Graph isomorphism, the hidden subgroup problem and identifying quantum states

Pranab Sen

NEC Laboratories America,
Princeton, NJ, U.S.A.

Joint work with Sean Hallgren and Martin Rötteler.

Quant-ph 0511148: Lower bound for graph isomorphism.
Quant-ph 0512085: Quantum state identification.

Part I:

Statement of the results.

Hidden subgroup problem (HSP)

Given: G: group, S: set, $f : G \to S$ via an oracle.

Promise: Subgroup $H \leq G$ such that f is constant on the left cosets of H and distinct on different cosets.

Task: Find the hidden subgroup H by querying f.

Example (Factoring integers):

- Given n;
- Choose randomly $1 < a < n$, $\gcd(a, n) = 1$;
- Define $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(x) := a^x \bmod n$;
- $H = \{rx : x \in \mathbb{Z}\}$, r is order of a modulo n;
- Finding r allows us to factor n.

Hidden subgroup problem (HSP)

Given: G: group, S: set, $f : G \to S$ via an oracle.

Promise: Subgroup $H \leq G$ such that f is constant on the left cosets of H and distinct on different cosets.

Task: Find the hidden subgroup H by querying f.

Example (Factoring integers):

- Given n;
- Choose randomly $1 < a < n$, $\gcd(a, n) = 1$;
- Define $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(x) := a^x \bmod n$;
- $H = \{rx : x \in \mathbb{Z}\}$, r is order of a modulo n;
- Finding r allows us to factor n.

Importance of HSP

Following important problems reduce to HSP:

- Integer factoring: $G = \mathbb{Z}$;
- Discrete logarithm over p: $G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$;
- Pell's equation: $G = \mathbb{R}$;
- Graph isomorphism: $G = S_{2n}$.

Abelian G: Efficient (polynomial in $\log |G|$) quantum algorithm.

Non-abelian G: General case, OPEN!
Few cases, efficient quantum algorithm.

Most super-polynomial speedups obtained so far by quantum algorithms fall under HSP framework.

Graph isomorphism and HSP

Lower bound actually for isomorphism of rigid graphs, Turing-equivalent to graph automorphism.

Isomorphism of rigid n-vertex graphs reduces to HSP in S_{2n}.

If rigid graphs G_0, G_1:

Have isomorphism π:
$H = \{e, (1, n+\pi(1)) \cdots (n, n+\pi(n))\}$.
H conjugate to
$H_0 := \{e, (1, n+1) \cdots (n, 2n)\}$.

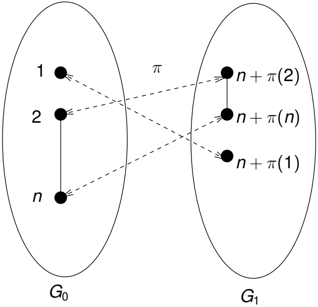
Are non-isomorphic:
$H = \{e\}$, the identity subgroup.

Graph isomorphism and HSP

Lower bound actually for isomorphism of rigid graphs, Turing-equivalent to graph automorphism.

Isomorphism of rigid n-vertex graphs reduces to HSP in S_{2n}.

If rigid graphs G_0, G_1:



Have isomorphism π:
$H = \{e, (1, n{+}\pi(1)) \cdots (n, n{+}\pi(n))\}$.
H conjugate to
$H_0 := \{e, (1, n+1) \cdots (n, 2n)\}$.

Are non-isomorphic:
$H = \{e\}$, the identity subgroup.

Coset state approach for HSP

G: group, H: hidden subgroup in G.

Hidden subgroup coset state:

$$\sigma_H := \frac{|H|}{|G|} \sum_{g \in G/H} |gH\rangle\langle gH|, \qquad \text{where } |gH\rangle := \frac{1}{\sqrt{|H|}} \sum_{x \in gH} |x\rangle.$$

The procedure:

- Repeat the following steps t times:

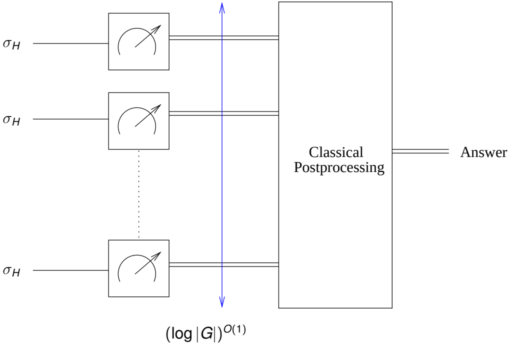
$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|0\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle \mapsto \sigma_H;$$

- Apply a POVM on $\sigma_H^{\otimes t}$ to identify H with high probability.

Single-register coset state algorithm

G: group, H: hidden subgroup, σ_H: coset state of H.

Algorithm measures one copy of σ_H at a time.



Single−register algorithm

Examples of single-register coset state algorithms

G: group, H: hidden subgroup, σ_H: coset state of H.

Single-register algorithms suffice information theoretically for the following HSPs:

- Abelian G: Based on quantum Fourier transform over G and is efficient;
- H normal subgroup of G: Uses weak quantum Fourier sampling over G;
- Few more examples: G dihedral, affine etc.

Problem: Identify more general classes of (G, H) where single register algorithms suffice information theoretically for the HSP.

Ensemble state identification and HSP

$\mathcal{S}$: general ensemble $\{\sigma_i\}_i$ of quantum states in $\mathbb{C}^n$.

State identification: Given ℓ copies of $\sigma_i \in \mathcal{S}$, identify i.

Coset state approach to HSP: $\mathcal{S} = \{\sigma_H\}_{H \leq G}$.

f: minimum pairwise Frobenius distance in $\mathcal{S}$.

