Applications of the Information-theoretic Method in Quantum Computation

Ashwin Nayak

University of Waterloo

Information Theory

- Originally developed as a theory of communication
- Has applications in seemingly unrelated domains
    - combinatorics
    - computational complexity
    - analysis of algorithms
    - cryptography
- Will describe two recent applications in Quantum Computation

Quantum Information

- Data are stored in physical devices
- Devices are quantum at atomic scale
- Data inherit quantum behaviour
- In current (classical) computers, quantum behaviour is suppressed
- Any advantage in using it ?

Quantum Information

- Data are stored in physical devices
- Devices are quantum at atomic scale
- Data inherit quantum behaviour
- In current (classical) computers, quantum behaviour is suppressed
- Any advantage in using it ?

- Indeed, e.g.,
  - unconditionally secure cryptography
  - exponentially faster algorithms
  - exponentially shorter communication

QI Basics

Classical Data: r.v. $X \in \{0,1\}^n$

distr. on strings

Operations: $X \mapsto$ function $f(x, z)$

indep. r.v.

Quantum

Data: Trace 1 PSD matrix $\rho \in \mathbb{C}^{2^n \times 2^n}$

distr. on vectors (state)

Operations: $\rho \mapsto U \rho U^*$

unitary

Measurement: $\left(M_y : \text{PSD}, \sum_y M_y = \mathbb{1} \right)$

outcome y with prob. $\mathrm{Tr}(M_y \rho)$

QI Basics : simple case

Quantum

Data : Trace 1 PSD matrix $\rho \in \mathbb{C}^{2^n} \times \mathbb{C}^{2^n}$

distr. on vectors

Operations : $\rho \mapsto U \rho U^*$ unitary

Measurement : $\left(M_y : \text{PSD}, \sum_y M_y = \mathbb{1} \right)$

outcome y with prob. $\mathrm{Tr}(M_y \rho)$

Data / state is rank 1 : $\rho = v v^*$

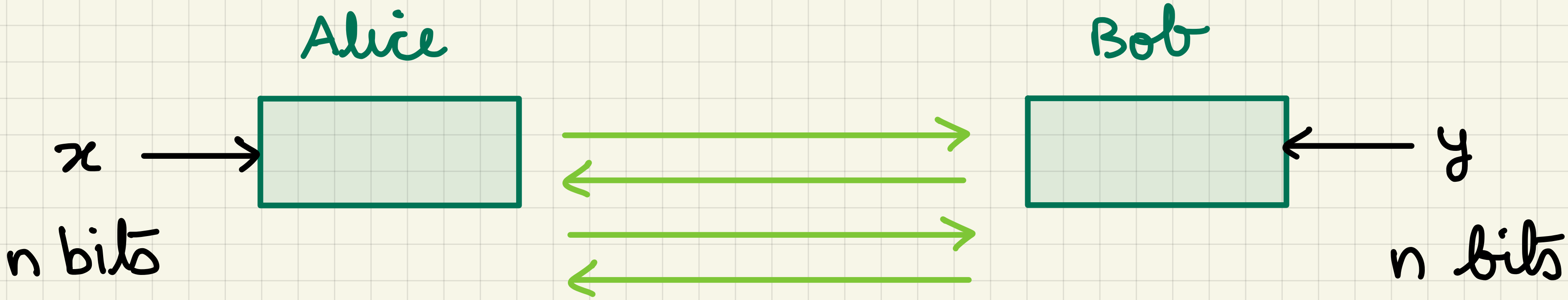
superposition

Operations : $v \mapsto Uv$

Measurement : o.n. basis $\{ e_y : y \in \{0,1\}^n \}$

outcome y with prob. $|\langle e_y, v \rangle|^2$

Example : Set Disjointness

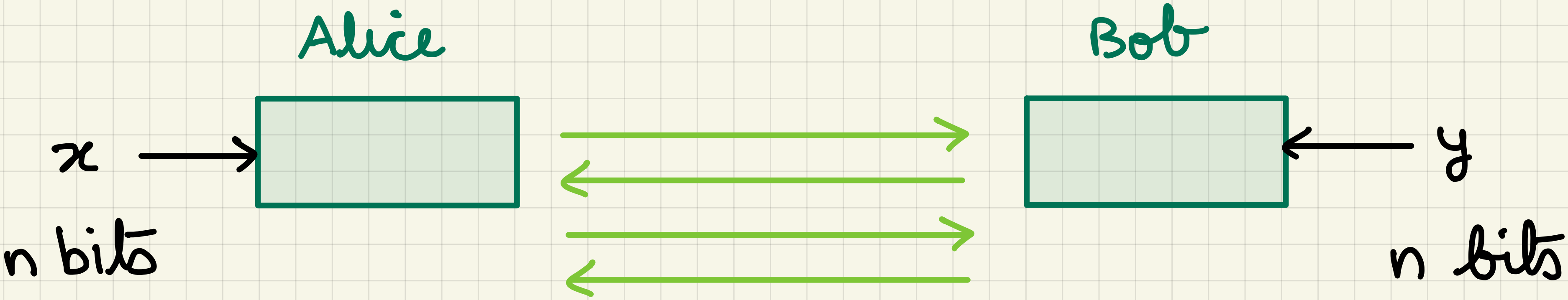


<u>Goal</u>: Is there i s.t. $x_i = y_i = 1$?

