text{ given } |\psi\rangle] = |\langle\psi_0|\psi\rangle|^2 = \frac{1+\cos\alpha}{2} = \frac{d_1}{2}$$

$$\Pr[|\psi_1\rangle \text{ given } |\psi\rangle] = |\langle\psi_1|\psi\rangle|^2 = \frac{1-\cos\alpha}{2} = \frac{d_0}{2}$$

Known results

Pure strategies

Only two specific QRACs are known when *pure quantum strategies* are allowed. That means:

1. Alice prepares a pure state,
2. Bob uses a projective measurement (not a POVM),
3. the worst case success probability must be at least $\frac{1}{2}$.

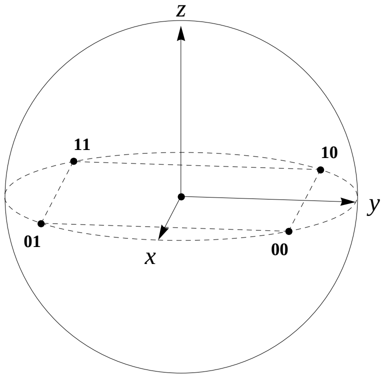
Note: shared randomness is not allowed.

Known QRACs

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

There is a $2 \overset{p}{\mapsto} 1$ code with $p = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$.

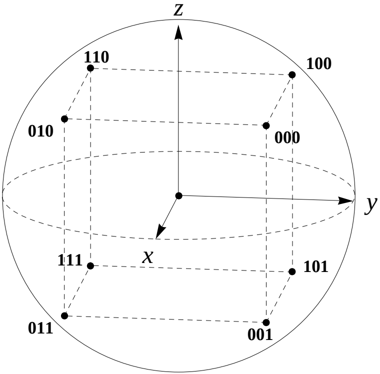
This code is optimal. [quant-ph/9804043]



Known QRACs

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

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



Known QRACs

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

There is no $4 \overset{p}{\mapsto} 1$ code for $p > \frac{1}{2}$.

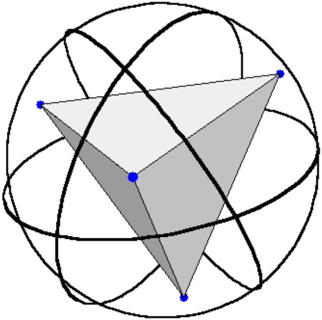
Proof idea – it is not possible to cut the surface of the Bloch sphere into 16 parts with 4 planes passing through its center. [quant-ph/0604061]

Known QRACs

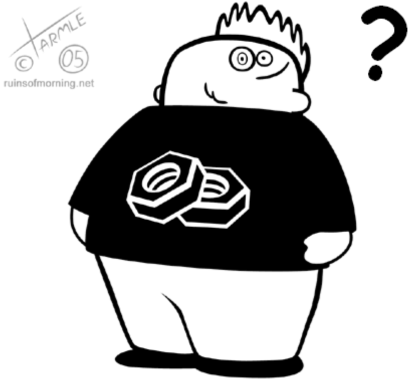
$4 \overset{p}{\mapsto} 1$ code

There is no $4 \overset{p}{\mapsto} 1$ code for $p > \frac{1}{2}$.

Proof idea – it is not possible to cut the surface of the Bloch sphere into 16 parts with 4 planes passing through its center. `[quant-ph/0604061]`



What can we do about this?



What can we do about this?

Use shared randomness!

Different kinds of quantum RACs

Definition

Pure quantum $n \mapsto 1$ *RAC* is an ordered tuple $(E, M_1, \ldots, M_n)$ that consists of *encoding function* $E : \{0,1\}^n \mapsto \mathbb{C}^2$ and n orthogonal measurements: $M_i = \left\{ \left| \psi_0^i \right\rangle, \left| \psi_1^i \right\rangle \right\}$.

Different kinds of quantum RACs

Definition

Pure quantum $n \mapsto 1$ *RAC* is an ordered tuple $(E, M_1, \ldots, M_n)$ that consists of *encoding function* $E : \{0,1\}^n \mapsto \mathbb{C}^2$ and n orthogonal measurements: $M_i = \left\{ \left|\psi_0^i\right\rangle, \left|\psi_1^i\right\rangle \right\}$.

Definition

Mixed quantum $n \mapsto 1$ *RAC* is an ordered tuple $(P_E, P_{M_1}, \ldots, P_{M_n})$ of probability distributions. P_E is a distribution over encoding functions E and P_{M_i} are probability distributions over orthogonal measurements of qubit.

