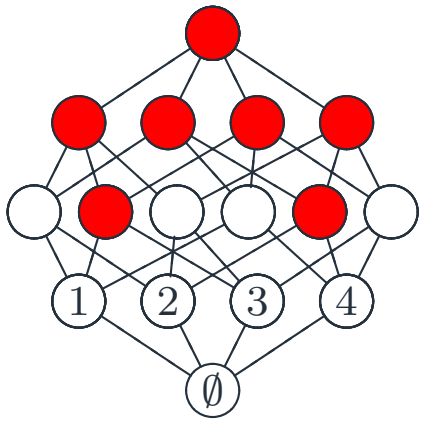
Quantum query complexity and the adversary bound
Part III: Dual learning graphs

Alexander Belov
University of Latvia

22nd EWSCS, 5-10 March 2017, Palmse

Learning graphs revisited

Definition again



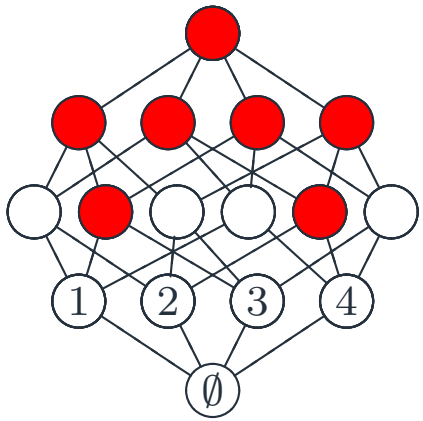
- Each arc e of the Hasse diagram is assigned weight $w_e \geq 0$.
- For each $M \in \mathcal{C}$, we construct flow $p_e(M)$ from $\emptyset$ to M.

Learning graph complexity of $\mathcal{C}$ is

$$\text{minimise} \quad \max_M \left\{ \sum_e w_e, \sum_e \frac{p_e(M)^2}{w_e} \right\}$$

$$\text{subject to} \quad p_e(M) \text{ is a flow of value } 1 \text{ from } \emptyset \text{ to } M$$

Definition again



- Each arc e of the Hasse diagram is assigned weight $w_e \geq 0$.
- For each $M \in \mathcal{C}$, we construct flow $p_e(M)$ from $\emptyset$ to M.

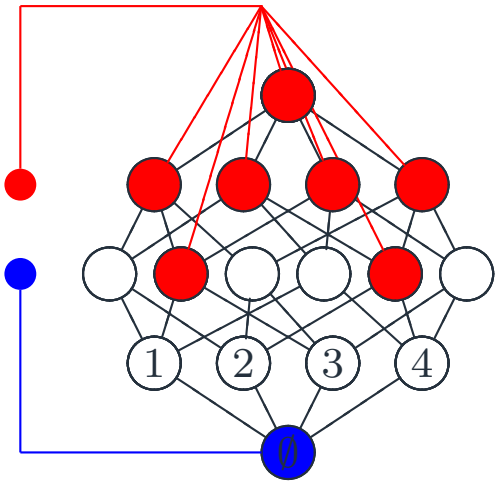
Learning graph complexity of $\mathcal{C}$ is

$$\text{minimise} \quad \sqrt{\sum_e w_e}$$

$$\text{subject to} \quad \sum_e \frac{p_e(M)^2}{w_e} \leq 1$$

$p_e(M)$ is a flow of value 1 from $\emptyset$ to M

Definition again



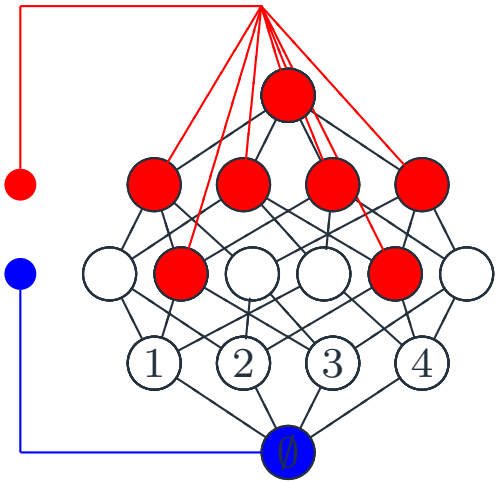
- Each arc e of the Hasse diagram is assigned weight $w_e \geq 0$.
- The weight is treated as conductance.

