d-Level Random Access Codes: a variant and its application

A. Ambainis*, M. Banik†, A. Chaturvedi⋆, D. Kravchenko*, & Ashutosh Rai*

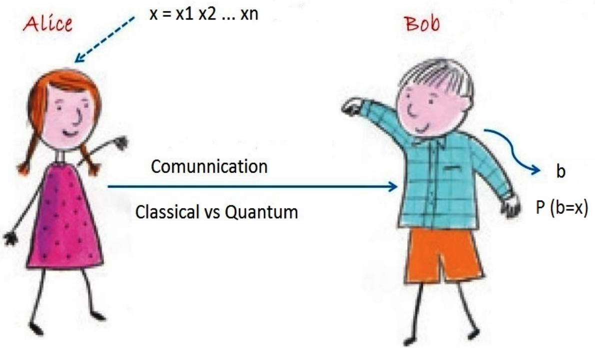
*University of Latvia, Riga, Latvia
† IMSc, Chennai, India
⋆NQIC, Gdansk, Poland

arXiv:1607.05490 [quant-ph]

Plan of this talk...

- **Random Access Codes**
- **A two party communication task**
  - **d-level parity oblivious random access codes (d-PORAC)**
  - **Optimal classical success of d-PORAC**
- **Operational theories and ontological models**
  - **Preparation contextuality**
  - **Bound of d-PORAC in any preparation noncontextual theory**
  - **Class of preparation noncontextuality inequalities**
- **Quantum violations**
  - **Explicit protocol for 3-PORAC**
  - **Quantum protocols for $d = 4, 5$**
- **Summary**

Words: $x = x_1 x_2 \ldots x_n$; Alphabets: $\{0, 1, \ldots, (d-1)\}$



- **Holevo's Theorem** $\Longrightarrow$ No quantum advantage.

Classical and Quantum Strategies in communication tasks

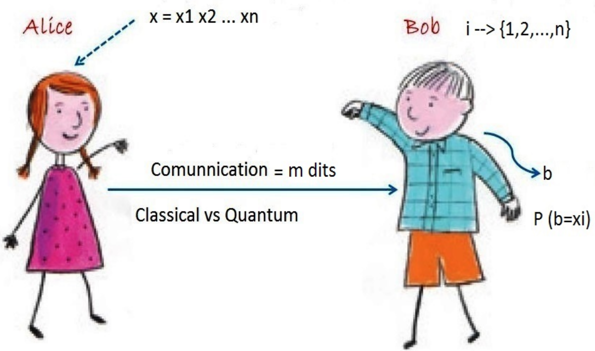
- **Classical encoding:** $E : x \longmapsto E(x)$ (in general probabilistically),
- **Classical decoding:** $D : E(x) \longmapsto x$ (in general probabilistically) .

- **Quantum encoding:** $E : x \longmapsto |\Psi\rangle_x$;
  Quantum state $|\Psi\rangle_x = \alpha_0|0\rangle + \alpha_1|1\rangle + ... + \alpha_{N-1}|N-1\rangle \in \mathbb{C}^N$.

- **Quantum decoding:**
  $D(|\Psi\rangle_x)$ is some quantum measurement $\sum_{\xi=0}^{d-1} P_\xi = \mathbb{I}_n$.
  P_ξ's are projectors on orthogonal subspaces of $\mathbb{C}^N$.
  Measurement gives d possible outcomes with $p(\xi) = |\langle\Psi_x|P_\xi|\Psi_x\rangle|^2$.