Classical communication :

$\Theta(n)$ bits necessary [KS]

Example : Set Disjointness



Goal: Is there i s.t. $x_i = y_i = 1$?

Classical communication :

$\Theta(n)$ bits necessary [KS]

Quantum :

Can solve with $O(\sqrt{n})$ qubit comm'n

[G'96, BCW'98, AA05]

The Protocol

(when $x_i = y_i = 1$ for at most one i)

Suppose $x_a = y_a = 1$.

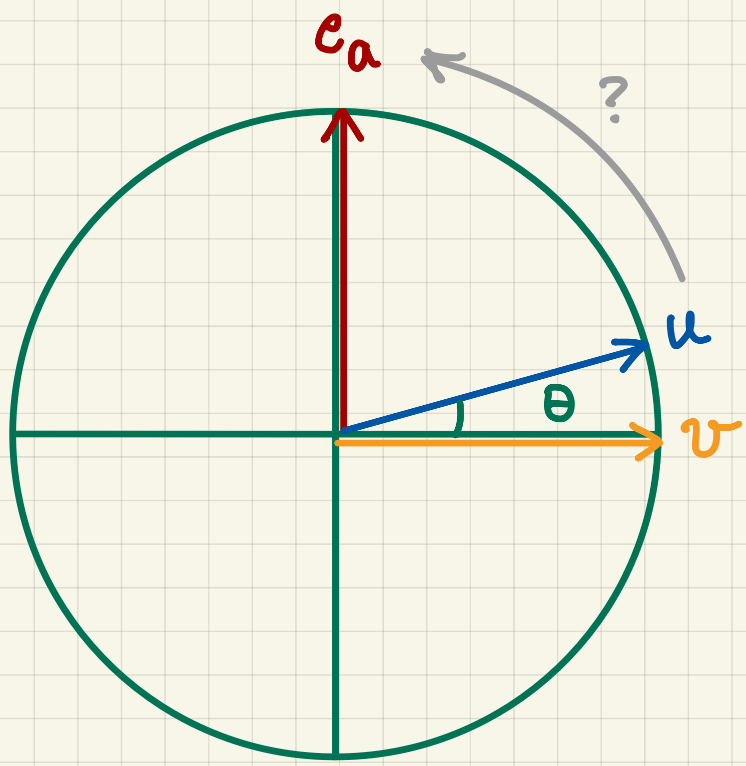
We start in the superposition

$$u := \frac{1}{\sqrt{n}} \sum_{i=1}^{n} e_i$$

uniform over all points.

We would like to map this to the target state e_a, where $x_a = y_a = 1$

[G'96]

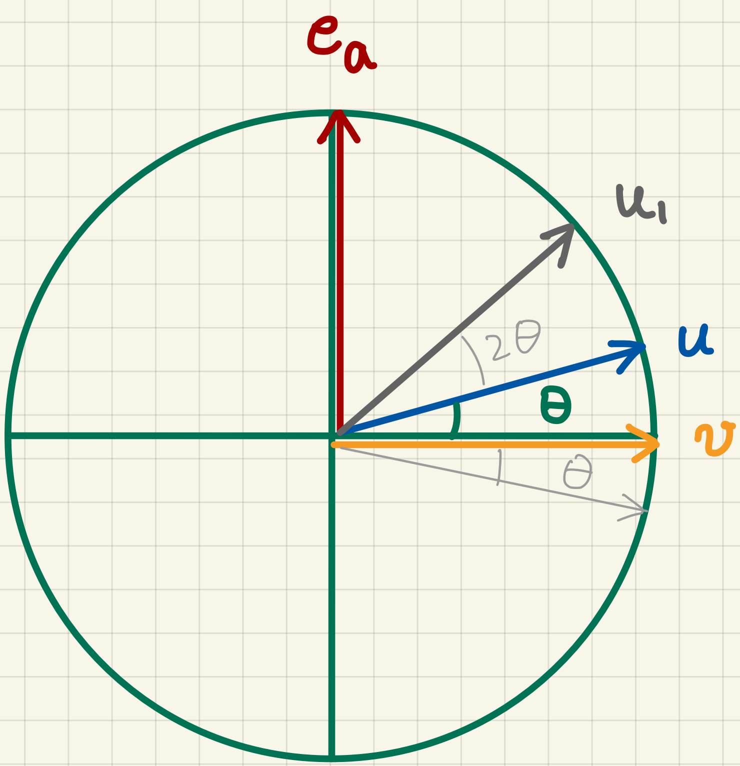


Can we rotate u to e_a (in the plane spanned by the two vectors) ?

Rotations are unitary, so this is conceivable.