Learning graph complexity of $\mathcal{C}$ is

minimise $\sqrt{\sum_e w_e}$

subject to Effective resistance from $\emptyset$ to M is at most 1

Consequence



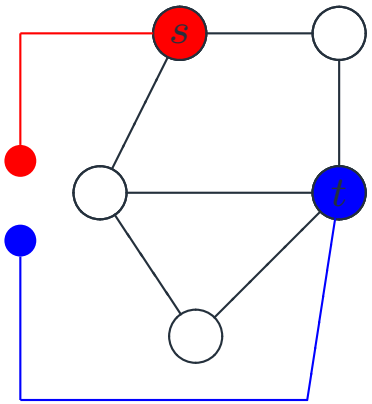
minimise $\sqrt{\sum_e w_e}$

subject to Effective resistance from $\emptyset$ to M is at most 1

Theorem. Hitting time of a random walk from s to t is at most $2RW$, where R is the effective resistance between s and t, and W is the total weight.

Hence, learning graphs provide at most quadratic speed-up.

Duality



Let G be an electric circuit with terminals s and t.

Two dual formulations of effective resistance:

First, effective resistance equals the minimum of

$$\sum_e \frac{p_e^2}{w_e}$$

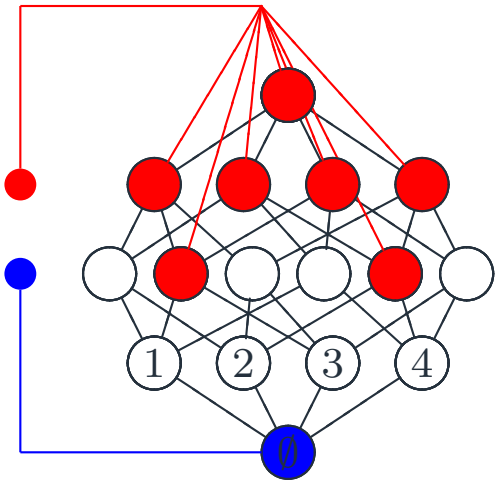
over all flows p_e of value 1 from s to t.

Second, effective conductance equals the maximum of

$$\sum_{uv} w_e(\alpha_u - \alpha_v)^2,$$

where α_u is the potential function satisfying $\alpha_s = 0$ and $\alpha_t = 1$.

Duality



minimise $\sqrt{\sum_e w_e}$

subject to Effective resistance from $\emptyset$ to M is at most 1

has dual formulation:

