The Hunt for a Quantum Algorithm for Graph Isomorphism

Cristopher Moore, University of New Mexico
Alexander Russell, University of Connecticut
Leonard J. Schulman, Caltech
The Hidden Subgroup Problem

• Given a function \( f(x) \), find the \( y \) such that

\[
f(x + y) = f(x)
\]

for all \( x \).

• Given a function \( f \) on a group \( G \), find the subgroup \( H \) consisting of \( h \) such that

\[
f(gh) = f(g)
\]

for all \( g \).
The Hidden Subgroup Problem

- This captures many quantum algorithms: indeed, most algorithms which give an exponential speedup.
  - $\mathbb{Z}_2^n$: Simon’s problem
  - $\mathbb{Z}_n^*$: factoring, discrete log (Shor)
  - $\mathbb{Z}$: Pell’s equation (Hallgren)

What can the non-Abelian HSP do?
Graph Isomorphism

- Define a function $f$ on $S_{2n}$. If both graphs are rigid, then either $f$ is 1–1 and $H = \{1\}$, or $f$ is 2–1 and $H = \{1, m\}$ for some involution $m$ (of a particular type).
Standard Method: Coset States

- Start with a uniform superposition, \[ \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \]

- Measuring \( f \) gives a random coset of \( H \):
  \[ |cH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch\rangle \]
  or, if you prefer, a mixed state:
  \[ \rho = \frac{1}{|G|} \sum_{c \in G} |cH\rangle \langle cH| \]
The Fourier Transform

- We now perform a basis change. In $\mathbb{Z}_n$, 
  
  $$|k\rangle = \frac{1}{\sqrt{n}} \sum_x e^{2\pi i k x / n}$$

  and in $\mathbb{Z}_2^n$, 
  
  $$|k\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{k \cdot x}$$

- Why? Because these are homomorphisms from $G$ to $\mathbb{C}$. These form a basis for $\mathbb{C}[G]$ with many properties (e.g. convolution)
Group Representations

- Homomorphisms from groups to matrices:
  \[ \sigma : G \rightarrow U(V) \]

- For instance, consider this three-dimensional representation of \( A_5 \).

- Any representation can be decomposed into a direct sum of irreducible representations.
Heartbreaking Beauty

- Given a “name” $\rho$ and a row and column $i, j$,

$$|\sigma, i, j\rangle = \sqrt{\frac{d_\sigma}{|G|}} \sum_g \sigma(g)_{ij}$$

- Miraculously, these form an orthogonal basis for $\mathbb{C}[G] :$

$$\sum_{\sigma \in \hat{G}} d^2_\sigma = |G|$$
Group Actions

- Given a state in $\mathbb{C}[G]$ and a group element $g$, we can apply various group actions:

$$ |x\rangle \rightarrow |xg\rangle \text{ or } |g^{-1}x\rangle \text{ or } |g^{-1}xg\rangle $$

- We can think of $\mathbb{C}[G]$ as a representation of $G$ under any of these actions.

- Under (left or right) multiplication, the regular representation contains $d_\sigma$ copies of each $\sigma \in \hat{G}$. 
For most group families, the QFT can be carried out efficiently, in polylog(|G|) steps [Beals 1997; Høyer 1997; M., Rockmore, Russell 2004]

- **Weak sampling**: just the name $\sigma$
- **Strong sampling**: name, row and column $\sigma, i, j$ in a basis of our choice (some bases may be much more informative than others)
- Intermediate: strong, but with a random basis
Fourier Sampling is Optimal

- The mixed state over (left) cosets
  \[ \rho = \frac{1}{|G|} \sum_{c \in G} |cH\rangle \langle cH| \]

  is left $G$-invariant, hence block-diagonal.

- Measuring the irrep name (weak sampling) loses no coherence.