(n, m, p)-Random Access Codes: gives some quantum advantage

Words: $x = x_1 x_2 ... x_n$; Alphabets: $\{0, 1, ..., (d-1)\}$



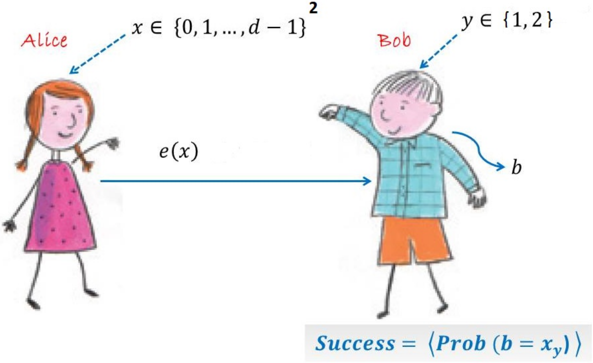
Success

1. Worst case success probability
2. Average success probability

Known results

- $(n \xrightarrow{p} m)$ Ambainis et al. (1999, 2002);
  $(2 \xrightarrow{p \approx 0.85} 1)$ and $(3 \xrightarrow{p \approx 0.79} 1)$.
  $(n \xrightarrow{p} m)$ RACs: a lower bound $m \geq (1 - H(p))n$.
- Hayashi et al. (2006) $(4 \xrightarrow{p} 1)$ QRACs does not exist.
- In Ambainis et al. (2009) RACs with shared randomness
  quantum advantage for $(n \xrightarrow{p} 1)$ RACs.
- Tavakoli et al. (2015): QRACs for d-level alphabets.
- Spekkens (2009): parity-oblivious RACs connected to preparation contextuality
  Ambainis et al. (2015): parity-oblivious RACs connected to quantum nonlocality.

The task: d-PORAC



- **Restriction (R): no information about the parity $(x_1 \oplus_d x_2)$ can be transferred.**

d-PORAC ....

The restriction, R: no info of $(x_1 \oplus_d x_2)$

- induces a parity-partition over the set $X = \{x = x_1x_2 \mid x_1, x_2 \in \{0, 1, ..., d-1\}\}$
- $\mathbb{P}_l := \{x_1x_2 \mid x_1 \oplus_d x_2 = l\}$, where $l \in \{0, ..., d-1\}$
- $\mathcal{C}(\mathbb{P}_l) = d, \ \forall\ l$; where $\mathcal{C}(*)$ denote cardinality
- **R**$\Rightarrow$ no information about to which $\mathbb{P}_l$ the x belongs can be transferred

Example: $d = 3$

$$X = \{00, 01, 02, 10, 11, 12, 20, 21, 22\}$$

parity-partition: $\mathbb{P}_0 = \{00, 12, 21\}$, $\mathbb{P}_1 = \{01, 10, 22\}$, $\mathbb{P}_2 = \{02, 20, 11\}$

- One example of allowed encoding $e(x)$:

  encoding-partition: $\mathbb{E}_0 = \{00, 01, 02\}$, $\mathbb{E}_1 = \{10, 11, 12\}$, $\mathbb{E}_2 = \{20, 21, 22\}$

$$e(x) = \begin{cases} 0, & \text{if } x \in \mathbb{E}_0 \\ 1, & \text{if } x \in \mathbb{E}_1 \\ 2, & \text{if } x \in \mathbb{E}_2 \end{cases}$$

Optimal classical success

Lemma

More than 1-dit information from Alice to Bob always carries some information about the parity $\mathbf{x_1 \oplus_d x_2}$.

Proof: A classical strategy can be: (i) Deterministic, or (ii) Randomized

Deterministic case

- sending more than 1-dit implies Alice's encoding is some *onto* map

$$e : \{0, .., d-1\}^2 \longrightarrow \{0, ..., k\}, \text{ where } d \leq k \leq d^2 - 1$$

- such a map partition the set X of all strings into $k+1$ parts $\mathbb{E}_j$, with $0 \leq j \leq k$
- to Bob, $e(x) = j \Rightarrow x \in \mathbb{E}_j$

Deterministic case...

- Bob gets no information about parity, if for all x, each parity is equally probable (i.e., for each parity, $Probability = 1/d$).
- so Bob has no information of parity *iff* for all encoding-partition $\mathbb{E}_j$

$$\mathcal{C}(\mathbb{E}_j \cap \mathbb{P}_l) = \mathcal{C}(\mathbb{E}_j \cap \mathbb{P}_{l'}),\ \forall\ l, l' \in \{0, ..., d-1\}$$

- since, $k \geq d, \exists$ at least one partition $\mathbb{E}_{j^*}$, s.t. $\mathcal{C}(\mathbb{E}_{j^*}) < d$
- therefore $\exists$ a partition $\mathbb{P}_{l^*}$ s.t. $\mathcal{C}(\mathbb{E}_{j^*} \cap \mathbb{P}_{l^*}) = 0$
- so on obtaining j^*, Bob can conclude that parity of the Alice's string is not l^*, and can thus guess some other parity with a probability $> 1/d$

Randomized case...