Consider the following operations on $|u\rangle$:

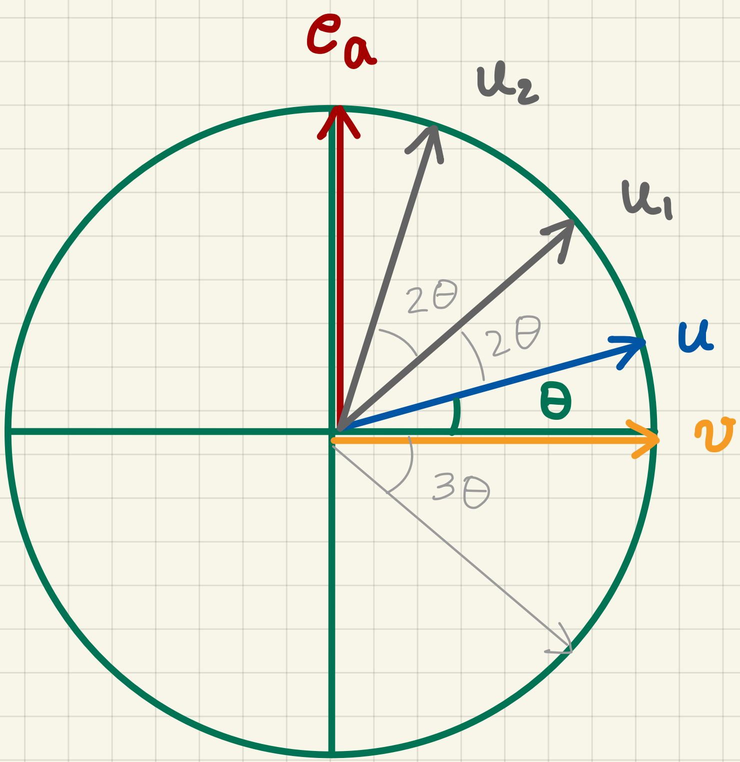
1) Reflect about v, then
2) Reflect about $|u\rangle$.



The composition of the two is a rotation by angle 2θ, in the plane spanned by e_a, u.

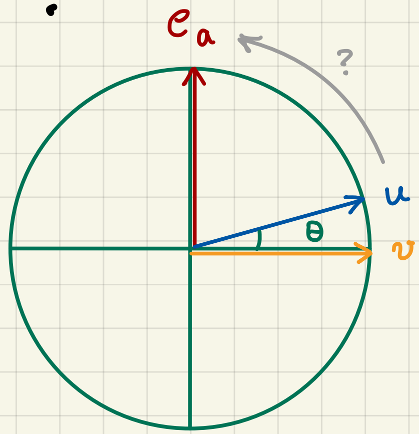
Repeat the same operations on u_1 :

1) Reflect about v , then
2) Reflect about u .



Each repetition of the operations (1) & (2) rotates the state by angle 2θ , towards $|a\rangle$.

How many iterations does it take, to rotate u close to e_a ?



The angle between u and e_a is $\frac{\pi}{2} - \theta$, and is given by

$$\cos\left(\frac{\pi}{2} - \theta\right) = \sin\theta = |\langle e_a, u\rangle| = \frac{1}{\sqrt{n}}.$$

So $\theta \approx 1/\sqrt{n}$ and $\pi/2 - \theta \approx \pi/2$.

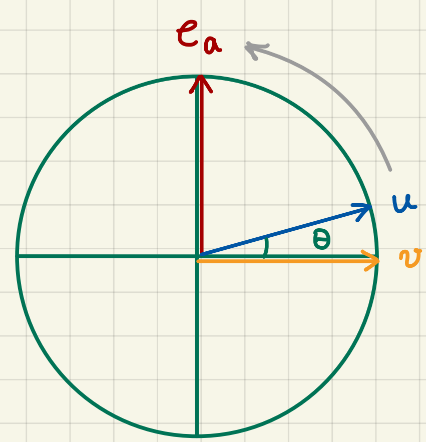
Since an iteration results in rotation by 2θ, total number of iterations $\approx \frac{\pi/2}{2\theta} \approx \frac{\pi}{4} \cdot \sqrt{n}$

Communication:

1) Reflection about v : $O(\log n)$

(Alice & Bob need to check if $x_i = y_i = 1$)

2) Reflection about u : 0 (indep. of 'a')



Total comm'n $= O(\sqrt{n} \log n)$

(can be improved to $O(\sqrt{n})$)

Quantum Communication

- counter-intuitive
- technically more challenging to analyse
- nonetheless, information theory turns out to be helpful

Application I

Learning Quantum States

(state tomography)

Input: some number of registers each in state $\rho \in \mathbb{C}^{d \times d}$ (samples)

Output: bit-description of approximation $\tilde{\rho} \in \mathbb{C}^{d \times d}$ ($\| \tilde{\rho} - \rho \|_1 \leq \varepsilon$)

How many samples are needed?

> Classical analogue: how many i.i.d. samples of a distribution $p \in \mathbb{R}^d$ are needed to find $\tilde{p} \in \mathbb{R}^d$: $\| \tilde{p} - p \|_1 \leq \varepsilon$?