Theorem: There is a single register algorithm identifying given $\sigma \in \mathcal{S}$ with $\ell = O\left(\frac{\log |\mathcal{S}|}{f^2}\right)$ copies.

Proof uses 'random POVMs'.

Corollary: There is a single register algorithm for HSP using polynomially many copies of σ_H, if rank of H is polynomially bounded or full in every irrep of G.

Generalises all previous positive results about single register algorithms for HSP and gives some new ones e.g. $G = \mathbb{Z}_p^n \rtimes \mathbb{Z}_p$.

Ensemble state identification and HSP

$\mathcal{S}$: general ensemble $\{\sigma_i\}_i$ of quantum states in $\mathbb{C}^n$.

State identification: Given ℓ copies of $\sigma_i \in \mathcal{S}$, identify i.

Coset state approach to HSP: $\mathcal{S} = \{\sigma_H\}_{H \leq G}$.

f: minimum pairwise Frobenius distance in $\mathcal{S}$.

Theorem: There is a single register algorithm identifying given $\sigma \in \mathcal{S}$ with $\ell = O\left(\frac{\log |\mathcal{S}|}{f^2}\right)$ copies.

Proof uses 'random POVMs'.

Corollary: There is a single register algorithm for HSP using polynomially many copies of σ_H, if rank of H is polynomially bounded or full in every irrep of G.

Generalises all previous positive results about single register algorithms for HSP and gives some new ones e.g. $G = \mathbb{Z}_p^n \rtimes \mathbb{Z}_p$.

Ensemble state identification and HSP

$\mathcal{S}$: general ensemble $\{\sigma_i\}_i$ of quantum states in $\mathbb{C}^n$.

State identification: Given ℓ copies of $\sigma_i \in \mathcal{S}$, identify i.

Coset state approach to HSP: $\mathcal{S} = \{\sigma_H\}_{H \leq G}$.

f: minimum pairwise Frobenius distance in $\mathcal{S}$.

Theorem: There is a single register algorithm identifying given $\sigma \in \mathcal{S}$ with $\ell = O\left(\frac{\log |\mathcal{S}|}{f^2}\right)$ copies.

Proof uses 'random POVMs'.

Corollary: There is a single register algorithm for HSP using polynomially many copies of σ_H, if rank of H is polynomially bounded or full in every irrep of G.

Generalises all previous positive results about single register algorithms for HSP and gives some new ones e.g. $G = \mathbb{Z}_p^n \rtimes \mathbb{Z}_p$.

Ensemble state identification and PGM

$\mathcal{S}$: general ensemble of quantum states in $\mathbb{C}^n$.
t: minimum pairwise trace distance in $\mathcal{S}$.

Corollary: There is a single register algorithm identifying given $\sigma \in \mathcal{S}$ with $\ell = O\left(\frac{n \log |\mathcal{S}|}{t^2}\right)$ copies.

No state identification result for general ensembles known previously.

The pretty good measurement (PGM) method says nothing about state identification for general ensembles with large pairwise trace distance.

Also, PGM typically does not give single register algorithms for state identification.

The single-register HSP algorithm

Rank of H is polynomially bounded or full in every irrep of G.

The algorithm:

Repeat $(\log |G|)^{O(1)}$ times:

- Apply QFT_G to one copy of σ_H;
- Observe the name of an irrep ρ of G;
- Measure using a ‘random POVM’.

Classical postprocessing to determine H.

Definition (Random POVM in $\mathbb{C}^n$): Got by choosing n independent random unit vectors in $\mathbb{C}^n$ and adding a ‘don’t know’ outcome for completeness.

Theorem: $\|\mathcal{M}(\sigma_1) - \mathcal{M}(\sigma_2)\|_1 \geq c \cdot \frac{\|\sigma_1 - \sigma_2\|_{\mathrm{F}}}{\log n}$, with prob. at least $1 - \exp(-cn)$, where $c > 0$ is a universal constant.

The single-register HSP algorithm

Rank of H is polynomially bounded or full in every irrep of G.

The algorithm:

Repeat $(\log |G|)^{O(1)}$ times:

- Apply QFT_G to one copy of σ_H;
- Observe the name of an irrep ρ of G;
- Measure using a 'random POVM'.

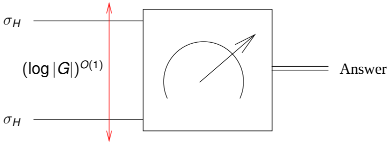
Classical postprocessing to determine H.

Definition (Random POVM in $\mathbb{C}^n$): Got by choosing n independent random unit vectors in $\mathbb{C}^n$ and adding a 'don't know' outcome for completeness.

Theorem: $\|\mathcal{M}(\sigma_1) - \mathcal{M}(\sigma_2)\|_1 \geq c \cdot \frac{\|\sigma_1 - \sigma_2\|_{\mathrm{F}}}{\log n}$, with prob. at least $1 - \exp(-cn)$, where $c > 0$ is a universal constant.

General non-abelian HSP

Fact (Ettinger, Høyer, Knill):



Problem: Above algorithm has running time $|G|^{O(\log|G|)}$.

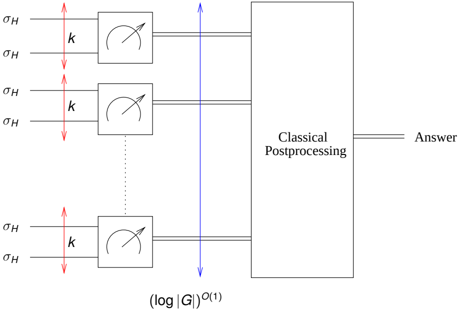
Only positive result known for general non-abelian G!

But it shows quantum query complexity of HSP is polynomial and uses only coset states of H.