- any randomized strategy is a probabilistic mixture of some deterministic strategies
- so sending more than 1-dit information in this case implies there is at least one deterministic strategy in the mixture for which, no. of encoding partitions, $k \geq d$
- thus in any randomized case also, some information of parity is transmitted

Optimal classical success

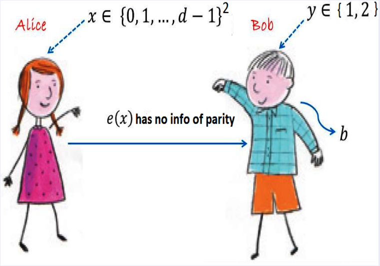
Theorem 1

The optimal classical success probability of d-PORAC is $1/2(1+1/d)$.

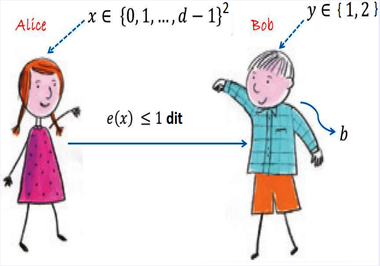
Proof: the proof follows from the lemma and a result in other work [AKR'15]

- *d*-PORAC is a restricted version of *d*-RAC

_d_-PORAC



_d_-RAC



Proof...

- $P_{success}^{optimal}$[d-PORAC] $\leq P_{success}^{optimal}$[d-RAC]

- it is known, $P_{success}^{optimal}$[d-RAC] $= 1/2(1 + 1/d)$ [AKR'15]

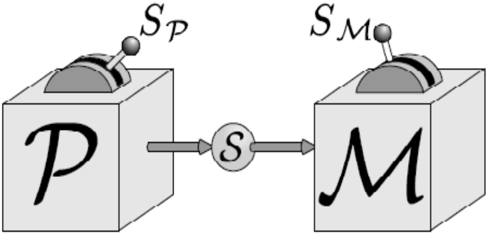
- thus, $P_{success}^{optimal}$[d-PORAC] $\leq 1/2(1 + 1/d)$

- the upper bound is achieved in a d-PORAC protocol: Alice always sends her first dit; Bob perfectly guesses the first dit and guesses the second dit randomly.

Success of d-PORAC in other operational theories

Next we show that this theorem extends to any **preparation noncontextual** theory.

Operational Theories [Spekkens'05]



General

- Preparation (P)
- Measurement (M)
- Prediction: $p(k|P, M)$

Quantum Theory

- P$\longrightarrow$ density operator ρ_P
- M $\longrightarrow$ POVM $\{E_{M,k}\}$
- Prediction: Born Rule $p(k|P, M) = \mathrm{Tr}(\rho_P E_{M,k})$

Equivalent preparations & preparation context...

Equivalence of preparation procedures

$p(k|P,M) = p(k|P',M)$ for all $M \in \mathcal{M}$ and for all k

Preparation context: Consider two preparations for a spin-$\frac{1}{2}$ system.

Preparation P1

$\rho_{\mathbf{P1}} = \frac{1}{2}|\mathbf{0_z}\rangle\langle\mathbf{0_z}| + \frac{1}{2}|\mathbf{1_z}\rangle\langle\mathbf{1_z}|$

Preparation P2

$\rho_{\mathbf{P2}} = \frac{1}{2}|\mathbf{0_x}\rangle\langle\mathbf{0_x}| + \frac{1}{2}|\mathbf{1_x}\rangle\langle\mathbf{1_x}|$

- $\rho_{\mathbf{P1}} = \rho_{\mathbf{P2}} = \frac{1}{2}\mathbb{I}$, and no measurement in quantum theory can distinguish these two preparation procedures
- **P1** and **P2** denote two different preparation contexts for the same quantum state.

