NP-Intermediate Problems and Quantum Algorithms

Tristram Bogart

Universidad de los Andes

31 May 2013

Outline

- Complexity classes and graph theory
- The graph isomorphism problem
- The hidden subgroup problem and quantum algorithms
- The abelian case
- The symmetric group case and graph isomorphisms

P and NP

A (yes-no) decision problem is in complexity class P if there is a algorithm (Turing machine) to solve it and a polynomial p such that for all n and all input of bit-length n, the algorithm terminates correctly in at most $p(n)$ steps.

P and NP

A (yes-no) decision problem is in complexity class P if there is a algorithm (Turing machine) to solve it and a polynomial p such that for all n and all input of bit-length n, the algorithm terminates correctly in at most $p(n)$ steps.

A decision problem is in class NP if a 'yes' answer can always be verified in polynomial time with the aid of an appropriate certificate. A problem is in co-NP if a 'no' answer can be similarly verified.

P and NP

A (yes-no) decision problem is in complexity class *P* if there is a algorithm (Turing machine) to solve it and a polynomial p such that for all n and all input of bit-length n, the algorithm terminates correctly in at most $p(n)$ steps.

A decision problem is in class NP if a 'yes' answer can always be verified in polynomial time with the aid of an appropriate certificate. A problem is in co-NP if a 'no' answer can be similarly verified.

Note that P $\subseteq$ NP $\cap$ co-NP.

Million-dollar question: Does P equal NP?

Graph problems in P

A graph is a finite set V of vertices and a set E of edges, given as pairs of vertices.

The following graph theoretic problems are in P:

- Connected: Given a graph Γ, is there a path between every pair of vertices?
- Bipartite: Given a graph Γ, can its vertices be partitioned into two sets A and B such that every edge has one end in A and the other in B?
- Eulerian circuit: Given a graph Γ, does Γ contain a (closed) circuit that includes each edge of Γ exactly once?

Graph problems in P

A graph is a finite set V of vertices and a set E of edges, given as pairs of vertices.

The following graph theoretic problems are in P:

- Connected: Given a graph Γ, is there a path between every pair of vertices?
- Bipartite: Given a graph Γ, can its vertices be partitioned into two sets A and B such that every edge has one end in A and the other in B?
- Eulerian circuit: Given a graph Γ, does Γ contain a (closed) circuit that includes each edge of Γ exactly once?

A graph has an Eulerian circuit if and only if every vertex has even degree.

Graph problems in NP

- k-Clique: Given a graph Γ and a number k, does Γ contain a complete subgraph with k vertices?
- k-Chromatic: Given a graph Γ and a number k, can the vertices of Γ be colored with k colors such that no two adjacent vertices have the same color?
- Hamiltonian: Given a graph Γ, does Γ contain a cycle that passes through each vertex exactly once?
- Graph Isomorphism: Given graphs Γ_1 and Γ_2, is there a bijection f from the vertices of Γ_1 to the vertices of Γ_2 such that $\{u, v\}$ is an edge of Γ_1 if and only if $\{f(u), f(v)\}$ is an edge of Γ_2?

Graph problems in NP

- k-Clique: Given a graph Γ and a number k, does Γ contain a complete subgraph with k vertices?
- k-Chromatic: Given a graph Γ and a number k, can the vertices of Γ be colored with k colors such that no two adjacent vertices have the same color?
- Hamiltonian: Given a graph Γ, does Γ contain a cycle that passes through each vertex exactly once?
- Graph Isomorphism: Given graphs Γ_1 and Γ_2, is there a bijection f from the vertices of Γ_1 to the vertices of Γ_2 such that $\{u, v\}$ is an edge of Γ_1 if and only if $\{f(u), f(v)\}$ is an edge of Γ_2?

In each case, the desired object is itself a certificate whenever the answer is YES. None of the problems are known to be in co-NP.

NP-completeness

A problem X is

- NP-hard if every problem in NP can be reduced to X in polynomial time.
- NP-complete if it is both in NP and NP-hard.
- NP-intermediate if it is NP, but neither in P nor NP-Hard.

By definition, if some NP-complete problem can be solved in polynomial-time, then P=NP.

