The hidden subgroup problem for infinite groups
QIP 2021

Greg Kuperberg

UC Davis

February 2, 2021

(E-print in preparation.)

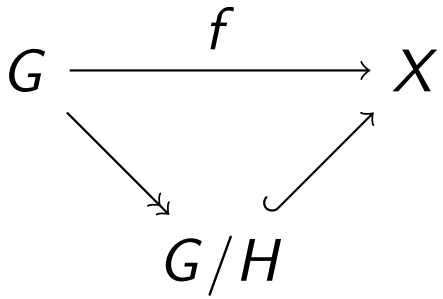
"The infinite Shor"

Florin Niculiu, *Infinite Shore*, 1983

I credit Peter Shor for HSP (+ Mosca-Ekert)

The hidden subgroup problem

Suppose that



where G is a discrete group, X is an unstructured set, f can be computed in polynomial time, and $H \leq G$ is a hidden subgroup. The hidden subgroup problem (HSP) is the computational problem of finding H, given f as functional input or an oracle. More explicitly, f hides H means that $f(x) = f(y)$ if and only if $x = yh$. f must be H-periodic, and otherwise 1-to-1.

The performance of HSP is rated by the bit complexity of the output.

Prior results on HSP

- Shor's algorithm solves HSP in BQP when $G = \mathbb{Z}$.
- The Shor-Kitaev algorithm solves HSP $G = \mathbb{Z}^k$ when $H \leq \mathbb{Z}^k$ has finite index (or rank k). It runs in BQP uniformly in the dimension k.
- Most other algorithms for HSP assume that G is finite:
  - G finite and H is normal [Hallgren-Russell-Ta-Shma].
  - G almost abelian [Grigni-Schulman-Vazirani-Vazirani].
  - G Heisenberg over $\mathbb{Z}/p$ [Bacon-Childs-van-Dam] or 2-step nilpotent [Ivanyos-Sanselme-Santha].
  - G dihedral [K.,Regev].
  - Some other cases.
- Some finite G look hard even for QC, *e.g.*, $G = S_n$.

Revisiting infinite HSP

If G is (discrete) infinite, then the quantum complexity of HSP amounts to a group property of G, rated against the complexity of $H \leq G$. Note that:

- Hardness results are interesting as a lens on groups.
- The complexity can depend on how elements of G are encoded.
- We assume that H is generated by elements of G reachable within the time budget.
- We can change the question by restricting H, *e.g.*, to be normal.

Negative results

Theorem (K.) If $G = (\mathbb{Q}, +)$, then HSP is NP-hard.

Theorem (K.) If $G = F_k$ is non-abelian free, then normal HSP is NP-hard.

Theorem (K.) If $G = \mathbb{Z}^k$ with unary vector encoding, then HSP is uSVP-hard. (Unique short vector in a lattice.)

We encode elements in $\mathbb{Q}$ as ordinary fractions; in F_k as reduced words; and in unary $\mathbb{Z}^k$ as commutative words:

$$\frac{993470124}{6798515} \in \mathbb{Q} \qquad aba^{-1}ba \in F_2 \qquad aaaab^{-1}b^{-1}b^{-1}ccccc \in \mathbb{Z}^3.$$

Positive results

Theorem (K.) If $G = \mathbb{Z}^k$ with binary encoding and H has infinite index, then H can be found in quantum polynomial time, uniformly in k and $\|H\|_{\text{bit}}$.

This is like Shor-Kitaev, but it requires new ideas.

Theorem (K.) If G is finitely generated and virtually abelian, then an arbitrary H can be found in time $\exp(\sqrt{\|H\|_{\text{bit}}})$.

This is a corollary of existing results on dihedral HSP = abelian hidden shift.

HSP in $\mathbb{Q}$

$d \in \mathrm{NP}$ means that there is a predicate $z \in \mathrm{P}$ such that $d(x) = \text{yes}$ if and only if $z(x, y) = \text{yes}$ for some witness y.

Step 1: We can take each y to be a prime number, by using the left $1/3$ of its bits as a data string [Ingham].

Step 2: We make an instance of HSP in $\mathbb{Q}$ from the predicate z. We generate H by 1 and the reciprocals of all witnesses:

$$H = \left\langle \left\{ \frac{1}{y} \mid z(x, y) = \text{yes} \right\} \cup \{1\} \right\rangle.$$

Step 3: We make an H-periodic function $f : \mathbb{Q} \to X = \mathbb{Q}$ by calculating a canonical representative $f(a/b) \in H + a/b$ for each coset of H.