maximise $\sqrt{\sum_{M \in \mathcal{C}} \alpha_\emptyset(M)^2}$

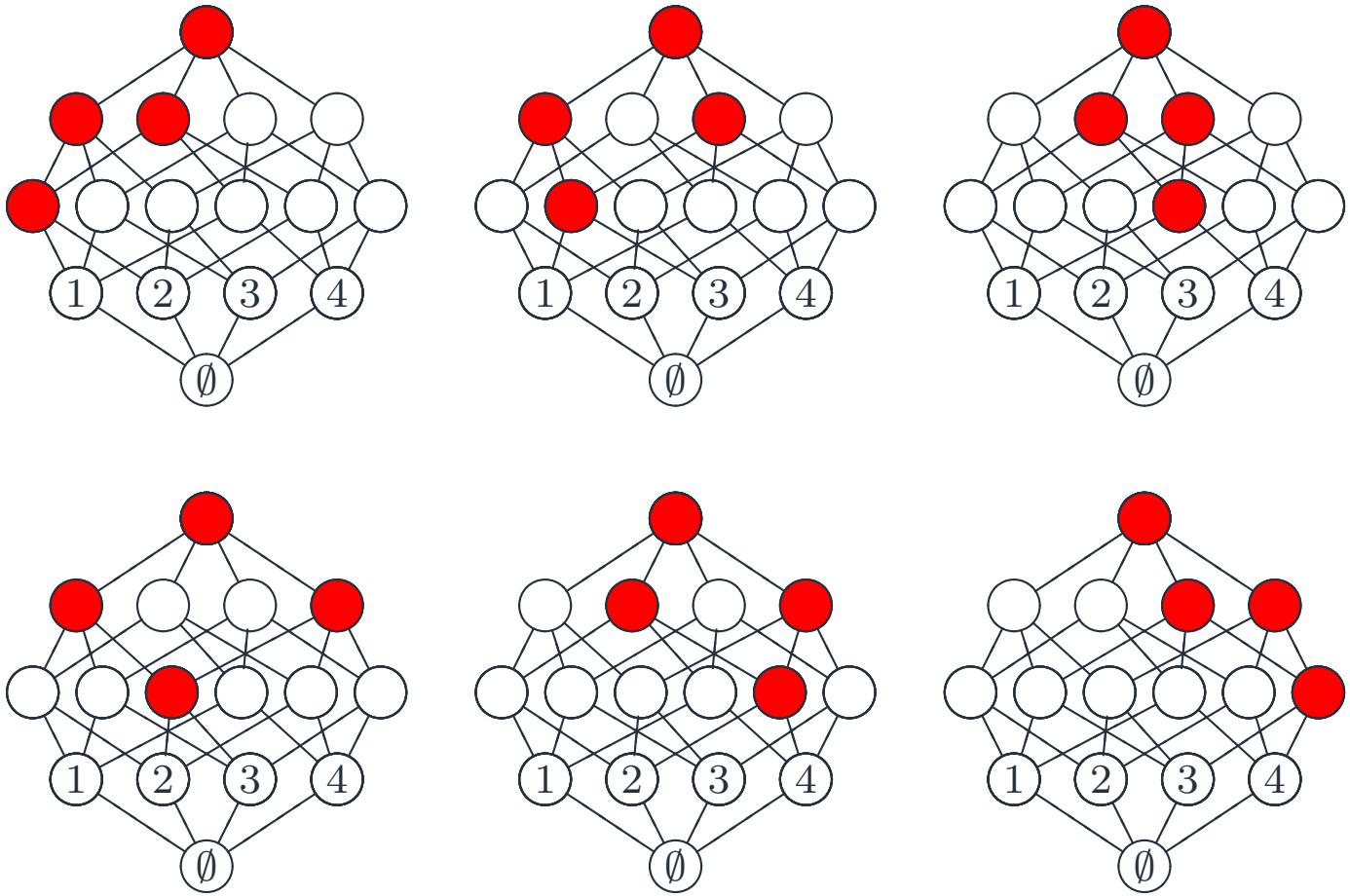
subject to $\sum_{M \in \mathcal{C}} \big(\alpha_S(M) - \alpha_{S \cup \{j\}}(M)\big)^2 \leq 1$ for all $j \notin S$;

$\alpha_S(M) = 0$ if $S \in M$.

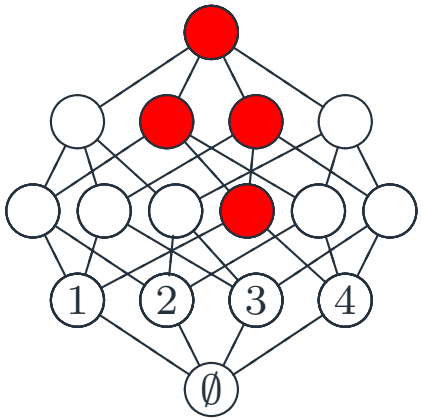
k-subset certificate structure

Definition

Formed by subsets of size k:



