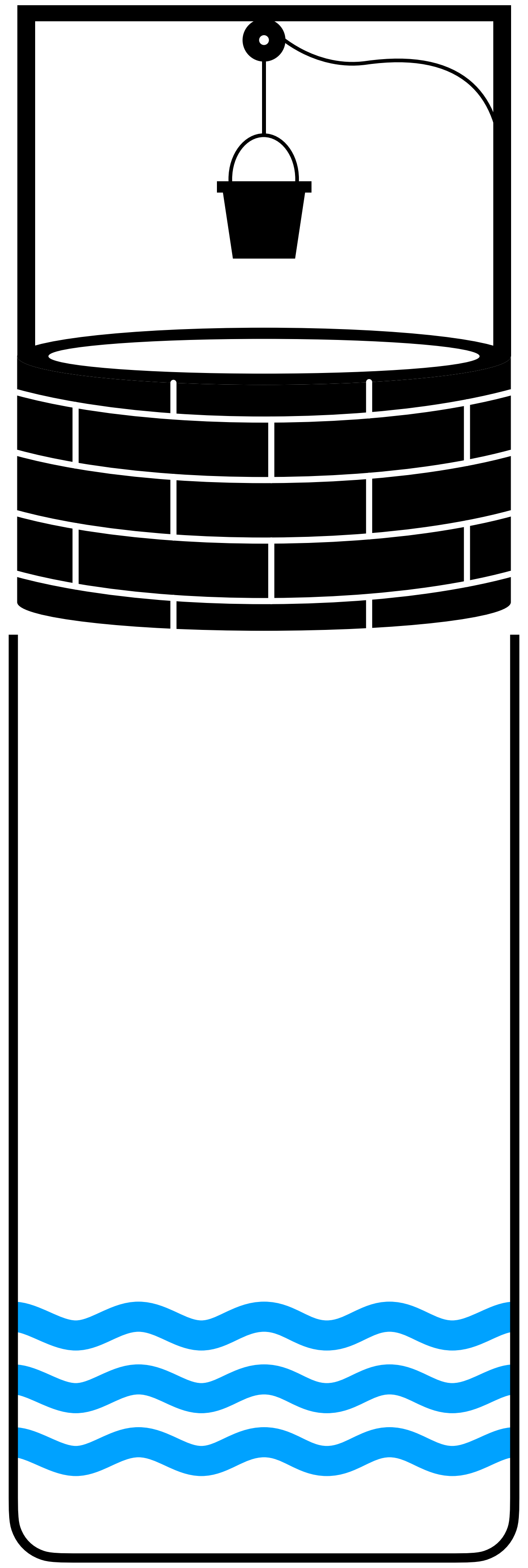
Quantum speedups

Structure, design, and application

Daochen Wang

Advisors: Dr. Andrew Childs and Dr. Carl Miller



Application

Quantum exploration algorithms for multi-armed bandits
[**W**YLC, AAAI 21]

Design

Quantum divide and conquer
[CKKS**W**, QIP 23]

Structure

Symmetries, graph properties, and quantum speedups
[BCGKP**W**, FOCS 20 & QIP 21]

Quantum algorithms for reinforcement learning with a generative model
[**W**SKKR, ICML 21]

Lattice-based quantum advantage from rotated measurements
[AMM**W**, 22]

Quantum exploration algorithms for multi-armed bandits
[**W**YLC, AAAI 21]

Efficient quantum measurement of Pauli operators in the presence of finite sampling error
[CvS**W**PCB, Quantum 21]

Parallel self-testing of EPR pairs under computational assumptions
[F**W**Z, 23]

Quantum divide and conquer
[CKKS**W**, QIP 23]

Possibilistic simulation of quantum circuits by classical circuits
[**W**, PRA 22]

A theory of quantum differential equation solvers: limitations and fast-forwarding
[AL**W**Z, 23]

Symmetries, graph properties, and quantum speedups
[BCGKP**W**, FOCS 20 & QIP 21]

Query complexity

Let $f: E \subseteq \Sigma^n \to \{0,1\}$, suppose an algorithm $\mathscr{A}$ computes $f(x)$ correctly with probability $\geq 2/3$ for all $x \in E$

How many queries to (the oracle encoding) input x does $\mathscr{A}$ need to make?

Answer denoted $D(f)$, $R(f)$, and $Q(f)$, when $\mathscr{A}$ is deterministic, randomized, and quantum, respectively

Quantum speedup $\iff Q(f) < R(f)$

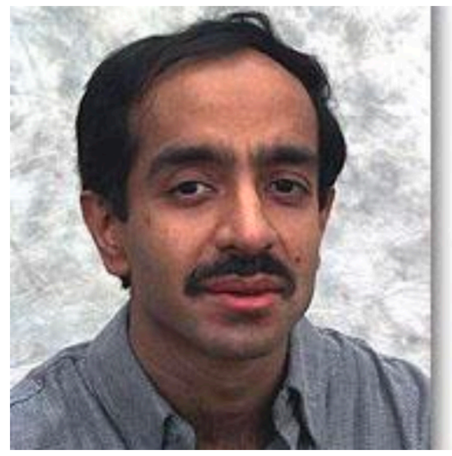
Classical query

$i \mapsto x_i$

Quantum query

$|i\rangle|a\rangle \mapsto |i\rangle|a + x_i\rangle$

Problem structure



Grover $\mathrm{OR}: \{0,1\}^n \to \{0,1\}$

$\mathrm{OR}(x) = x_1 \vee x_2 \vee \ldots \vee x_n$

$R(\mathrm{OR}) = \Theta(n)$ and $Q(\mathrm{OR}) = \Theta\left(\sqrt{n}\right)$

Key component of Shor's algorithm

Simon $f_{\mathrm{Simon}}: E \subseteq \{1,\ldots,n\}^n \to \{0,1\}$, n is a power of 2

