Introduction to Quantum Computing

A subexponential-time quantum algorithm for the dihedral hidden subgroup problem

Colombo Alberto

Table of Contents

Preliminaries

Hidden Subgroup Problem: Given an efficiently computable function $f : G \to S$, from a finite group G to a set S, that is constant on (left) cosets of some subgroup $H \leq G$ and takes distinct values on distinct cosets, *i.e.*

$$f(g_1) = f(g_2) \iff g_1, g_2 \in cH \text{ for some } c \in G,$$

find a set of generators for H.

Period Finding as HSP

Goal: find the order (or period) r of

$$f(a) = x^a \bmod N.$$

If we define $G = \mathbb{Z}_{\phi(N)}$, $H = \langle r \rangle = \{0, r, 2r, ..., \phi(N) - r\}$, where ϕ is the Euler function, we can cast the problem as an HSP. Indeed, f is constant on cosets $s + H$ and distinct on different cosets.

Algorithm for Abelian HSP

1. Compute $\sum_{g \in G} |g\rangle |f(g)\rangle$ and measure the second register $f(g) = f(c)$ for some $c \in G$. The resulting state is $|cH\rangle = \sum_{h \in H} |ch\rangle$ for some coset cH.
2. Compute the Fourier transform of the resulting state, obtaining

$$\sum_{\sigma \in \hat{G}} \frac{1}{\sqrt{|H||G|}} \sum_{h \in H} \sigma(ch) |\sigma\rangle ,$$

   where $\hat{G}$ is the set of irreducible representations of G.
3. Measure the first register and observe a representation σ.

Algorithm for Abelian HSP

1. Compute $\sum_{g\in G} |g\rangle\,|f(g)\rangle$ and measure the second register $f(g) = f(c)$ for some $c \in G$. The resulting state is $|cH\rangle = \sum_{h\in H} |ch\rangle$ for some coset cH.
2. Compute the Fourier transform of the resulting state, obtaining

$$\sum_{\sigma\in\hat{G}} \frac{1}{\sqrt{|H||G|}} \sum_{h\in H} \sigma(ch)\,|\sigma\rangle\,,$$

   where $\hat{G}$ is the set of irreducible representations of G.
3. Measure the first register and observe a representation σ.

Key fact: the distribution (measurement probability) of σ does not depend on c.

Algorithm for Period Finding

In the order finding example, we have

1. Compute $\sum_{j=0}^{N-1} |j\rangle |f(j)\rangle$ and measure the second register $f(j) = f(c)$ for some $c \in \{0, 1, ..., N-1\}$. The resulting state is $\sum_{k=0}^{m-1} |c + kr\rangle$ where m is the smallest integer for which $mr + c \geq N$.
2. Compute the Fourier transform of the resulting state, obtaining

$$\sum_{y=0}^{N-1} \frac{1}{\sqrt{Nm}} \sum_{k=0}^{m-1} e^{\frac{2\pi i}{N}(c+kr)y} |y\rangle .$$

3. Measure the first register and observe a representation label y.

Non Abelian Groups

1. Compute $\sum_{g \in G} |g\rangle |f(g)\rangle$ and measure the second register $f(g) = f(c)$ for some $c \in G$. The resulting state is $|cH\rangle = \sum_{h \in H} |ch\rangle$ for some coset cH.
2. Compute the Fourier transform of the coset state, obtaining

$$\sum_{\sigma \in \hat{G}} \sqrt{\frac{d_\sigma}{|H||G|}} \left(\sum_{h \in H} \sigma(ch) \right)_{ij} |\sigma\rangle |i\rangle |j\rangle ,$$

   where $\hat{G}$ is the set of irreducible representations of G.
3. Measure the first register and observe a representation label σ.

