Adversary Lower Bound for the k-sum Problem

Alexander Belov
University of Latvia

Robert Špalek
Google, Inc.

January 22, 2013
QIP 2013, Beijing, China

IEGULDĪJUMS TAVĀ NĀKOTNĒ

This work has been supported by the European Social Fund within the project "Support for Doctoral Studies at University of Latvia"

On the Power of Learning Graphs

Alexander Belov
University of Latvia

Ansis Rosmanis
University of Waterloo

Robert Špalek
Google, Inc.

Based on arXiv:1206.6528 and arXiv:1210.3279

Query Complexity

Problem

Computational Problem

The amount of resources required to solve it?

Ideally: Time necessary for a quantum computer to solve it.

Problem

Computational Problem

The amount of resources required to solve it?

Ideally: Time necessary for a quantum computer to solve it.

Alas, we don't know much about it.

Problem

Computational Problem

The amount of resources required to solve it?

Ideally: ~~Time necessary~~ for a quantum computer to solve it.
Simplification: Number of accesses to the input string

Quantum Query Complexity

Function

$$f\colon [q]^n \supseteq \mathcal{D} \to \{0,1\}$$

Query algorithm:	calculate $f(x_1, x_2, \ldots, x_n)$, can access individual x_j in one query.
Quantum query complexity:	number of queries the best quantum query algorithm makes on the worst input.

Quantum Query Complexity

Function

$$f\colon [q]^n \supseteq \mathcal{D} \to \{0,1\}$$

Query algorithm:	calculate $f(x_1, x_2, \ldots, x_n)$, can access individual x_j in one query.
Quantum query complexity:	number of queries the best quantum query algorithm makes on the worst input.

Does this make things simpler?..

Quantum query complexity admits formulation as an SDP:
Adversary Bound

$$\begin{array}{lll} \text{maximize} & \|\Gamma\| & \\ \text{subject to} & \|\Gamma \circ \Delta_j\| \leq 1 & \text{for all } j \in [n]. \end{array}$$

Here: Γ is an $f^{-1}(1) \times f^{-1}(0)$-matrix with real entries, and

$$\Delta_j[\![x, y]\!] = \begin{cases} 1, & x_j \neq y_j; \\ 0, & \text{otherwise.} \end{cases}$$

Certificate Structures

Simplification

Simplification II:
Only consider the *positions* of certificates inside the input string.
Not the values therein.

Example/Motivation

Quantum walk on the Johnson Graph

Ambainis developed it to solve k-distinctness:

Given $(x_1, \ldots, x_n)$, detect whether there are k equal elements among them.

Quantum walk on subsets of $[n]$.
Accept if the values of variables in $S \subseteq [n]$ are enough to deduce $f(x) = 1$.

Runs in $O\left(n^{k/(k+1)}\right)$ quantum queries.

Example/Motivation

Quantum walk on the Johnson Graph
Ambainis developed it to solve k-distinctness:
Given $(x_1, \ldots, x_n)$, detect whether there are k equal elements among them.

Quantum walk on subsets of $[n]$.
Accept if the values of variables in $S \subseteq [n]$ are enough to deduce $f(x) = 1$.

Runs in $O\left(n^{k/(k+1)}\right)$ quantum queries.

Childs and Eisenberg:
The same algorithm can be used for *any* function with small certificates:

k-distinctness, k-sum, graph collision, matrix product verification...

k-sum:
Given $(x_1, \ldots, x_n) \in [q]^n$, detect whether there are k elements whose sum is divisible by q.

Certificate Structure

Function

$$f\colon [q]^n \supseteq \mathcal{D} \to \{0,1\}$$

For $x \in f^{-1}(1)$, write out:

$$M_x = \{S \subseteq [n] \mid S \text{ is enough to deduce } f(x) = 1 \}.$$

The set of all M_x is a *certificate structure* $\mathcal{C}$.
(Interested in inclusion-wise minimal M_x only.)

