Symmetries, Graph Properties, and Quantum Speedups

QIP 2021

Shalev Ben-David, Andrew M. Childs, András Gilyén,
William Kretschmer, Supartha Podder, Daochen Wang

arXiv:2006.12760
February 5, 2020

Introduction

What are quantum computers good for?

Factoring and discrete logarithms:

$\widetilde{O}(n^2)$ quantumly $\quad\quad$ $2^{\widetilde{O}(n^{1/3})}$ classically

What are quantum computers good for?

Factoring and discrete logarithms:

$\widetilde{O}(n^2)$ quantumly $\quad 2^{\widetilde{O}(n^{1/3})}$ classically

... but only conjecturally!

Query Complexity

$$x = \boxed{x_1 \mid x_2 \mid x_3 \mid \cdots \mid x_N}$$

$$f : \Sigma^N \to \{0, 1\}$$

Query Complexity

$$x = \boxed{x_1}\boxed{x_2}\boxed{x_3}\boxed{\cdots}\boxed{x_N}$$

$$f : \Sigma^N \to \{0, 1\}$$

$$U_x : |i, b, w\rangle \to |i, b \oplus x_i, w\rangle$$

Query Complexity

$$x = \boxed{x_1 \mid x_2 \mid x_3 \mid \cdots \mid x_N}$$

$$f : \Sigma^N \to \{0,1\}$$

$$U_x : |i, b, w\rangle \to |i, b \oplus x_i, w\rangle$$

$Q(f) :=$ Bounded-error quantum query complexity of f

$R(f) :=$ Bounded-error randomized query complexity of f

Why query complexity?

- Unconditional separations
- Captures most quantum algorithms

Why query complexity?

- Unconditional separations
- Captures most quantum algorithms

$$Q(\textsc{PeriodFinding}_N) = O(1)$$
$$R(\textsc{PeriodFinding}_N) = \Omega\left(N^{1/4}\right)$$

Shor's algorithm: factoring n-bit integers reduces to $\textsc{PeriodFinding}_{2^{O(n)}}$

Structure in quantum speedups

Theorem (ABKRT'20, improving BBC$^+$'01)

$R(f) = O(Q(f)^4)$ for all **total** *functions $f : \{0,1\}^n \to \{0,1\}$.*

Structure in quantum speedups

Theorem (ABKRT'20, improving BBC$^+$'01)

$R(f) = O(Q(f)^4)$ for all **total** *functions $f : \{0,1\}^n \to \{0,1\}$.*

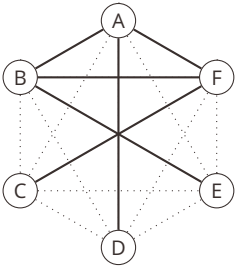
Theorem (Cha'18, improving AA'14)

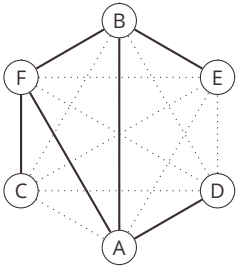
$R(f) = O(Q(f)^3)$ for all **permutation-invariant** *partial functions $f : \Sigma^n \to \{0,1\}$, i.e.:*

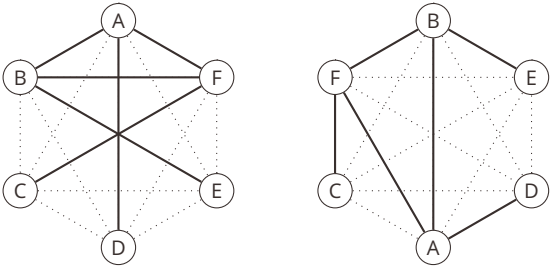
$$f(x_1, x_2, \ldots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$$

for every permutation π.