$x \in E \iff x$ is a permutation of $[n] = \{1,\ldots,n\}$ or x has a hidden period

$R\left(f_{\mathrm{Simon}}\right) = \Theta\left(\sqrt{n}\right)$ and $Q\left(f_{\mathrm{Simon}}\right) = \Theta(\log n)$

Observations

- Polynomial speedup
- Unstructured

- Exponential speedup
- Highly structured

Symmetries and graph properties

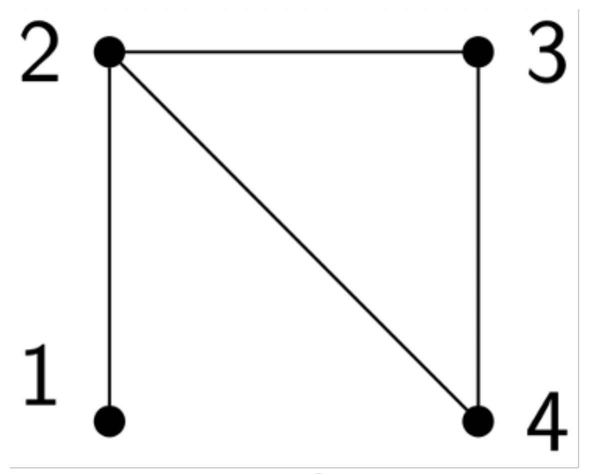
Let $f\colon E \subseteq \Sigma^M \to \{0,1\}$ and $G \leq S_M$, we say f is symmetrical under G if

$$x \in E \implies x_{\sigma(1)}\ldots x_{\sigma(M)} \in E \quad \text{and} \quad f(x) = f\left(x_{\sigma(1)}\ldots x_{\sigma(M)}\right) \text{ for all } \sigma \in G$$

Prior work: f symmetrical under $G = S_M \implies R(f) \leq O\left(Q(f)^3\right)$ [Aaronson, Ambainis 14; Chailloux 18]

Observation. Suppose $\Sigma = \{0,1\}$ and $M = C_2^n = n(n-1)/2$, then

1. $\Sigma^M \leftrightarrow$ set of adjacency matrices of (simple) graphs on n vertices
2. $f =$ graph property $\iff f$ symmetrical under $G = \{\text{Permutations induced by } S_n\} \leq S_M$

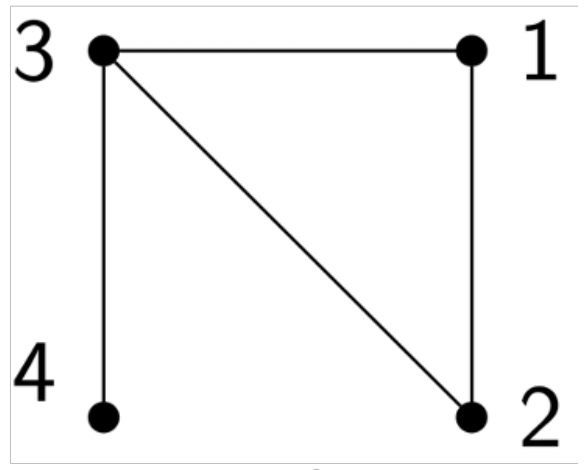


Graph A

Graph A: $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \leftrightarrow 100111$, Graph B: $\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \leftrightarrow 110101$

$\pi \in S_n$ induces $\{u, v\} \mapsto \{\pi(u), \pi(v)\}$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ induces $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 5 & 2 & 4 & 1 \end{pmatrix}$



Graph B

Graph properties* $\implies$ polynomial quantum speedup

Suppose $f: E \subseteq \{0,1\}^{n^2} \to \{0,1\}$ symmetrical under $G = S_n^{(2)} \leq S_{n^2}$ consisting of permutations of $[n^2]$ induced by S_n: $\pi \in S_n$ induces $(u, v) \in [n] \times [n] \cong [n^2] \mapsto (\pi(u), \pi(v))$

Chailloux's lemma (adapted). Suppose it takes at least $\Omega\left(r^{1/c}\right)$ quantum queries to distinguish a random $\sigma \in G$ from a random range-r function in $\mathrm{Func}\left([n^2], [n^2]\right)$, then $R(f) = O(Q(f)^c)$

Observation. If we can distinguish a random $\sigma \in G$ from a random range-r^2 function in $\mathrm{Func}\left([n^2], [n^2]\right)$ with q quantum queries, then we can distinguish a random $\pi \in S_n$ from a random range-r function in $\mathrm{Func}([n], [n])$ with q quantum queries

Proof extends to l-uniform hypergraph properties

Then [Zhandry 15] $\implies q = \Omega\left(r^{1/3}\right) = \Omega\left((r^2)^{1/6}\right)$

Conclusion. The hypothesis of Chailloux's lemma holds with $c = 6$, so $R(f) = O\left(Q(f)^6\right)$