Classically, the query complexity is exponential.

k-register algorithm for HSP

Algorithm measures at most k copies of σ_H at a time.



k-register algorithm

Hope: May give insight into efficient algo. for HSP for (G, H).

Goal: Study info. theoretically how small k can be for (G, H).

Graph isomorphism and coset state algorithms

Holy grail: How small can k be for $G = S_{2n}$, H subgroup relevant for graph isomorphism?

Rank of H is exponentially large but not full for most irreps of G. In fact, single register random Fourier sampling fails (Grigni, Schulman, Vazirani, Vazirani).

(Moore, Russell, Schulman): $k = 1$ impossible.

(Moore, Russell): $k = 2$ impossible.

Our result: $k \leq 0.08 n \log n$ impossible, even if adaptive!

(Ettinger, Høyer, Knill): $k = 4 n \log n$ possible.

Graph isomorphism and coset state algorithms

Holy grail: How small can k be for $G = S_{2n}$, H subgroup relevant for graph isomorphism?

Rank of H is exponentially large but not full for most irreps of G. In fact, single register random Fourier sampling fails (Grigni, Schulman, Vazirani, Vazirani).

(Moore, Russell, Schulman): $k = 1$ impossible.

(Moore, Russell): $k = 2$ impossible.

Our result: $k \leq 0.08 n \log n$ impossible, even if adaptive!

(Ettinger, Høyer, Knill): $k = 4n \log n$ possible.

Graph isomorphism and coset state algorithms

Holy grail: How small can k be for $G = S_{2n}$, H subgroup relevant for graph isomorphism?

Rank of H is exponentially large but not full for most irreps of G. In fact, single register random Fourier sampling fails (Grigni, Schulman, Vazirani, Vazirani).

(Moore, Russell, Schulman): $k = 1$ impossible.

(Moore, Russell): $k = 2$ impossible.

Our result: $k \leq 0.08n \log n$ impossible, even if adaptive!

(Ettinger, Høyer, Knill): $k = 4n \log n$ possible.

Graph isomorphism and coset state algorithms

Holy grail: How small can k be for $G = S_{2n}$, H subgroup relevant for graph isomorphism?

Rank of H is exponentially large but not full for most irreps of G. In fact, single register random Fourier sampling fails (Grigni, Schulman, Vazirani, Vazirani).

(Moore, Russell, Schulman): $k = 1$ impossible.

(Moore, Russell): $k = 2$ impossible.

Our result: $k \leq 0.08 n \log n$ impossible, even if adaptive!

(Ettinger, Høyer, Knill): $k = 4 n \log n$ possible.

Graph isomorphism and coset state algorithms

Holy grail: How small can k be for $G = S_{2n}$, H subgroup relevant for graph isomorphism?

Rank of H is exponentially large but not full for most irreps of G. In fact, single register random Fourier sampling fails (Grigni, Schulman, Vazirani, Vazirani).

(Moore, Russell, Schulman): $k = 1$ impossible.

(Moore, Russell): $k = 2$ impossible.

Our result: $k \leq 0.08 n \log n$ impossible, even if adaptive!

(Ettinger, Høyer, Knill): $k = 4 n \log n$ possible.

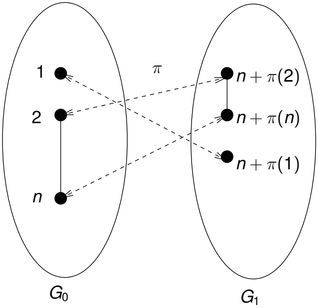
Part II:

The multi-register lower bound for HSP

Recall: Graph isomorphism and HSP

Isomorphism of rigid n-vertex graphs reduces to HSP in $S_n \wr S_2 \leq S_{2n}$.

If rigid graphs G_0, G_1:



Have isomorphism π:
Hidden subgroup
$\{e, (1, n+\pi(1))\cdots(n, n+\pi(n))\}$,
conjugate to
$H = \{e, (1, n+1)\cdots(n, 2n)\}$.

Are non-isomorphic:
Hidden subgroup is identity $\{e\}$.

Form of our multi-register lower bound

G: group, H: fixed subgroup $\{1, h\}$.

Possible hidden subgroups: Conjugates $H^g := gHg^{-1}$, $g \in G$ and identity subgroup $\{1\}$.

$\mathcal{M}$: POVM on k coset states, $\mathcal{M}_H$: prob. dist. on $\sigma_H^{\otimes k}$.

Theorem: Choose parameter ε, $0 < \varepsilon < 0.5k^{-1}$. Then, $\mathrm{E}_g[\|\mathcal{M}_{H^g} - \mathcal{M}_{\{1\}}\|_1] \leq 2^k f(G, h, \varepsilon) =: \delta$.

If ε can be chosen to make δ exponentially small $\Rightarrow$ No efficient $\log f(G, h, \varepsilon)$-register algorirthm for HSP.

For some groups like $G = S_n \wr S_2$, ε can be chosen so that δ is exponentially small unless $k = \Omega(\log |G|)$.

For some groups like abelian G, even for $k = 1$, δ is a constant for all possible ε.

Form of our multi-register lower bound

G: group, H: fixed subgroup $\{1, h\}$.

Possible hidden subgroups: Conjugates $H^g := gHg^{-1}$, $g \in G$ and identity subgroup $\{1\}$.

$\mathcal{M}$: POVM on k coset states, $\mathcal{M}_H$: prob. dist. on $\sigma_H^{\otimes k}$.

Theorem: Choose parameter ε, $0 < \varepsilon < 0.5k^{-1}$. Then, $\mathrm{E}_g[\|\mathcal{M}_{H^g} - \mathcal{M}_{\{1\}}\|_1] \leq 2^k f(G, h, \varepsilon) =: \delta$.

