From optical measurement to efficient quantum algorithms for the hidden subgroup problem and beyond

Overall outline:
1. Hidden subgroup problem, optimal measurement for the dihedral HSP
2. General approach to optimal measurements for HSPs in semidirect product groups
3. Examples: dihedral, metacyclic, Heisenberg
4. Generalized abelian hidden shift problem

Part 1
Outline:
* The HSP
* Applications
  * Known algorithms
  * Standard approach
  * Fourier sampling
  * HSP as stable distinguishability
  * Dihedral group
  * Dihedral cost states: the subset sum problem
  * Pretty good measurement
  * Obtaining of PGM
  * Success probability of PGM
  * Invariance of PGM
  * Prolegomena of subset sum

The hidden subgroup problem

Problem: Fix a group $G$ (known) and a subgroup $H \triangleleft G$ (unknown).
Given a black box function $f: G \to \mathbb{C}$ that is

1. constant on left cosets of $H \in G$
2. distinct on different left cosets of $H \in G$

Find (a generating set for) $H$.

An efficient algorithm has run time $\text{poly}(\log |G|)$.

Example: Simon's problem $G = \mathbb{Z}_2^n$. Fix a hidden bitstring $s \in G$.
Given an oracle $f = \varphi^{s}$ a 1-to-1 function satisfying $f(x \oplus s) = f(x)$. So $H = \{0, s\}$.$\subseteq \mathbb{Z}_2^n$

Even this very simple case is hard for classical computers: can prove that finding $s$ requires exponentially many queries to $f$.

But there is an efficient quantum algorithm:

(Need a quantum black box for $f$: $|x\rangle \mapsto |x, f(x)\rangle$ (答案)
$|x\rangle |y\rangle \mapsto |x, y \oplus f(x)\rangle$ (量子)
Applications

- $G$ abelian
  This can be used to solve factoring, discrete log, Pell’s equation, etc.
  Can always be solved efficiently

- $G$ dihedral
  This can be used to solve the poly($d$) unique shortest vector problem [Regan 02]
  It can be reduced to a certain average case subset sum problem [Regan 02]
  There is an efficient quantum algorithm that produces data (essentially) which no-theoretically determines the answer [Ettinger - Hoyer 02]
  That is, a quantum algorithm with run time $2^{O(\sqrt{N})}$ [Kuperberg 03]

- $G$ symmetric
  This can be used to solve graph isomorphism
  No nontrivial algorithms

Standard approach

$$\frac{1}{\mid G \mid} \sum_{g \in G} |g\rangle \mapsto \frac{1}{\mid G \mid} \sum_{g \in G} |g\rangle \cdot f(g) \rangle \text{ discard 2nd register}$$

then we get a coset state,

$$|gH\rangle := \frac{1}{\mid H \mid} \sum_{h \in H} |gh\rangle \quad \text{with } g \in G \text{ uniformly random (unknown)}$$

equivalently, we have a hidden subgroup state,

$$\rho_H = \frac{1}{\mid G \mid} \sum_{g \in G} |gH\rangle \langle gH|$$

Note that this is not the only way to query $f$. But it is natural, and all known algorithms use this approach.

Fourier sampling

The symmetry of these states tells us a lot about how to deal with them.

$$\rho_H = \frac{1}{\mid G \mid} \sum_{g \in G} \sum_{h \in H} |gh\rangle \langle gh|$$

$$= \frac{1}{\mid G \mid} \sum_{g \in G} \sum_{h \in H} R(h^{-1})|g\rangle \langle g| R(h)$$

where $R$ is the right regular representation of

$$R(g_1)g_2 \rangle = |g_2 g_1^{-1}\rangle$$

$$= \frac{1}{\mid G \mid} \sum_{h \in H} R(h)$$

$$= \frac{1}{\mid G \mid} \sum_{h \in H} R(h)$$

Now the regular representation is block diagonalized by the Fourier transform

$$\hat{F} G = \sum_{g \in G} \sum_{g' \in G} \sum_{m=1}^{\mid G \mid} \frac{1}{\mid G \mid} \langle g' | \sigma(g)m \rangle \langle \sigma(g)m | g \rangle$$
Let \( \Phi_{\hat{H}} \) be the set of all states labeled by \( \sigma \in \hat{G} \). Can measure this WLOG: (make Fourier shifts.) In general, not enough info here.