Ontological model and preparation contextuality [Spekkens'05]

Ontological model

- an ontological model provides a finer description of the operational theory
- here, ontic states are the collection of the properties of the system, that might not get revealed at operational level, and is denoted as $\lambda \in \Lambda$
- an operational preparation P gives a distribution $p(\lambda|P)$ over the ontic states
- measurement M on λ yields outcome k with probability $p(k|\lambda, M)$.
- predictions of operational theory is reproduced by the model iff $p(k|P, M) = \int d\lambda \; p(k|\lambda, M) \; p(\lambda|P)$.

Preparation Non-Contextual model

An ontological model of an operational theory is called preparation noncontextual if:

$$\forall M, k : p(k|P, M) = p(k|P', M) \Longrightarrow p(\lambda|P) = p(\lambda|P')$$

for all equivalent preparation of the operational theory.

Playing d-PORAC in an arbitrary operational theory

General protocol

- Alice encodes her strings x in some state (preparation) P_x and sends the encoded state to Bob.
- for decoding y^{th} dit, Bob performs some d outcome measurement M_y and guess the dit according to the measurement results.
- the average success probability can be expressed as:

$$p(b = x_y) = \frac{1}{2 \times d^2} \sum_{y \in \{1,2\}} \sum_{x \in \{0,\dots,d-1\}^2} p(b = x_y | P_x, M_y).$$

- the parity oblivious condition is satisfied if:

$$\sum_{x \in \mathbb{P}_l} p(P_x | k, M) = \sum_{x \in \mathbb{P}_{l'}} p(P_x | k, M), \quad \forall\ k, M,$$
$$\text{and} \quad \forall\ l, l' \in \{0, ..., d-1\}.$$

No-Go theorem

Theorem 2

In any preparation noncontextual theory the success probability of d-PORAC can not be more than the optimal classical success probability, i.e., $1/2(1+1/d)$.

Proof:

- Consider a mixed preparation P_l produced by choosing uniformly at random some preparation P_x corresponding to the string x belonging to the partition $\mathbb{P}_l$, i.e,

$$P_l = \frac{1}{d}\sum_{x\in\mathbb{P}_l} P_x$$

.

- Given the preparation P_l, the probability of obtaining outcome k for the measurement M is,

$$p(k|P_l, M) = \frac{1}{d}\sum_{x\in\mathbb{P}_l} p(k|P_x, M). \tag{1}$$

- Also the preparation P_l yields the distribution on the ontic state λ,

$$p(\lambda|P_l) = \frac{1}{d}\sum_{x\in\mathbb{P}_l} p(\lambda|P_x). \tag{2}$$

Proof continued ...

- recall that, the parity oblivious condition is,

$$\sum_{x\in\mathbb{P}_l} p(P_x|k,M) = \sum_{x\in\mathbb{P}_{l'}} p(P_x|k,M), \ \ \forall\ k, M, \text{and} \ \ \forall\ l,l' \in \{0,...,d-1\}. \tag{3}$$

- Bayes theorem and uniform distribution of Alice's strings implies

$$\sum_{x\in\mathbb{P}_l} p(k|P_x,M) = \sum_{x\in\mathbb{P}_{l'}} p(k|P_x,M), \ \ \forall\ k, M, \text{and} \ \ \forall\ l,l' \in \{0,...,d-1\}. \tag{4}$$

- which implies

$$p(k|P_l,M) = p(k|P_{l'},M), \ \ \forall\ k, M, \text{and} \ \ \forall\ l,l' \in \{0,...,d-1\}. \tag{5}$$

  in other words different preparations P_l corresponding to different partitions $\mathbb{P}_l$ are operationally equivalent.

Proof continued ...