***In the adjacency matrix model**

Exponential quantum speedup in the adjacency list model

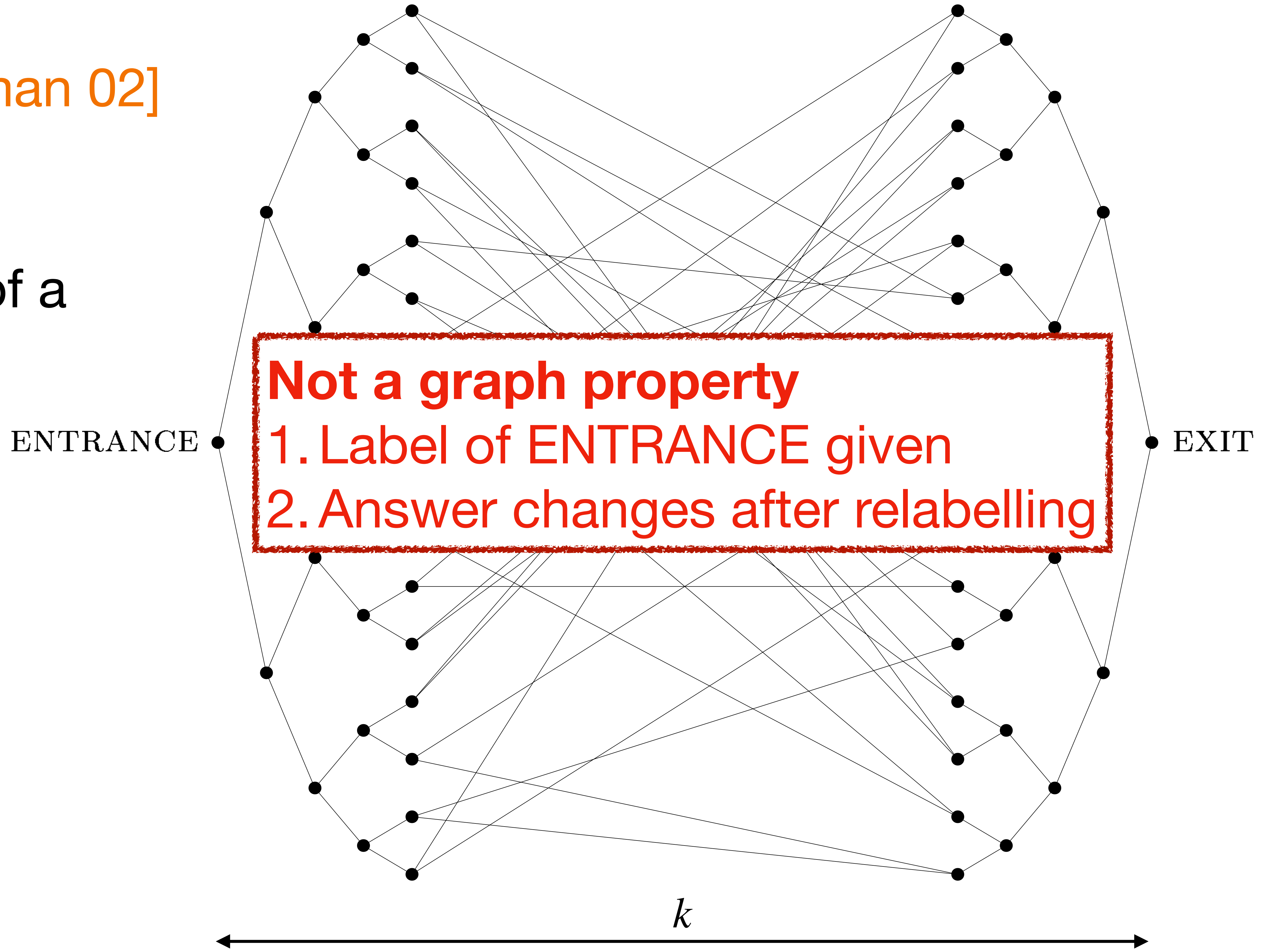
Adjacency list oracle: query by $i \in [n]$, oracle returns the labels of neighbours of vertex labelled i

Glued-trees problem
[Childs, Cleve, Deotto, Farhi, Gutmann, Spielman 02]

Find label of EXIT given adjacency list oracle of a glued trees graph and label of its ENTRANCE