- State is block diagonal, with blocks labeled by irreps \( \sigma \in \hat{G} \).
- Row state is maximally mixed. Discard it.
- Column state is basis dependent. How to measure?

### HSP or state distinguishability

We have a state distinguishability problem: given \( \Phi_{\hat{H}} \) for some unknown \( \hat{H} \), determine \( \hat{H} \).

More generally, we can make \( k = \text{poly}(\log |\hat{G}|) \) states \( \Phi_{\hat{H}}^{(k)} \) (equivalently, \( k \) copies) \( (g_1 \hat{H}, g_2 \hat{H}, \ldots, g_k \hat{H}) \) with each \( g_i \in \hat{G} \) independent, uniformly random.

#### Good news

In principle, this is enough information to poly \( \log |\hat{G}| \) asset states to determine \( \hat{H} \), for any \( \hat{G} \) [Effinger-Heuer-Knill].

#### Bad news

Some groups require entangled measurements on \( \Omega(\log |\hat{G}|) \) asset states to determine \( \hat{H} \). [Moore-Russell-Schulman, Hallgren-Rötteler-Su]

How can we identify measurements with nice properties that are likely to identify the states?

Idea: Try to understand the optimal measurement.

### Dihedral group

- Generic element: \( (a, b) \in \mathbb{Z}_N \times \mathbb{Z}_2 \), \( G = \mathbb{Z}_N \rtimes \mathbb{Z}_2 \)
- \((a,b)(c,d) = (a+(-1)^b c, b+d)\)

**Fact [Effinger-Heuer]:** To solve the HSP in the dihedral group, it is sufficient to be able to identify a hidden reflection, \( \hat{H} = \{ (0,0), (a,1) \} \). (Prove later)

note: \( (a,1)^2 = (a-a, 1+1) = (0,0) \)
Dihedral coset states and the subset sum problem

For any subgroup \( \{ (0,0), (a,1) \} \), the elements \( \{ (a', 0) : a' \in \mathbb{Z}_n \} \) form a complete set of coset reps.

Coset state: \( \{ (a', 0) H_a \} = \frac{1}{\sqrt{2}} (|a', 0 \rangle + |a + a', 1 \rangle) \), \( a' \in \mathbb{Z}_n \) uniformly random.

FT in 1st register over \( \mathbb{Z}_n \): \( \frac{1}{\sqrt{n}} \sum_{x \in \mathbb{Z}_n} \omega^{ax} |x \rangle \langle 0 | (10 \rangle + \omega^{ax} |11 \rangle) (|0 \rangle + \omega^{-ax} |1 \rangle) \)

now the mixed state is \( \frac{1}{\sqrt{n}} \sum_{x \in \mathbb{Z}_n} \omega^{ax} |x \rangle \langle x | (10 \rangle + \omega^{ax} |11 \rangle) (|0 \rangle + \omega^{-ax} |1 \rangle) \)

which is block diagonal! (here \( x \) is basically the recipe name + row label)

so WLOG we can measure \( x \), discarding a global phase, we have

\( \frac{1}{\sqrt{n}} (10 \rangle + \omega^{ax} |11 \rangle) \) (note \( a' \) disappears, cf. abelian HSP)

Goal: using \( k \) qubits like this, find \( a' \)

\( k \) copies:

\( \frac{1}{\sqrt{n}} (10 \rangle + \omega^{ax} |11 \rangle) \otimes \cdots \otimes \frac{1}{\sqrt{n}} (10 \rangle + \omega^{ax} |11 \rangle) \)

\( \frac{1}{\sqrt{2^n}} \sum_{b \in \mathbb{Z}_n^k} \omega^{ab} |b \rangle \)

Now we would like to let \( w = b' x \) and do the sum over \( w \) instead of \( b \).

