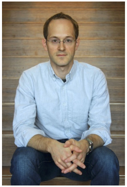
Symmetries, graph properties, and quantum speedups

Daochen Wang (Maryland)
ASQC 2022, full version: arXiv: 2006.12760

Shalev Ben-David
(Waterloo)



Andrew Childs
(Maryland)

András Gilyén
(Rényi)

William Kretschmer
(UT Austin)

Supartha Podder
(Stony Brook)

Quantum speedups and symmetric functions

Classical and quantum query complexity

Let $f : \mathcal{D} \subseteq \Sigma^n \to \{0,1\}$ be a known function.

- How many positions of input $x \in \mathcal{D}$ are necessary and sufficient to query to compute $f(x)$ with high probability in the worst case? Answer denoted $R(f)$ and $Q(f)$ in the classical and quantum cases respectively. Quantumly, we can query x in superposition: $\sum_{i=1}^n \alpha_i |i\rangle |0\rangle \mapsto \sum_{i=1}^n \alpha_i |i\rangle |x_i\rangle$. Fact: $R(f) \leq Q(f)$ because can always simulate a classical (possibly randomized) algorithm quantumly.
- Examples:
  1. $f : \{0,1\}^3 \to \{0,1\}; x \mapsto (x_1 \wedge x_3) \vee (x_2 \wedge \neg x_3)$.
  2. $\mathrm{OR} : \{0,1\}^n \to \{0,1\}$; $f(x) = 1$ iff at least one bit of x is 1.
  3. $\mathrm{PARITY} : \{0,1\}^n \to \{0,1\}; x \mapsto x_1 \oplus x_2 \oplus \cdots \oplus x_n$.
- $R(\mathrm{OR}) = \Theta(n)$ and $R(\mathrm{PARITY}) = \Theta(n)$.
  (Think of $\alpha = O(\beta)$, $\alpha = \Theta(\beta)$, $\alpha = \Omega(\beta)$ as $\alpha \leq \beta$, $\alpha = \beta$, $\alpha \geq \beta$, respectively.)

Quantum speedups in query complexity

Given a family of $f : \mathcal{D} \subseteq \Sigma^n \to \{0,1\}$.

When is $R(f)$ super-polynomially larger than $Q(f)$ (large quantum speedup) and when is $R(f)$ only polynomially larger than $Q(f)$ (small quantum speedup)?

Examples:

1. Small quantum speedups: 1. $f = \mathrm{OR}$ with $\mathcal{D} := \{0,1\}^n$ has $R(f) = \Theta(n)$ and $Q(f) = \Theta(\sqrt{n})$. 2. $f = \mathrm{ED}$ (element distinctness) with $\mathcal{D} = \Sigma^n = [n]^n$ has $R(f) = \Theta(n)$ and $Q(f) = \Theta(n^{2/3})$. Note $[n] := \{1, \ldots, n\}$.
2. Large quantum speedup: $f =$ "Simon's function" has $R(f) = \Theta(\sqrt{n})$ and $Q(f) = \Theta(\log(n))$. f has $\Sigma = [n]$, where $n = 2^k$. View the n positions of input $x \in \mathcal{D}$ as labelled by $\{0,1\}^k$. Promised that either the x_i's are distinct for all $i \in [n]$ ($f = 0$) or there exists an $a \neq 0^k$ such that $x_i = x_{i \oplus a}$ for all $i \in [n]$ ($f = 1$).

Symmetric functions

Definition

Let $f : \mathcal{D} \subseteq \Sigma^n \to \{0,1\}$ be a function. f is *symmetric under a permutation group* G on $[n]$ iff, for all $\pi \in G$,

1. $x = (x_1, \ldots, x_n) \in \mathcal{D} \implies x \circ \pi := (x_{\pi(1)}, \ldots, x_{\pi(n)}) \in \mathcal{D}$ and
2. $f(x) = f(x \circ \pi)$ for all $x \in \mathcal{D}$.