Complexity



$$\max. \sqrt{\sum_{M \in \mathcal{C}} \alpha_\emptyset(M)^2}$$

$$\sum_{M \in \mathcal{C}} \big(\alpha_S(M) - \alpha_{S \cup \{j\}}(M)\big)^2 \leq 1$$

$$\alpha_S(M) = 0 \quad \text{whenever } S \in M$$

Define

$$\alpha_S(M) = \begin{cases} \binom{n}{k}^{-1/2} \max\{n^{k/(k+1)} - |S|,\ 0\}, & S \notin M \\ 0, & \text{otherwise.} \end{cases}$$

Learning graph complexity is $\Theta\big(n^{k/(k+1)}\big)$.

Tightness

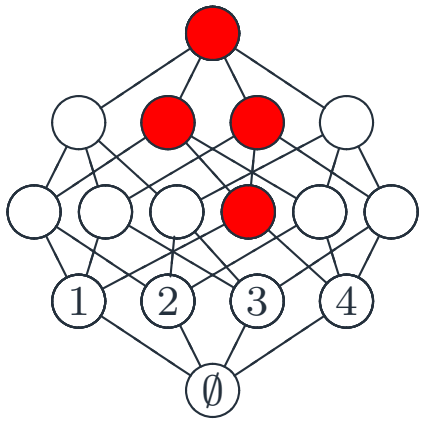
Learning graphs are tight:

Theorem. For any certificate structure $\mathcal{C}$, there exists a function f possessing $\mathcal{C}$ such that the quantum query complexity of f is at least the learning graph complexity of $\mathcal{C}$ up to a constant factor.

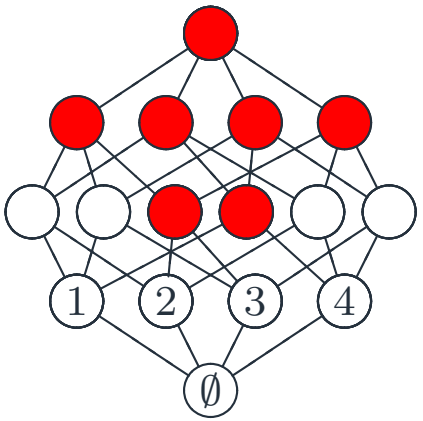
Boundedly generated certificate structures

A certificate structure $\mathcal{C}$ is boundedly generated if, for any $M \in \mathcal{C}$, one can find a subset $A_M \subseteq [n]$ such that $|A_M| = O(1)$, and $S \in M$ if and only if $S \supseteq A_M$.

The k-subset certificate structure is boundedly generated:



The collision certificate structure is not:



Tightness II

A certificate structure $\mathcal{C}$ is boundedly generated if, for any $M \in \mathcal{C}$, one can find a subset $A_M \subseteq [n]$ such that $|A_M| = O(1)$, and $S \in M$ if and only if $S \supseteq A_M$.

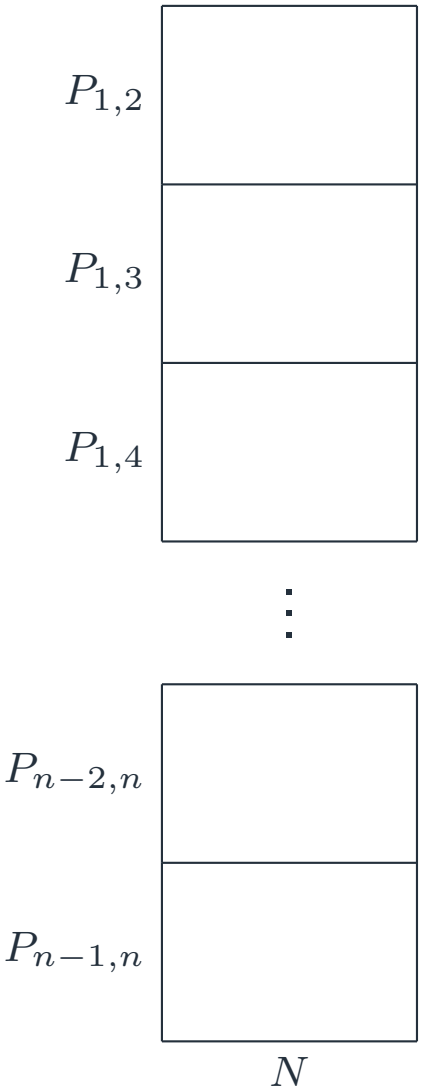
$\mathcal{C}$-sum problem.
Given $(x_1, \ldots, x_n) \in [q]^n$, decide whether there exists $M \in \mathcal{C}$ such that $\sum_{j \in A_M} x_j$ is divisible by q.