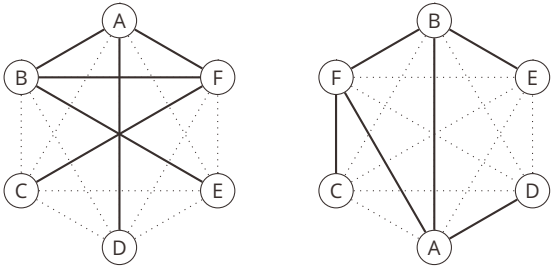
What is the role of **symmetry** in quantum query speedups?


A
B
F
C
E
D


B
F
E
C
D
A

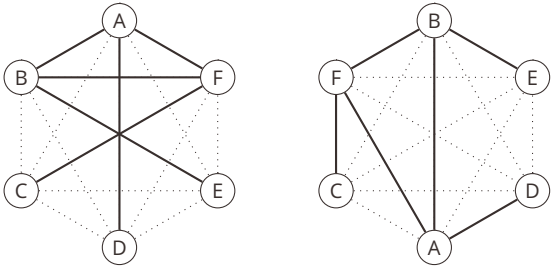


$$n! \ll \binom{n}{2}!$$



$$n! \ll \binom{n}{2}!$$

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$



$$n! \ll \binom{n}{2}!$$

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

A	→	B	D	F
B	→	A	E	F
C	→	F		
D	→	A		
E	→	B		
F	→	A	B	C

Results

Theorem (This work)

*$R(f) = O(Q(f)^{3k})$ for all partial functions $f : \Sigma^m \to \{0,1\}$ symmetric under k-**uniform hypergraph** symmetries with n vertices, where $m = \binom{n}{k}$.*

Corollary

*$R(f) = O(Q(f)^{6})$ for all **graph properties** f in the adjacency matrix model.*

Definition

Let $f : \Sigma^n \to \{0,1\}$ be a partial function. Let G be a permutation group. We say that f is *symmetric under G* if for every $\pi \in G$:

$$f(x_1, x_2, \ldots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$$

Definition

Let $f : \Sigma^n \to \{0,1\}$ be a partial function. Let G be a permutation group. We say that f is *symmetric under G* if for every $\pi \in G$:

$$f(x_1, x_2, \ldots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$$

Theorem (This work, informal)

*Permutation groups constructed out of hypergraph symmetries are essentially the **only** groups inconsistent with super-polynomial quantum speedups.*

Theorem (This work)

Let G be a primitive permutation group. Then:

(1) *If $b(G) = n^{\Omega(1)}$, then for every partial $f : \Sigma^n \to \{0,1\}$ symmetric under G, $R(f) = Q(f)^{O(1)}$.*

(2) *If $b(G) = n^{o(1)}$, then there exists a partial $f : \Sigma^n \to \{0,1\}$ symmetric under G such that $R(f) = Q(f)^{\omega(1)}$.*

- "Small" primitive groups allow speedup, "large" primitive groups do not
- CFSG $\implies$ groups satisfy (1) iff they look like hypergraph symmetries

Theorem (This work)

In the **adjacency list** *model, there is a graph property* $\mathcal{P}_k$ *such that deciding* $\mathcal{P}_k$ *can be done in* **poly(k)** *quantum queries, whereas* **exp(k)** *queries are needed classically.*

Theorem (This work)

In the **adjacency list** *model, there is a graph property $\mathcal{P}_k$ such that deciding $\mathcal{P}_k$ can be done in* **poly(k)** *quantum queries, whereas* **exp(k)** *queries are needed classically.*

In fact, even for property *testing*: distinguish $\mathcal{P}_k$ and ϵ-far from $\mathcal{P}_k$.

Part 1: No Quantum Speedup for Adjacency Matrix Graph Properties

Theorem (Zha'15)

Distinguishing a random function $\alpha : [n] \to [n]$ with range size r from a random permutation $\pi \in S_n$ requires $\Omega(r^{1/3})$ quantum queries.

$\pi =$	$\pi(1)$	$\pi(2)$	$\pi(3)$	$\cdots$	$\pi(n)$
$\alpha =$	$\alpha(1)$	$\alpha(2)$	$\alpha(3)$	$\cdots$	$\alpha(n)$

Corollary (Cha'18)

$R(f) = O(Q(f)^3)$ for all permutation-invariant f.