Examples:

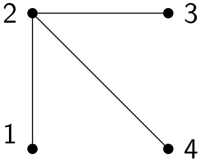
- $f = \mathrm{OR} : \{0^n, 10^{n-1}, 010^{n-2}, \ldots, 0^{n-1}1\} \subseteq \{0,1\}^n \to \{0,1\}$ and $f = \mathrm{ED} : [n]^n \to \{0,1\}$ are both symmetric under $G = S_n$, which consists of all permutations on $[n]$. Aaronson and Ambainis (2009) and Chailloux (2018) showed that such functions only admit small quantum speedups.
- **Our main example.** $f =$ a graph property in the adjacency matrix model is symmetric under $G =$ graph symmetries.

Graph properties in the adjacency matrix model

Adjacency matrix model of graphs

In the adjacency matrix model, a (simple) graph on n vertices is modelled by a symmetric $n \times n$ matrix.

Example with $n = 4$:

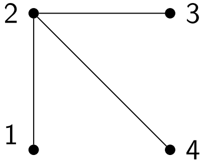


$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Adjacency matrix model of graphs

In the adjacency matrix model, a (simple) graph on n vertices is modelled by a symmetric $n \times n$ matrix.

Example with $n = 4$:



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

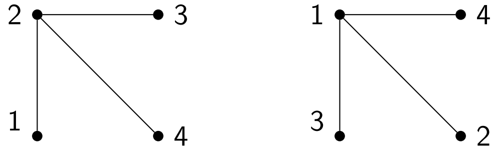
Equivalently, a graph is modelled by a $\binom{n}{2}$-bit string by collapsing the matrix. For example, the graph above is modelled by 100110.

Graph properties in the adjacency matrix model

A graph property in the adjacency matrix model is a function f from a set of graphs specified in the adjacency matrix model to $\{0, 1\}$ that is symmetric under graph symmetries, i.e., isomorphisms.

Examples:

1. Having a triangle or not is a graph property.
2. f must evaluate to the same value on the following two isomorphic graphs. Note that the graphs are not the *same*: the left one is 100110, but the right one is 111000.



Graph symmetries

The set of graph symmetries of a graph with n vertices is denoted S_n^2. S_n^2 is a permutation group on $[\binom{n}{2}]$ of size $n!$ that is "naturally induced" by S_n.

Identify $[\binom{n}{2}]$ with $\{\{i,j\}\}_{i,j\in[n]}$, the set of possible edges on n vertices. Then, S_n^2 consists of permutations

$$\{i,j\} \mapsto \{\sigma(i),\sigma(j)\},$$

where $\sigma \in S_n$. For example, when $n = 4$, $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right) \in S_4$ gives

$$\begin{pmatrix} \{1,2\} & \{1,3\} & \{1,4\} & \{2,3\} & \{2,4\} & \{3,4\} \\ \{2,3\} & \{2,4\} & \{1,2\} & \{3,4\} & \{1,3\} & \{1,4\} \end{pmatrix}.$$

Remarks. 1. S_n^2 is *much* smaller than the set of all permutations on $[\binom{n}{2}]$. 2. For integer $p \geq 1$, the set of p-uniform hypergraph symmetries of a hypergraph with n vertices is denoted S_n^p.

Chailloux's proof (2018)

Suppose $f : \mathcal{D} \subseteq \Sigma^n \to \{0, 1\}$ is symmetric under S_n.

Given an algorithm for computing f, if we replace the input $x \in \mathcal{D}$ by $x \circ \pi := (x_{\pi(1)}, \ldots, x_{\pi(n)})$ for a random $\pi \in S_n$, then the algorithm still correctly computes f.

Main idea. Replace π by a random range-r function, $\alpha : [n] \to [n]$ with $|\alpha([n])| = r$.

If a quantum algorithm distinguishes $x \circ \pi$ from $x \circ \alpha$, then it distinguishes π from α. (If it cannot distinguish π from α then it cannot distinguish $x \circ \pi$ from $x \circ \alpha$.)