Different kinds of quantum RACs

Definition

Pure quantum $n \mapsto 1$ *RAC* is an ordered tuple $(E, M_1, \ldots, M_n)$ that consists of *encoding function* $E : \{0,1\}^n \mapsto \mathbb{C}^2$ and n orthogonal measurements: $M_i = \left\{ \left|\psi_0^i\right\rangle, \left|\psi_1^i\right\rangle \right\}$.

Definition

Quantum $n \mapsto 1$ *RAC with shared randomness* is a probability distribution over pure quantum RACs.

Finding QRACs with SR

Recall

Let $\vec{r}_1$ and $\vec{r}_2$ be the Bloch vectors corresponding to qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$. Then $|\langle\psi_1|\psi_2\rangle|^2 = \frac{1}{2}(1 + \vec{r}_1 \cdot \vec{r}_2)$.

Finding QRACs with SR

Recall

Let $\vec{r}_1$ and $\vec{r}_2$ be the Bloch vectors corresponding to qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$. Then $|\langle\psi_1|\psi_2\rangle|^2 = \frac{1}{2}(1 + \vec{r}_1 \cdot \vec{r}_2)$.

Qubit ($\mathbb{C}^2$) $\Rightarrow$ Bloch sphere ($\mathbb{R}^3$)

Finding QRACs with SR

Recall

Let $\vec{r}_1$ and $\vec{r}_2$ be the Bloch vectors corresponding to qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$. Then $|\langle\psi_1|\psi_2\rangle|^2 = \frac{1}{2}(1 + \vec{r}_1 \cdot \vec{r}_2)$.

Qubit ($\mathbb{C}^2$) $\Rightarrow$ Bloch sphere ($\mathbb{R}^3$)

- encoding of string $x \in \{0,1\}^n$: $|E(x)\rangle \Rightarrow \vec{r}_x$,

Finding QRACs with SR

Recall

Let $\vec{r}_1$ and $\vec{r}_2$ be the Bloch vectors corresponding to qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$. Then $|\langle\psi_1|\psi_2\rangle|^2 = \frac{1}{2}(1 + \vec{r}_1 \cdot \vec{r}_2)$.

Qubit ($\mathbb{C}^2$) $\Rightarrow$ Bloch sphere ($\mathbb{R}^3$)

- encoding of string $x \in \{0,1\}^n$: $|E(x)\rangle \Rightarrow \vec{r}_x$,
- measurement of the ith bit: $\left\{\left|\psi_0^i\right\rangle, \left|\psi_1^i\right\rangle\right\} \Rightarrow \{\vec{v}_i, -\vec{v}_i\}$.

Finding QRACs with SR

Recall

Let $\vec{r}_1$ and $\vec{r}_2$ be the Bloch vectors corresponding to qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$. Then $|\langle\psi_1|\psi_2\rangle|^2 = \frac{1}{2}(1 + \vec{r}_1 \cdot \vec{r}_2)$.

Qubit ($\mathbb{C}^2$) $\Rightarrow$ Bloch sphere ($\mathbb{R}^3$)

- encoding of string $x \in \{0,1\}^n$: $|E(x)\rangle \Rightarrow \vec{r}_x$,
- measurement of the ith bit: $\left\{\left|\psi_0^i\right\rangle, \left|\psi_1^i\right\rangle\right\} \Rightarrow \{\vec{v}_i, -\vec{v}_i\}$.

Optimize

The average success probability is:

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

Optimal quantum encoding

Probability

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

Optimal quantum encoding

Probability

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

Observe

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

Optimal quantum encoding

Probability

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

Observe

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

Optimal encoding

Given $\{\vec{v}_i\}$, optimal encoding of x is a unit vector $\vec{r}_x$ in direction of

$$\sum_{i=1}^{n} (-1)^{x_i} \vec{v}_i$$

Optimal quantum encoding

Probability

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

Observe

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

Optimal encoding

Given $\{\vec{v}_i\}$, optimal encoding of x is a unit vector $\vec{r}_x$ in direction of

$$\sum_{i=1}^{n} (-1)^{x_i} \vec{v}_i$$

Note: if all $\vec{v}_i$ are equal, this corresponds to the optimal classical (majority) encoding.