Problem: given \( x \in \mathbb{Z}_n^k \) and \( w \in \mathbb{Z}_n \), what \( b' = \omega \) have \( b' x = w \)?

This is the subset sum problem. (a classic NP-hard problem, but we have random \( x \) s, not worst case. more on this later)

Solutions:

\( S_w := \frac{1}{\sqrt{2^n}} \sum_{b \in \mathbb{Z}_n^k} \omega^{ab} |b \rangle \) \( \eta_w := |S_w \rangle \)

and also define \( |S_w \rangle := \frac{1}{\sqrt{\eta_w}} \sum_{b \in \mathbb{Z}_n^k} \omega^{ab} |b \rangle \) (or 0 if \( \eta_w = 0 \))

Then the \( k \)-copy state is

\( \frac{1}{\sqrt{2^n}} \sum_{w \in \mathbb{Z}_n} \omega^{aw} \sqrt{\eta_w} |S_w \rangle \)

Here we see that if we could replace \( |S_w \rangle \) by \( |w \rangle \), and if the \( \eta_w \)'s were close to uniform, then a FT would reveal \( a \). This is exactly what the optimal measurement does!

Pretty good measurement.

We will find the optimal measurement by looking at a particular explicit POVM and showing it is optimal.

States \( p_j \), POVM in prior probabilities \( p_j \).

Define \( \Sigma = \sum p_j p_j^* \). Then let \( E_j := \frac{1}{\sqrt{p_j}} p_j p_j^* \). Clearly, \( \Sigma E_j = 1 \).

This is the maximum and at the same time (for HSWA decoding). Sometimes it is optimal.
Theorem. [Heilmann, Yuen - Kennedy - Lax] For an ensemble of states \( \rho_j \) with prob. \( p_j \), and a POVM \( \mathcal{E}_j \), define \( R = \sum p_j \rho_j \mathcal{E}_j \). Then the POVM maximizes the probability of successfully identifying the state \( \sum p_j \text{tr}(\rho_j \mathcal{E}_j) \) iff

1. \( R = R^\dagger \)
2. \( R \geq \rho_j \rho_j^\dagger \forall j \)

Note: the problem of finding the (or any) optimal POVM is a semidefinite program!

Optimality of the PGM for the DHSP (uniform ensemble):

States: \( \rho_a = \frac{1}{2N} \sum_{w \in \mathbb{Z}_n} \omega^{a(w, v)} \sqrt{\eta_w^0 \eta_w^0} |S_w^0 \rangle \langle S_w^0| \quad \forall x \in \mathbb{Z}_n^N, a \in \mathbb{C}_n \)

\[
\sum = \frac{1}{2N} \sum_{w \in \mathbb{Z}_n} \sum_{x \in \mathbb{Z}_n} \omega^{a(w, v)} \sqrt{\eta_w^0 \eta_w^0} |S_w^0 \rangle \langle S_w^0| \\
= \frac{1}{2N} \sum_{w \in \mathbb{Z}_n} \eta_w^0 |S_w^0 \rangle \langle S_w^0| 
\]

so the PGM is: \( E_a = \frac{1}{\sqrt{N}} \rho_a \frac{1}{\sqrt{N}} = \frac{1}{N} \sum_{w \in \mathbb{Z}_n} \omega^{a(w, v)} |S_w^0 \rangle \langle S_w^0| \)

(Note: The \( \rho_a \)'s are non-orthogonal pure states: \( \rho_a = |\psi_a \rangle \langle \psi_a| \) with \( |\psi_a \rangle = \frac{1}{\sqrt{N}} \sum \omega^{a(w, v)} \eta_v^0 |S_w^0 \rangle \).