The hiding function

Partial fractions for actual fractions

Partial fractions in $\mathbb{R}[x]$ are taught in calculus, but they also exist in $\mathbb{Q}$:

$$\frac{x^8+5}{x^4+x} = x^4 - x - \frac{3x-2}{x^2-x+1} - \frac{2}{x+1} + \frac{5}{x}$$

$$\frac{1}{60} = -2 + \frac{1}{2} + \frac{1}{4} + \frac{2}{3} + \frac{3}{5}$$

The right side is a canonical form with terms r/p^k with $1 \leq r < p$ with p prime, plus an integer. Calculating these partial fractions requires integer factorization, but we have that in BQP!

The hiding function

To calculate $f(a/b)$, expand a/b in partial fractions:

$$\frac{1}{60} = -2 + \frac{1}{2} + \frac{1}{4} + \frac{2}{3} + \frac{3}{5}$$

Then strike the integer term, and each term r/p with p an accepted witness:

$$f\left(\frac{1}{60}\right) = \cancel{-2} + \frac{1}{2} + \frac{1}{4} + \frac{2}{3} + \cancel{\frac{3}{5}} = \frac{1}{2} + \frac{1}{4} + \frac{2}{3} = \frac{17}{12}$$

Key point: You don't need to know the accepted witnesses, you only need to be able to ask the predicate $z(x, p)$.

Conclusion: If you can calculate whether $H \not\supseteq \mathbb{Z}$ from this f, then you can calculate $d(x)$ with $d \in \mathrm{NP}$.

An HSP algorithm in $\mathbb{Z}^k$

Suppose that $f : \mathbb{Z}^k \to X$ hides a sublattice $H \leq \mathbb{Z}^k$ of some rank $\ell \leq k$. Given parameters $Q \gg S \gg 1$, we follow one standard quantum opening for this HSP:

1. Prepare an approximate Gaussian state on a cube in $\mathbb{Z}^k$:

$$|\psi_G\rangle \propto \sum_{\substack{\vec{x}\in\mathbb{Z}^k \\ \|\vec{x}\|_\infty < Q/2}} \exp(-\pi\|\vec{x}\|_2^2/S^2)|\vec{x}\rangle$$

2. Apply the hiding function f to $|\psi_G\rangle$ to obtain:

$$U_f|\psi_G\rangle \propto \sum_{\vec{x}} \exp(-\pi\|\vec{x}\|_2^2/S^2)|\vec{x}, f(\vec{x})\rangle$$

   Throw away the output, leaving a mixed state on $\mathbb{C}[(\mathbb{Z}/Q)^k]$.

3. Apply the quantum Fourier operator $F_{(\mathbb{Z}/Q)^k}$ and measure a Fourier mode $\vec{y}_0 \in (\mathbb{Z}/Q)^k$.

Dual samples

The quantum part of the algorithm produces a sample $\vec{y}_0 \in (\mathbb{Z}/Q)^k$ which we can rescale to obtain:

$$\vec{y}_1 = \frac{\vec{y}_0}{Q} \in (\mathbb{R}/\mathbb{Z})^k$$

Then $\vec{y}_1$ is approximately a randomly chosen element of the dual group

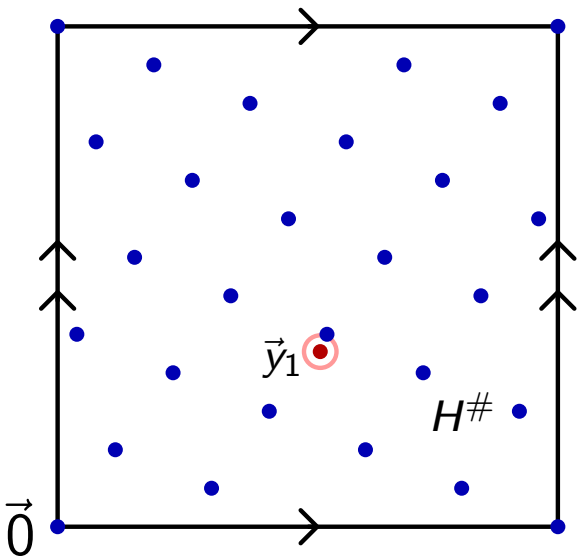
$$H^\# = \widehat{\mathbb{Z}^k/H} \leq (\mathbb{R}/\mathbb{Z})^k,$$

Explicitly, $H^\#$ consists of those $\vec{y}$ such that $\vec{x} \cdot \vec{y} \in \mathbb{Z}$ for all $\vec{x} \in H$.