Upper bound

Success probability using optimal encoding

$$p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{2^n \cdot n} \sum_{a \in \{1,-1\}^n} \left\| \sum_{i=1}^{n} a_i \vec{v}_i \right\| \right)$$

Upper bound

Success probability using optimal encoding

$$p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{2^n \cdot n} \sum_{a \in \{1,-1\}^n} \left\| \sum_{i=1}^{n} a_i \vec{v}_i \right\| \right)$$

Lemma

For any unit vectors $\vec{v}_1, \ldots, \vec{v}_n$ *we have:*

$$\sum_{a_1,\ldots,a_n \in \{1,-1\}} \|a_1 \vec{v}_1 + \cdots + a_n \vec{v}_n\|^2 = n \cdot 2^n$$

Upper bound

Success probability using optimal encoding

$$p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{2^n \cdot n} \sum_{a \in \{1,-1\}^n} \left\| \sum_{i=1}^{n} a_i \vec{v}_i \right\| \right)$$

Lemma

For any unit vectors $\vec{v}_1, \ldots, \vec{v}_n$ we have:

$$\sum_{a_1,\ldots,a_n \in \{1,-1\}} \|a_1\vec{v}_1 + \cdots + a_n\vec{v}_n\|^2 = n \cdot 2^n$$

Think of this as a generalization of the parallelogram identity

$$\|\vec{v}_1 + \vec{v}_2\|^2 + \|\vec{v}_1 - \vec{v}_2\|^2 = 2\left(\|\vec{v}_1\|^2 + \|\vec{v}_2\|^2\right)$$

Upper bound

Success probability using optimal encoding

$$p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{2^n \cdot n} \sum_{a \in \{1,-1\}^n} \left\| \sum_{i=1}^{n} a_i \vec{v}_i \right\| \right)$$

Lemma

For any unit vectors $\vec{v}_1, \ldots, \vec{v}_n$ we have:

$$\sum_{a_1,\ldots,a_n \in \{1,-1\}} \|a_1\vec{v}_1 + \cdots + a_n\vec{v}_n\|^2 = n \cdot 2^n$$

To remove the square, use inequality that follows form $(x-y)^2 \geq 0$:

$$xy \leq \frac{1}{2}(x^2 + y^2)$$

Upper bound

Success probability using optimal encoding

$$p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{2^n \cdot n} \sum_{a \in \{1,-1\}^n} \left\| \sum_{i=1}^{n} a_i \vec{v}_i \right\| \right)$$

Lemma

For any unit vectors $\vec{v}_1, \ldots, \vec{v}_n$ we have:

$$\sum_{a_1,\ldots,a_n \in \{1,-1\}} \|a_1\vec{v}_1 + \cdots + a_n\vec{v}_n\| \leq \sqrt{n} \cdot 2^n$$

Upper bound

Success probability using optimal encoding

$$p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{2^n \cdot n} \sum_{a \in \{1,-1\}^n} \left\| \sum_{i=1}^{n} a_i \vec{v}_i \right\| \right)$$

Lemma

For any unit vectors $\vec{v}_1, \ldots, \vec{v}_n$ *we have:*

$$\sum_{a_1,\ldots,a_n \in \{1,-1\}} \|a_1\vec{v}_1 + \cdots + a_n\vec{v}_n\| \leq \sqrt{n} \cdot 2^n$$

Theorem

For any $n \overset{p}{\mapsto} 1$ *QRAC with shared randomness:* $p \leq \dfrac{1}{2} + \dfrac{1}{2\sqrt{n}}$.

Upper bound

Success probability using optimal encoding

$$p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{2^n \cdot n} \sum_{a \in \{1,-1\}^n} \left\| \sum_{i=1}^{n} a_i \vec{v}_i \right\| \right)$$

Lemma

For any unit vectors $\vec{v}_1, \ldots, \vec{v}_n$ *we have:*

$$\sum_{a_1,\ldots,a_n \in \{1,-1\}} \|a_1\vec{v}_1 + \cdots + a_n\vec{v}_n\| \leq \sqrt{n} \cdot 2^n$$

Theorem

For any $n \overset{p}{\mapsto} 1$ *QRAC with shared randomness:* $p \leq \dfrac{1}{2} + \dfrac{1}{2\sqrt{n}}$.

Note: this holds even if Bob can use a POVM measurement.