Quantum: $O(\mathrm{poly}(k))$

Randomized: $2^{\Omega(k)}$

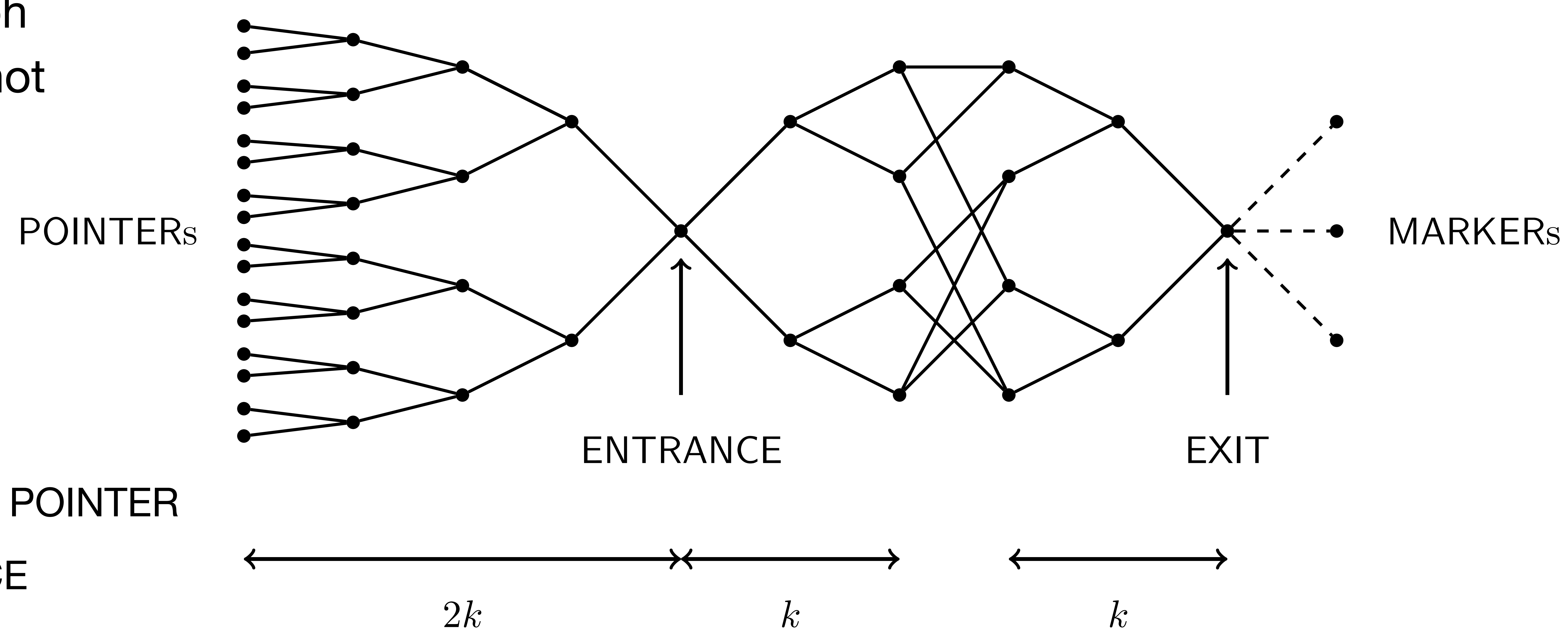


Not a graph property

1. Label of ENTRANCE given
2. Answer changes after relabelling

Upgrade to a graph property

Problem. Decide if the graph has maximum degree 5 or not

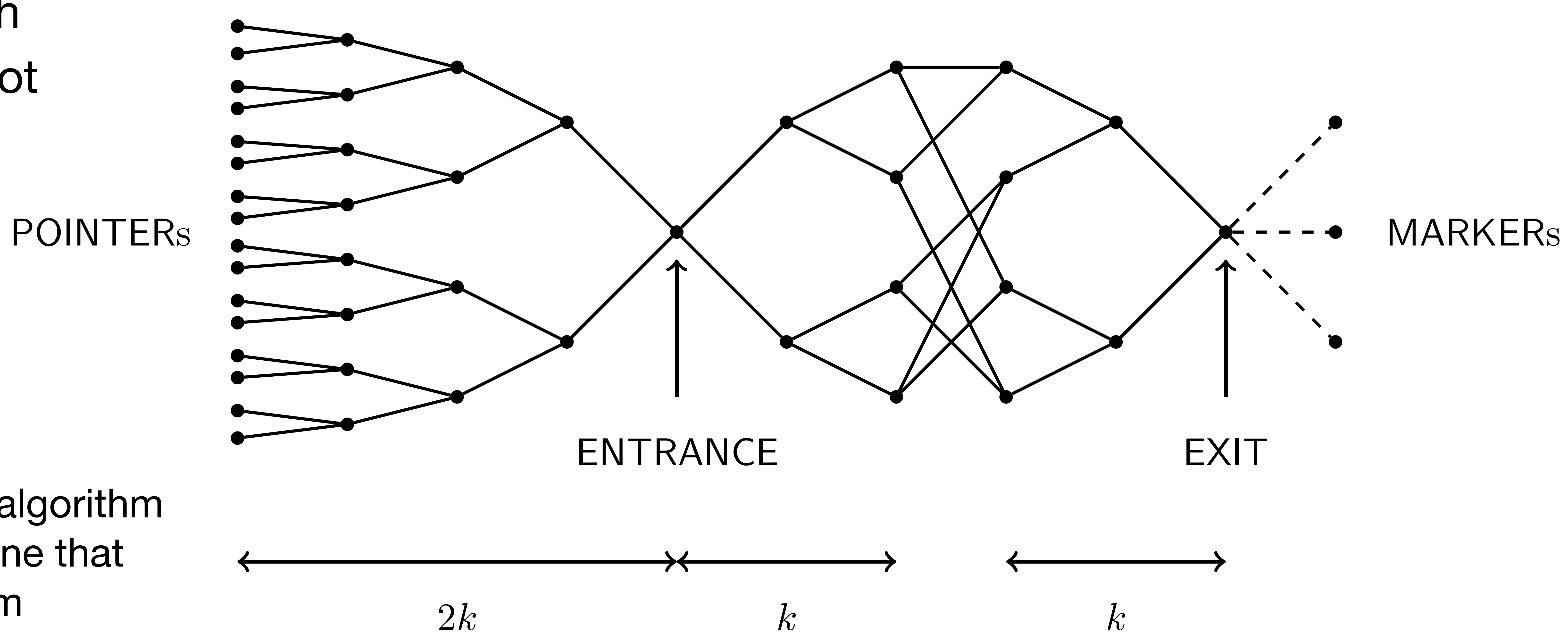


Quantum: $O(\mathrm{poly}(k))$

1. Sample random label until hit POINTER
2. Classically walk to ENTRANCE
3. Run quantum algorithm in [CCDFGS 02] to find EXIT