But \( \langle E_a | E_b \rangle = \frac{1}{N} \sum \omega^{a(w, v) + b(w, v)} |S_w^0 \rangle \langle S_w^0| = \frac{1}{N} \sum \omega^{a+b(w, v)} = \delta_{a, b} \) in general.

So the PGM is an orthogonal measurement.

Now \( R = \frac{1}{N} \sum_{a \in \mathbb{Z}_n} \rho_a E_a = \frac{1}{N^2} \sum_{a \in \mathbb{Z}_n} \sum_{b \in \mathbb{Z}_n} \omega^{a+b(w, v)} \sqrt{\eta_a^0 \eta_b^0} |S_w^0 \rangle \langle S_w^0| \\
= \frac{1}{N^2} \sum_{w \in \mathbb{Z}_n} \sqrt{\eta_w^0 \eta_w^0} |S_w^0 \rangle \langle S_w^0| = R^\dagger \)

and check \( R \geq \frac{1}{N} \rho_a \forall a \in \mathbb{Z}_n \): clearly \( R \geq 0 \), and

\[
\langle \rho_a | R | \rho_a \rangle = \frac{1}{N^2} \sum_{w \in \mathbb{Z}_n} \sum_{b \in \mathbb{Z}_n} \omega^{a-b(w, v)} \sqrt{\eta_a^0 \eta_b^0} \\
\geq \frac{1}{N} \sum_{w \in \mathbb{Z}_n} \sqrt{\eta_w^0 \eta_w^0} = \frac{1}{N} 
\]

now using (by Cauchy - Schwarz): \( \sum a_j \cdot \Sigma b_j \geq (\Sigma a_j b_j)^2 \), we have

\[
\frac{1}{N^2} \sum_{w \in \mathbb{Z}_n} \sum_{v \in \mathbb{Z}_n} \omega^w \sqrt{\eta_w^0 \eta_v^0} \geq \left( \frac{1}{N^2} \sum_{w \in \mathbb{Z}_n} \sqrt{\eta_w^0 \eta_w^0} \right)^2 = 1 
\]

which proves \( R \geq \frac{1}{N} \rho_a \).
Success probability of the dihedral PGM:

\[ \Pr(\text{success}) = \frac{1}{N} \mathbb{E}_\varphi \left( \prod_{i=1}^{N} \left( \sum_{x \in \mathbb{Z}_N^d} \eta_x \right)^2 \right) \]

This is for fixed \( x \), averaging over (uniformly random) \( x \in \mathbb{Z}_N^d \), we have

\[ \Pr(\text{success}) = \frac{1}{2^N N!} \sum_{x \in \mathbb{Z}_N^d} \left( \sum_{x \in \mathbb{Z}_N^d} \frac{1}{N} \right)^2 \]

This will be big when the \( \eta_x \)'s are spread out.

Consider subset sum problem: let \( k = \sqrt{\log N} \), \( \nu = \text{"density"} \)

\( \nu = 1 \): few numbers, most subsets hard, a distinct sum
\( \nu > 1 \): many numbers, most sums are achieved a comparable \# of times.
\( \eta_x \)'s uniform \( \Rightarrow \) \( \Pr(\text{success}) \) close to 1.

Later we will see how to prove this.

Implementing the dihedral PGM

We want to project onto a basis \( |E_o\rangle = \frac{1}{N} \sum_{w} |w, x\rangle \)

i.e., we want to do \( |E_o\rangle \mapsto |0\rangle \) followed by a standard measurement.

This can be done as follows:

\[ |E_o\rangle \overset{\text{FT}}{\mapsto} \frac{1}{\sqrt{N}} \sum_{w} \omega^w |w\rangle \]

The key step here is the inverse of the quantum sampling from solutions to subset sum:

\( |w\rangle \mapsto |S\rangle \) (an isometry): replace \( |w\rangle \) by uniform superposition of solutions to subset sum \( \langle x, w \rangle \)

Hardness of subset sum

As previously mentioned, subset sum is NP-hard. But random instances at fixed \( \nu \) are easier.