Lower bound

Success probability using optimal encoding

$$p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{2^n \cdot n} \sum_{a \in \{1,-1\}^n} \left\| \sum_{i=1}^{n} a_i \vec{v}_i \right\| \right)$$

Lower bound

Success probability using optimal encoding

$$p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{2^n \cdot n} \sum_{a \in \{1,-1\}^n} \left\| \sum_{i=1}^{n} a_i \vec{v}_i \right\| \right)$$

Random measurements

Alice and Bob can sample each $\vec{v}_i$ at random. This can be done near uniformly given enough shared randomness. Observe

$$\mathop{\mathbb{E}}_{\{\vec{v}_i\}} \left(\sum_{a \in \{1,-1\}^n} \left\| \sum_{i=1}^{n} a_i \vec{v}_i \right\| \right) = 2^n \cdot \mathop{\mathbb{E}}_{\{\vec{v}_i\}} \left\| \sum_{i=1}^{n} \vec{v}_i \right\|$$

Lower bound

Success probability using random measurements

$$\mathop{\mathbb{E}}_{\{\vec{v}_i\}} p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{n} \cdot \mathop{\mathbb{E}}_{\{\vec{v}_i\}} \left\| \sum_{i=1}^{n} \vec{v}_i \right\|\right)$$

Random measurements

Alice and Bob can sample each $\vec{v}_i$ at random. This can be done near uniformly given enough shared randomness. Observe

$$\mathop{\mathbb{E}}_{\{\vec{v}_i\}} \left(\sum_{a \in \{1,-1\}^n} \left\| \sum_{i=1}^{n} a_i \vec{v}_i \right\| \right) = 2^n \cdot \mathop{\mathbb{E}}_{\{\vec{v}_i\}} \left\| \sum_{i=1}^{n} \vec{v}_i \right\|$$

Lower bound

Success probability using random measurements

$$\mathop{\mathbb{E}}_{\{\vec{v}_i\}} p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{n} \cdot \mathop{\mathbb{E}}_{\{\vec{v}_i\}} \left\| \sum_{i=1}^{n} \vec{v}_i \right\| \right)$$

Random measurements

Alice and Bob can sample each $\vec{v}_i$ at random. This can be done near uniformly given enough shared randomness. Observe

$$\mathop{\mathbb{E}}_{\{\vec{v}_i\}} \left(\sum_{a \in \{1,-1\}^n} \left\| \sum_{i=1}^{n} a_i \vec{v}_i \right\| \right) = 2^n \cdot \mathop{\mathbb{E}}_{\{\vec{v}_i\}} \left\| \sum_{i=1}^{n} \vec{v}_i \right\|$$

What is the average distance traveled in 3D after n steps of unit length if the direction of each step is chosen uniformly at random?

Lower bound

Success probability using random measurements

$$\mathop{\mathbb{E}}_{\{\vec{v}_i\}} p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{n} \cdot \mathop{\mathbb{E}}_{\{\vec{v}_i\}} \left\| \sum_{i=1}^{n} \vec{v}_i \right\| \right)$$

Random walk

Probability density to arrive at point $\vec{R}$ after performing $n \gg 1$ steps of random walk [Chandrasekhar 1943]:

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

Lower bound

Success probability using random measurements

$$\mathop{\mathbb{E}}_{\{\vec{v}_i\}} p(\{\vec{v}_i\}) = \frac{1}{2}\left(1 + \frac{1}{n} \cdot \mathop{\mathbb{E}}_{\{\vec{v}_i\}} \left\| \sum_{i=1}^{n} \vec{v}_i \right\| \right)$$

Random walk

Probability density to arrive at point $\vec{R}$ after performing $n \gg 1$ steps of random walk [Chandrasekhar 1943]:

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

Thus the average distance traveled is

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

Lower bound

Success probability using random measurements

$$\underset{\{\vec{v}_i\}}{\mathbb{E}}\, p(\{\vec{v}_i\}) = \frac{1}{2} + \sqrt{\frac{2}{3\pi n}}$$

Random walk

Probability density to arrive at point $\vec{R}$ after performing $n \gg 1$ steps of random walk [Chandrasekhar 1943]:

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

Thus the average distance traveled is

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

Lower bound

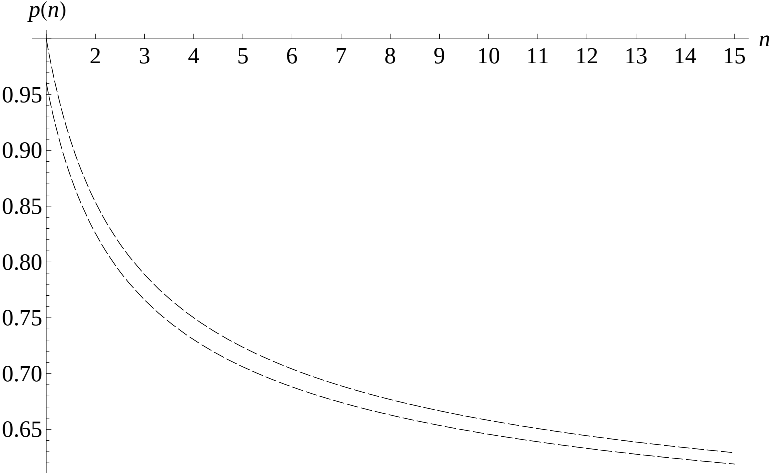
Success probability using random measurements

$$\mathop{\mathbb{E}}_{\{\vec{v}_i\}} p(\{\vec{v}_i\}) = \frac{1}{2} + \sqrt{\frac{2}{3\pi n}}$$

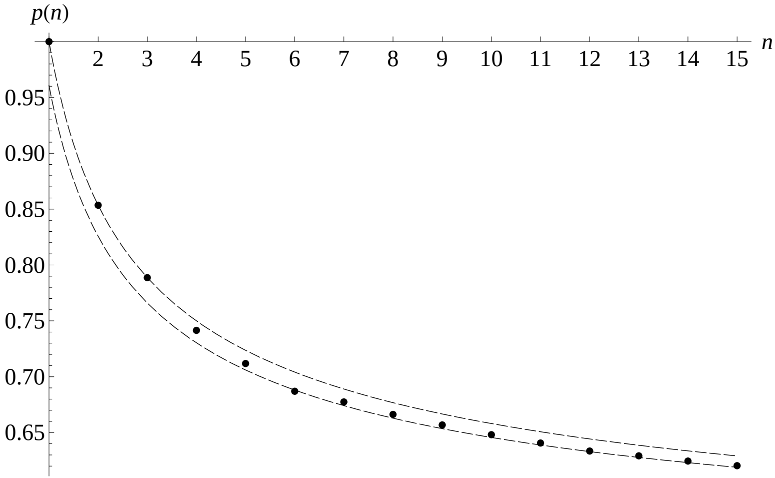
Theorem

There exists $n \overset{p}{\mapsto} 1$ QRAC with SR such that $p = \dfrac{1}{2} + \sqrt{\dfrac{2}{3\pi n}}$.

Quantum upper and lower bounds



Quantum upper and lower bounds



Black dots correspond to a lower bound obtained using measurements on orthogonal Bloch vectors.

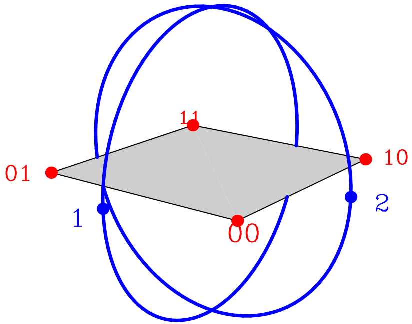
Results of numerical optimization

Results of numerical optimization

See our homepage

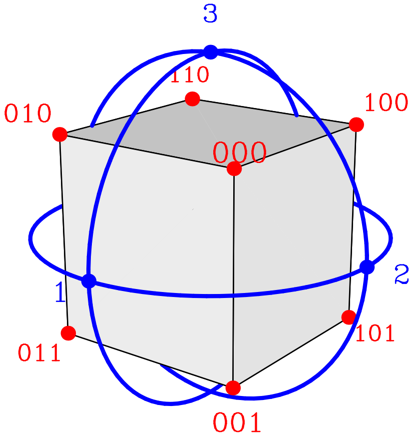
`http://home.lanet.lv/~sd20008/RAC/RACs.htm`

Numerical $2 \mapsto 1$ QRAC



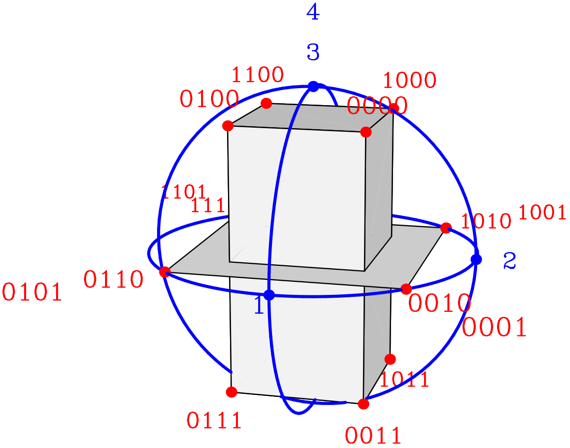
$$p = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.8535533906$$