Classical lower bound

Problem. Decide if the graph has maximum degree 5 or not



Randomized: $2^{\Omega(k)}$

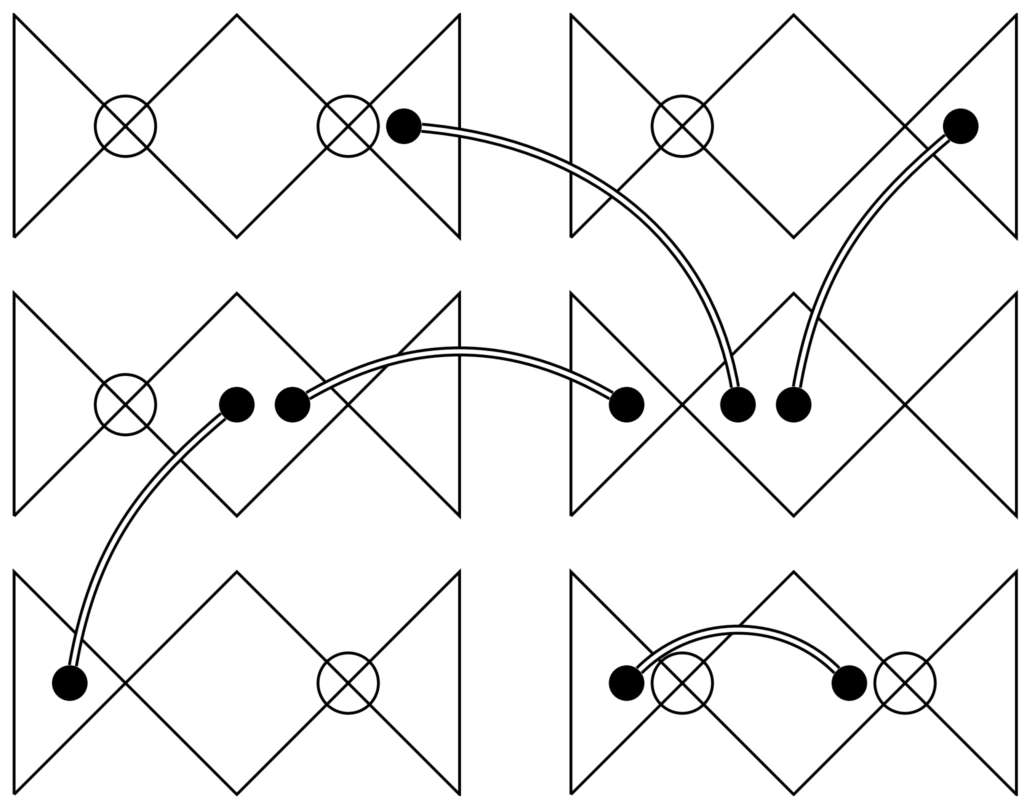
1. Can convert any randomized algorithm for solving this problem into one that solves the glued-trees problem

2. Result follows from [CCDFGS 02]

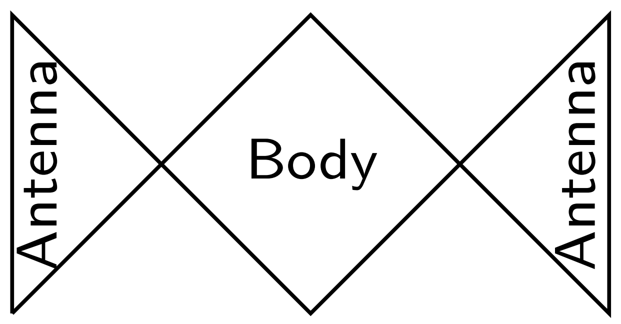
Further developments

- Complete characterization of the quantum speedup admitted by functions $f\colon E \subseteq \Sigma^n \to \{0,1\}$ symmetric under primitive permutation group $G \leq S_n$
    1. If G corresponds to l-uniform hypergraph symmetries, then $\forall f,\ R(f) \leq O\left(Q(f)^{3l}\right)$
    2. Otherwise, $\exists f$ with $R(f) = \Omega\left(\sqrt{n}\right)$ and $Q(f) = O(\log n)$

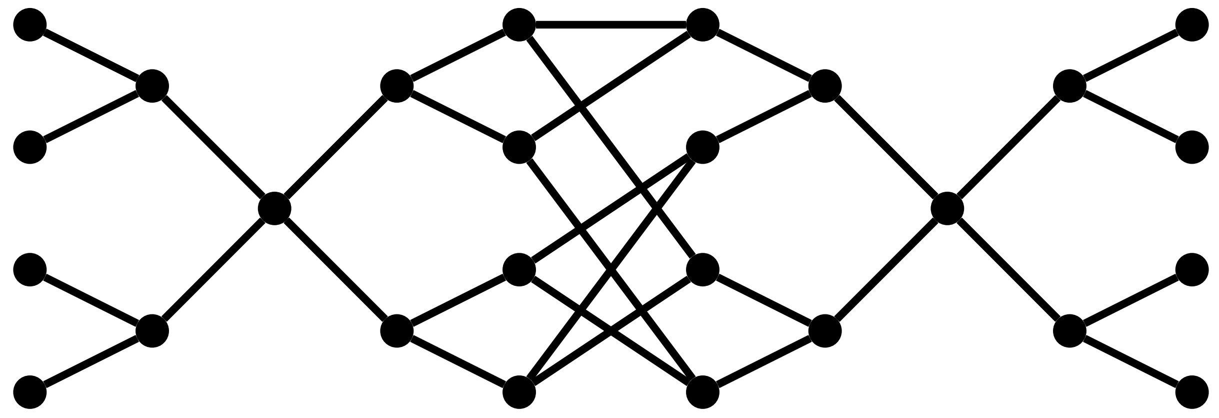
  $\rightarrow$ Near-complete characterization of how quantum speedup relate to symmetry under arbitrary G
- Exponential quantum speedup graph property *testing* in the adjacency list model



where



$=$

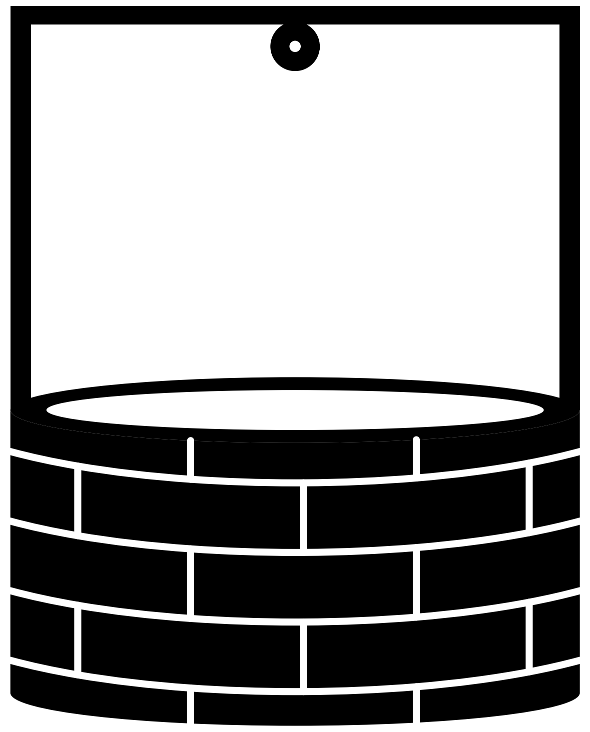


[BCGKPW 20]