NP-completeness

A problem X is

- NP-hard if every problem in NP can be reduced to X in polynomial time.
- NP-complete if it is both in NP and NP-hard.
- NP-intermediate if it is NP, but neither in P nor NP-Hard.

By definition, if some NP-complete problem can be solved in polynomial-time, then P=NP.

Theorem (Cook, '71) The problem SAT (satisfiability of Boolean functions) is NP-complete.
Theorem (Karp, '72) The problems k-Clique, k-Chromatic, Hamiltonian (and several others) are NP-complete.

NP-completeness

A problem X is

- NP-hard if <u>every</u> problem in NP can be reduced to X in polynomial time.
- NP-complete if it is both in NP and NP-hard.
- NP-intermediate if it is NP, but neither in P nor NP-Hard.

By definition, if some NP-complete problem can be solved in polynomial-time, then P=NP.

Theorem (Cook, '71) The problem SAT (satisfiability of Boolean functions) is NP-complete.
Theorem (Karp, '72) The problems k-Clique, k-Chromatic, Hamiltonian (and several others) are NP-complete.

In fact most problems in NP are either known to be in P or are NP-complete. Graph Isomorphism is an exception, as is factoring.

Friendliness of Graph Isomorphism

- There are polynomial-time algorithms for important special cases such as planar graphs, graphs of bounded vertex degree, and graphs whose adjacency matrices have bounded eigenvalue multiplicity.
- Non-isomorphic graphs usually can be easily distinguished by degree sequence, counting small subgraphs, or eigenvalues of the adjacency matrix
- There are algorithms that usually run in polynomial time in practice, though take exponential time in the worst case.
- The problem of counting isomorphisms reduces in polynomial time to the decision problem, unlike for many NP-hard problems.

Isomorphisms and automorphisms

Let Γ_1 and Γ_2 be graphs on n vertices and Γ be their disjoint union. An isomorphism between Γ_1 and Γ_2 is an automorphism σ of Γ that interchanges $V(\Gamma_1)$ with $V(\Gamma_2)$.

Isomorphisms and automorphisms

Let Γ_1 and Γ_2 be graphs on n vertices and Γ be their disjoint union. An isomorphism between Γ_1 and Γ_2 is an automorphism σ of Γ that interchanges $V(\Gamma_1)$ with $V(\Gamma_2)$.

Given generators of $\mathrm{Aut}(\Gamma)$, we can check in polynomial time if any automorphism has the interchange property. So Graph Isomorphism reduces to finding generators for $\mathrm{Aut}(\Gamma) \leq S_{2n}$, a special case of ...

The hidden subgroup problem

Given a finite group G, find generators of an unknown subgroup H. We are allowed to call a function f on G that satisfies:

$$f(x) = f(y) \Leftrightarrow x, y \text{ are in the same coset of } H.$$

The hidden subgroup problem

Given a finite group G, find generators of an unknown subgroup H. We are allowed to call a function f on G that satisfies:

$$f(x) = f(y) \Leftrightarrow x, y \text{ are in the same coset of } H.$$

Example: Let $G = \mathbb{Z}_2^3 = \langle y_1, y_2, y_3 \rangle$ and $H = \langle y_1 + y_2 \rangle$, a two-element subgroup. Define $f : G \to \mathbb{Z}_2^2$ by $f(a, b, c) = (a + b, c)$. Then f is constant on the cosets of H and distinguishes them.

The hidden subgroup problem

Given a finite group G, find generators of an unknown subgroup H. We are allowed to call a function f on G that satisfies:

$$f(x) = f(y) \Leftrightarrow x, y \text{ are in the same coset of } H.$$

Example: Let $G = \mathbb{Z}_2^3 = \langle y_1, y_2, y_3 \rangle$ and $H = \langle y_1 + y_2 \rangle$, a two-element subgroup. Define $f : G \to \mathbb{Z}_2^2$ by $f(a, b, c) = (a + b, c)$. Then f is constant on the cosets of H and distinguishes them.

To solve the hidden subgroup problem, we will study representations of the group G: homomorphisms ρ from G to $\mathrm{GL}_n(\mathbb{C})$. The number $d_\rho := n$ is the dimension of the representation. The character $\chi_\rho(g)$ is the trace of the matrix $\rho(g)$.