Non Abelian Groups

1. Compute $\sum_{g \in G} |g\rangle |f(g)\rangle$ and measure the second register $f(g) = f(c)$ for some $c \in G$. The resulting state is $|cH\rangle = \sum_{h \in H} |ch\rangle$ for some coset cH.
2. Compute the Fourier transform of the coset state, obtaining
$$\sum_{\sigma \in \hat{G}} \sqrt{\frac{d_\sigma}{|H||G|}} \left(\sum_{h \in H} \sigma(ch) \right)_{ij} |\sigma\rangle |i\rangle |j\rangle ,$$
where $\hat{G}$ is the set of irreducible representations of G.
3. Measure the first register and observe a representation label σ.

Remark (1): σ has no longer dimension 1, but it is actually a $d_\sigma \times d_\sigma$ matrix.

1. Compute $\sum_{g\in G} |g\rangle |f(g)\rangle$ and measure the second register $f(g) = f(c)$ for some $c \in G$. The resulting state is $|cH\rangle = \sum_{h\in H} |ch\rangle$ for some coset cH.
2. Compute the Fourier transform of the coset state, obtaining

$$\sum_{\sigma\in\hat{G}} \sqrt{\frac{d_\sigma}{|H||G|}} \left(\sum_{h\in H} \sigma(ch)\right)_{ij} |\sigma\rangle |i\rangle |j\rangle ,$$

   where $\hat{G}$ is the set of irreducible representations of G.
3. Measure the first register and observe a representation label σ.

Remark (2): the procedure above is known as *weak Fourier sampling*, and it suffices for solving some instances of HSP, e.g. when H is a normal subgroup of G ($gHg^{-1} = H \ \forall g \in G$).

HSP in the Dihedral group

The dihedral group D_N is the group of symmetries of a regular N-gon

$$D_N = \langle x, y \,|\, x^N = y^2 = yxyx = 1 \rangle = \{y^t x^s \,|\, t = 0, 1 \; s = 0, 1, ..., N\}.$$

The hidden subgroup of interest is the subgroup of reflections

$$H = \langle yx^{\bar{s}} \rangle$$

for some unknown *slope* parameter $\bar{s}$. Indeed, it can be proven that finding any $H \leq D_N$ can be reduced to finding an hidden reflection (Prop 2.1).

Main Algorithm

Observation

<u>Remark</u>: (consider $N = 2^n$) D_N contains two subgroups that are isomorphic to $D_{N/2}$,

$$F_0 = \langle x^2, y \rangle, \quad F_1 = \langle x^2, yx \rangle.$$

The hidden reflection group H is contained in $F_{\bar{s} \bmod 2}$, so if we know an algorithm to find the parity of s, then we can apply it again on $F_{\bar{s} \bmod 2}$ and repeat $\log_2 N$ times.

Algorithm steps

1. Compute the constant pure state

$$|D_N\rangle = \frac{1}{\sqrt{|D_N|}} \sum_{t,\,s} |y^t x^s\rangle \, .$$

Algorithm steps

2. Compute $U_f |D_N\rangle \propto \sum_{g \in D_N} |g\rangle |f(g)\rangle$, where U_f is the unitary embedding of f, and measure the second register obtaining in the first register

$$|cH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch\rangle$$

for some random $c \in D_N$.

Algorithm steps

3. Compute the (abelian) QFT on the n qubits used for describing s, as

$$F_N : |s\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i k s/N} |k\rangle .$$

Then measure $k \in \mathbb{Z}/N$ and obtain the qubit state (on the register representing t)

$$|\psi_k\rangle \propto |0\rangle + e^{2\pi i k \bar{s}/N} |1\rangle .$$

Algorithm steps

4. Consider two of the previous states $|\psi_k\rangle$, $|\psi_\ell\rangle$, and compute

$$\mathrm{CNOT}(|\psi_k\rangle \otimes |\psi_\ell\rangle). \tag{1}$$

If we now measure the second qubit, depending on the output of the measurement, we get

$$|\psi_{k\pm\ell}\rangle \propto |0\rangle + e^{2\pi i(k\pm\ell)\bar{s}/N} |1\rangle .$$

Since we know k and ℓ from previous measurements we can choose them in such a way they have $m = \lceil\sqrt{n-1}\rceil$ common trailing bits, so that the resulting state $|\psi_{k-\ell}\rangle$ have m more trailing zeroes than the original ones.