Theorem. If $\mathcal{C}$ is boundedly generated and f is the $\mathcal{C}$-sum problem with $q > 2|\mathcal{C}|$, then the quantum query complexity of f equals the learning graph complexity of f up to a constant factor.

Corollary. The quantum query complexity of the k-sum problem is $\Theta(n^{k/(k+1)})$.

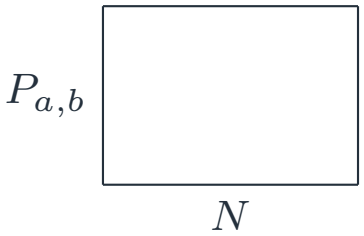
Proof

Adversary Matrix

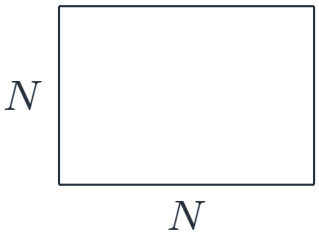


N : negative inputs

$P_{a,b}$: positive inputs x with $x_a = x_b$



will try to mimic

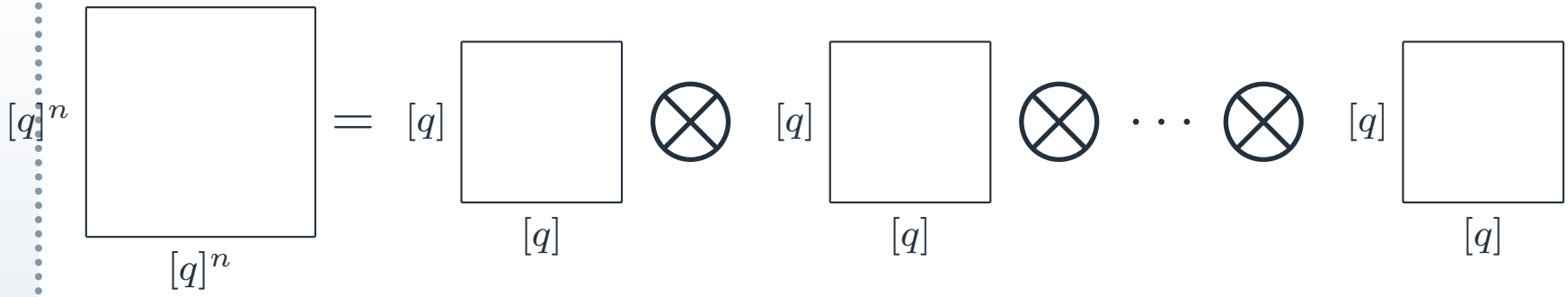


Negative Inputs

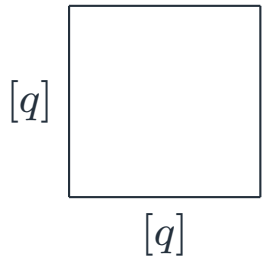
If q is large, almost all inputs are negative.

- Approximate negative inputs by all inputs: $N = [q]^n$.