A quantum algorithm for the HSP

Define a state $|g\rangle$ for each $g \in G$. Define states $|(\rho, i, j)\rangle$ for each irreducible representation ρ and each matrix entry (i, j)

A quantum algorithm for the HSP

Define a state $|g\rangle$ for each $g \in G$. Define states $|(\rho, i, j)\rangle$ for each irreducible representation ρ and each matrix entry (i, j)

Define the following operators:

- An operator S that superposes the elements of G.
- An operator U_f that evaluates f; that is,

$$U_f\left(|g\rangle \otimes |00\ldots0\rangle\right) = |g\rangle \otimes |f(g)\rangle$$

- The quantum Fourier transform $\mathcal{F}$ that superposes all possible irreducible representations of a given element of G.

For appropriate groups G, each can be implemented with polynomially many basic quantum operations.

A quantum algorithm for the HSP, continued

- Initialize two quantum registers, one for elements of G and another for values of f.
- Apply S to the first register to get

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |00\ldots0\rangle \, .$$

- Apply U_f to get

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle \, .$$

- Measure the second register. The result is $f(c)$ for some random $c \in G$, giving

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |hc\rangle \otimes |f(c)\rangle \, .$$

A quantum algorithm for the HSP, continued

- Ignore the second register and apply $\mathcal{F}$ to the first, giving

$$\sum_{\rho \text{ irrep of } G} \sum_{i,j=1}^{d_\rho} \frac{\sqrt{d_\rho}}{\sqrt{|G|\,|H|}} \left(\sum_{h \in H} \rho(ch)_{i,j} \, |\rho, i, j\rangle \right).$$

- Measure the representation ρ. The probability of a given ρ is

$$\frac{d_\rho \sum_{h \in H} \chi_\rho(h)}{|G|}.$$

- Repeat enough times to effectively sample H.

Representations of abelian groups

The representations of a cyclic group $\mathbb{Z}_n = \langle y \rangle$ are all one-dimensional, given by $y \mapsto e^{\frac{2\pi ik}{n}}, \quad 0 \leq k \leq n-1$. The quantum Fourier transform in this case is the regular Fourier transform.

In particular, for $\mathbb{Z}_2$, we have the trivial representation given by $y \mapsto 1$ and the sign representation given by $y \mapsto -1$.

Representations of abelian groups

The representations of a cyclic group $\mathbb{Z}_n = \langle y \rangle$ are all one-dimensional, given by $y \mapsto e^{\frac{2\pi ik}{n}}$, $0 \leq k \leq n-1$. The quantum Fourier transform in this case is the regular Fourier transform.

In particular, for $\mathbb{Z}_2$, we have the trivial representation given by $y \mapsto 1$ and the sign representation given by $y \mapsto -1$.

For $\mathbb{Z}_2^n = \langle y_1, y_2, \ldots, y_n \rangle$ we have 2^n representations given by $y_i \mapsto \pm 1$ for each i. Given such a ρ,

$$\rho\left(\sum_{i \in I} y_i\right) = -1^{\#\{i \in I : \rho(y_i) = -1\}}.$$

That is, the representations give the (vector space) dual to $\mathbb{Z}_2^n$.

An abelian example

Let $G = \mathbb{Z}_2^3 = \langle y_1, y_2, y_3 \rangle$ and $H = \langle y_1 + y_2 \rangle \simeq \mathbb{Z}_2$.

ρ	$\rho(e)$	$\rho(y_1 + y_2)$	Prob(ρ)
(+,+,+)	1	1	2/8
(+,+,-)	1	1	2/8
(+,-,+)	1	-1	0
(+,-,-)	1	-1	0
(-,+,+)	1	-1	0
(-,+,-)	1	-1	0
(-,-,+)	1	1	2/8
(-,-,-)	1	1	2/8

An abelian example

Let $G = \mathbb{Z}_2^3 = \langle y_1, y_2, y_3 \rangle$ and $H = \langle y_1 + y_2 \rangle \simeq \mathbb{Z}_2$.