Theorem (This work)

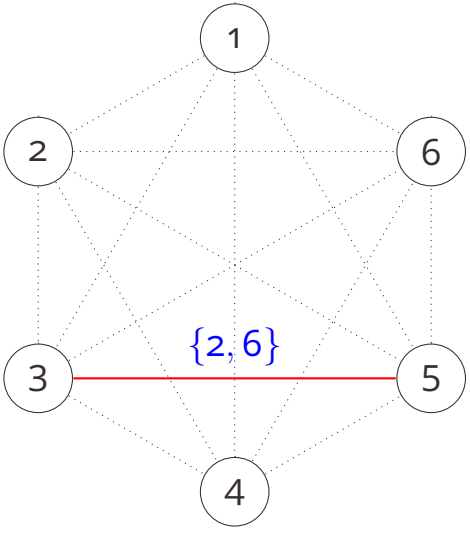
Distinguishing a random function $\alpha : [n] \to [n]$ with range size r from a random permutation $\pi \in \mathbf{G}$ requires $\Omega(r^{1/3\mathbf{k}})$ quantum queries, where $\mathbf{G} = \mathbf{k}$-uniform hypergraph symmetries.

$\pi =$	$\pi(1)$	$\pi(2)$	$\pi(3)$	$\cdots$	$\pi(n)$
$\alpha =$	$\alpha(1)$	$\alpha(2)$	$\alpha(3)$	$\cdots$	$\alpha(n)$

Corollary (This work)

$R(f) = O(Q(f)^{3\mathbf{k}})$ for all $\mathbf{G}$-invariant f, where $\mathbf{G} = \mathbf{k}$-uniform hypergraph symmetries.

i	1	2	3	4	5	6
$\alpha(i)$	1	6	2	5	6	2



Part 2: Characterizing Groups that Allow Quantum Speedup

Theorem (Lie'84)

Let G be a primitive permutation group acting on $[n]$. Then either:

(1) *G is a subgroup of $S_\ell \wr S_m$ containing $A_m^{\times \ell}$, where the action of S_m is on p-element subsets of $[m]$ and the wreath product has the product action of degree $n = \binom{m}{p}^\ell$, or*

(2) *$b(G) < 9 \log_2 n$.*

Theorem (Lie'84)

Let G be a primitive permutation group acting on $[n]$. Then either:

(1) *G is a subgroup of $S_\ell \wr S_m$ containing $A_m^{\times \ell}$, where the action of S_m is on p-element subsets of $[m]$ and the wreath product has the product action of degree $n = \binom{m}{p}^\ell$, or*