- Strong sampling is the only thing left to do!
For each irrep $\sigma$, we have a projection operator

$$\pi_H^\sigma = \frac{1}{|H|} \sum_{h \in H} \sigma(h)$$

The probability we observe $\sigma$ is

$$\frac{d_\sigma |H| \text{ rk } \pi_H^\sigma}{|G|}$$

Compare with the Plancherel distribution

$$\frac{d_\sigma^2}{|G|}$$

($H = \{1\}$, the completely mixed state)
Weak Sampling Fails

- If $H = \{1, m\}$, we have $\left( \chi_{\sigma}(g) = \text{tr} \sigma(g) \right)$

$$\text{rk } \pi^\sigma_H = \frac{d_\sigma}{2} \left( 1 + \frac{\chi_\sigma(m)}{d_\sigma} \right)$$

- In $S_n$, $\chi_\sigma(m)/d_\sigma$ is exponentially small, so the observed distribution is very close to Plancherel

Weak sampling fails [Hallgren, Russell, Ta-Shma 2000]

Random basis fails [Grigni, Schulman, Vazirani, Vazirani 2001]

But, strong is stronger for some $G$... [MRRS 2004]
Now for Strong Sampling

- But what about a basis of our choice? Given $\sigma$, we observe a basis vector $\mathbf{b}$ with probability

$$\frac{\|\pi_H \mathbf{b}\|^2}{\text{rk } \pi_H}$$

- Here we have $\|\pi_H \mathbf{b}\|^2 = \frac{1}{2}(1 + \langle \mathbf{b}, m\mathbf{b} \rangle)$

- How much does $\langle \mathbf{b}, m\mathbf{b} \rangle$ vary with $m$?
Controlling the Variance

- Expectation of an irrep $\sigma$ over $m$’s conjugates is

$$\text{Exp}_m \sigma(m) = \frac{\chi_\sigma(m)}{d_\sigma} \mathbb{1}$$

so $\text{Exp}_m \langle b, mb \rangle = \frac{\chi_\sigma(m)}{d_\sigma}$

- To turn the second moment into a first moment,

$$|\langle b, mb \rangle|^2 = \langle b \otimes b^*, m(b \otimes b^*) \rangle$$
Controlling the Variance

- Decompose $\sigma \otimes \sigma^*$ into irreducibles:

$$\sigma \otimes \sigma^* \cong \bigoplus_{\tau \in \hat{G}} a_\tau \tau$$

Then

$$\text{Var}_m \|\pi_H b\|^2 \leq \frac{1}{4} \sum_{\tau \in \hat{G}} \frac{\chi_\tau(m)}{d_\tau} \left\| \Pi_\tau^{\sigma \otimes \sigma^*} (b \otimes b^*) \right\|^2$$

- How much of $b \otimes b^*$ lies in low-dimensional $\tau$?
Using simple counting arguments, we show that almost all of $b \otimes b^*$ lies in high-dimensional subspaces $\tau$ of $\sigma \otimes \sigma^*$.

Since $\chi_\tau(m)/d_\tau$ is exponentially small, the observed distribution on $b$ for any basis is exponentially close to uniform.

No subexponential set of experiments on coset states can solve Graph Isomorphism.

[M., Russell, Schulman 2005]
Entangled Measurements

• For any group, there exists a measurement on the tensor product of coset states

\[ \rho \otimes \cdots \otimes \rho \]

with \( k = \text{poly}(\log |G|) \) [Ettinger, Høyer, Knill 1999]

• What can we prove about entangled measurements?
Bounds on Multiregister Sampling

- Weak sample each register, observing

\[ \sigma = \sigma_1 \otimes \cdots \otimes \sigma_k \]

- Given a subset \( I \) of the \( k \) registers, decompose that part of the tensor product:

\[ \bigotimes_{i \in I} \sigma_i \cong \bigoplus_{\tau \in \widehat{G}} a^{I}_{\tau} \tau \]

- This group action multiplies these registers by \( g \) and leaves the others fixed.
Bounds on Multiregister Sampling