Low density: for \( k < \sqrt{\log N} \), \( \exists \) an efficient algorithm [Lagerkvist, Odlyzko, 85]. But this is too good for BHP: it has \( \nu = 0(1) \).

High density: for \( k > 2\sqrt{\log N} \), \( \exists \) a poly \((k)\) algorithm [Feldman, Prezdelnik, 05] this is exactly where Kuperberg's algorithm works; closely related, but even this is not good enough for optimal measurements; can only find 1 solution, rather than quantum sampling.
Outline:
- Semidirect product groups; known algorithms
- Reduction to cyclic subgroups
- Cacti states and the matrix sum problem
- Pretty good measurement (which is optimal)
- PGM success probability; general lower and upper bounds
- Implementation by quantum sampling; approximate q-sampling is good enough

Semidirect product groups

\[ G = A \rtimes B \quad \text{(where \( A \leq G \), \( B \) acts on \( A \) (perm.)}) \]

set of elements: \( A \times B \), write \((a, b) \in A \times B \), \( a \in A \), \( b \in B \)

\[ \Phi : B \rightarrow A + A \quad \text{a homomorphism} \]

\[ (a, b)(a', b') = (a + \Phi(b)a', b + b') \]

\[ (a, b)^{-1} = (\Phi(-b)(-a), -b) \]

Specialize to \( B = \mathbb{Z}_p \), \( p \) prime. Then \( \Phi(1) \) defines \( \Phi : \mathbb{Z}_p \rightarrow A \). Here \( \Phi : A \rightarrow A \) is an automorphism of \( A \).

Denote \( \Phi^b = \Phi(b) \). Here \( \Phi : A \rightarrow A \) is an isomorphism of \( A \).

Cyclic subgroups \( \langle (a, 1) \rangle \):

\[ (a, 1)^2 = (a, 1)(a, 1) = (a + \Phi(a), 2) \]

\[ (a, 1)^3 = (a, 1)(a + \Phi(a), 2) = (a + \Phi(a) + \Phi^2(a), 3) \]

\[ \vdots \]

\[ (a, 1)^b = (\Phi^b(a), b \mod p) \quad b \in \mathbb{N} \]

where \( \Phi^b(a) = \sum_{i=0}^{b} \Phi^i(a) \) \( (\Phi^b : A \rightarrow A) \)

Known algorithms

\[ \mathbb{Z}_2 \rtimes \mathbb{Z}_2 = (\mathbb{Z}_2 \times \mathbb{Z}_2^*) \times \mathbb{Z}_2 \quad \text{[Rötteler, Beth 95]} \]

\[ \mathbb{Z}_2^p \rtimes \mathbb{Z}_2 \quad \text{(p-ary)} \]

\[ \mathbb{Z}_p \rtimes \mathbb{Z}_p \quad p \equiv 3 \pmod{4}, \text{prime} \quad \text{[Moor et al. 04]} \]

\[ \mathbb{Z}_p \rtimes \mathbb{Z}_p \quad p \equiv 3 \pmod{4}, \text{prime} \quad \text{[Ivleva, Le Gall 04]} \]

Reduction to cyclic subgroups

Lemma: To find an efficient algorithm for the HSP over \( A \rtimes \mathbb{Z}_p \), it suffices to find an efficient algorithm for the HSP over \( A_2 \rtimes \mathbb{Z}_p \) for any \( A \) with the promise that \( A_2 \rtimes \mathbb{Z}_p \) is cyclic for some \( \Phi(2), 1 \leq p \).

Proof: Like Effiee - Hoque for dihedral, with one additional possible complication.