Certificate Structure

Function

$$f\colon [q]^n \supseteq \mathcal{D} \to \{0,1\}$$

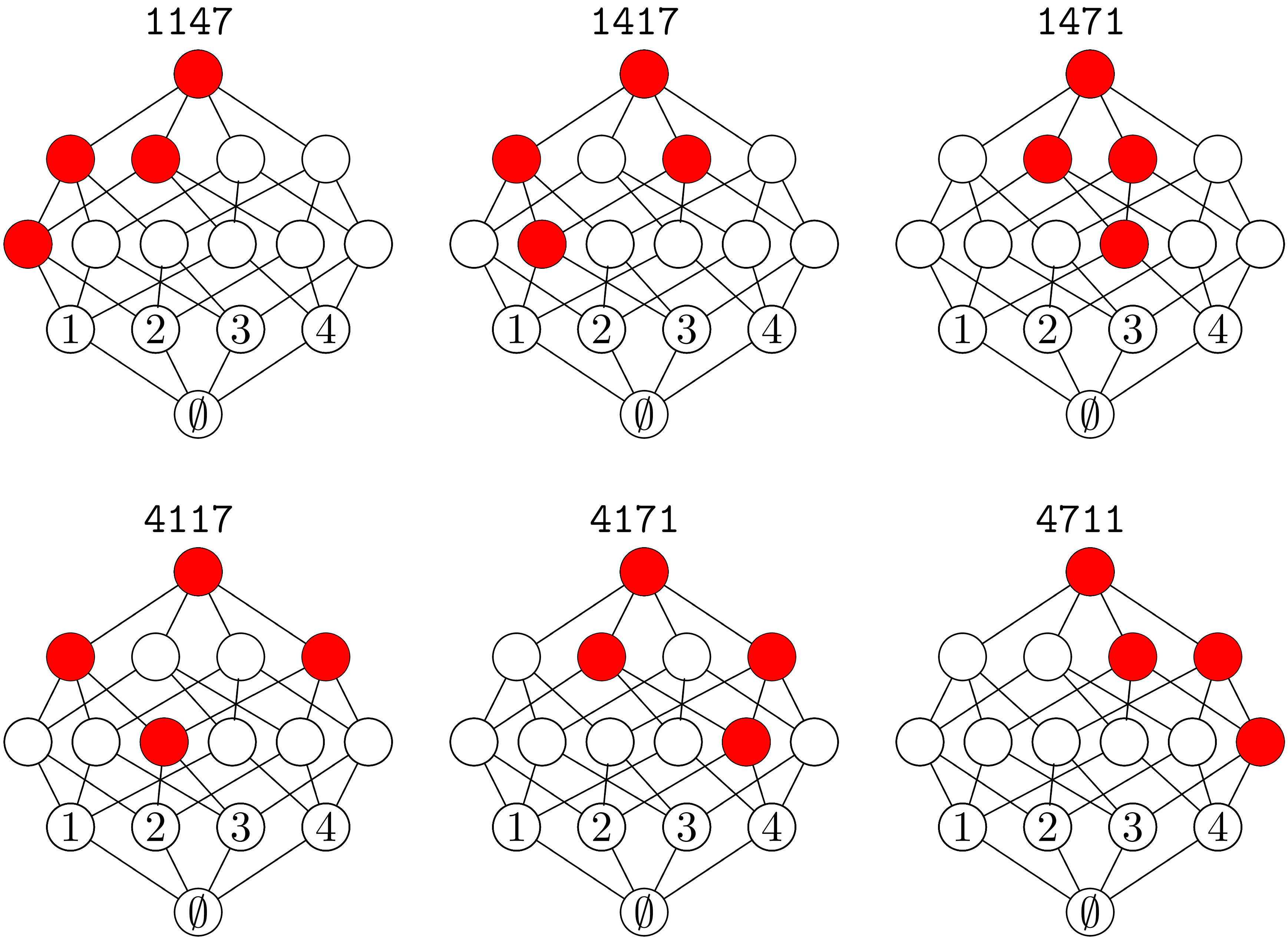
For $x \in f^{-1}(1)$, write out:

$$M_x = \{ S \subseteq [n] \mid S \text{ is enough to deduce } f(x) = 1 \}.$$

The set of all M_x is a *certificate structure* $\mathcal{C}$.
(Interested in inclusion-wise minimal M_x only.)

k-**subset certificate structure**
Mutual certificate structure of k-distinctness and k-sum.

2-subset on 4 variables:



(Only interested in *inclusion-minimal* M_x.)

Example/Motivation

Quantum walk on subsets of $[n]$.
Accept if the values of x in $S \subseteq [n]$ are enough to deduce $f(x) = 1$.

Runs in $O\left(n^{k/(k+1)}\right)$ quantum queries.

Conjecture (Childs and Eisenberg). *Quantum walk on the Johnson graph is optimal for the k-sum problem.*

Example/Motivation

Quantum walk on subsets of $[n]$.
Accept if the values of x in $S \subseteq [n]$ are enough to deduce $f(x) = 1$.

Runs in $O\left(n^{k/(k+1)}\right)$ quantum queries.

Conjecture (Childs and Eisenberg)**.** *Quantum walk on the Johnson graph is optimal for the k-sum problem.*

Intuition: Even if we are given $k-1$ elements of a k-tuple, we have absolutely no additional information whether the k-tuple forms a certificate.

The k-sum problem does not possess any structure.