Learning Quantum States

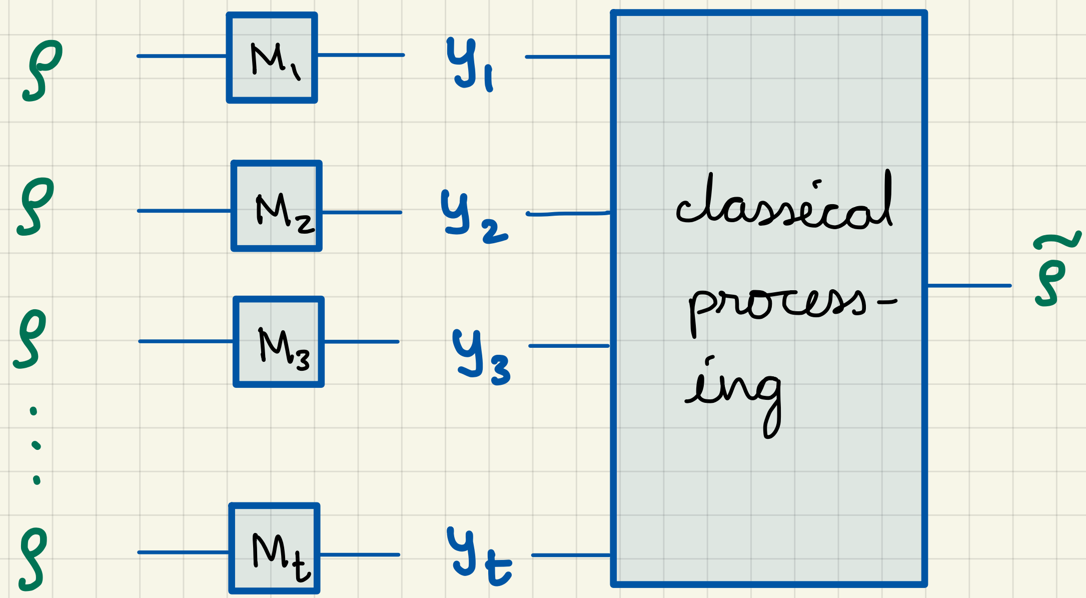
Input: some number of registers each in state $\rho \in \mathbb{C}^{d \times d}$ (samples)

Output: bit-description of approximation $\tilde{\rho} \in \mathbb{C}^{d \times d}$ ($\|\tilde{\rho} - \rho\|_1 \leq \varepsilon$)

How many samples are needed?

- $\Theta(d^2/\varepsilon^2)$ samples necessary & sufficient [OD15, OD17, HHJWY17]
- Optimal algorithm: not known to be efficient, uses joint measurements, out of reach for near-term experiments

Single-copy measurements



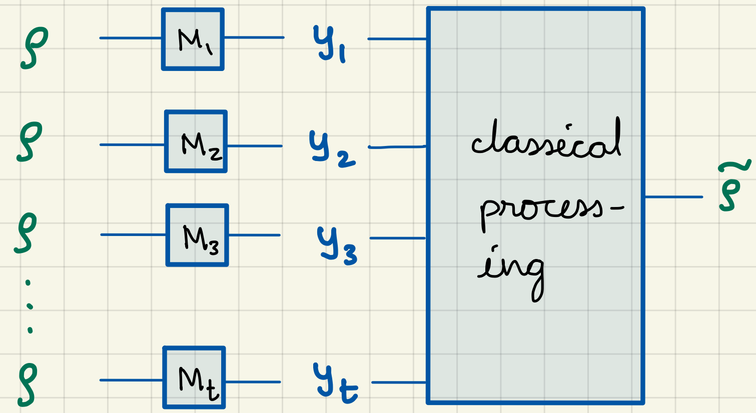
- Non-adaptive measurements : $\Theta(d^3/\varepsilon^2)$

  [HHJWY17]

- Adaptive ? $\Omega(d^4/\log d)$ for Pauli meas.

  [FGLE12]

Single-copy measurements



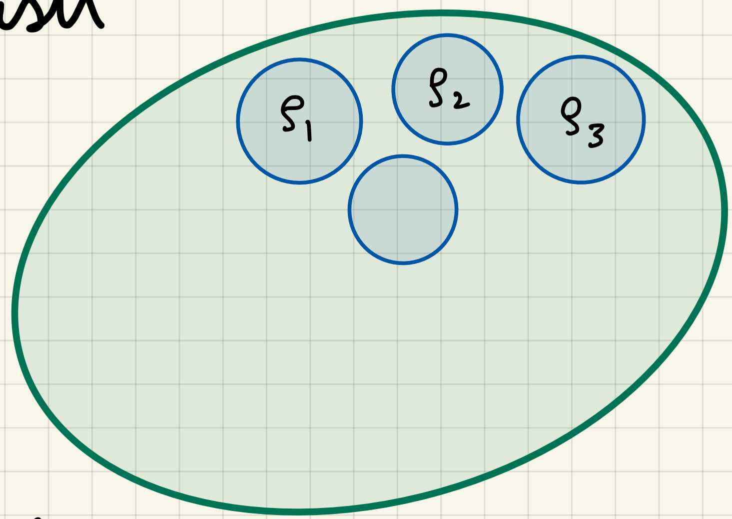
- Adaptive? $\Omega(d^4/\log d)$ for Pauli meas. [FGLE12]