If ε can be chosen to make δ exponentially small $\Rightarrow$ No efficient $\log f(G, h, \varepsilon)$-register algorirthm for HSP.

For some groups like $G = S_n \wr S_2$, ε can be chosen so that δ is exponentially small unless $k = \Omega(\log |G|)$.

For some groups like abelian G, even for $k = 1$, δ is a constant for all possible ε.

Representation theory

G: group.

Representation ρ: Group homomorphism $\rho : G \to \mathrm{U}(d)$, d is some positive integer called the dimension of ρ.

Irrep ρ: In above, if no non-trivial subspace of $\mathbb{C}^d$ is invariant under the action of matrices $\rho(g)$, $g \in G$.

Fundamental fact: Every representation ρ is a direct sum of irreps τ, i.e.,

$$\rho \cong \bigoplus_{\tau} a_{\tau}^{\rho} \tau,$$

where a_{τ}^{ρ} is the multiplicity of τ in ρ. Projector Π_{τ}^{ρ} onto $\oplus a_{\tau}^{\rho} \tau$ is called isotypic projection for τ in ρ.

Character χ_ρ: Function $\chi_\rho : G \to \mathbb{C}$ defined as $\chi_\rho(g) := \mathrm{Tr}\rho(g)$.

The multi-register lower bound theorem

G: group, H: fixed subgroup $\{1, h\}$.

Possible hidden subgroups: Conjugates $H^g := gHg^{-1}$, $g \in G$ and identity subgroup $\{1\}$.

$\mathcal{M}$: POVM on k coset states, $\mathcal{M}_H$: prob. dist. on $\sigma_H^{\otimes k}$.

Choose ε, $0 < \varepsilon < 0.5k^{-1}$.

$\widehat{G}$: complete set of inequivalent irreps of G.

$\mathcal{S}_\varepsilon := \left\{ \tau \in \widehat{G} : \frac{|\chi_\tau(h_0)|}{d_\tau} \geq \varepsilon \right\}$, the non-smooth irreps of G.

$D_\varepsilon := \sum_{\tau \in \mathcal{S}_\varepsilon} d_\tau^2$.

Then,

$$\mathrm{E}_g[\|\mathcal{M}_{H_0^g} - \mathcal{M}_{\{1\}}\|_1] \leq 2^k \cdot \left[4 \left(\varepsilon + D_\varepsilon |\widehat{G}|^{1/2} |G|^{-1/2} \right)^{1/2} \right].$$

The multi-register lower bound theorem

G: group, H: fixed subgroup $\{1, h\}$.

Possible hidden subgroups: Conjugates $H^g := gHg^{-1}$, $g \in G$ and identity subgroup $\{1\}$.

$\mathcal{M}$: POVM on k coset states, $\mathcal{M}_H$: prob. dist. on $\sigma_H^{\otimes k}$.

Choose ε, $0 < \varepsilon < 0.5k^{-1}$.

$\widehat{G}$: complete set of inequivalent irreps of G.

$\mathcal{S}_\varepsilon := \left\{ \tau \in \widehat{G} : \frac{|\chi_\tau(h_0)|}{d_\tau} \geq \varepsilon \right\}$, the non-smooth irreps of G.

$D_\varepsilon := \sum_{\tau \in \mathcal{S}_\varepsilon} d_\tau^2$.

Then,

$$\mathrm{E}_g[\|\mathcal{M}_{H_0^g} - \mathcal{M}_{\{1\}}\|_1] \leq 2^k \cdot \left[4 \left(\varepsilon + D_\varepsilon |\widehat{G}|^{1/2} |G|^{-1/2} \right)^{1/2} \right].$$

The multi-register lower bound theorem

G: group, H: fixed subgroup $\{1, h\}$.

Possible hidden subgroups: Conjugates $H^g := gHg^{-1}$, $g \in G$ and identity subgroup $\{1\}$.

$\mathcal{M}$: POVM on k coset states, $\mathcal{M}_H$: prob. dist. on $\sigma_H^{\otimes k}$.

Choose ε, $0 < \varepsilon < 0.5k^{-1}$.

$\widehat{G}$: complete set of inequivalent irreps of G.

$\mathcal{S}_\varepsilon := \left\{ \tau \in \widehat{G} : \frac{|\chi_\tau(h_0)|}{d_\tau} \geq \varepsilon \right\}$, the non-smooth irreps of G.

$D_\varepsilon := \sum_{\tau \in \mathcal{S}_\varepsilon} d_\tau^2$.

Then,

$$\mathrm{E}_g[\|\mathcal{M}_{H_0^g} - \mathcal{M}_{\{1\}}\|_1] \leq 2^k \cdot \left[4 \left(\varepsilon + D_\varepsilon |\widehat{G}|^{1/2} |G|^{-1/2} \right)^{1/2} \right].$$

Proof: wlog do quantum Fourier transform

G: group, H': subgroup, $\mathcal{M}$: POVM on k coset states.

Definition ($\rho(H')$): ρ irrep of G, $\rho(H') := |H'|^{-1} \sum_{h' \in H'} \rho(h')$.

Quantum Fourier transform QFT_G: A unitary transformation:

$$\mathrm{QFT}_G : |g\rangle \mapsto \sum_{\rho,i,j} \sqrt{\frac{d_\rho}{|G|}} \cdot \rho_{ij}(g) \, |\rho, i, j\rangle .$$

QFT_G simultaneously block-diagonalises $\sigma_{H'}$ for all $H' \leq G$.

Wlog, POVM $\mathcal{M}$ on $\sigma_{H'}^{\otimes k}$ respects Fourier block structure, i.e.:

- $\mathcal{M}$ applies $\mathrm{QFT}_G^{\otimes k}$ and measures names of k irreps of G;
- Then, $\mathcal{M}$ measures the reduced state $\rho_1(H') \otimes \cdots \otimes \rho_k(H')$ normalised by an orthonormal basis $\mathcal{B}$.