Theorem [Zhandry (2015)]. Distinguishing a random range-r function from a random permutation in S_n needs $\Omega(r^{1/3})$ quantum queries.

Taking $r = Q(f)^3$ implies a $Q(f)$-query quantum algorithm cannot distinguish $x \circ \pi$ from $x \circ \alpha$. But a quantum algorithm on $x \circ \alpha$ can be simulated with r classical queries. So $R(f) = O(Q(f)^3)$.

Graph symmetries and quantum speedups

Let G be a permutation group on $[n]$. Suppose we need $\Omega(r^{1/c})$ quantum queries to distinguish a random range-r function from a random $\pi \in G$. (We say such a G is *well-shuffling* with exponent c.) Chailloux $\implies R(f) = O(Q(f)^c)$ for all f symmetric under G.

For graph symmetries, first consider $G = S_n^{(2)}$ on $[n^2]$, which consists of permutations $(i,j) \in [n^2] \mapsto (\pi(i), \pi(j))$ for $\pi \in S_n$.

If we can distinguish a random $\pi \in S_n^{(2)}$ from a random range-r^2 function on $[n^2]$ using q quantum queries, then we can distinguish a random $\tau \in S_n$ from a random range-r function on $[n]$ using $2q$ quantum queries. So $2q = \Omega(r^{1/3}) = \Omega((r^2)^{1/6})$, so $S_n^{(2)}$ is well-shuffling with exponent $c = 6$.

Can similarly argue that S_n^2 on $[\binom{n}{2}]$ is well-shuffling with exponent $c = 6$. In fact, argument generalizes to show S_n^p on $[\binom{n}{p}]$ is well-shuffling with exponent $c = 3p$. (Recall S_n^p denotes the set of p-uniform hypergraph symmetries.)

Functions symmetric under primitive permutation groups

Primitive permutation groups

Definition

A permutation group G on $[n]$ is *transitive* iff for all $x, y \in [n]$, there exists $\sigma \in G$ such that $\sigma(x) = y$.

Definition

A permutation group G on $[n]$ is *primitive* iff G is transitive and the only partitions $\mathcal{B} := \{B_1, \ldots, B_k\}$ of $[n]$ preserved by G, i.e., $\pi(\mathcal{B}) := \{\pi(B_i)\}_{i=1}^k = \mathcal{B}$ for all $\pi \in G$, are $\{G\}$ and the partition into singletons, i.e., $\{\{g\} \mid g \in G\}$.

Example of a G that is transitive but imprimitive:

Let $n = 4$, consider the permutation group $G = \langle \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}\right) \rangle$ of [4]. G is transitive, but preserves

$$\mathcal{B} = \{B_1 = \{1, 3\},\, B_2 = \{2, 4\}\},$$

so is imprimitive.

Base of permutation groups

Definition

A *base* of a permutation group G on $[n]$ is a set $S \subseteq [n]$ such that if $h \in G$ and $h(x) = x$ for all $x \in S$ then h is the identity element in G. The *base size* $b(G)$ of G is the minimal size of a base.

Examples:

1. S_3 on $[3]$ has base size 2; a base is $\{1, 2\}$;
   S_n of $[n]$ has base size $n - 1$; a base is $\{1, 2, \ldots, n - 1\}$.
2. $\mathrm{GL}_n(\mathbb{F}_2)$, invertible $n \times n$ matrices over $\mathbb{F}_2$, on $\mathbb{F}_2^n$ has base size n; a base is $\{(1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}$ (standard basis of $\mathbb{F}_2^n$). Note that the base size is very small in the sense that it equals $\log_2(|\mathbb{F}_2^n| = 2^n)$.
3. **Important.** If $h, k \in G$ agree on a base, then hk^{-1} fixes that base, so $h = k$ by definition. So if you know how h behaves on a base, you can identify h.