- $\boxed{\Omega(d^3/\varepsilon^2) \text{ samples necessary, when each measurement } M_i \text{ is efficient}}$

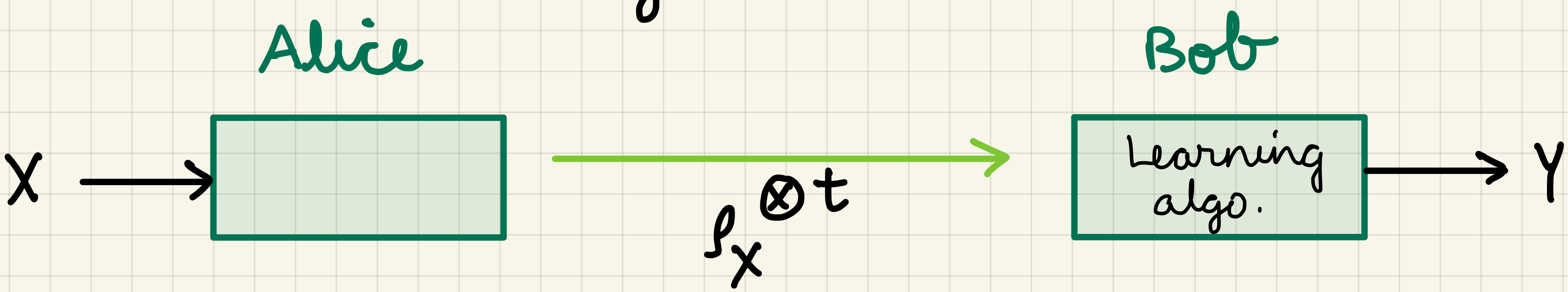
[LN'22]

Proof Sketch

- Construct ε-net of states that are hard to distinguish

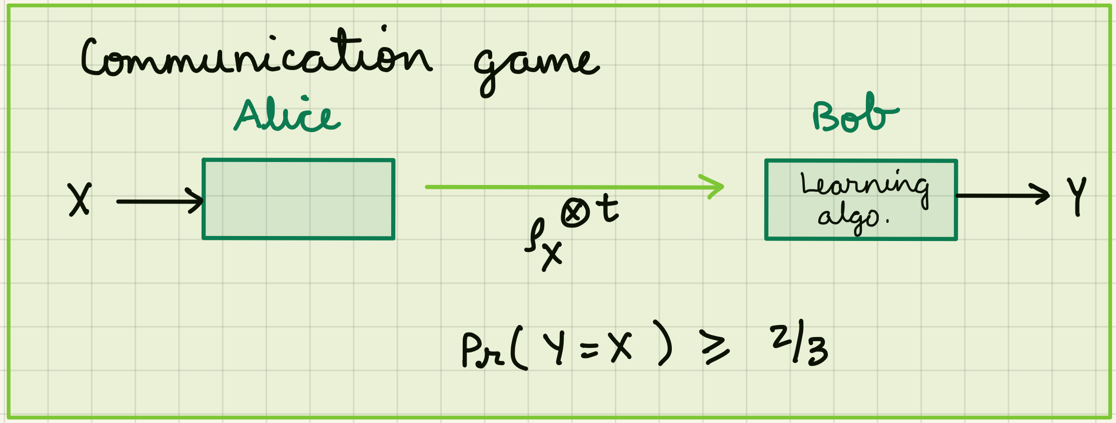


- Communication game



$$\Pr(Y = X) \geq 2/3$$

Proof Sketch



- By Fano : $I(X:Y) \geq$ const. $\log(\#\text{states})$

  in ε-net

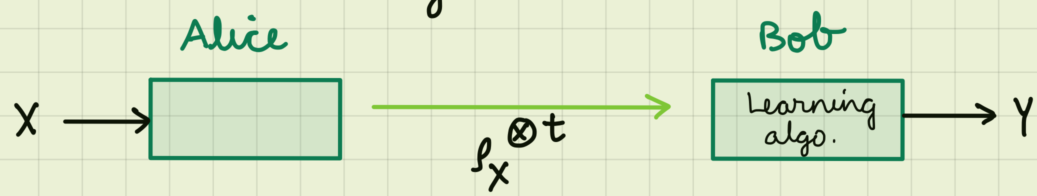
- Chain rule :

$$I(X:Y) = \sum_{i=1}^{t} I(X : Y_i \mid Y_{<i})$$

$$I(X : Y_i \mid Y_{<i}) \leq \mathbb{E}_{X Y_{<i}} \chi^2(Y_i | X \,\|\, Y_i)$$

Proof Sketch

Communication game



$\Pr(Y = X) \geq 2/3$

- By Fano : $I(X:Y) \geq$ const. $\log(\#$ states$)$
  in ε-net
- $I(X:Y) \leq \mathbb{E}_{X Y_{<i}} \chi^2(Y_i | X \,\|\, Y_i)$