Another Example

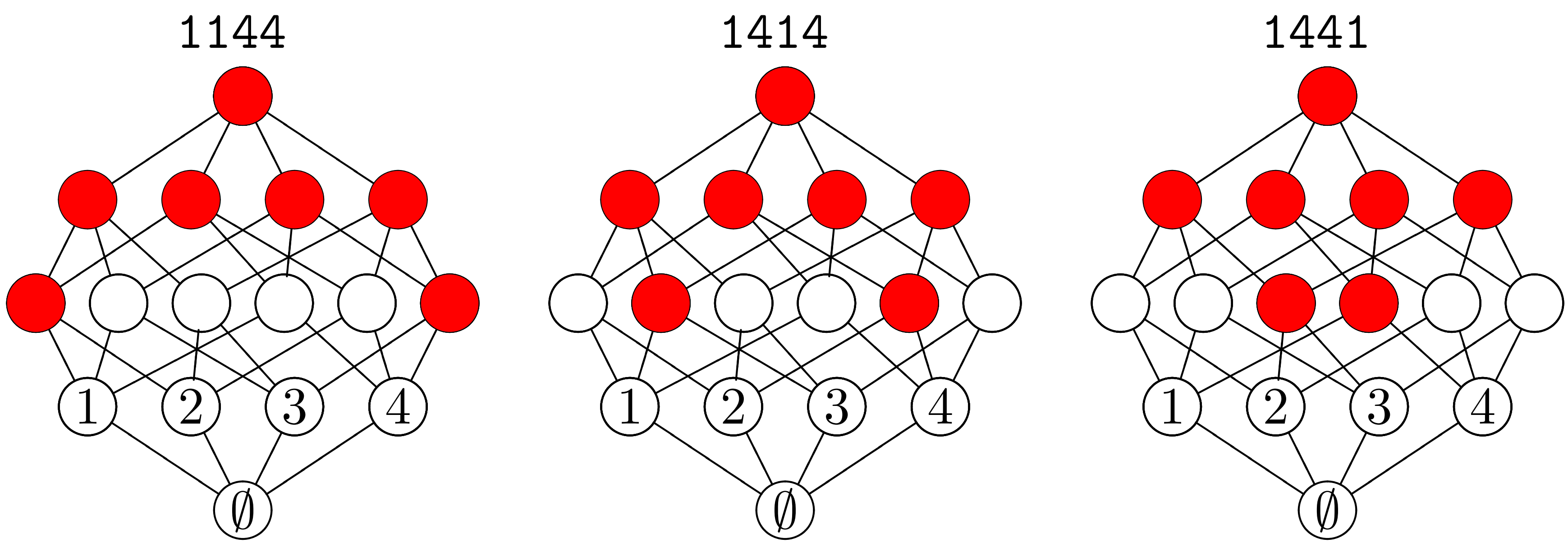
Collision Problem

Distinguish between two cases

Negative: each symbol in the input string is unique; or

Positive: each symbol in the input string has exactly two appearances.

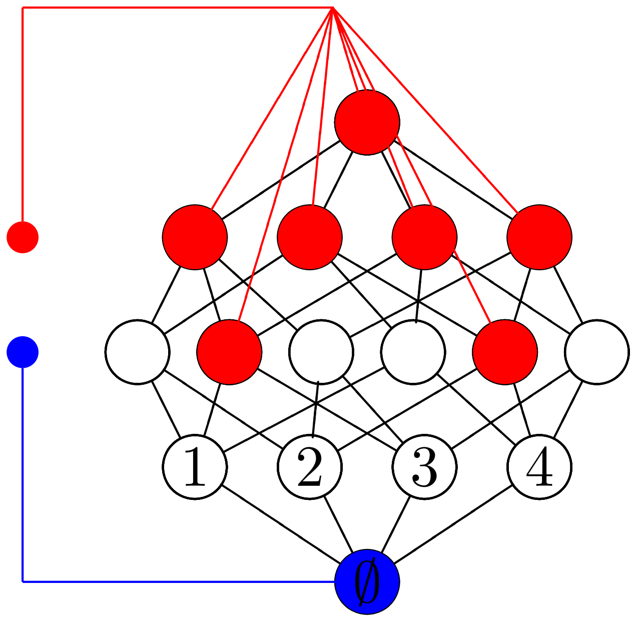
E.g., negative input: 2746 and three variants of positive inputs:



Learning graphs

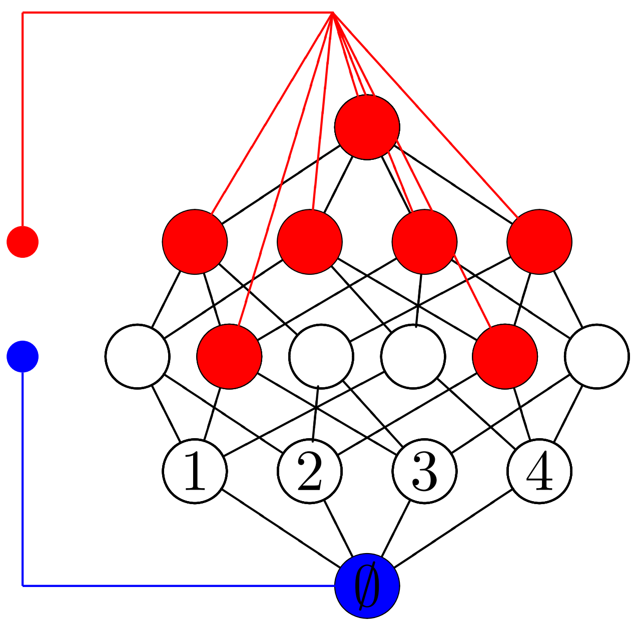
- Computational model that relies on the certificate structure by definition.
- Generalizes quantum walk on the Johnson graph.