Algorithm steps

5. We can now repeat previous steps in order to produce the state

$$|\psi_{2^n-1}\rangle \propto |0\rangle + (-1)^{\bar{s}} |1\rangle ,$$

which measured in the $|\pm\rangle$ basis reveals the parity of $\bar{s}$.

Algorithm steps - Summary

1. Make a list of L_0 copies of the state $|cH\rangle$ by applying U_f to $|D_N\rangle$ and measuring the second register. Extract $|\psi_k\rangle$ form each $|cH\rangle$ with a QFT-based measurement.
2. For $0 \leq j < m$ ($m = \lceil \sqrt{n-1} \rceil$) we assume L_j is a list of $|\psi_k\rangle$ with at least mj trailing zeroes. Divide L_j into pairs of qubits $|\psi_k\rangle\, |\psi_\ell\rangle$ that share m additional trailing bits. Extract the state $|\psi_{k\pm\ell}\rangle$ from each pair and include in the new list L_{j+1} all states of the form $|\psi_{k-\ell}\rangle$.
3. The final list is L_m, and it consists of states $|\psi_0\rangle$ and $|\psi_{2^{n-1}}\rangle$ with equal probabilities. Measure one of the states $|\psi_{2^{n-1}}\rangle$ in the $|\pm\rangle$ basis to determine the parity of the slope $\bar{s}$.
4. Repeat 1-3 with the subgroup $F_{\bar{s} \bmod 2} \leq D_N$.

Proof of complexity

Theorem
Previous algorithm requires $\mathcal{O}(8^{\sqrt{n}})$ queries and $\tilde{\mathcal{O}}(8^{\sqrt{n}})$ computation time.

Proof of complexity

We can assume that if $|L_j| \gg 2^m$, then we are able to pair almost every k and ℓ such that they share m additional low bits. Approximately half of the pair will then form the new set L_{j+1}, so that

$$\frac{|L_{j+1}|}{|L_j|} \approx \frac{1}{4}.$$

If we then set for the final list $|L_m| = \Theta(2^m)$, working backward we get $|L_0| = \Theta(8^m)$. The computational complexity will only have logarithmic overhead due to the subroutine for matching k and ℓ.

Remark: we should formally still prove that the assumption $|L_j| \gg 2^m$ is enough to ensure $|L_m| = \Theta(2^m)$ with high probability.

General Idea

From representation theory we have the following orthogonal decomposition of the Hilbert space $\mathbb{C}[D_N] = \mathrm{span}\{|g\rangle \mid g \in D_N\}$

$$\mathbb{C}[D_N] \cong \bigoplus_{k \in \mathbb{Z}/N} V_k.$$

The projective measurement corresponding to such a decomposition can be computed using QFT.

Since the state $|cH\rangle$ is invariant under the represented action of H, the residual state $|\psi_k\rangle$ is too.

Moreover, each V_k is irreducible except for $k = 0$ and $k = N/2$. The target of Kuperberg's algorithm is indeed $V_{N/2}$ since the measurement corresponding to its irreducible decomposition reveals the parity of $\bar{s}$.

The Character Measurement & Strong Fourier Sampling

Another representation-theoretic decomposition of $\mathbb{C}[G]$ is the *Burnside decomposition*

$$\mathbb{C}[G] = \bigoplus_V V \otimes V^*,$$

where the sum is over the set of irreducible representations (irrep) of G. The factor V^* is called the *row space* and V is the *column space* in light of matrix identification.

The decomposition is orthogonal, thus it corresponds to a projective measurement called *character measurement*.