Proof: wlog do quantum Fourier transform

G: group, H': subgroup, $\mathcal{M}$: POVM on k coset states.
Definition ($\rho(H')$): ρ irrep of G, $\rho(H') := |H'|^{-1} \sum_{h' \in H'} \rho(h')$.

Quantum Fourier transform QFT_G: A unitary transformation:

$$\mathrm{QFT}_G : |g\rangle \mapsto \sum_{\rho,i,j} \sqrt{\frac{d_\rho}{|G|}} \cdot \rho_{ij}(g) \, |\rho, i, j\rangle.$$

QFT_G simultaneously block-diagonalises $\sigma_{H'}$ for all $H' \leq G$.

Wlog, POVM $\mathcal{M}$ on $\sigma_{H'}^{\otimes k}$ respects Fourier block structure, i.e.:

- $\mathcal{M}$ applies $\mathrm{QFT}_G^{\otimes k}$ and measures names of k irreps of G;
- Then, $\mathcal{M}$ measures the reduced state $\rho_1(H') \otimes \cdots \otimes \rho_k(H')$ normalised by an orthonormal basis $\mathcal{B}$.

Proof: the view in the Fourier basis

G: group, H: fixed subgroup $\{1, h\}$, H^g: conjugate gHg^{-1}.

$$\frac{\mathrm{rank}(\rho(H))}{d_\rho} = \frac{1}{2}\left(1 + \frac{\chi_\rho(h)}{d_\rho}\right).$$

Assume $\mathrm{rank}(\rho(H^g)) = \mathrm{rank}(\rho(H)) = 0.5 d_\rho$ for all irreps ρ of G. Factor of 4 takes care of error due to above approximation.

In Fourier basis, $\mathrm{E}_g[\|\mathcal{M}_{H^g} - \mathcal{M}_{\{1\}}\|_1] = 2^k \mathrm{E}_{\rho,\mathbf{b},g}[|X(\rho, \mathbf{b}, g)|]$:

- $\rho := \rho_1 \otimes \cdots \otimes \rho_k$, ρ_i irrep of G;
- Plancherel distribution for ρ, $\Pr(\rho) := 2^{-k} \cdot d_{\rho_1}^2 \cdots d_{\rho_k}^2$;
- Uniform distribution for $\mathbf{b} \in \mathcal{B}$, $\mathcal{B}$ orthonormal basis of ρ;
- Uniform distribution for $g \in G$;
- $X(\rho, \mathbf{b}, g) := \langle \mathbf{b} \,|\rho_1(H^g) \otimes \cdots \otimes \rho_k(H^g)|\, \mathbf{b}\rangle - 2^{-k}$.

Proof: the view in the Fourier basis

G: group, H: fixed subgroup $\{1, h\}$, H^g: conjugate gHg^{-1}.

$$\frac{\mathrm{rank}(\rho(H))}{d_\rho} = \frac{1}{2}\left(1 + \frac{\chi_\rho(h)}{d_\rho}\right).$$

Assume $\mathrm{rank}(\rho(H^g)) = \mathrm{rank}(\rho(H)) = 0.5 d_\rho$ for all irreps ρ of G.
Factor of 4 takes care of error due to above approximation.

In Fourier basis, $\mathrm{E}_g[\|\mathcal{M}_{H^g} - \mathcal{M}_{\{1\}}\|_1] = 2^k \mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}[|X(\boldsymbol{\rho}, \mathbf{b}, g)|]$:

- $\boldsymbol{\rho} := \rho_1 \otimes \cdots \otimes \rho_k$, ρ_i irrep of G;
- Plancherel distribution for $\boldsymbol{\rho}$, $\Pr(\boldsymbol{\rho}) := 2^{-k} \cdot d_{\rho_1}^2 \cdots d_{\rho_k}^2$;
- Uniform distribution for $\mathbf{b} \in \mathcal{B}$, $\mathcal{B}$ orthonormal basis of $\boldsymbol{\rho}$;
- Uniform distribution for $g \in G$;
- $X(\boldsymbol{\rho}, \mathbf{b}, g) := \langle \mathbf{b} \,|\rho_1(H^g) \otimes \cdots \otimes \rho_k(H^g)|\, \mathbf{b}\rangle - 2^{-k}$.

Proof: The second moment comes in

G: group, H: fixed subgroup $\{1, h\}$, H^g: conjugate gHg^{-1}.
$X(\boldsymbol{\rho}, \mathbf{b}, g) := \langle \mathbf{b} \,|\rho_1(H^g) \otimes \cdots \otimes \rho_k(H^g)|\, \mathbf{b}\rangle - 2^{-k}$.

Aim: Bound $\mathrm{E}_g[\|\mathcal{M}_{H^g} - \mathcal{M}_{\{1\}}\|_1] = 2^k \mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}[|X(\boldsymbol{\rho}, \mathbf{b}, g)|]$.

Strategy: $\mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}[|X(\boldsymbol{\rho}, \mathbf{b}, g)|] \leq \left(\mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}[X(\boldsymbol{\rho}, \mathbf{b}, g)^2]\right)^{1/2}$.

By Schur's lemma, $\mathrm{E}_g[X(\boldsymbol{\rho}, \mathbf{b}, g)^2] = \sum_\tau \frac{\chi_\tau(h)}{d_\tau} \left\| \Pi_\tau^{\boldsymbol{\rho}\otimes\boldsymbol{\rho}}(\mathbf{b} \otimes \mathbf{b}) \right\|^2$.

- τ: irrep of G;
- $\Pi_\tau^{\boldsymbol{\rho}\otimes\boldsymbol{\rho}}$: isotypic projection for τ in the diagonal representation $\boldsymbol{\rho} \otimes \boldsymbol{\rho}$ of G.