Learning graphs



- Each edge e of the Hasse diagram is assigned non-negative conductance c_e.
- For each $M \in \mathcal{C}$, we connect $\emptyset$ to one terminal, and all $S \in M$ to the other terminal of a current source.

Learning graphs

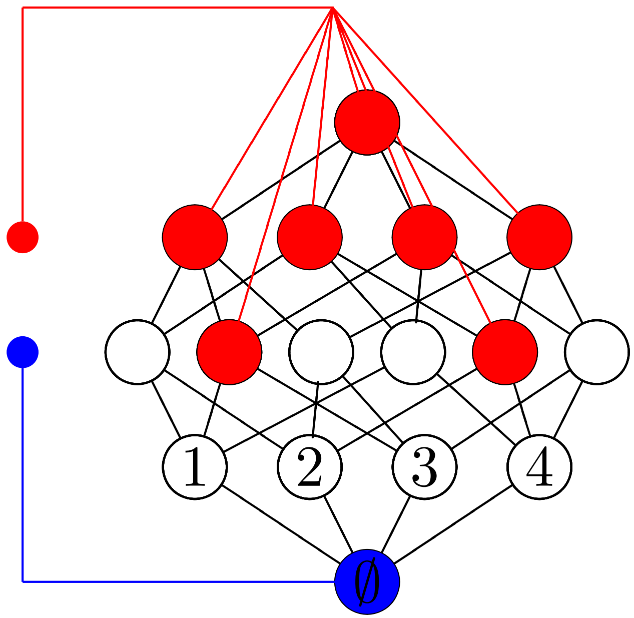


- Each edge e of the Hasse diagram is assigned non-negative conductance c_e.
- For each $M \in \mathcal{C}$, we connect $\emptyset$ to one terminal, and all $S \in M$ to the other terminal of a current source.

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

minimize	$\sqrt{\sum_{e \in \mathcal{E}} c_e}$
subject to	effective resistance from $\emptyset$ to M is at most 1 for all $M \in \mathcal{C}$

Learning graphs



- Each edge e of the Hasse diagram is assigned non-negative conductance c_e.
- For each $M \in \mathcal{C}$, we connect $\emptyset$ to one terminal, and all $S \in M$ to the other terminal of a current source.

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

minimize	$\sqrt{\sum_{e \in \mathcal{E}} c_e}$
subject to	effective resistance from $\emptyset$ to M is at most 1 for all $M \in \mathcal{C}$

Theorem (Belov and Lee). *For each f having certificate structure $\mathcal{C}$, there exists a quantum query algorithm with complexity equal to the learning graph complexity of $\mathcal{C}$ up to a constant factor.*

Our Results

Outline

- We derive a dual formulation of the learning graph complexity.
- We use it to give (almost) tight lower bounds for some certificate structures:

k-subset, collision, hidden shift, triangle.

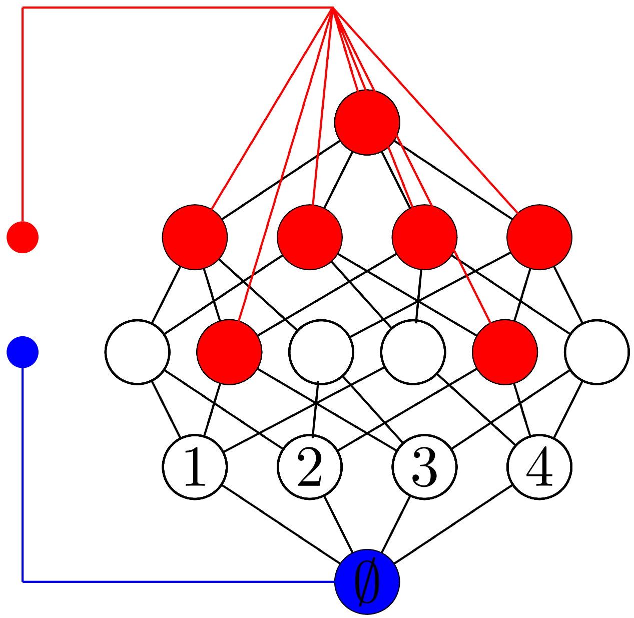
Outline

- We derive a dual formulation of the learning graph complexity.
- We use it to give (almost) tight lower bounds for some certificate structures:

  k-subset, collision, hidden shift, triangle.

- We prove learning graphs are tight for any certificate structure.
- We prove an analogue of Childs-Eisenberg conjecture for a wide range of certificate structures.
  (Implies the original conjecture).