The Character Measurement & Strong Fourier Sampling

The mixed state

$$\rho_{G/H} = \frac{1}{|G|} \sum |cH\rangle \langle cH| \,,$$

is equivalent to the pure state $|cH\rangle$ (before/ignoring measurement of $|f(g)\rangle$).

$\rho_{G/H}$ is the uniform state on all H-invariant vectors in $\mathbb{C}[G]$, and can be related to Burnside decomposition through

$$\rho_{G/H} = \bigoplus_{V} \rho_{V^H} \otimes \rho_{V^*} \,,$$

where ρ_{V^H} is the uniform state over V^H, the invariant space of V w.r.t. the action of H, and ρ_{V^*} is the uniform state over V^*.

The Character Measurement & Strong Fourier Sampling

From this we conclude that no information about H is hidden in the row space V^*, and the state $\rho_{G/H}$ is equivalent to a process that provides the name of a irrep V and the column state ρ_{V^H} (Prop 8.1).

From this we conclude that no information about H is hidden in the row space V^*, and the state $\rho_{G/H}$ is equivalent to a process that provides the name of a irrep V and the column state ρ_{V^H} (Prop 8.1).

$\rightarrow$ We here can introduce the notion of *purely H-invariant state* as a state ρ which has support over an H-invariant space V^H.

The Character Measurement & Strong Fourier Sampling

From this we conclude that no information about H is hidden in the row space V^*, and the state $\rho_{G/H}$ is equivalent to a process that provides the name of a irrep V and the column state ρ_{V^H} (Prop 8.1).

$\rightarrow$ We here can introduce the notion of *purely H-invariant state* as a state ρ which has support over an H-invariant space V^H.

$\rightarrow$ In more recent literature, an approach that uses the character measurement is often referred as *strong Fourier sampling*, in opposition to the *weak Fourier sampling* (which only measure the label of the representation).

Generalizations

So far, the main innovation of Kuperberg's algorithm lies in the construction of the *sieve* that starts from copies of $|\psi_k\rangle$ and $|\psi_\ell\rangle$ and produces a measurement of the parity of the slope.

A generalization of it can be obtained by identifying the state indices k, ℓ as labels of two irreducible representations V, W. Then, the extraction of $|\psi_{k\pm\ell}\rangle$ can be seen as a decomposition of their tensor product, as

$$V \otimes W \cong \bigoplus_X \mathcal{H}_X^{W,V} \otimes X,$$

where X is an irrep of $V \otimes W$, and the Hilbert space $\mathcal{H}_X^{W,V}$ is the multiplicity factor of the decomposition ($\dim \mathcal{H}_X^{W,V}$ is the number of times X appears in the decomposition).

Abstract algorithm for HSP on Dihedral groups

1. Make a list of L copies of $\rho_{G/H}$, and extract an irrep V with a purely H-invariant state from each copy.
2. Choose an objective function $\alpha(\cdot)$ on the set of irreps of G.
3. Find a pair of irreps V, W in L s.t. $\alpha(V)$ and $\alpha(W)$ are both low, but s.t. α is significantly higher in at least one summand of $V \otimes W$. Extract an irreducible summand X and replace V and W in L with X (discard the multiplicity factor).
4. Repeat step 3 until α is maximized on some irrep V. Perform tomography on V to reveal information about H.
5. Repeat previous steps to fully identify H.

Algorithm extensions

In the article, Kuperberg also derived explicit algoritms for

- general case N;
- accelerated version for $N = r^n$;
- G is the generalized dihedral group

$$G = D_A \cong C_2 \ltimes \exp(A),$$

with

$$xyxy = 1 \quad \forall x \in A, \forall y \in C_2.$$

In particular applied to the *abelian hidden shift problem*, the *hidden reflection problem* and the *hidden substring problem*.

Reference

Greg Kuperberg. *A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem.* SIAM J. Comput. 35, 1 (2005), 170–188. https://doi.org/10.1137/S0097539703436345