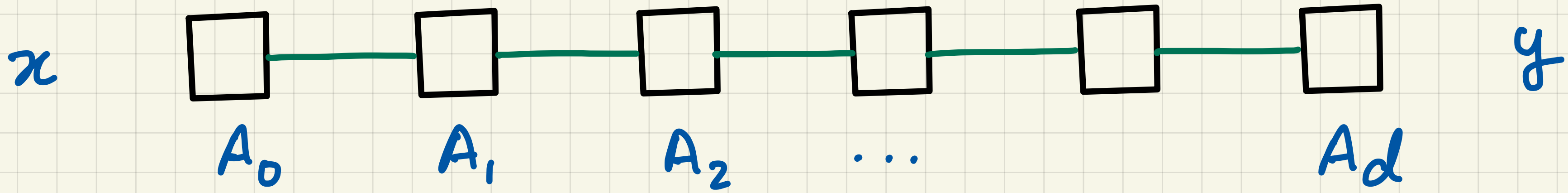
- We construct an ε-net with $\exp(c \cdot d^2)$ states
  s.t. χ^2 term $\leq c_1 \cdot \varepsilon^2/d \quad \forall i$ (efficient meas.)

$\Rightarrow \quad c \cdot d^2 \leq t \cdot c_1 \cdot \varepsilon^2/d$

$\Rightarrow \quad t \in \Omega(d^3/\varepsilon^2)$

Application II

Line Disjointness $L_{n,d}$



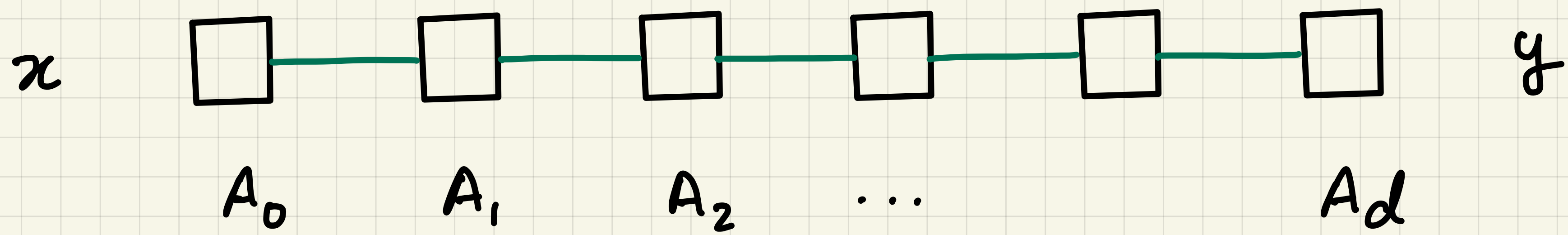
- $d+1$ processors, polylog(n) comm'n./round

- Inputs : x, y, n bits each
  given to A_0, A_d, resp.

- Output : $x_i = y_i = 1$ for some i ?
  (Set Disjointness)

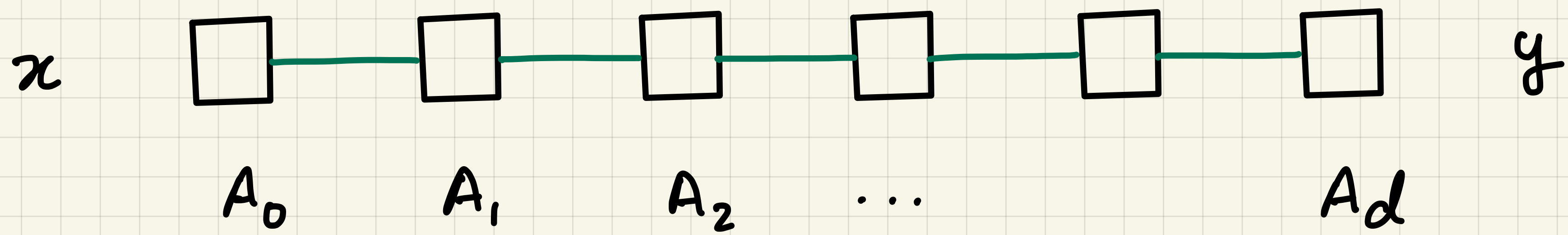
- Goal: Compute with least # rounds

Line Disjointness $L_{n,d}$



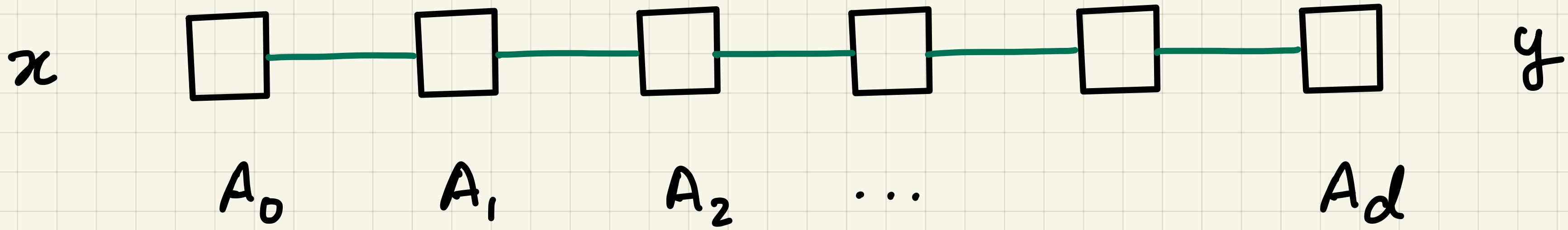
- Randomized algorithms: $\tilde{\Theta}(n)$ rounds
  - Lower bound - Disj_n, $d=1$
    [KS, Razborov, BJKS]