Little bit of cheating above, should consider pairs of non-empty subsets of $[k]$, but morally okay!

Proof: The second moment comes in

G: group, H: fixed subgroup $\{1, h\}$, H^g: conjugate gHg^{-1}.
$X(\rho, \mathbf{b}, g) := \langle \mathbf{b} \,|\rho_1(H^g) \otimes \cdots \otimes \rho_k(H^g)|\, \mathbf{b}\rangle - 2^{-k}$.

Aim: Bound $\mathrm{E}_g[\|\mathcal{M}_{H^g} - \mathcal{M}_{\{1\}}\|_1] = 2^k \mathrm{E}_{\rho,\mathbf{b},g}[|X(\rho, \mathbf{b}, g)|]$.

Strategy: $\mathrm{E}_{\rho,\mathbf{b},g}[|X(\rho, \mathbf{b}, g)|] \leq \left(\mathrm{E}_{\rho,\mathbf{b},g}[X(\rho, \mathbf{b}, g)^2]\right)^{1/2}$.

By Schur's lemma, $\mathrm{E}_g[X(\rho, \mathbf{b}, g)^2] = \sum_\tau \frac{\chi_\tau(h)}{d_\tau} \left\| \Pi_\tau^{\rho\otimes\rho}(\mathbf{b} \otimes \mathbf{b}) \right\|^2$.

- τ: irrep of G;
- $\Pi_\tau^{\rho\otimes\rho}$: isotypic projection for τ in the diagonal representation $\rho \otimes \rho$ of G.

Little bit of cheating above, should consider pairs of non-empty subsets of $[k]$, but morally okay!

Proof: The second moment comes in

G: group, H: fixed subgroup $\{1, h\}$, H^g: conjugate gHg^{-1}.
$X(\rho, \mathbf{b}, g) := \langle \mathbf{b} \,|\rho_1(H^g) \otimes \cdots \otimes \rho_k(H^g)|\, \mathbf{b}\rangle - 2^{-k}$.

Aim: Bound $\mathrm{E}_g[\|\mathcal{M}_{H^g} - \mathcal{M}_{\{1\}}\|_1] = 2^k \mathrm{E}_{\rho,\mathbf{b},g}[|X(\rho, \mathbf{b}, g)|]$.

Strategy: $\mathrm{E}_{\rho,\mathbf{b},g}[|X(\rho, \mathbf{b}, g)|] \leq \left(\mathrm{E}_{\rho,\mathbf{b},g}[X(\rho, \mathbf{b}, g)^2]\right)^{1/2}$.

By Schur's lemma, $\mathrm{E}_g[X(\rho, \mathbf{b}, g)^2] = \sum_\tau \frac{\chi_\tau(h)}{d_\tau} \left\| \Pi_\tau^{\rho\otimes\rho}(\mathbf{b} \otimes \mathbf{b}) \right\|^2$.

- τ: irrep of G;
- $\Pi_\tau^{\rho\otimes\rho}$: isotypic projection for τ in the diagonal representation $\rho \otimes \rho$ of G.

Little bit of cheating above, should consider pairs of non-empty subsets of $[k]$, but morally okay!

Proof: smooth irreps are no problem

G: group, H: fixed subgroup $\{1, h\}$, ε: smoothness parameter.

$$\mathrm{E}_g[X(\rho, \mathbf{b}, g)^2] = \sum_{\tau} \frac{\chi_\tau(h)}{d_\tau} \left\|\Pi_\tau^{\rho\otimes\rho}(\mathbf{b} \otimes \mathbf{b})\right\|^2 .$$

Recall: For smooth irreps τ, $\frac{|\chi_\tau(h)|}{d_\tau} < \varepsilon$.

For non-smooth irreps $\tau \in \mathcal{S}_\varepsilon$, we will use $\frac{|\chi_\tau(h)|}{d_\tau} \leq 1$.

$$\mathrm{E}_g[X(\rho, \mathbf{b}, g)^2] < \varepsilon + \sum_{\tau\in\mathcal{S}_\varepsilon} \left\|\Pi_\tau^{\rho\otimes\rho}(\mathbf{b} \otimes \mathbf{b})\right\|^2 .$$

Technical challenge: Bound $\left\|\Pi_\tau^{\rho\otimes\rho}(\mathbf{b} \otimes \mathbf{b})\right\|^2$ for non-smooth irreps τ of G.

Proof: apply isotypic projection formula

Moore, Russell and Schulman bounded $\left\|\Pi_\tau^{\rho\otimes\rho}(\mathbf{b}\otimes\mathbf{b})\right\|^2$ for non-smooth τ by a geometric dimension counting argument.

That argument fails for $k \geq 3$ when $G = S_n \wr S_2$ and H is a subgroup relevant to graph isomorphism.

Our idea: Use the fact that $\Pi_\tau^{\rho\otimes\rho}$ is an isotypic projection and it is applied to $\mathbf{b}\otimes\mathbf{b}$.

Fact (Isotypic projection): $\Pi_\tau^{\rho\otimes\rho} = d_\tau \mathrm{E}_g[\chi_\tau(g)^* \cdot (\rho\otimes\rho)(g)]$.

$$\mathrm{E}_g[X(\rho,\mathbf{b},g)^2] < \varepsilon + \left(\sum_{\tau\in\mathcal{S}_\varepsilon} d_\tau^2\right)\left(\mathrm{E}_g\left[|\langle\mathbf{b}\,|\rho(g)|\,\mathbf{b}\rangle|^2\right]\right).$$

Proof: apply isotypic projection formula

Moore, Russell and Schulman bounded $\left\|\Pi_\tau^{\rho\otimes\rho}(\mathbf{b}\otimes\mathbf{b})\right\|^2$ for non-smooth τ by a geometric dimension counting argument.