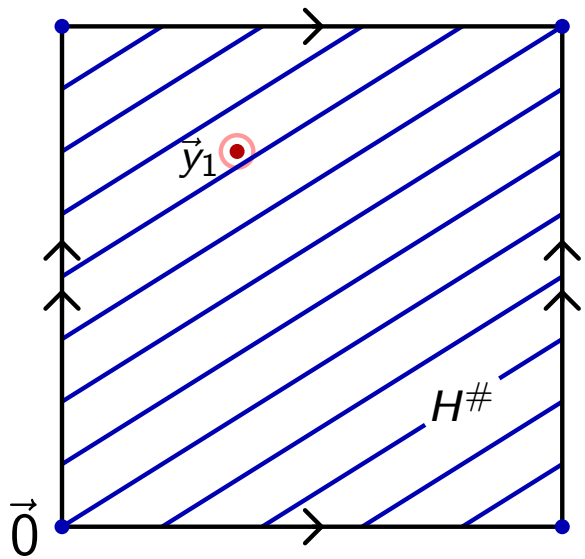
The sample $\vec{y}_1$ also has noise due to both Gaussian blur and discretization. This noise is exponentially small, but so is the feature scale of $H^\#$.

Examples of $H^{\#}$

Here are two examples of $H^{\#}$ and a noisy sample $\vec{y}_1 \in\!\!\!\!\sim\, H^{\#}$.



$(\mathbb{R}/\mathbb{Z})^2$



$(\mathbb{R}/\mathbb{Z})^2$

On the left, H has full rank and $H^{\#}$ is a finite group. On the right, when H has lower rank, $H^{\#}$ a striped pattern whose connected subgroup $H_1^{\#}$ is a complicated torus.

Solving for $H^\#$ from random samples

The easy case

Goal: Find $H^\# \leq (\mathbb{R}/\mathbb{Z})^k$ from noisy random samples $\vec{y}_1 \mathrel{\tilde{\in}} H^\#$.

Shor-Kitaev: If H has full rank and $H^\#$ is finite, then we can find rational approximations to the coordinates of $\vec{y}_1$ using the continued fraction algorithm. In this case, $O(\log |H^\#|)$ samples are enough to probably generate $H^\#$. This includes Shor's case $H = h\mathbb{Z} \leq \mathbb{Z}$, whence $H^\# = \frac{1}{h}\mathbb{Z}/h \leq \mathbb{R}/\mathbb{Z}$.

New: If H has rank $\ell < k$, then $\dim H^\# = k - \ell$. Any one coordinate of $\vec{y}_1$ is uniformly random in $\mathbb{R}/\mathbb{Z}$. Rational approximation of the coordinates does not work. Happily, LLL (Lenstra-Lenstra-Lovasz) works instead.

Solving for $H^\#$ from random samples

The hard case

A random $\vec{y}_0 \in H^\#$ densely generates the connected subgroup $H_1^\#$ (almost surely), so we look for multiples of $\vec{y}_1 \Subset H^\#$ near $\vec{0}$.

- Using a single sample $\vec{y}_1$, make a lattice $L \leq \mathbb{R}^{k+1}$ with basis

$$\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_k, (\widetilde{\vec{y}}_1, 1/T),$$

  where $S \gg T \gg R$, and $1/R$ is the feature scale of $H^\#$.
- Find a LLL basis of short vectors of L:

$$\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_{k+1} \in L \leq \mathbb{R}^{k+1}$$

  The first $k - \ell + 1$ vectors are $\sim$ tangent to $H^\# \oplus \mathbb{R}$ at $\vec{0}$.
- Put the first $k + \ell - 1$ LLL vectors in RREF form, then clean them up with rational approximation to find $T_{\vec{0}}(H^\# \oplus \mathbb{R})$ and $H_{\mathbb{R}} = H \otimes \mathbb{R}$. This reduces the problem to Shor-Kitaev.

Ideas behind the other hardness results

For NHSP in a free group F_k, $f : F_k \to F_k$ is a canonical word function in the quotient $Q = F_k/H$. Q is a presented groups whose relators are accepted witnesses for an NP predicate z. There is a class of groups Q where canonical words can be computed in P, even though the relators are "guess and check".

For NSHP in $\mathbb{Z}^k$ with unary encoding, an algorithm in BQP is only tasked to find the part of a lattice $L \leq \mathbb{Z}^k$ generated by short vectors. We can exploit this to know if there are any short vectors! If this sounds cheap, it is in the spirt of some of Regev's hardness reductions for lattice problems.