Line Disjointness $L_{n,d}$



- Randomized algorithms: $\tilde{\Theta}(n)$ rounds
  - Lower bound - Disj_n, $d=1$
    [KS, Razborov, BJKS]
- Quantum: $O(\sqrt{nd})$, parallel search
  - Partition x, y: d blocks of n/d
  - Search for common 1 [Grover]
    in each: $d \times \sqrt{n/d} = \sqrt{nd}$

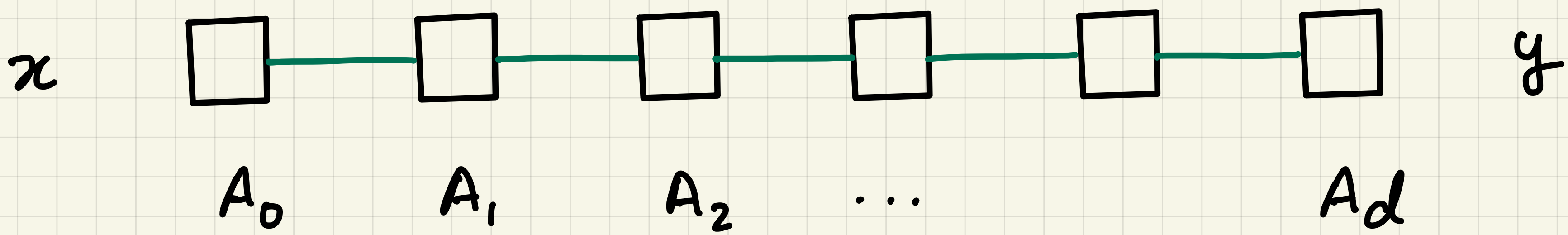
Line Disjointness $L_{n,d}$



- Quantum : better algorithms?
  - $\tilde{\Omega}(\sqrt{n})$ rounds , Disj_n [Razborov'02]
  - $\tilde{\Omega}(\sqrt{nd})$ rounds , round complexity of Disj_n [LM'18]

Assumes: polylog memory / A_i , $1 \le i \le d-1$

Line Disjointness $L_{n,d}$



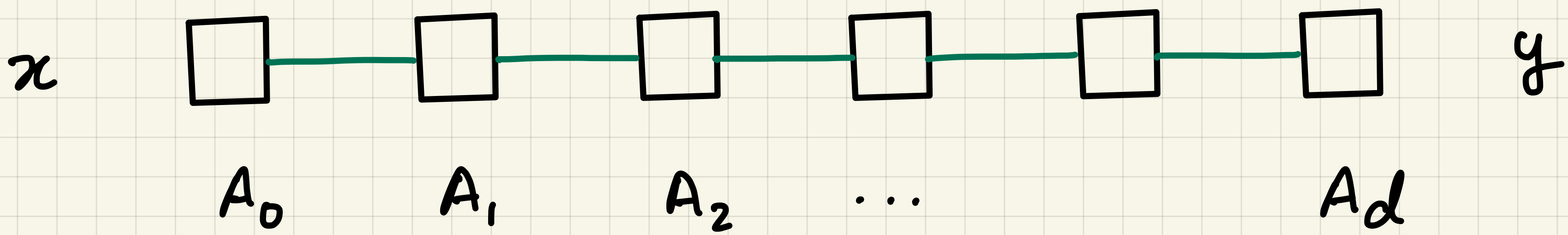
- Quantum : better algorithms ?

- New lower bound : $\tilde{\Omega}(\sqrt[3]{nd^2})$ [MN'20]

- Implies $\tilde{\Omega}(\sqrt[3]{p\Delta^2})$ lower bound for Diameter in Congest model

  (p processors, diameter Δ)