- Second moment: analogous to one register, consider \( \sigma \otimes \sigma^* \). Given subsets \( I \) and \( J \), define

\[
E^{I,J}(b) = \sum_{\tau \in \hat{G}} \frac{\chi_\tau(m)}{d_\tau} \left\| \Pi_{I,J}^{I,J}(b \otimes b^*) \right\|^2
\]

- For an arbitrary entangled basis, [M., Russell 2005]

\[
\text{Var}_m \left\| \Pi_H b \right\|^2 \leq \frac{1}{4k} \sum_{I,J \subseteq [k]: I, J \neq \emptyset} E^{I,J}(b)
\]
Bounds on Multiregister Sampling

- With some additional work, this general bound can be used to show that $\Omega(n \log n)$ registers are necessary for $S_n$ [Hallgren, Rötteler, Sen; M., Russell]
- But what form might this measurement take?
- Note that each subset of the registers contributes some information...
Subset Sum and the Dihedral Group

- The HSP in the dihedral group $D_n$ reduces to random cases of Subset Sum [Regev 2002]
- Leads to a $2^{O(\sqrt{\log n})}$-time and -register algorithm [Kuperberg 2003]
- Subset Sum gives the optimal multiregister measurement [Bacon, Childs, van Dam 2005]
More Abstractly...

- If \( H = \{1, m\} \), there is a missing harmonic:

\[
\sum_{h \in H} \pi(h) = 0
\]

- Weak sampling gives random two-dimensional irreps \( \sigma_j \); think of these as integers \( \pm j \).

- Tensor products: \( \sigma_j \otimes \sigma_k \cong \sigma_{j+k} \oplus \sigma_{j-k} \)

- Find subset that gives \( \sigma_0 \cong 1 \oplus \pi \).
Suppose $H$ has a missing harmonic $\tau$.

For each subset $I$, consider the subspace $W^I_\tau$ resulting from applying the group action to $I$. (In $D_n$, this flips the integers $j$ in this subset.)

If the hidden subgroup is a conjugate of $H$, then the state is perpendicular to $W^I_\tau$ for all $I$.

How much of $\mathbb{C}[G^k]$ does this leave? What fraction is spanned by the $W^I_\tau$?
Independent Subspaces

Say that two subspaces \( V, W \) of a space \( U \) are independent if, just as for random vectors in \( U \),

\[
\mathbb{E}_{v \in V} \left\| \Pi_W v \right\|^2 = \frac{\dim W}{\dim U}
\]

or equivalently

\[
\frac{\text{tr} \, \Pi_V \Pi_W}{\dim U} = \frac{\text{tr} \, \Pi_V}{\dim U} \frac{\text{tr} \, \Pi_W}{\dim U}
\]

- Being in \( V \) or \( W \) are “independent events.”
Each Subset Contributes

- For $I \neq J$, $W^I_\tau$ and $W^J_\tau$ are independent.

- Therefore, $W_\tau = \text{span}_I W^I_\tau$ is large:
  \[
  \frac{\dim W_\tau}{\dim \mathbb{C}[G^k]} \geq 1 - \frac{1}{1 + 2^k/|G|}
  \]

- If $k \geq \log_2 |G|$, probability of “some subset being in $\tau$” is $\geq 1/2$ if the hidden subgroup is trivial, but is zero if it is a conjugate of $H$.

[M., Russell 2005]
Divide $\mathbb{C}[G^k]$ into subspaces; for each one, find a subset $I$ for a large fraction of the completely mixed state is in $W^I_T$: e.g. $\sigma_0 \cong 1 \oplus \pi$ in $D_n$.

“Pretty Good Measurement” (i.e., Subset Sum for $D_n$) is optimal for Gel’fand pairs... [MR 2005]

...but it is not optimal for $S_n$ [Childs]. What is? And, is it related to Subset Something?
The Hunt Continues

Beauty and Truth vs. The Adversary
Acknowledgments