Elements become independent:



One symbol

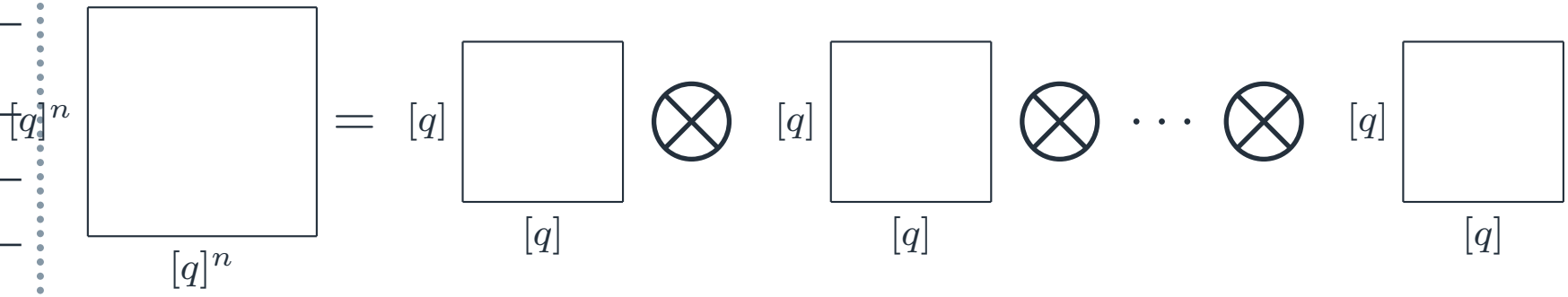


$$E_0 = \frac{1}{q}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix} \qquad I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

I contains E_0, hence, we consider

$$E_1 = I - E_0 = \frac{1}{q}\begin{pmatrix} q-1 & -1 & \cdots & -1 \\ -1 & q-1 & \cdots & -1 \\ \vdots & & \ddots & \vdots \\ -1 & -1 & \cdots & q-1 \end{pmatrix}$$

Projectors



Define

$$E_S = E_{s_1} \otimes E_{s_2} \otimes \cdots \otimes E_{s_n}$$

with $S \subseteq [n]$, and

$$s_j = \begin{cases} 1, & j \in S; \\ 0, & j \notin S. \end{cases}$$

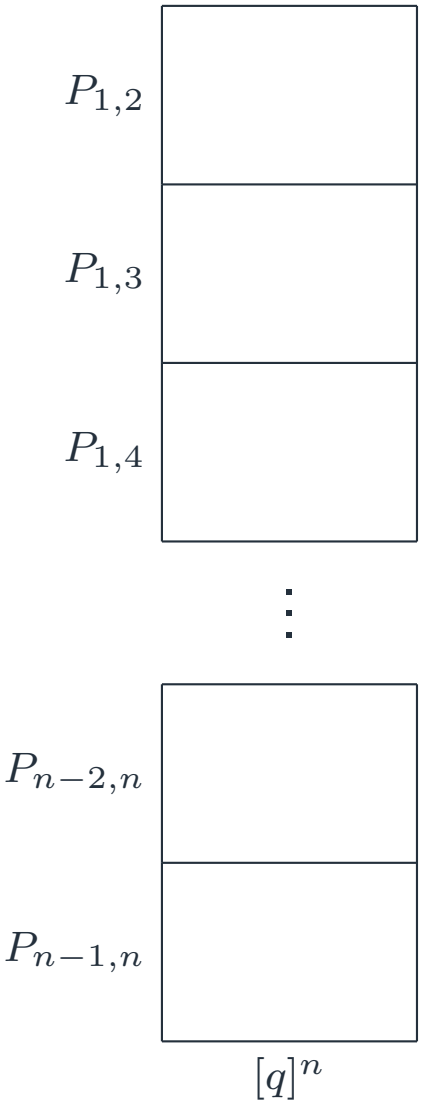
- Orthogonal projectors
- E_S: values of variables in S are known