Line Disjointness $L_{n,d}$

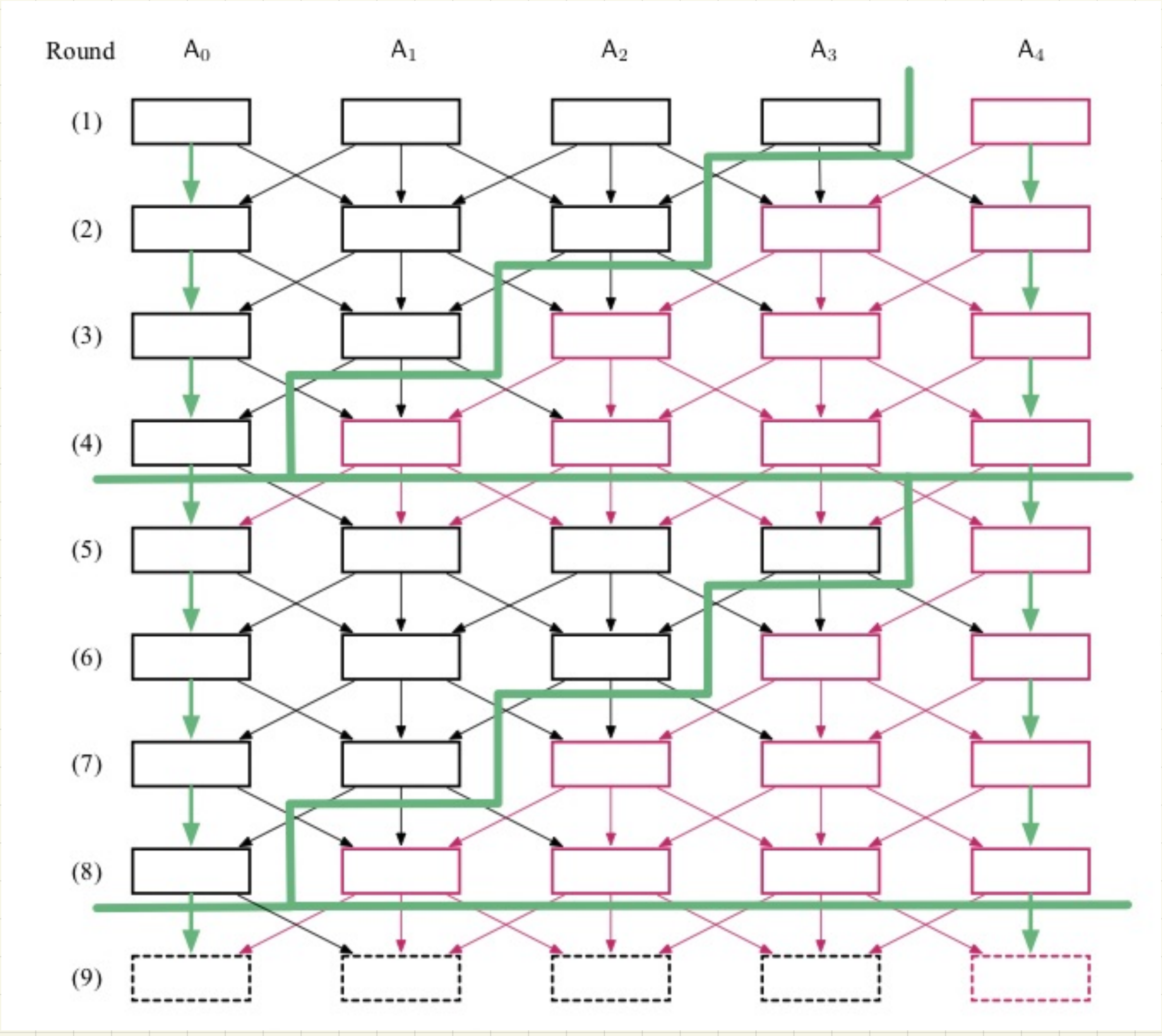


Given a protocol for $L_{n,d}$, we derive one for Set-Disjointness (two party case)

Two-party protocol from algorithm

$d = 4$, $r = 8$ rounds

x



y

Two-party protocol from algorithm

- Round "compression"

  r round algorithm, $d+1$ processors

  $\Longrightarrow$ $2(r/d)$ round protocol, 2 parties

Two-party protocol from algorithm

- Round "compression"

  r round algorithm, $d+1$ processors

  $\Rightarrow$ $2(r/d)$ round protocol, 2 parties

- Information leaked about input/round

  $\leq$ polylog(n)

  $\Rightarrow$ 2-party protocol : message leaks

  $\leq$ d polylog(n) bits of info per round

Formal argument

- Information Leakage $\widetilde{IL}(\Pi \mid XYZ)$
  (X, Y independent given Z)

$$= \sum_{k \text{ odd}} I(X : \underbrace{B_k \tilde{Y}}_{} \mid Z) + \sum_{k \text{ even}} I(X : B_k \tilde{Y} \mid Z)$$

Alice speaks

Bob's registers after kth msg
Y in superposition

- We show

$$\widetilde{IL}(\Pi \mid XYZ) \leq \left(\frac{4r^2}{d}\right) \text{polylog}(n)$$

Improved lower bound

- Implicit in [JRS'03] : Set Disjointness

  $\exists$ XYZ : X, Y independent given Z,

$$\widetilde{\mathrm{IL}}(\Pi \mid XYZ) \geq n / (\#\text{ rounds})$$

- Round complexity of $L_{n,d}$

$$\left(\frac{4r^2}{d}\right) \mathrm{polylog}(n) \geq n/(2r/d)$$

$$\Rightarrow \quad r \in \tilde{\Omega}\left(\sqrt[3]{nd^2}\right)$$

Remarks

- Several problems related to learning states and their properties remain open

- Optimal round complexity of Line Disj, Diameter in Congest model, remain open

- Information theory : powerful means of studying computational models, has been applied in several other contexts. Yet more applications on the horizon!