A quantum algorithm for the dihedral hidden subgroup problem

Greg Kuperberg

arXiv:quant-ph/0302112

Main existing quantum algorithms

1) Arbitrary combinatorial search:

$$f : S \to \{0, 1\}$$

with $|S| = N$. Find $f(x) = 1$ with k solutions.
Classical time complexity: $\Theta(N/k)$.
Quantum complexity (Grover): $\Theta(\sqrt{N/k})$.

2) Period-finding (c.f. factoring, discrete log):

$$f : \mathbb{Z} \to S \qquad f(x+s) = f(x)$$

and f is otherwise 1-to-1. Find s.
Classical complexity: $\tilde{\Theta}(\sqrt{s})$.
Quantum complexity (Shor): $O((\log s)^\alpha)$.

Both algorithms have interesting variations due to Ettinger, Høyer, Tapp, Heiligman, Ambainis, Hallgren, Ip, van Dam, ...

The (deterministic) hidden subgroup problem

In HSP, G is a group, H is a subgroup, and

$$f : G \to S$$

is constant on cosets Ha and otherwise 1-to-1. G is explicit rather than black-box.) We want to find H.

If G is abelian, Shor's algorithm finds H using the quantum Fourier transform.

If G is residually finite and H is normal, a quantum character transform reveals H in quantum polynomial time.

If G is dihedral and H is a reflection, the character transform reveals little.

If G is the symmetric group, HSP is harder still.

Dihedral HSP

The dihedral group:

$$D_N = \langle x, y | x^N = y^2 = xyxy = 1 \rangle$$

A reflection subgroup:

$$H = \langle x^s y \rangle.$$

The problem is to find s, the *slope* of H.

DHSP is equivalent to the hidden shift problem. Here

$$f : \mathbb{Z}/N \to S \qquad g : \mathbb{Z}/N \to S$$

are injective with

$$g(x) = f(x + s).$$

The shift s is the same as the slope. The $N \hookrightarrow 2N$ hidden substring problem is also roughly equivalent.

Complexity of DHSP

DHSP requires $\Theta(\sqrt{N})$ classical queries.

The good news: $O((\log G)^{\alpha})$ quantum queries suffice for any finite HSP (Ettinger-Høyer-Knill).

The bad news: With few queries, DHSP appears to reduce to a hard subset-sum problem (Regev).

Theorem *There is a quantum algorithm for DHSP with $2^{O(\sqrt{\log N})}$ quantum time and query complexity.*

The moral: There is a good compromise between queries and time per query.

Abelian HSP

We abbreviate a constant pure state:

$$|S\rangle = \frac{1}{\sqrt{|S|}} \sum_{s \in S} |s\rangle$$

1. Apply $f : G \to S$ to the input $|G\rangle$ and discard the output. The result (by partial measurement) is the mixed state:

$$\rho_{G/H} = \frac{|H|}{|G|} \sum_{Ha} |Ha\rangle\langle Ha|.$$

2. Use a QFT to set up the measurement

$$\mathbb{C}[G] \cong \bigoplus_{\chi \in \widehat{G}} L_\chi.$$

Non-abelian HSP

If G is finite and non-abelian, you can still make

$$\rho_{G/H} = \frac{|H|}{|G|} \sum_{Ha} |Ha\rangle\langle Ha|.$$

You can take $\rho_{G/H}$ to be the oracle instead of f. This is *coherent HSP*.

Or most (all?) finite G, you can compute the measurement

$$\mathbb{C}[G] \cong \bigoplus_V (\dim V)V,$$

where the sum is over irreps. of G (Burnside).

Non-abelian HSP

If H is normal (Hallgren, Russel, Ta-Shma), then all outcomes are irreps. of G/H. If H is almost normal (Grigni, Schulman, Vazirani, Vazirani), then the outcomes still reveal H.

In many cases, character measurement reveals little. But V is has information! Its state ρ_V is *strongly H-invariant*: a mixture of H-invariant pure states. Here it is the uniform state on V^H.

If we could choose V, we could find H with state tomography. An idea: Given V and W, do the partial measurement

$$V \otimes W \cong \bigoplus m_{V,W}^X X.$$

The new ρ_X is also strongly H-invariant! Maybe we like X better than V or W.

Dihedral HSP

Recall the case $G = D_N$ and $H = \langle x^s y \rangle$ a reflection. Assume $N = 2^n$ and that we start with $\rho_{G/H}$.

1. Using a QFT, we can set up the measurement

$$\mathbb{C}[D_N] \cong \bigoplus_k 2V_k$$

for 2-dimensional induced representations

$$V_k = L_k \oplus L_{-k}.$$

The index k is uniformly random. The state on V_k (a qubit) is:

$$|0\rangle + \omega^{ks}|1\rangle,$$

where $\omega = \exp(2\pi i/2^N)$.

The DHSP algorithm (continued)

2. We will obtain $V_{2^{n-1}}$, which is reducible and reveals $s \bmod 2$.

3. Given V_k and V_ℓ, we can measure

$$V_k \otimes V_\ell \cong V_{k+\ell} \bigoplus V_{k-\ell}.$$

4. Given $2^{O(\sqrt{n})}$ separate V_k's, tensor them in pairs to cancel $\sim \sqrt{n}$ low bits of k. This shortens the list by a factor of 4. It requires $2^{O(\sqrt{n})}$ queries and quasilinear work in queries. Repeat $\sim \sqrt{n}$ times to obtain $V_{2^{n-1}}$.

5. Once we know $s \bmod 2$, we can pass to $D_{N/2}$ and repeat.

Variant algorithms

If N is odd:

1. We can cancel high bits instead of low bits to obtain V_1.

2. The map $x \mapsto x^2$ is a group automorphism that takes V_k to V_{2k}. So we can obtain V_{2^a} for any a.

3. Given a few copies of $V_1, V_2, V_4, \ldots$, we can measure N with state tomography. Or (Høyer), given one copy each, a QFT reveals N directly.

If $N = 2^n M$ with M odd, then

$$D_N \hookrightarrow D_M \times D_{2^n},$$

and we can combine both approaches.

The bad news

For most irreps of most groups, the tensor decomposition

$$V \otimes W \cong \bigoplus_X m_{V,W}^X X$$

has many ($\sim \dim V$) terms. There is very little control over the extracted summand, hence no clear way to climb and improve.

Since

$$D_{2\cdot 3\cdot 5 \cdots p} \hookrightarrow S_{2+3+5+\cdots+p},$$

symmetric HSP cannot be much easier than dihedral HSP. It is probably much harder.

Regev showed that DHSP cannot be much easier or much harder than lattice reduction.

Other comments

1. DHSP is not much different from general hidden shift. E.g.:

$$\mathbb{Z}/2 \ltimes \mathbb{Z}^d \sim D_N$$

for some N.

2. If you optimize the sieve (cancel low bits greedily), it conjecturally requires $O(4^{\sqrt{n}})$ queries.

4. Possible next cases of general HSP: SL$(2, p)$, the Sylow 2-subgroup of GL$(n, 2)$ or S_n.

5. Special DHSP (van Dam, Hallgren, Ip) seems faster than general DHSP. I conjecture that graph isomorphism is much faster than general SymHSP.