- if we assume that an operational theory is preparation noncontextual then we have,

$$p(\lambda|P_l) = p(\lambda|P_{l'}), \quad \forall \quad l, l' \in \{0, ..., d-1\}, \tag{6}$$

or equivalently, for all l, l',

$$\sum_{x \in \mathbb{P}_l} p(\lambda|P_x) = \sum_{x \in \mathbb{P}_{l'}} p(\lambda|P_x). \tag{7}$$

- Applying Bayes theorem, for all l, l',

$$\sum_{x \in \mathbb{P}_l} p(P_x|\lambda) = \sum_{x \in \mathbb{P}_{l'}} p(P_x|\lambda). \tag{8}$$

- Thus for preparation noncontextual models, parity obliviousness at the operational level implies similar consequence at the ontic level.
- Since ontic state λ provides a classical encoding of x and for preparation noncontextual theory it can not contain any information of parity, therefore the classical bound can not exceeded in any such theory.

Class of noncontextual inequalities

The no go theorem tells that, if the *d*-PORAC game is played by using resources from any preparation noncontextual theory, the optimal success probability is bounded

$$\mathbf{P}^{\mathbf{optimal}}_{\mathbf{non-contx}} \leq \frac{1}{2}\left(1 + \frac{1}{d}\right)$$

Therefore, if in some operational theory the success probability for d-PORAC game is more than the optimal classical (noncontextual) success then the operational theory must be preparation contextual.

Next, we show quantum violation for some of these inequalities.

Quantum violation of noncontextuality inequalities

Quantum protocol for 3-PORAC

Alice's encoding

$$
\begin{aligned}
|\psi_{21}\rangle &= |0\rangle, \\
|\psi_{12}\rangle &= |1\rangle, \\
|\psi_{00}\rangle &= |2\rangle; \\
|\psi_{01}\rangle &= \frac{1}{3}(2|0\rangle + |1\rangle - 2|2\rangle), \\
|\psi_{10}\rangle &= \frac{1}{3}(|0\rangle + 2|1\rangle + 2|2\rangle), \\
|\psi_{22}\rangle &= \frac{1}{3}(2|0\rangle - 2|1\rangle + |2\rangle); \\
|\psi_{02}\rangle &= \frac{1}{3}(\omega^2|0\rangle + 2\omega|1\rangle + 2|2\rangle), \\
|\psi_{20}\rangle &= \frac{1}{3}(2\omega^2|0\rangle + \omega|1\rangle - 2|2\rangle), \\
|\psi_{11}\rangle &= \frac{1}{3}(2\omega^2|0\rangle - 2\omega|1\rangle + |2\rangle);
\end{aligned}
$$

Bob's decoding

Measurement for 1^{st} trit

$$
\begin{aligned}
|E_0\rangle &= \frac{1}{\sqrt{7}}\left(|\psi_{00}\rangle - |\psi_{01}\rangle + |\psi_{02}\rangle\right), \\
|E_1\rangle &= \frac{1}{\sqrt{7}}\left(|\psi_{12}\rangle + |\psi_{10}\rangle + e^{\frac{\pi \mathbf{i}}{3}}|\psi_{11}\rangle\right), \\
|E_2\rangle &= \frac{1}{\sqrt{7}}\left(|\psi_{21}\rangle + |\psi_{22}\rangle + e^{\frac{2\pi \mathbf{i}}{3}}|\psi_{20}\rangle\right);
\end{aligned}
$$

Measurement for 2^{nd} trit

$$
\begin{aligned}
|F_0\rangle &= \frac{1}{\sqrt{7}}\left(|\psi_{00}\rangle + |\psi_{10}\rangle - |\psi_{20}\rangle\right), \\
|F_1\rangle &= \frac{1}{\sqrt{7}}\left(|\psi_{21}\rangle + |\psi_{01}\rangle + e^{\frac{2\pi \mathbf{i}}{3}}|\psi_{11}\rangle\right), \\
|F_2\rangle &= \frac{1}{\sqrt{7}}\left(-|\psi_{12}\rangle + |\psi_{22}\rangle + e^{\frac{\pi \mathbf{i}}{3}}|\psi_{02}\rangle\right).
\end{aligned}
$$

Quantum protocol: $d = 3$

$$\mathcal{A}_0 = \{|\psi_{00}\rangle, |\psi_{12}\rangle, |\psi_{21}\rangle\}$$
$$\mathcal{A}_1 = \{|\psi_{01}\rangle, |\psi_{10}\rangle, |\psi_{22}\rangle\}$$
$$\mathcal{A}_2 = \{|\psi_{02}\rangle, |\psi_{20}\rangle, |\psi_{11}\rangle\}$$

$\mathcal{A}_0$, $\mathcal{A}_1$, $\mathcal{A}_2$ form 3 orthonormal basis in $\mathbb{C}^3$. Therefore, the parity-obliviousness is satisfied.