Base of permutation groups and quantum speedups (1/2)

Theorem

Let G be a permutation group on $[n]$, and let $f : \mathcal{D} \subseteq \Sigma^n \to \{0,1\}$. Then, there exists $h : \widetilde{\mathcal{D}} \subseteq \widetilde{\Sigma}^n \to \{0,1\}$ that is symmetric under G such that $Q(h) \leq Q(f) + b(G)$ and $R(h) \geq R(f)$.

Corollary

If G has $b(G) = n^{o(1)}$, then there exists a function, symmetric under G, that admits a super-polynomial quantum speedup.

Proof of corollary.

In the theorem take f to be Simon's function, then $Q(f) = O(\log n)$, but $R(f) = \Omega(\sqrt{n})$. Therefore

$$Q(h) \leq Q(f) + b(G) = O(\log n) + n^{o(1)} = n^{o(1)},$$
$$R(h) \geq R(f) = \Omega(\sqrt{n}).$$

Hence a super-polynomial quantum speedup for computing h. $\square$

Base of permutation groups and quantum speedups (2/2)

Theorem

Let G be a permutation group on $[n]$, and let $f : \mathcal{D} \subseteq \Sigma^n \to \{0,1\}$. Then, there exists $h : \widetilde{\mathcal{D}} \subseteq \widetilde{\Sigma}^n \to \{0,1\}$ that is symmetric under G such that $Q(h) \leq Q(f) + b(G)$ and $R(h) \geq R(f)$.

Proof sketch.

Example with $n = 2$: $\mathcal{D} = \{(a,a),(b,a)\} \subseteq \Sigma^n = \{a,b\}^2$ and $G = S_2$. Construct the set $\widetilde{\mathcal{D}}$ of "G-permutations of $\mathcal{D}$":

$$\widetilde{\mathcal{D}} := \{[(a,1),(a,2)],\ [(a,2),(a,1)],\ [(b,1),(a,2)],\ [(a,2),(b,1)]\}$$
$$\subseteq (\Sigma \times [n])^n = \{(a,1),\ (a,2),\ (b,1),\ (b,2)\}^2.$$

Let h be "the same as" f. Then $h : \widetilde{\mathcal{D}} \subseteq (\Sigma \times [n])^n \to \{0,1\}$ is symmetric under G. $Q(h) \leq Q(f) + b(G)$: classically query the indices in the base to identify the G-permutation, then reverse this permutation, and use algorithm for computing f to compute h. $R(h) \geq R(f)$: clear as h is harder to compute than f.

$\square$

Primitive permutation groups and quantum speedups

Theorem (Liebeck, 1984)

Let G be a primitive permutation group on $[n]$. Then one of the following cases hold:

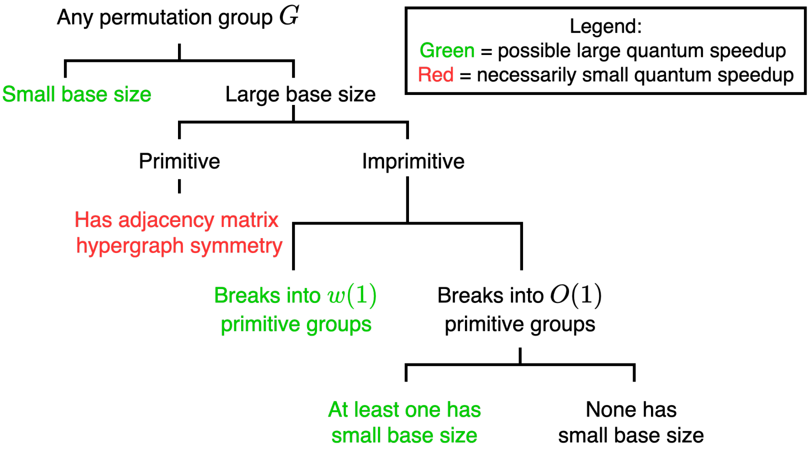
1. $n = \binom{m}{p}^{\ell}$ *and G contains permutations on* $[n] = [\binom{m}{p}]^{\ell}$ *that permutes each of the ℓ-entries according to* $A_m^p \subseteq S_m^p$*, i.e., essentially p-uniform hypergraph symmetries.*
2. $b(G) < 9 \log_2(n)$.