Learning Graph Revisited



More details (using electric flow):

minimize $\sqrt{\sum_{e\in\mathcal{E}} c_e}$

subject to $\sum_{e\in\mathcal{E}} \frac{p_e(M)^2}{c_e} \le 1$ for all $M \in \mathcal{C}$;

for each $M \in \mathcal{C}$, $p_e(M)$ form a flow from $\emptyset$ to M of value 1

The *dual formulation* (using potentials):

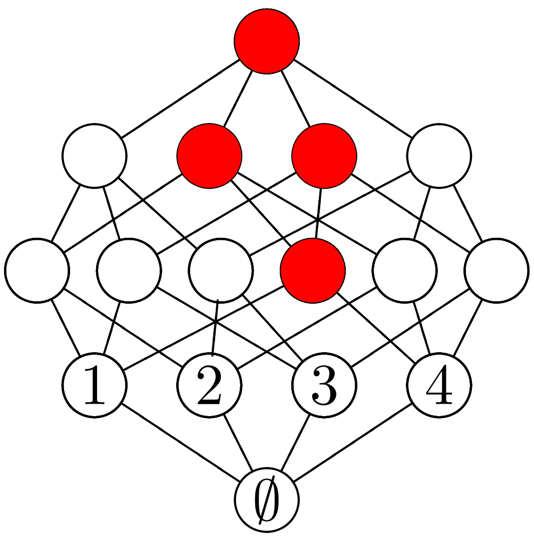
maximize $\sqrt{\sum_{M\in\mathcal{C}} \alpha_\emptyset(M)^2}$

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

$\alpha_S(M) = 0$ whenever $S \in M$;

k-subset certificate structure

Theorem. *The learning graph complexity of the k-subset certificate structure is* $\Omega(n^{k/(k+1)})$.



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

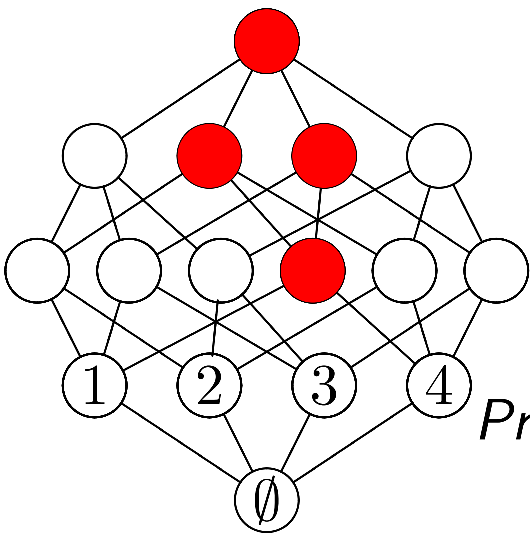
$$\sum_{M \in \mathcal{C}} \big(\alpha_S(M) - \alpha_{S \cup \{j\}}(M)\big)^2 \le 1$$

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

k-subset certificate structure

Theorem. *The learning graph complexity of the k-subset certificate structure is $\Omega(n^{k/(k+1)})$.*

max. $\sqrt{\sum_{M \in \mathcal{C}} \alpha_\emptyset(M)^2}$
$\sum_{M \in \mathcal{C}} \big(\alpha_S(M) - \alpha_{S\cup\{j\}}(M)\big)^2 \leq 1$ $\alpha_S(M) = 0$ whenever $S \in M$



Proof. Define

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

Perform simple calculations. $\square$

Other Certificate Structures

We also prove that the learning graph complexity

of the collision and the hidden shift certificate structures is $\Omega(\sqrt[3]{n})$

and

of the triangle certificate structure is $\tilde{\Omega}(n^{9/7})$.

Corollary. *The learning graph for the triangle problem from the next presentation is essentially tight.*

Tightness I

We prove learning graphs are tight:

Theorem. *For any certificate structure $\mathcal{C}$, there exists 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.*

Tightness I

We prove learning graphs are tight:

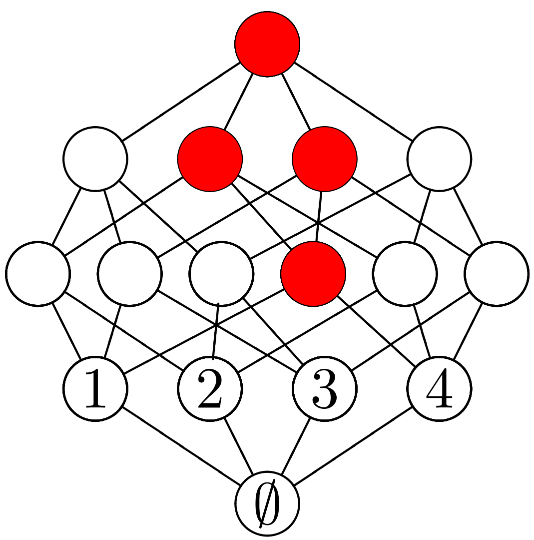
Theorem. *For any certificate structure $\mathcal{C}$, there exists f possessing $\mathcal{C}$ such that the quantum query complexity of f is at least the learning graph complexity of $\mathcal{C}$ up to a constant factor.*

For the analogue of the Childs-Eisenberg conjecture, we need more notions...