Quantum algorithm design

- Fourier sampling
- Grover search/amplitude amplification
- Quantum walk
- Span programs
- Adiabatic optimization/QAOA
- Quantum signal processing/QSVT
- Quantum divide and conquer [CKKSW 22]

...



Applications

- Recognizing regular languages [Aaronson, Grier, Schaeffer 19]
- String rotation and string suffix [Akmal, Jin 22]
- Longest increasing subsequence New!
- Longest common subsequence New!

...

Divide and conquer

1. Divide a problem into subproblems

2. Recursively solve each subproblem

3. Combine the solutions of the subproblems to solve the full problem

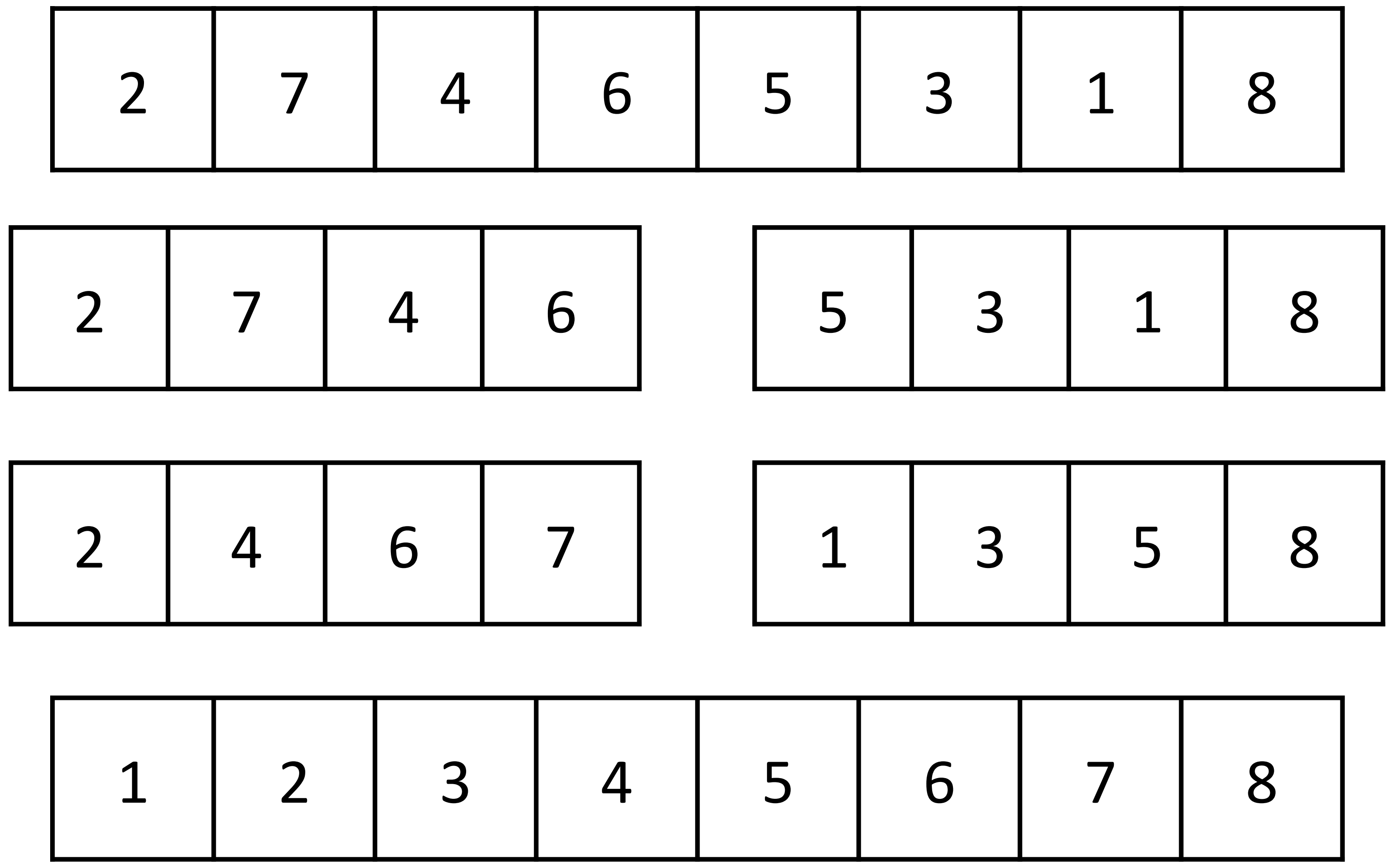
Merge sort

Recurrence:

Cost of solving auxiliary problem

$$C(n) = 2C(n/2) + O(n) \implies C(n) = O(n \log n)$$

Cost of solving subproblem



Quantum divide and conquer

Every $f\colon \Sigma^n \to \{0,1\}$ can be associated with its adversary quantity, $\mathrm{Adv}(f) \geq 0$