(2) *$b(G) < 9 \log_2 n$.*

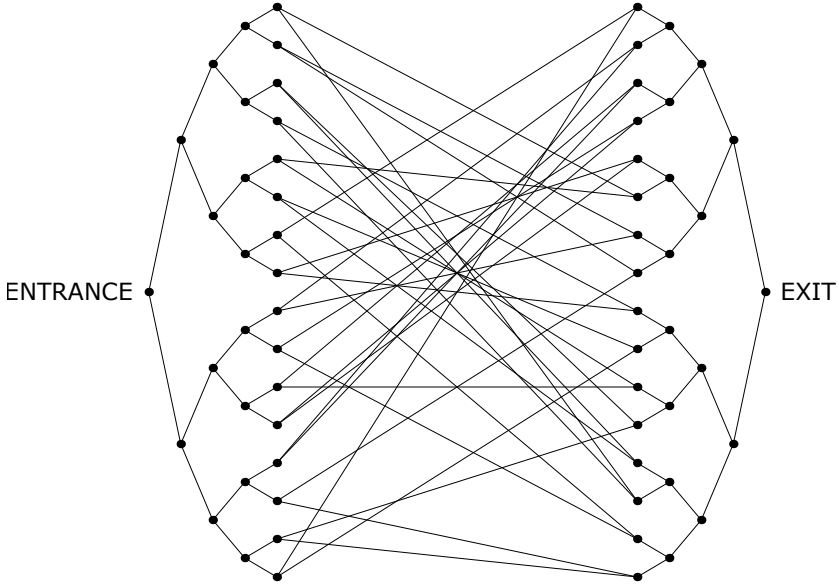
Translation

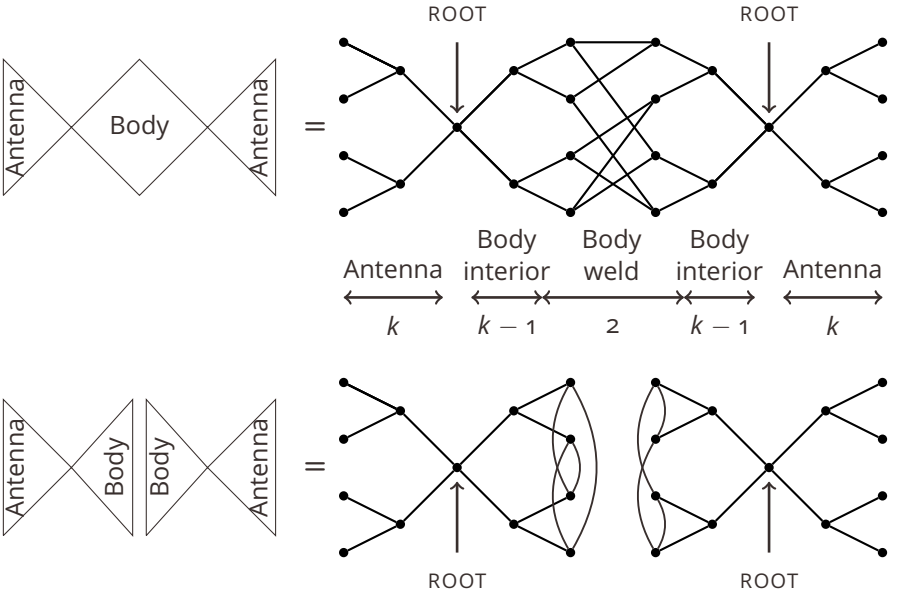
Either:

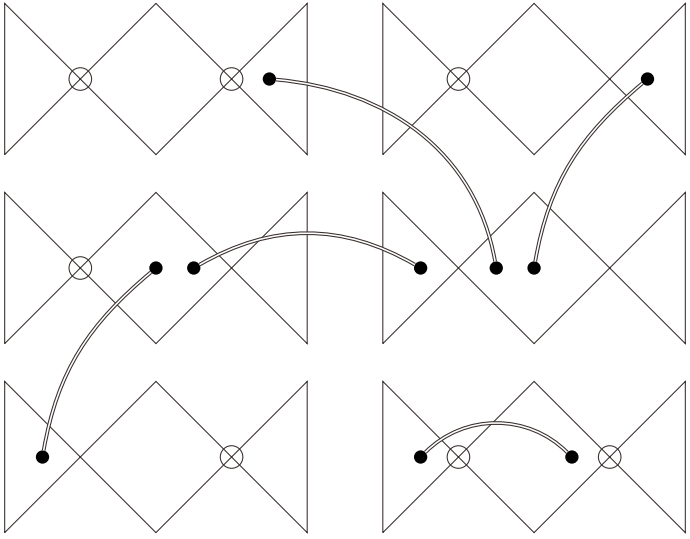
(1) G contains the symmetries of a p-uniform hypergraph with m vertices, or

(2) "Minimal base size" $b(G)$ is really small!

Part 3: Exponential Speedup for Adjacency List Property Testing


ENTRANCE
EXIT


Antenna
Body
Antenna
=
ROOT
ROOT
Antenna
Body interior
Body weld
Body interior
Antenna
k
k − 1
2
k − 1
k
Antenna
Body
Body
Antenna
=
ROOT
ROOT



William Kretschmer

https://www.cs.utexas.edu/~kretsch/

kretsch@cs.utexas.edu

The University of Texas at Austin

Computer Science