That argument fails for $k \geq 3$ when $G = S_n \wr S_2$ and H is a subgroup relevant to graph isomorphism.

Our idea: Use the fact that $\Pi_\tau^{\rho\otimes\rho}$ is an isotypic projection and it is applied to $\mathbf{b}\otimes\mathbf{b}$.

Fact (Isotypic projection): $\Pi_\tau^{\rho\otimes\rho} = d_\tau \mathrm{E}_g[\chi_\tau(g)^* \cdot (\rho\otimes\rho)(g)]$.

$$\mathrm{E}_g[X(\rho,\mathbf{b},g)^2] < \varepsilon + \left(\sum_{\tau\in\mathcal{S}_\varepsilon} d_\tau^2\right)\left(\mathrm{E}_g\left[|\langle\mathbf{b}\,|\rho(g)|\,\mathbf{b}\rangle|^2\right]\right).$$

Proof: apply isotypic projection formula

Moore, Russell and Schulman bounded $\left\|\Pi_\tau^{\rho\otimes\rho}(\mathbf{b}\otimes\mathbf{b})\right\|^2$ for non-smooth τ by a geometric dimension counting argument.

That argument fails for $k \geq 3$ when $G = S_n \wr S_2$ and H is a subgroup relevant to graph isomorphism.

Our idea: Use the fact that $\Pi_\tau^{\rho\otimes\rho}$ is an isotypic projection and it is applied to $\mathbf{b}\otimes\mathbf{b}$.

Fact (Isotypic projection): $\Pi_\tau^{\rho\otimes\rho} = d_\tau \mathrm{E}_g[\chi_\tau(g)^* \cdot (\rho\otimes\rho)(g)]$.

$$\mathrm{E}_g[X(\rho,\mathbf{b},g)^2] < \varepsilon + \left(\sum_{\tau\in\mathcal{S}_\varepsilon} d_\tau^2\right)\left(\mathrm{E}_g\left[\left|\langle \mathbf{b}\,|\rho(g)|\,\mathbf{b}\rangle\right|^2\right]\right).$$

Proof: apply Schur normalisation

$$\mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}[X(\rho,\mathbf{b},g)^2] < \varepsilon + \left(\sum_{\tau\in\mathcal{S}_\varepsilon} d_\tau^2\right)\left(\mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}\left[\left|\langle\mathbf{b}\,|\rho(g)|\,\mathbf{b}\rangle\right|^2\right]\right).$$

Our next idea:

- Decompose ρ into isotypic components of ν, ν irreps of G.
- **Schur normalisation:** $\mathrm{E}_g[|\langle b\,|\nu(g)|\,b\rangle|^2] = \frac{1}{d_\nu}$, for any irrep ν of G and any vector b in ν.

We also use a lemma by Moore and Russell bounding expected multiplicities of irrep ν in isotypic decomposition of ρ.

Fact (Moore-Russell): $\mathrm{E}_{\boldsymbol{\rho}}\left[\frac{a_\nu^\rho}{d_\nu}\right] = \frac{d_\nu}{|G|}$.

Proof: apply Schur normalisation

$$\mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}[X(\boldsymbol{\rho},\mathbf{b},g)^2] < \varepsilon + \left(\sum_{\tau\in\mathcal{S}_\varepsilon} d_\tau^2\right)\left(\mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}\left[|\langle \mathbf{b}\,|\boldsymbol{\rho}(g)|\,\mathbf{b}\rangle|^2\right]\right).$$

Our next idea:

- Decompose $\boldsymbol{\rho}$ into isotypic components of ν, ν irreps of G.
- **Schur normalisation:** $\mathrm{E}_g[|\langle b\,|\nu(g)|\,b\rangle|^2] = \frac{1}{d_\nu}$, for any irrep ν of G and any vector b in ν.

We also use a lemma by Moore and Russell bounding expected multiplicities of irrep ν in isotypic decomposition of ρ.

Fact (Moore-Russell): $\mathrm{E}_{\boldsymbol{\rho}}\left[\frac{a_\nu^\rho}{d_\nu}\right] = \frac{d_\nu}{|G|}$.

Proof: apply Schur normalisation

$$\mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}[X(\rho,\mathbf{b},g)^2] < \varepsilon + \left(\sum_{\tau\in\mathcal{S}_\varepsilon} d_\tau^2\right)\left(\mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}\left[|\langle\mathbf{b}\,|\rho(g)|\,\mathbf{b}\rangle|^2\right]\right).$$

Our next idea:

- Decompose $\boldsymbol{\rho}$ into isotypic components of ν, ν irreps of G.
- **Schur normalisation:** $\mathrm{E}_g[|\langle b\,|\nu(g)|\,b\rangle|^2] = \frac{1}{d_\nu}$, for any irrep ν of G and any vector b in ν.

We also use a lemma by Moore and Russell bounding expected multiplicities of irrep ν in isotypic decomposition of $\boldsymbol{\rho}$.

Fact (Moore-Russell): $\mathrm{E}_{\boldsymbol{\rho}}\left[\frac{a_\nu^\rho}{d_\nu}\right] = \frac{d_\nu}{|G|}$.

Proof: bounding contribution of non-smooth irreps

Finally, we require Moore, Russell and Schulman's original geometric argument of counting dimensions.

Fact: If W is a subspace of V and b is chosen uniformly from an orthonormal basis for V,

$$\mathrm{E}_b\left[\left\|\Pi_W^V(b)\right\|^2\right] = \frac{\dim W}{\dim V}.$$

Putting everything together:

$$\mathrm{E}_{\rho,\mathbf{b},g}\left[\left|\langle\mathbf{b}\,|\rho(g)|\,\mathbf{b}\rangle\right|^2\right] \leq \sum_{\nu} \frac{d_\nu}{|G|}.$$

Proof: finally!