ρ	$\rho(e)$	$\rho(y_1 + y_2)$	Prob(ρ)
(+,+,+)	1	1	2/8
(+,+,-)	1	1	2/8
(+,-,+)	1	-1	0
(+,-,-)	1	-1	0
(-,+,+)	1	-1	0
(-,+,-)	1	-1	0
(-,-,+)	1	1	2/8
(-,-,-)	1	1	2/8

Thus the algorithm gives a random representation dual to H. The same holds for any subgroup K of $\mathbb{Z}_2^n$. With high probability, K^* is generated by $2n$ random elements of it. Finally, K^* determines K.

Irreducible representations of the symmetric group S_3

- Trivial representation: $\rho_{\text{triv}}(\sigma) = 1$ for all permutations σ.
- Sign representation: $\rho_{\text{sign}}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$
- Standard representation ρ_{std}: let S_3 act on $\mathbb{C}^3$ by permuting coordinates. Restrict the action to the plane given by $x_1 + x_2 + x_3 = 0$. Choose a basis for the plane: say $\{e_1 - e_2, e_2 - e_3\}$.

Irreducible representations of the symmetric group S_3

- Trivial representation: $\rho_{\text{triv}}(\sigma) = 1$ for all permutations σ.
- Sign representation: $\rho_{\text{sign}}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$
- Standard representation ρ_{std}: let S_3 act on $\mathbb{C}^3$ by permuting coordinates. Restrict the action to the plane given by $x_1 + x_2 + x_3 = 0$. Choose a basis for the plane: say $\{e_1 - e_2, e_2 - e_3\}$.

The respective dimensions are 1, 1, and 2. Since $1^2 + 1^2 + 2^2 = 6 = |S_3|$, Matschke's theorem guarantees that they are the only irreducible representations of S_3 over $\mathbb{C}$

Sampling subgroups of S_3

$\sigma \in S_3$	$\rho_{\text{triv}}(\sigma)$	$\rho_{\text{sgn}}(\sigma)$	$\rho_{\text{std}}(\sigma)$	$\chi_{\text{std}}(\sigma)$
e	1	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	2
(12)	1	-1	$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$	0
(23)	1	-1	$\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$	0
(13)	1	-1	$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$	0
(123)	1	1	$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$	-1
(132)	1	1	$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$	2

Sampling subgroups of S_3, continued

For the trivial group $\{e\}$:

$$\begin{aligned}
\Pr(\rho_{\mathrm{triv}}) &= 1 \cdot \frac{\chi_{\mathrm{triv}}(e)}{6} &= 1/6 \\
\Pr(\rho_{\mathrm{sgn}}) &= 1 \cdot \frac{\chi_{\mathrm{sgn}}(e)}{6} &= 1/6 \\
\Pr(\rho_{\mathrm{std}}) &= 2 \cdot \frac{\chi_{\mathrm{std}}(e)}{6} &= 4/6
\end{aligned}$$

Sampling subgroups of S_3, continued

For the trivial group $\{e\}$:

$$\begin{aligned}
\Pr(\rho_{\text{triv}}) &= 1 \cdot \frac{\chi_{\text{triv}}(e)}{6} &= 1/6 \\
\Pr(\rho_{\text{sgn}}) &= 1 \cdot \frac{\chi_{\text{sgn}}(e)}{6} &= 1/6 \\
\Pr(\rho_{\text{std}}) &= 2 \cdot \frac{\chi_{\text{std}}(e)}{6} &= 4/6
\end{aligned}$$

For the group $H = \langle (12) \rangle = \{e, (12)\} \simeq \mathbb{Z}/2$:

$$\begin{aligned}
\Pr(\rho_{\text{triv}}) &= 1 \cdot \frac{\chi_{\text{triv}}(e)+\chi_{\text{triv}}((12))}{6} &= (1+1)/6 &= 2/6 \\
\Pr(\rho_{\text{sgn}}) &= 1 \cdot \frac{\chi_{\text{sgn}}(e)+\chi_{\text{sgn}}((12))}{6} &= (1-1)/6 &= 0 \\
\Pr(\rho_{\text{std}}) &= 2 \cdot \frac{\chi_{\text{std}}(e)+\chi_{\rho}((12))}{6} &= 2 \cdot (2+0)/6 &= 4/6
\end{aligned}$$