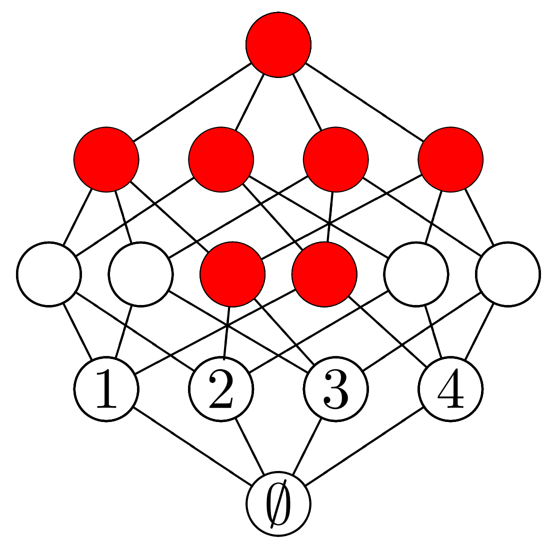
Boundedly generated certificate structures

Definition. 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

Definition. 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.*

Proof Sketch

Adversary Bound

We use the adversary bound

$$\begin{array}{lll} \text{maximize} & \|\Gamma\| & \\ \text{subject to} & \|\Gamma \circ \Delta_j\| \leq 1 & \text{for all } j \in [n]. \end{array}$$

Here: Γ is an $f^{-1}(1) \times f^{-1}(0)$-matrix with real entries, and

$$\Delta_j[\![x, y]\!] = \begin{cases} 1, & x_j \neq y_j; \\ 0, & \text{otherwise.} \end{cases}$$

Former Modes of Applications

Adversary bound has been used as:

1. **Non-negative weight adversary**
   Original version by Ambainis. Combinatorial reasoning. Easy to use.
   Has strong limitations (certificate complexity, property testing barriers).
   Fails for our applications.
2. **Small functions**
   By solving the optimization problem on computer.
3. **Tight composition theorems**
   Composing functions from the second point. Formulae evaluation.

We use spectral analysis via embedding.

Hamming Association Scheme

Two orthogonal projectors on $\mathbb{C}^q$:

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

For $S \subseteq [n]$, define

$$E_S = \bigotimes_{j=1}^{n} E_{S[\![j]\!]}.$$

These are orthogonal projectors on $\mathbb{C}^{q^n}$.

Action of Δ

$$\text{subject to } \|\Gamma \circ \Delta_j\| \leq 1 \qquad \text{for all } j \in [n].$$

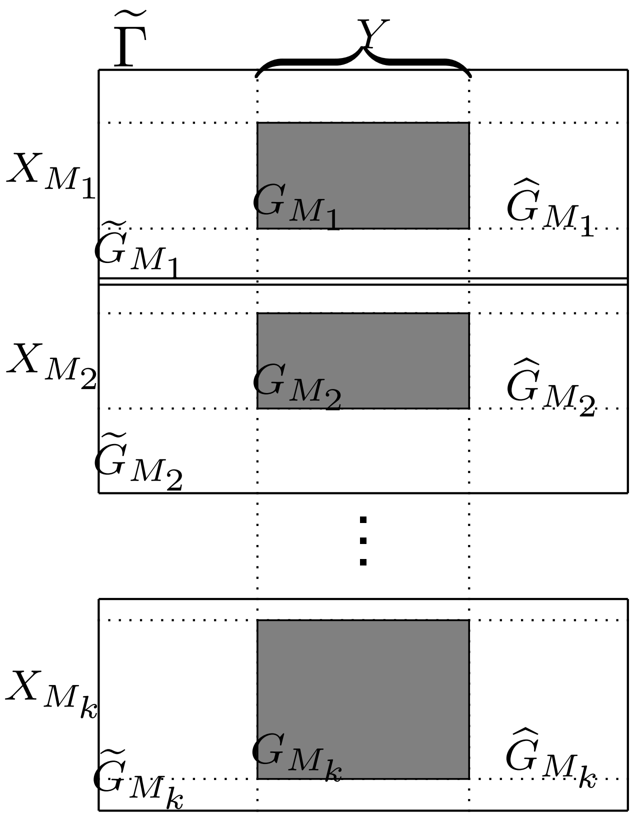
For

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

we have

$$E_0 \mapsto E_0 \qquad E_1 \mapsto -E_0.$$

Embedding Γ into $\widetilde{\Gamma}$



$\mathcal{C}$-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.