Each vector from any of the set has similar overlap with vectors from the remaining two sets. This feature has a resemblance to a set of mutually unbiased basis (MUB), except that in a MUB all overlaps are equal, therefore, we call the set of bases a *mutually asymmetric-biased basis* (MABB).

- it turns out that, $|\langle E_i|\psi_{ij}\rangle|^2 = |\langle F_j|\psi_{ij}\rangle|^2 = 7/9$ for $i, j = 0, 1, 2$.
- Therefore, the average success probability

$$P = 1/18 \sum_{i,j=0,1,2} (|\langle E_i|\psi_{ij}\rangle|^2 + |\langle F_j|\psi_{ij}\rangle|^2) = 7/9$$

which is strictly greater than the corresponding classical (noncontextual) bound, i.e., $1/2(1 + 1/3) = 2/3$.

Other quantum protocols

- for $d = 4$ we find a protocol (using $\mathbb{C}^4$ encoding) with average success probabilities taking values 0.7405, where the corresponding classical bound is 0.625.
- also for $d = 5$ we find another protocol (using $\mathbb{C}^5$ encoding) with average success probabilities 0.7177, where the corresponding classical bound is 0.6.
- all the three protocols are optimal over all possible pure state encodings in the respective dimentions and projective measurements on them.
- from these protocols we observe that the ratios of quantum to classical success are 1.167, 1.185, 1.196 for $d = 3, 4, 5$ respectively.

Concluding remarks

- In [SBKTP'09] preparation contextuality of completely mixed state of qubit is revealed by an another communication task, called parity-oblivious-multiplexing (POM). The quantum protocols for POM tasks are same as the $2 \mapsto 1$ and $3 \mapsto 1$ quantum random access code (QRAC) protocols [ANTV'02]. This fails for higher d: the d-level QRAC protocols in [THMB'15] fail to satisfy the restriction **R** defined in our information task for $d = 3$.

- The information processing tasks defined in this work lead to noncontextuality inequalities for any finite values of d. We show quantum violation of these inequalities for some values of d. Finding the optimal quantum violations of contextuality inequalities derived in this work may be an interesting problem for future research.

- More importantly, we believe that, the operational task defined in this work is sufficient to reveal preparation contextuality of maximally mixed states of any finite dimensional quantum system. For proving this, construction of generic quantum protocols for arbitrary values of d is required, and which in an interesting open problem.
  [Tavakoli arXiv 1609.09301 (2016)] .

Referrences

1. [**Spekkens'05**] R. W. Spekkens, Contextuality for preparations, transformations, and unsharp measurements, Phys. Rev. A 71, 052108 (2005).
2. [**SBKTP'09**] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, Preparation Contextuality Powers Parity-Oblivious Multiplexing, Phys. Rev. Lett. 102, 010401 (2009).
3. [**THMB'15**] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Quantum Random Access Codes Using Single *d*-Level Systems, Phys. Rev. Lett. 114, 170502 (2015).
4. [**AKR'15**] A. Ambainis, D. Kravchenko, and A. Rai, Optimal Classical Random Access Codes Using Single d-level Systems, arXiv:1510.03045 [quant-ph].
5. [**ANTV'02**] A. Ambainis, A. Nayak, A. Ta-Shma, U. Vazirani, Dense Quantum Coding and Quantum Finite Automata, Journal of the ACM 49, 496 (2002).
6. [**ABCKR'16**] A. Ambainis, M. Banik, A. Chaturvedi, D. Kravchenko, and A. Rai, Parity Oblivious *d*-Level Random Access Codes and Class of Noncontextuality Inequalities, arXiv:1607.05490 [quant-ph].

Questions or Comments !