Numerical $3 \mapsto 1$ QRAC



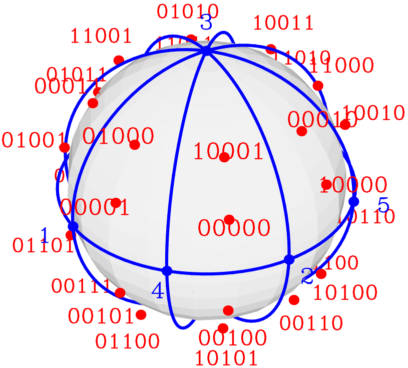
$$p = \frac{1}{2} + \frac{1}{2\sqrt{3}} \approx 0.7886751346$$

Numerical $4 \mapsto 1$ QRAC



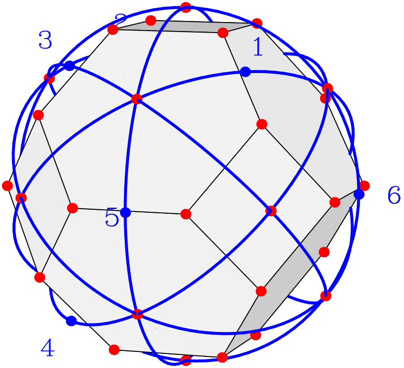
$$p = \frac{1}{2} + \frac{1+\sqrt{3}}{8\sqrt{2}} \approx 0.7414814566$$

Numerical $5 \mapsto 1$ QRAC



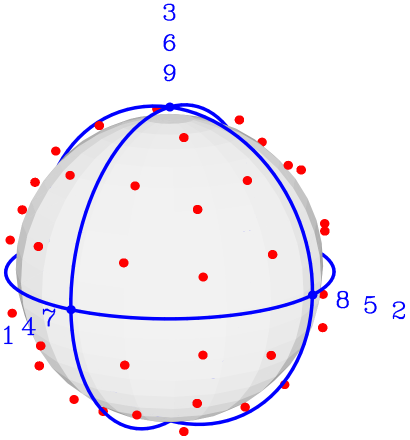
$$p = \frac{1}{2} + \frac{1}{20}\sqrt{2(5+\sqrt{17})} \approx 0.7135779205$$

Numerical $6 \mapsto 1$ QRAC



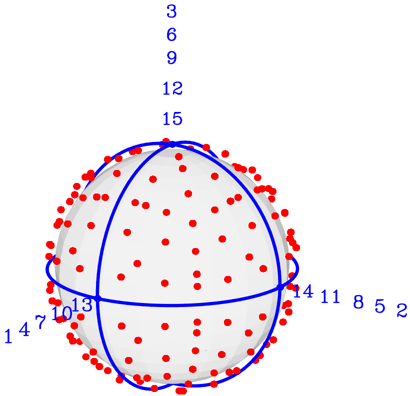
$$p = \frac{1}{2} + \frac{2 + \sqrt{3} + \sqrt{15}}{16\sqrt{6}} \approx 0.6940463870$$

Numerical $9 \mapsto 1$ QRAC



$$p = \frac{1}{2} + \frac{192 + 10\sqrt{3} + 9\sqrt{11} + 3\sqrt{19}}{384} \approx 0.6568927813$$

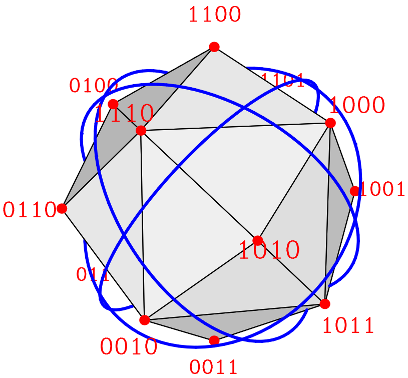
Numerical $15 \mapsto 1$ QRAC



$$p = \frac{1}{2} + \frac{152\sqrt{3}+100\sqrt{11}+50\sqrt{19}+20\sqrt{35}+5\sqrt{43}+2\sqrt{51}+\sqrt{59}}{8192} \approx 0.6203554614$$