Theorem [Høyer, Lee, Špalek 07; Lee, Mittal, Reichardt, Špalek 10]. $Q(f) = \Theta(\mathrm{Adv}(f))$

- AND-OR. Suppose f is computed as $f_1 \square f_2 \square \ldots \square f_a \square f_{\mathrm{aux}}$, where each $\square \in \{\wedge, \vee\}$

$$\mathrm{Adv}(f)^2 \leq \sum_{i=1}^{a} \mathrm{Adv}(f_i)^2 + O\big(Q(f_{\mathrm{aux}})^2\big)$$

- SWITCH-CASE. Suppose f is computed by first computing $s = f_{\mathrm{aux}}(x)$ and then some function $g_s(x)$, then

$$\mathrm{Adv}(f) \leq \max_s \mathrm{Adv}(g_s) + O\big(Q(f_{\mathrm{aux}})\big)$$

→ **Divide and conquer recurrences in the quantum setting**

Recognizing regular languages

Let $\Sigma = \{0,1,2\}, f_n : \Sigma^n \to \{0,1\}$ such that $f_n(x) = 1$ iff $x \in \Sigma^*20^*2\Sigma^*$

02002110 ✅ 02102112 ⛔

Observation. Let $g_n(x) = \left(x_{\text{left}} \in \Sigma^*20^*\right) \wedge \left(x_{\text{right}} \in 0^*2\Sigma^*\right)$, then

$$f_n(x) = f_{n/2}\left(x_{\text{left}}\right) \vee f_{n/2}\left(x_{\text{right}}\right) \vee g_n(x)$$

Let $a(n) = \mathrm{Adv}(f_n)$, then $a(n)^2 \leq 2a^2(n/2) + O\left(Q(g_n)^2\right)$

But $Q(g_n) = O\left(\sqrt{n}\right)$, so $a(n) = O\left(\sqrt{n \log n}\right)$

Longest common subsequence

k-common subsequence (k-CS). Given $x, y \in \Sigma^n$, do x and y share a subsequence of length k?

E	i	n	s	t	e	i	n		$k \leq 4$ ✅
E	n	t	w	i	n	e	d		$k > 4$ ⛔

- $R(k\text{-CS}) = \Theta(n)$ for $k \geq 1$
- $Q(1\text{-CS}) = \Theta\left(n^{2/3}\right)$ ← bipartite element distinctness [Aaronson, Shi 04; Ambainis 03]
- $Q(k\text{-CS}) = O\left(n^{2k/(2k+1)}\right)$ ← using [Ambainis 03]

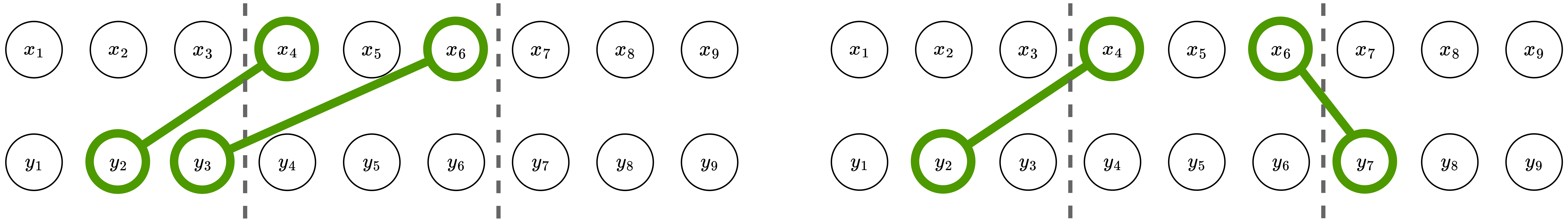
Can we do better?

Simple and composite k-CS

Theorem. Let $a_k(n) =$ adversary quantity for k-CS on input length n. Then $a_k(n) = O\left(n^{2/3}\log^{k-1} n\right)$

Divide the two input strings x and y into m parts each. Then, a k-CS can either be **simple** or **composite**

- A simple k-CS is a k-CS formed by symbols within a *single* part of x and a *single* part of y
- A composite k-CS is any k-CS that is not simple