- E_S: values of variables in S are known

Say, $n = 6$ and $S = \{2, 5\}$

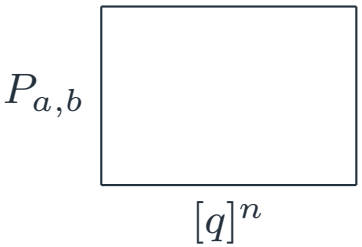
E_0	E_1	E_0	E_0	E_1	E_0
1	1	1	1	1	1
1	1	1	1	1	2
⋮	⋮	⋮	⋮	⋮	
15	6	49	8	2	22
⋮	⋮	⋮	⋮	⋮	
37	1	3	19	54	1
⋮	⋮	⋮	⋮	⋮	
q	q	q	q	q	$q-1$
q	q	q	q	q	q

Adversary Matrix

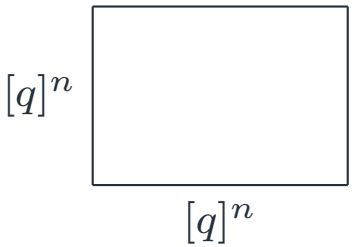


N : strings from $[q]^n$

$P_{a,b}$: strings x from $[q]^n$ such that $x_a = x_b$, each repeated q times



will try to mimic



Mimicking

E_1	E_0
1	1
1	1
⋮	⋮
1	1
2	2
2	2
⋮	⋮
2	2
⋮	⋮
q	q
⋮	⋮
q	q
q	q

looks like

E_1	E_0
1	1
1	2
⋮	⋮
1	q
2	1
2	2
⋮	⋮
2	q
⋮	⋮
q	1
⋮	⋮
q	$q-1$
q	q

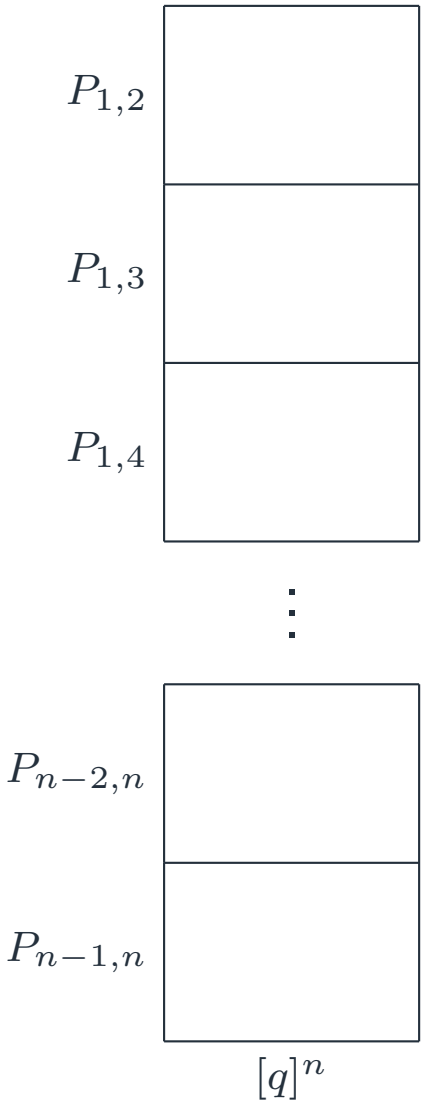
E_0	E_1
1	1
1	1
⋮	⋮
1	1
2	2
2	2
⋮	⋮
2	2
⋮	⋮
q	q
⋮	⋮
q	q
q	q

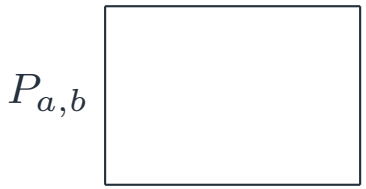
looks like

E_0	E_1
1	1
2	1
⋮	⋮
q	1
1	2
2	2
⋮	⋮
q	2
⋮	⋮
1	q
⋮	⋮
$q-1$	q
q	q

$E_1 \otimes E_1$ cannot be mimicked!

Mimicking





successfully mimics

$$\sum_{S \subseteq [n]} \alpha_{a,b;S} E_S$$

with $\alpha_{a,b;S} = 0$ if $\{a, b\} \subseteq S$.