Symmetric (but not optimal) constructions

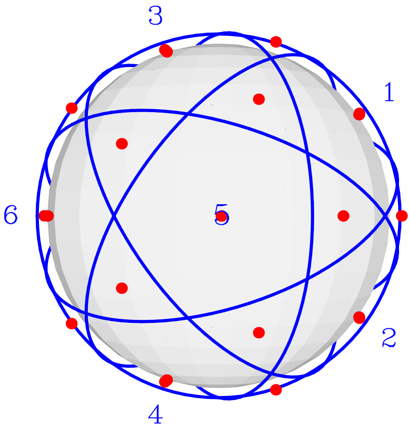
Symmetric $4 \mapsto 1$ QRAC



$$p = \frac{1}{2} + \frac{2+\sqrt{3}}{16} \approx 0.7332531755$$

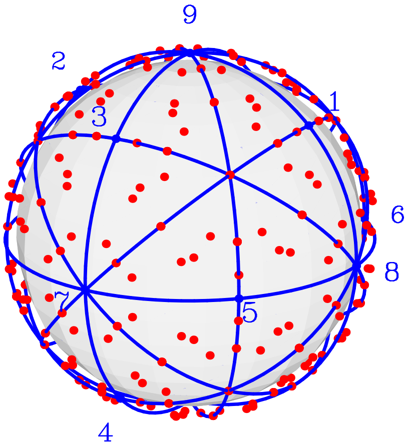
$$\leq 0.7414814566$$

Symmetric $6 \mapsto 1$ QRAC



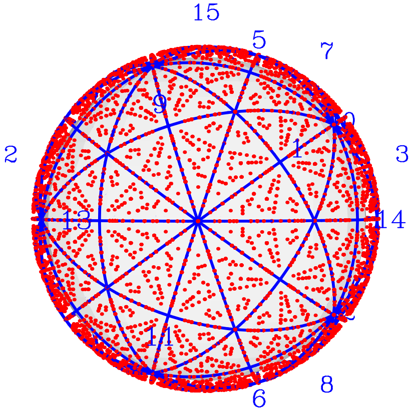
$$p = \frac{1}{2} + \frac{\sqrt{5}}{32} + \frac{1}{96}\sqrt{75 + 30\sqrt{5}} \approx 0.6940418856$$
$$\leq 0.6940463870$$

Symmetric $9 \mapsto 1$ QRAC



$$p \approx 0.6563927998$$
$$\leq 0.6568927813$$

Symmetric $15 \mapsto 1$ QRAC



$$p \approx 0.6201829084$$
$$\leq 0.6203554614$$

Summary

Summary

Classical RACs with SR

Summary

Classical RACs with SR

- exact success probability of optimal RAC:
  $p(2m) = p(2m+1) = \dfrac{1}{2} + \dfrac{1}{2^{2m+1}}\binom{2m}{m},$

Summary

Classical RACs with SR

- exact success probability of optimal RAC:
  $p(2m) = p(2m+1) = \dfrac{1}{2} + \dfrac{1}{2^{2m+1}}\binom{2m}{m}$,
- asymptotic success probability: $p(n) \approx \dfrac{1}{2} + \dfrac{1}{\sqrt{2\pi n}}$.

Summary

Classical RACs with SR

- exact success probability of optimal RAC:
  $p(2m) = p(2m+1) = \dfrac{1}{2} + \dfrac{1}{2^{2m+1}}\binom{2m}{m}$,
- asymptotic success probability: $p(n) \approx \dfrac{1}{2} + \dfrac{1}{\sqrt{2\pi n}}$.

Quantum RACs with SR

Summary

Classical RACs with SR

- exact success probability of optimal RAC:
  $p(2m) = p(2m+1) = \dfrac{1}{2} + \dfrac{1}{2^{2m+1}}\binom{2m}{m}$,
- asymptotic success probability: $p(n) \approx \dfrac{1}{2} + \dfrac{1}{\sqrt{2\pi n}}$.