Simple $\quad k = 2,\ m = 3 \quad$ Composite

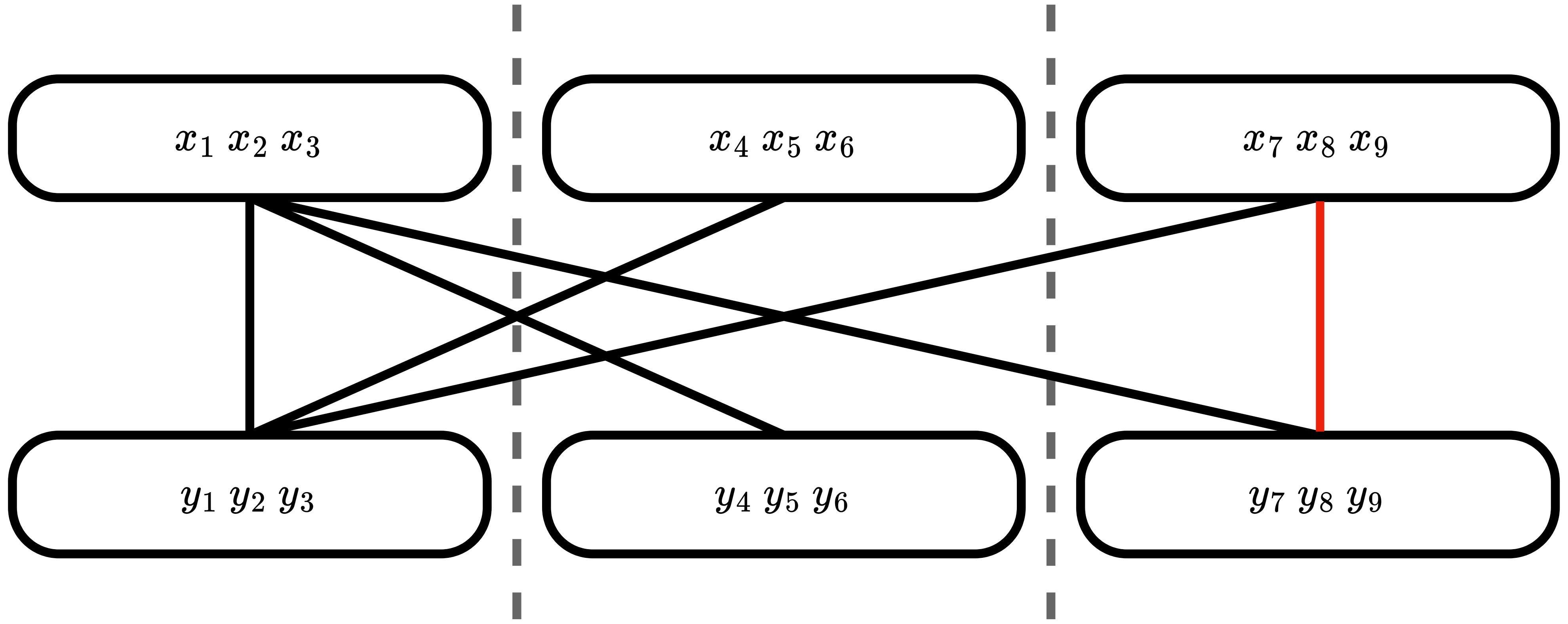
Quantum divide and conquer on k-CS

Theorem. Let $a_k(n)$ = adversary quantity for k-CS on input length n. Then $a_k(n) = O\left(n^{2/3}\log^{k-1} n\right)$

Observations.

- Detecting composite k-CS takes $O\left(n^{2/3}\log^{k-1} n\right)$ using inductive hypothesis and binary search
- Need to detect if there exists a simple k-CS between $\leq 2m-1$ pairs of length-(n/m) substrings

$m = 3$



Line between parts =
parts share common symbol

Cost of computing lines =
$m^2 \cdot O\left(n^{2/3}\right)$

Quantum divide and conquer $\rightarrow$ $a_k(n) \leq O\left(n^{2/3}\log^{k-1} n\right) + m^2 \cdot O\left(n^{2/3}\right) + \sqrt{2m-1}\, a_k(n/m)$

which solves to $a_k(n) = O\left(n^{2/3}\log^{k-1} n\right)$, provided $\log_m\left(\sqrt{2m-1}\right) < 2/3 \iff m \geq 7$

New speedups from old

Search. Find a marked item from list of items ↔ given oracle access to $x \in \{0,1\}^n$, find i such that $x_i = 1$

$$O_x |i\rangle|0\rangle = |i\rangle|x_i\rangle$$

Question. What if the items can be partially marked and the goal is to find the most heavily marked item?
↔ given oracle access to $p \in [0,1]^n$, find i such that p_i is maximal

$$O_p |i\rangle|0\rangle = |i\rangle\left(\sqrt{p_i}\,|1\rangle + \sqrt{1-p_i}\,|0\rangle\right)$$

Multi-armed bandit exploration problem

Theorem [WYLC 21].

Let $H = \sum_{k=2}^{n} (q_1 - q_k)^{-2}$, where q_k is the kth largest element of $\{p_i\}_i$ (assume $q_1 > q_2$), then the largest p_i can be identified using $\Theta\left(\sqrt{H}\right)$ calls to O_p

Upper bound: uses a variable-time algorithm [Ambainis 12]
Lower bound: uses modified adversary method [Ambainis 00]

Real-world applications?

Equivalently, can we instantiate the oracle in the real world? **Yes!**

Example. Finding the best move in chess

You have n candidate moves, where move i can lead to a set $X(i)$ of possible subsequent games

- Assume you have computer code that, for move i and game $g \in X(i)$, computes $f(i, g) = 1$ if you win and $= 0$ if you lose
- We can instantiate one call to O_p using one call to f:

$$|i\rangle|0\rangle|0\rangle \mapsto |i\rangle|0\rangle\frac{1}{\sqrt{|X(i)|}}\sum_{g\in X(i)}|g\rangle \overset{f}{\mapsto} |i\rangle\sum_{g\in X(i)}\frac{1}{\sqrt{|X(i)|}}|f(i,g)\rangle|g\rangle = |i\rangle\left(\sqrt{p_i}|1\rangle|u_i\rangle + \sqrt{1-p_i}|0\rangle|v_i\rangle\right)$$

where $|u_i\rangle$ and $|v_i\rangle$ are some junk states and p_i equals the empirical probability that move i leads to your win (our algorithm also works when O_p involves junk states)

Conclusion

1. Structure: showed how symmetry relates to quantum speedups, in particular, graph symmetries

2. Design: described a framework for divide and conquer in the quantum setting

3. Application: to multi-armed bandits by generalizing Grover's speedup for search

Open question: is there a **useful** problem with a **massive** quantum speedup?

Appendix: adversary quantity

For any $f\colon \Sigma^n \to \{0,1\}$,

$$\text{Adv}(f) = \max_{\Gamma} \frac{\|\Gamma\|}{\max_{i\in[n]} \|\Gamma_i\|},$$

max over $|\Sigma|^n \times |\Sigma|^n$ real symmetric matrices Γ with $f(x) = f(y) \implies \Gamma_{xy} = 0$ and

$$\left(\Gamma_i\right)_{xy} = \begin{cases} \Gamma_{xy} & \text{if } x_i \neq y_i \\ 0 & \text{if } x_i = y_i \end{cases}$$