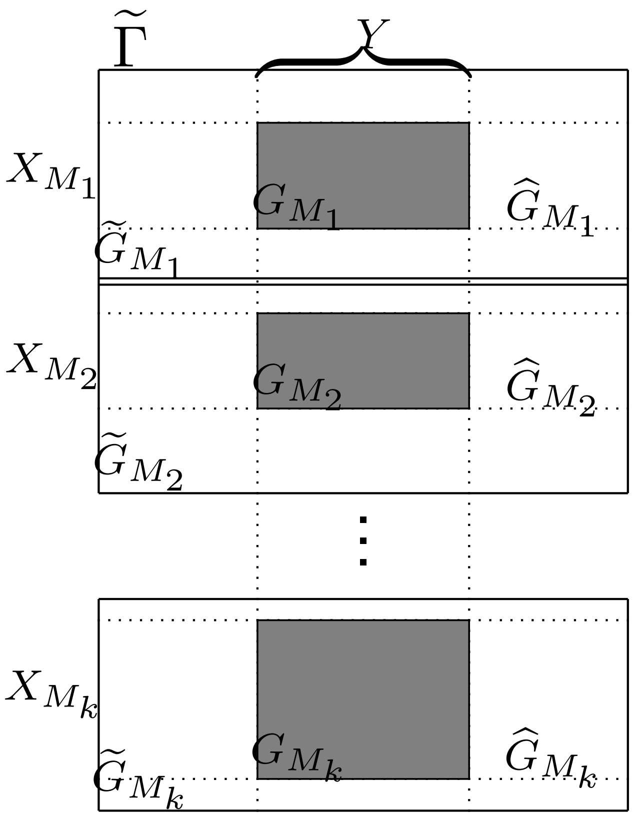
$\widetilde{G}_M$ is $[q]^n \times [q]^n$-matrix.

$X_M = \{x \in [q]^n \mid \sum_{j \in A_M} x_j \equiv 0 \pmod{q}\}$
$|X_M| = q^{n-1}$

Y is the set of negative inputs
$q \geq 2|\mathcal{C}| \implies |Y| \geq q^n/2$

Defining $\widetilde{\Gamma}$

max. $\|\Gamma\|$
$\|\Gamma \circ \Delta_j\| \leq 1$



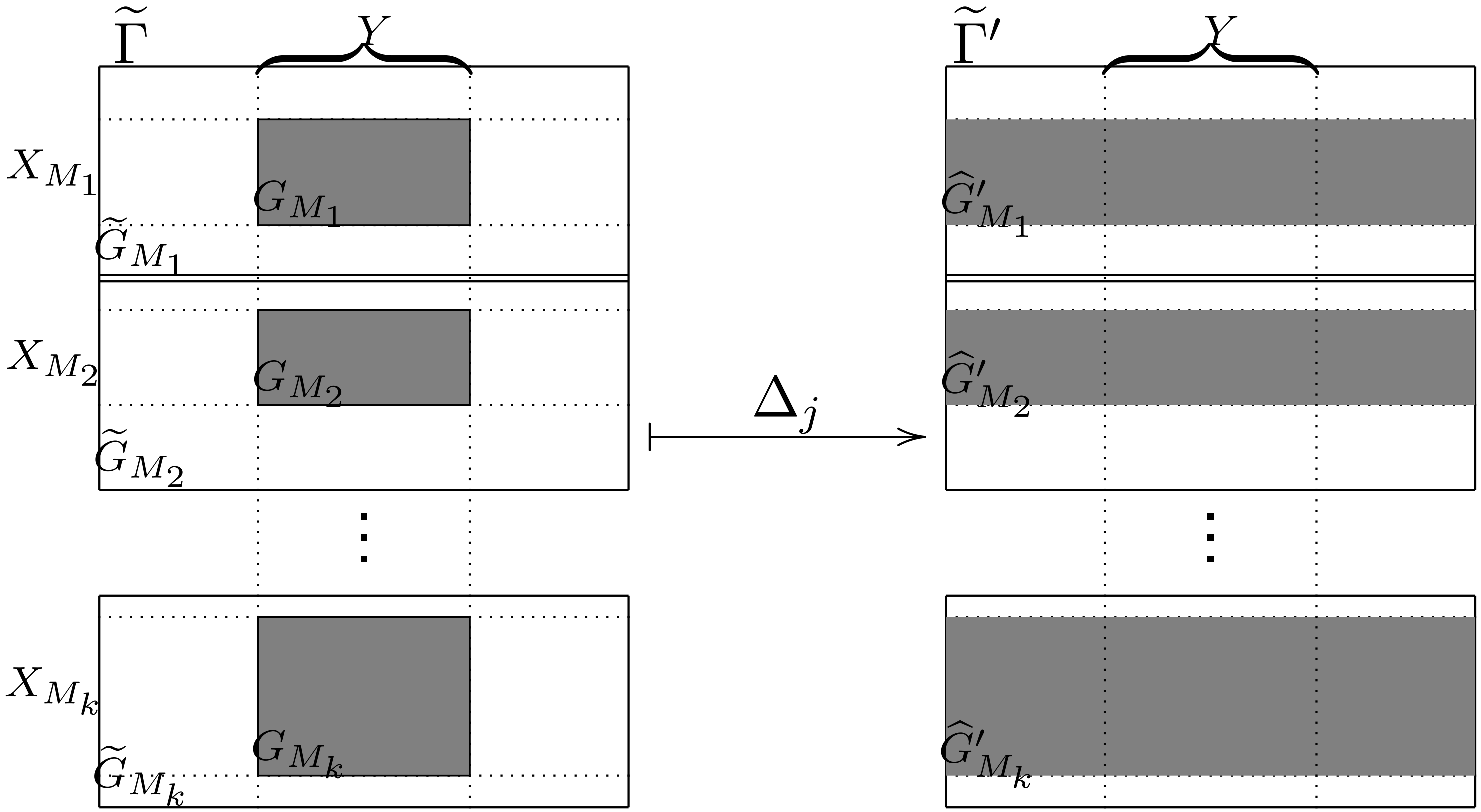
max. $\sqrt{\sum_{M \in \mathcal{C}} \alpha_\emptyset(M)^2}$
$\sum_{M \in \mathcal{C}} \left(\alpha_S(M) - \alpha_{S \cup \{j\}}(M)\right)^2 \leq 1$ $\alpha_S(M) = 0$ whenever $S \in M$