Sampling subgroups of S_3, continued

For the trivial group $\{e\}$:

$$\begin{aligned}
\Pr(\rho_{\mathrm{triv}}) &= 1 \cdot \frac{\chi_{\mathrm{triv}}(e)}{6} &= 1/6 \\
\Pr(\rho_{\mathrm{sgn}}) &= 1 \cdot \frac{\chi_{\mathrm{sgn}}(e)}{6} &= 1/6 \\
\Pr(\rho_{\mathrm{std}}) &= 2 \cdot \frac{\chi_{\mathrm{std}}(e)}{6} &= 4/6
\end{aligned}$$

For the group $H = \langle (12) \rangle = \{e, (12)\} \simeq \mathbb{Z}/2$:

$$\begin{aligned}
\Pr(\rho_{\mathrm{triv}}) &= 1 \cdot \frac{\chi_{\mathrm{triv}}(e)+\chi_{\mathrm{triv}}((12))}{6} &= (1+1)/6 &= 2/6 \\
\Pr(\rho_{\mathrm{sgn}}) &= 1 \cdot \frac{\chi_{\mathrm{sgn}}(e)+\chi_{\mathrm{sgn}}((12))}{6} &= (1-1)/6 &= 0 \\
\Pr(\rho_{\mathrm{std}}) &= 2 \cdot \frac{\chi_{\mathrm{std}}(e)+\chi_{\rho}((12))}{6} &= 2\cdot(2+0)/6 &= 4/6
\end{aligned}$$

To distinguish $\langle (12) \rangle$ from the trivial group, we need to know with high probability that ρ_{sgn} does not show up.

Negative results for S_n

Theorem (Hallgren-Russell-Ta-Shma, '00) Fourier sampling cannot distinguish the trivial subgroup of S_n from certain subgroups of order two in polynomial time with high probability.

Negative results for S_n

Theorem (Hallgren-Russell-Ta-Shma, '00) Fourier sampling cannot distinguish the trivial subgroup of S_n from certain subgroups of order two in polynomial time with high probability.

In particular, if Γ_1 and Γ_2 are two rigid graphs, then the isomorphism problem reduces to this case of the hidden subgroup problem.

Negative results for S_n

Theorem (Hallgren-Russell-Ta-Shma, '00) Fourier sampling cannot distinguish the trivial subgroup of S_n from certain subgroups of order two in polynomial time with high probability.

In particular, if Γ_1 and Γ_2 are two rigid graphs, then the isomorphism problem reduces to this case of the hidden subgroup problem.

Strong Fourier sampling is a variant of the algorithm where we keep track of not just the character of a representation ρ), but the whole matrix.

Negative results for S_n

Theorem (Hallgren-Russell-Ta-Shma, '00) Fourier sampling cannot distinguish the trivial subgroup of S_n from certain subgroups of order two in polynomial time with high probability.

In particular, if Γ_1 and Γ_2 are two rigid graphs, then the isomorphism problem reduces to this case of the hidden subgroup problem.

Strong Fourier sampling is a variant of the algorithm where we keep track of not just the character of a representation ρ), but the whole matrix.

Theorem (Moore-Russell-Schulman, '08 Strong Fourier sampling also cannot distinguish hidden subgroups of S_n in polynomial time with high probability.

Question: Can more intricate quantum algorithms efficiently solve the hidden subgroup problem for S_n?

References

- Scott Aaronson: BQP and the polynomial hierarchy, Proceedings of the 42nd ACM symposium on theory of computing (2010) 141–150.
- Jörg Bühler: Quantum approaches to the graph isomorphism problem, Diplomarbeit, Universität Karlsruhe (2006).
- M.R. Garey and D.S. Johnson: Computers and Intractability: A Guide to the Theory of NP-Completeness, W.H. Freeman and Co. (1979). Alisa Bokulich and Gregg Jaeger (eds.): Philosophy of Quantum Information and Entanglement, Cambridge University Press (2010).
- A.Yu. Kitaev, A.H. Shen, and M.N.Vyalyi: Classical and Quantum Computation, Graduate Studies in Mathematics 47 (2002)
- Cristopher Moore, Alexander Russell, and Leonard J. Schulman: The symmetric group defies strong Fourier sampling, SIAM J. Comput. 37(6) (2008), 1842–1864.