Quantum RACs with SR

- upper bound: $p(n) \leq \dfrac{1}{2} + \dfrac{1}{2\sqrt{n}}$,

Summary

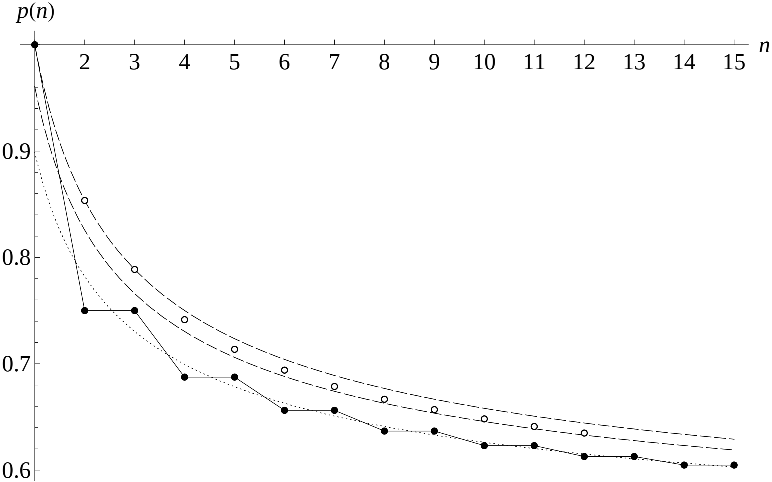
Classical RACs with SR

- exact success probability of optimal RAC:
  $p(2m) = p(2m+1) = \dfrac{1}{2} + \dfrac{1}{2^{2m+1}}\binom{2m}{m}$,
- asymptotic success probability: $p(n) \approx \dfrac{1}{2} + \dfrac{1}{\sqrt{2\pi n}}$.

Quantum RACs with SR

- upper bound: $p(n) \leq \dfrac{1}{2} + \dfrac{1}{2\sqrt{n}}$,
- lower bound: $p(n) \geq \dfrac{1}{2} + \sqrt{\dfrac{2}{3\pi n}}$.

Comparison of classical and quantum RACs with SR



White dots correspond to QRACs obtained using numerical optimization.
Black dots correspond to optimal classical RAC.

Open problems

Open problems

Optimality

Prove the optimality of any of the numerically obtained $n \mapsto 1$ QRACs with SR for $n \geq 4$.

Open problems

Optimality

Prove the optimality of any of the numerically obtained $n \mapsto 1$ QRACs with SR for $n \geq 4$.

Lower bound

Give a lower bound of success probability of $(3n) \mapsto 1$ QRAC with SR using n measurements along each coordinate axis (this requires less SR than random measurements).

Open problems

Optimality

Prove the optimality of any of the numerically obtained $n \mapsto 1$ QRACs with SR for $n \geq 4$.

Lower bound

Give a lower bound of success probability of $(3n) \mapsto 1$ QRAC with SR using n measurements along each coordinate axis (this requires less SR than random measurements).

Generalizations

What happens if we...

Open problems

Optimality

Prove the optimality of any of the numerically obtained $n \mapsto 1$ QRACs with SR for $n \geq 4$.

Lower bound

Give a lower bound of success probability of $(3n) \mapsto 1$ QRAC with SR using n measurements along each coordinate axis (this requires less SR than random measurements).

Generalizations

What happens if we...

- use a qudit instead of a qubit (consider also classical case),

Open problems

Optimality

Prove the optimality of any of the numerically obtained $n \mapsto 1$ QRACs with SR for $n \geq 4$.

Lower bound

Give a lower bound of success probability of $(3n) \mapsto 1$ QRAC with SR using n measurements along each coordinate axis (this requires less SR than random measurements).

Generalizations

What happens if we...

- use a qudit instead of a qubit (consider also classical case),
- allow $m > 1$ (consider classical and quantum $n \overset{p}{\mapsto} m$ RACs),

Open problems

Optimality

Prove the optimality of any of the numerically obtained $n \mapsto 1$ QRACs with SR for $n \geq 4$.

Lower bound

Give a lower bound of success probability of $(3n) \mapsto 1$ QRAC with SR using n measurements along each coordinate axis (this requires less SR than random measurements).

Generalizations

What happens if we...

- use a qudit instead of a qubit (consider also classical case),
- allow $m > 1$ (consider classical and quantum $n \overset{p}{\mapsto} m$ RACs),
- allow POVM measurements (for $m = 1$ does not help),

Open problems

Optimality

Prove the optimality of any of the numerically obtained $n \mapsto 1$ QRACs with SR for $n \geq 4$.

Lower bound

Give a lower bound of success probability of $(3n) \mapsto 1$ QRAC with SR using n measurements along each coordinate axis (this requires less SR than random measurements).

Generalizations

What happens if we...

- use a qudit instead of a qubit (consider also classical case),
- allow $m > 1$ (consider classical and quantum $n \overset{p}{\mapsto} m$ RACs),
- allow POVM measurements (for $m = 1$ does not help),
- allow shared entanglement?

Another open problem. . .

[Biosphere, Montreal]

Is this a QRAC?

Thank you for your attention!