$\widehat{G}$: set of irreps of G, $\mathcal{S}_\varepsilon := \left\{\tau : \frac{|\chi_\tau(h)|}{d_\tau} \geq \varepsilon\right\}$. $D_\varepsilon := \sum_{\tau\in\mathcal{S}_\varepsilon} d_\tau^2$.

The main result:

$$
\begin{aligned}
&\mathrm{E}_g[\|\mathcal{M}_{H^g} - \mathcal{M}_{\{1\}}\|_1] \\
&\quad = \quad 2^k \cdot 4 \cdot \mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}[|X(\boldsymbol{\rho},\mathbf{b},g)|] \quad \ldots \operatorname{rank}(\rho(H)) = 0.5 d_\rho \text{ approx.} \\
&\quad \leq \quad 2^k \cdot 4 \cdot \left(\mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}[X(\boldsymbol{\rho},\mathbf{b},g)^2]\right)^{1/2} \\
&\quad \leq \quad 2^k \cdot 4 \cdot \left(\varepsilon + \left(\sum_{\tau\in\mathcal{S}_\varepsilon} d_\tau^2\right)\left(\mathrm{E}_{\boldsymbol{\rho},\mathbf{b},g}\left[|\langle \mathbf{b}\,|\rho(g)|\,\mathbf{b}\rangle|^2\right]\right)\right)^{1/2} \\
&\quad \leq \quad 2^k \cdot 4 \cdot \left(\varepsilon + D_\varepsilon\left(\sum_\nu \frac{d_\nu}{|G|}\right)\right)^{1/2} \\
&\quad \leq \quad 2^k \cdot 4 \cdot \left(\varepsilon + D_\varepsilon |\widehat{G}|^{1/2} |G|^{-1/2}\right)^{1/2} \quad \ldots \text{Cauchy-Schwarz.}
\end{aligned}
$$

Lower bound for graph isomorphism

The main result:

$$\mathrm{E}_g[\|\mathcal{M}_{H^g} - \mathcal{M}_{\{1\}}\|_1] \leq 4 \cdot 2^k \cdot \left(\varepsilon + D_\varepsilon |\widehat{G}|^{1/2} |G|^{-1/2}\right)^{1/2}.$$

Applying this result with $\varepsilon := n^{-0.2n}$ for $G = S_n \wr S_2$ and $H = \{e, (1, n+1) \cdots (n, 2n)\}$ gives:

$$\mathrm{E}_g[\|\mathcal{M}_{H^g} - \mathcal{M}_{\{1\}}\|_1] \leq 2^k \cdot 4 \cdot n^{-0.09n}.$$

This implies that any efficient k-register coset state algorithm for graph isomorphism requires $k > 0.08 n \log n$!

Part III:

Discussion.

Importance of rank of hidden subgroup

Want: k-register information theoretic algorithm for HSP for (G, H) using only polynomially many coset states of H.

For ‘most’ irreps ρ of G, if rank of $\rho(H)$ is:

- Polynomially bounded or full: $k = 1$ suffices by single register random Fourier sampling.
- Exponential but not full: Examples like graph isomorphism and some more groups where $k = \Omega(\log |G|)$ required.

Random POVMs and questions of efficiency

Generating a single random vector is provably inefficient for a quantum computer!

Unclear how to efficiently postprocess the classical information got from single-register random Fourier sampling.

Leads us to the open question of efficient pseudo-random measurement bases!

Pseudo-random unitary model of Emerson et al. seems inadequate for our purposes.

Further research

More techniques for designing multi-register algorithms.

Examples:

- Clebsch-Gordan pairing method of Kuperberg for HSP in the dihedral group;
- Pretty good measurement method of Bacon, Childs and van Dam for HSP in the Heisenberg group;
- Missing harmonic idea of Moore and Russell for isomorphism of rigid graphs.

Important research project

Find new paradigms for designing HSP algorithms that go beyond using just coset states of the hidden subgroup H.

Main known paradigm: Orbit coset framework with Friedl, Ivanyos, Magniez and Santha.

- Uses coset states of subgroups NH, where N ranges over various normal subgroups of G, instead of just coset states of the hidden subgroup H;

A curious example: The group $(S_4)^n$.

- Our methods show any algorithm for HSP in $(S_4)^n$ using only coset states of H needs $k = \Omega(n)$;
- Orbit coset framework gives an efficient $\Theta(n)$-register algorithm for HSP in $(S_4)^n$, but uses coset states of NH.
- Only known example of a group with an efficient HSP algorithm where one can prove $k = \Omega(\log |G|)$.

Important research project

Find new paradigms for designing HSP algorithms that go beyond using just coset states of the hidden subgroup H.

Main known paradigm: Orbit coset framework with Friedl, Ivanyos, Magniez and Santha.

- Uses coset states of subgroups NH, where N ranges over various normal subgroups of G, instead of just coset states of the hidden subgroup H;

A curious example: The group $(S_4)^n$.

- Our methods show any algorithm for HSP in $(S_4)^n$ using only coset states of H needs $k = \Omega(n)$;
- Orbit coset framework gives an efficient $\Theta(n)$-register algorithm for HSP in $(S_4)^n$, but uses coset states of NH.
- Only known example of a group with an efficient HSP algorithm where one can prove $k = \Omega(\log |G|)$.

The challenging open problem!

Efficient quantum algorithm for graph isomorphism.

Only non-HSP quantum idea for graph isomorphism to date is based on creating the uniform superposition of all graphs isomorphic to a given graph.

Aharonov and Ta-Shma have proposed creating this superposition by quantum sampling a Markov chain, however, very little is known about this approach.

Thank you!