Consequence. Complete characterization of quantum speedups for functions symmetric under primitive permutation groups:

1. Case 1: at most a $3\ell p$-power polynomial quantum speedup.
2. Case 2: super-polynomial quantum speedup.

General permutation groups and quantum speedups

Prior art[1]: small quantum speedup for f symmetric under $G = S_n$.
This work: general permutation groups are "built from" primitive permutation groups $\implies$ near-complete characterization theorem.



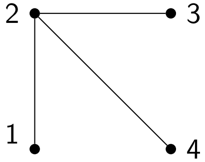
[1] Aaronson and Ambainis (2009); Chailloux (2018).

Graph properties in the adjacency list model

Adjacency list model of graphs

In the adjacency list model, a (simple) graph on n vertices of degree bounded by d is modelled by a list of length $n \times d$.

Example with $n = 4$ and $d = 3$:

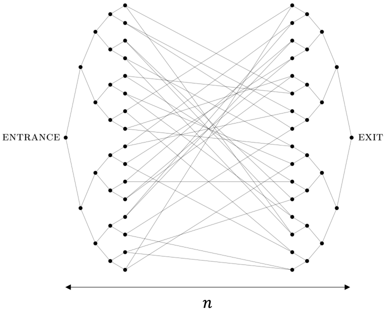


2	$\perp$	$\perp$
1	3	4
2	$\perp$	$\perp$
2	$\perp$	$\perp$

Super-polynomial quantum speedup for graph property testing in the adjacency list model (1/2)

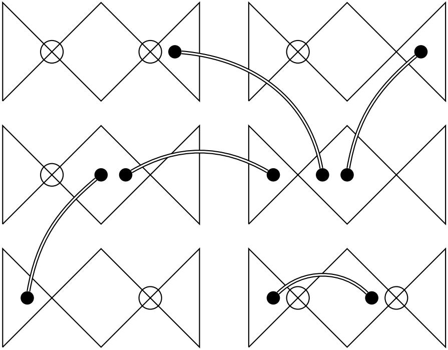
Graph property testing: given a graph promised to either have a property or is far from having it, decide which is the case.

Main idea. Upgrade the glued-trees problem[2], which has a super-polynomial quantum speedup in the adjacency list model, to a graph property testing problem.



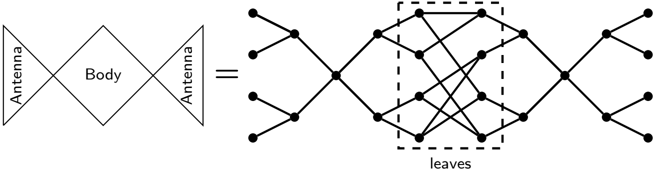
[2]Childs, Cleve, Deotto, Farhi, Gutmann, and Spielman (2003).

Super-polynomial quantum speedup for graph property testing in the adjacency list model (2/2)



Six "candy" subgraphs and five of the many double-edges that connect each body vertex to a distinct antenna vertex. The circles in the figure represent self-loops at the roots of the candy graphs, which provide advice about whether a body vertex is a leaf or non-leaf. Even parity of circles indicates non-leaf, odd parity indicates leaf.

where



Open problems

Open problems

Thank you for your attention! Here are some of our open problems:

1. We showed that $R(f) = O(Q(f)^{3p})$ for computing p-uniform hypergraph properties f in the adjacency matrix model, but what is the largest possible separation? That is, what is the largest k for which there exists such an f with $R(f) = \Omega(Q(f)^k)$? Know $k \geq p$. Open *even for* $p = 1$.
2. Can we get a complete characterization theorem regarding which permutation groups allow super-polynomial quantum speedups and which do not? Close already.
3. Does there exist a graph property testing problem *of practical interest* in the adjacency list model that admits a super-polynomial quantum speedup? We also conjecture that deciding a *monotone* graph property cannot admit a super-polynomial quantum speedup.