$$\widetilde{G}_M = \sum_{S \subseteq [n]} \alpha_S(M) E_S$$

$$\widehat{G}_M = \sqrt{q}\, \widetilde{G}_M [\![X_M, [q]^n]\!]$$

$$G_M = \widehat{G}_M [\![X_M, Y]\!]$$

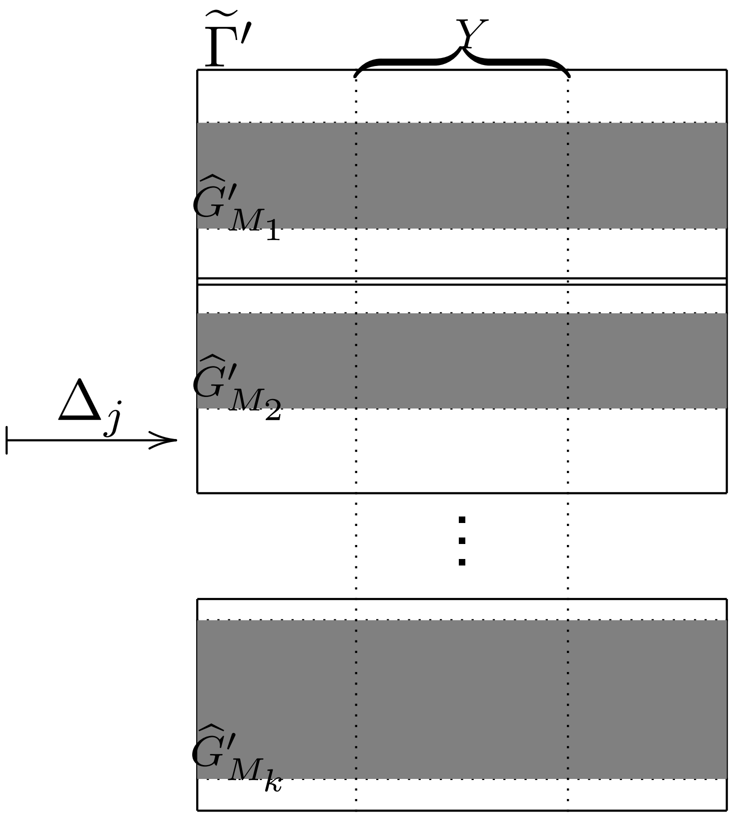
Transformation



Properties of $\widetilde{\Gamma}'$

max. $\|\Gamma\|$
$\|\Gamma \circ \Delta_j\| \leq 1$

max. $\sqrt{\sum_{M \in \mathcal{C}} \alpha_\emptyset(M)^2}$
$\sum_{M \in \mathcal{C}} \big(\alpha_S(M) - \alpha_{S\cup\{j\}}(M)\big)^2 \leq 1$
$\alpha_S(M) = 0$ whenever $S \in M$



Due to $E_0 \mapsto E_0$ and $E_1 \mapsto -E_0$, we get

$$\widetilde{G}'_M = \sum_{S \not\ni j} (\alpha_S(M) - \alpha_{S\cup\{j\}}(M)) E_S$$

$$\widehat{G}'_M = \sqrt{q}\, \widetilde{G}'_M [\![X_M, [q]^n]\!]$$

We prove this does not increase the norm a lot.

Summary

- We defined the notion of certificate structure.

- We derived a dual formulation of the learning graph complexity.
- We used it to give (almost) tight lower bounds for some certificate structures:

$$k\text{-subset, collision, hidden shift, triangle.}$$

- We proved learning graphs are tight for any certificate structure.
- We defined boundedly generated certificate structures.
- We proved an analogue of Childs-Eisenberg conjecture for boundedly generated certificate structures.

Thank you!