Action of Δ

$$E_0: \quad \frac{1}{q}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix} \qquad \frac{1}{q}\begin{pmatrix} q-1 & -1 & \cdots & -1 \\ -1 & q-1 & \cdots & -1 \\ \vdots & & \ddots & \vdots \\ -1 & -1 & \cdots & q-1 \end{pmatrix} \quad :E_1$$

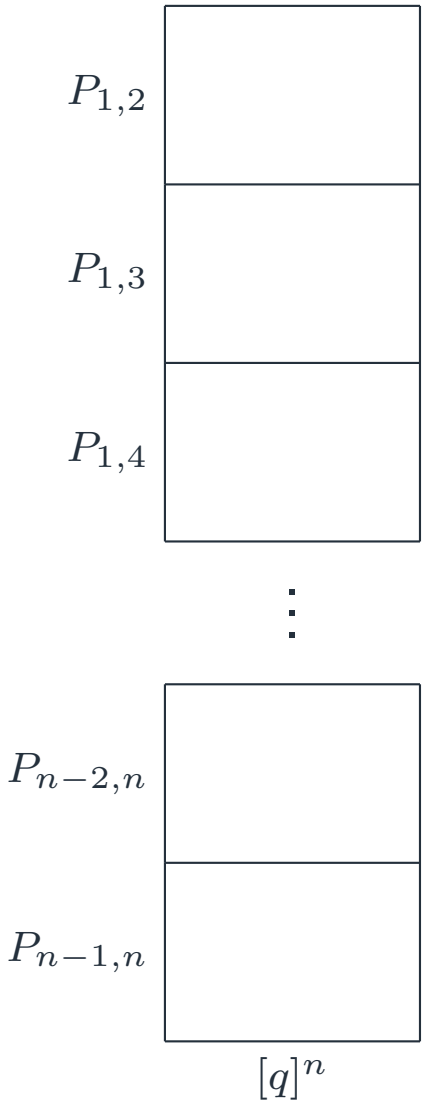
$$\Downarrow \qquad\qquad \Downarrow$$

$$\frac{1}{q}\begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{pmatrix} \qquad \frac{1}{q}\begin{pmatrix} 0 & -1 & \cdots & -1 \\ -1 & 0 & \cdots & -1 \\ \vdots & & \ddots & \vdots \\ -1 & -1 & \cdots & 0 \end{pmatrix}$$

Approximate:

$$E_0 \mapsto E_0 \qquad \text{and} \qquad E_1 \mapsto -E_0$$

Finishing off



$$E_0 \mapsto E_0 \qquad \text{and} \qquad E_1 \mapsto -E_0$$

$$E_S \circ \Delta_j = \begin{cases} E_S & j \notin S; \\ -E_{S \setminus \{j\}} & j \in S; \end{cases}$$

maximize	$\|\Gamma\|$
subject to	$\|\Gamma \circ \Delta_j\| \leq 1$ for all $j \in [n]$

$$\Gamma^* \Gamma = \sum_{S \subseteq [n]} \left[\sum_{a,b} \alpha^2_{a,b;S} \right] E_S.$$

Finishing off

$$E_S \circ \Delta_j = \begin{cases} E_S & j \notin S; \\ -E_{S\setminus\{j\}} & j \in S; \end{cases} \qquad \Gamma^*\Gamma = \sum_{S\subseteq[n]} \left[\sum_{a,b} \alpha^2_{a,b;S} \right] E_S.$$

maximize	$\|\Gamma\|$
subject to	$\|\Gamma \circ \Delta_j\| \le 1$ for all $j \in [n]$

We get:

maximize $\sqrt{\sum_{a,b} \alpha^2_{a,b;\emptyset}}$

subject to $\sum_{a,b} (\alpha_{a,b;S} - \alpha_{a,b;S\cup\{j\}})^2 \le 1$ for all $j \notin S \subseteq [n]$;

$\alpha_{a,b;S} = 0$ if $\{a,b\} \subseteq S$.

Thank you!