Let \( G_r = A \rtimes \mathbb{Z}_2 \)

\[ H_r = H \cap G_r = A \times \mathbb{Z}_2 \]

Since \( f \) restricted to \( G_r \) induces \( H_r \), and \( G_r \) is abelian, we can efficiently factor \( f^b \).

Now: \( H_r \leq G ? \) (If so, we'll factor it out.)

Let \( g = (a, b) \in G \)

\[ h = (h_0, 0) \in H \]

Then \( g h g^{-1} = (a, b)(h_0, 0)(a, b)^{-1} = (a + \Phi^b(h, 0), b)(a, b)^{-1} = (\Phi^b(h), 0) \]

\[ \Rightarrow g h g^{-1} \text{ or } \Phi^b \]
We claim that this shows $H, G \neq G \Rightarrow H = H$. 

If $H \neq H$, then there is some $(a_1, b) \in A$, and by the previous calculation, we have $(a_1, b) = (a, b) \in A$. Let $G_2 = A / A_1$, so $G_2 = A / A$. 

So we check whether $H \neq G_2$. (This can be done efficiently, since $G_2$ is solvable.)

- If $H \neq G_2$, we're done.
- If not, $H = G_2$, and we're done.

Let $G_2 = G / H_2 \cong A_2 / \mathbb{Z}_p$. Then $A_2 = A / A_1$. 

If $G_2 = H_2$, then $H_2$ is trivial.

Otherwise, $G_2 = \langle H_2 \rangle$: we must have some $(a_1, b) \in H_2$, and for any additional $(a', b')$, 

$$(a_1, b)(a', b')^{-1} = (a', b')^{-1} = (a' - b', 0) \in A_1,$$ 

so $(a_1, b)$ is necessary.

Therefore, 

$$H_2 = \langle (a_1, 0) \rangle / \langle (a_1, 0) \rangle = \langle (a_1, 0) \rangle \text{ for some } a \in A_2 \text{ (clearly order } p).$$

If we check identity, then $H_2$ is non-trivial, then this also handles the case where $H_2$ is trivial (just check). \[ \square \]

Coset states

We're considering $G = A \times \mathbb{Z}_p$.

$H = \langle (a_1, 0) \rangle$ of order $p$.

We can label left cosets by $(b, 0)$ where $b \in A$: there are $p$ of them, and they are distinct.

Coset state: $| (b, 0) \rangle H = \frac{1}{p} \sum_{b \in \mathbb{Z}_p} \langle b | (b, 0) \rangle \langle \Phi \rangle (a, b) \rangle = \frac{1}{p} \sum_{b \in \mathbb{Z}_p} (b, 0) \rangle \langle \Phi \rangle (a, b) \rangle$

now FT the 1st register over $A$: \[ \frac{1}{p} \sum_{b \in \mathbb{Z}_p} \sum_{x \in A} \chi_x (b + \Phi (a)) \langle x, b \rangle. \]

Just as we argued for dihedral case, the state is block diagonal in $x$, so we can measure it phase $X_x (a)$ disappears $= \exp (2 \pi i x y)$.

$$= \frac{1}{p} \sum_{b \in \mathbb{Z}_p} \chi_x (\Phi (a)) \langle b \rangle \langle b \rangle$$

Next one can show $\forall \Phi: \langle a \rangle \rightarrow A$ such that $\chi_x (\Phi (a)) = \chi_x (b) \langle a \rangle$.

For $A = \mathbb{Z}_p$, $\Phi (a) = x a$ for $a \in \mathbb{Z}_p$, $\Phi (a) = \exp (2 \pi i x a)$. For $A = \mathbb{Z}_p$, $\Phi (a) = x a$ for $a \in \mathbb{Z}_p$, $\Phi (a) = \exp (2 \pi i x a)$. 

so we have $\frac{1}{p} \sum_{b \in \mathbb{Z}_p} \chi_x (\Phi (a)) \langle b \rangle \langle b \rangle$ and for $k$ copies, $\frac{1}{p^k} \sum_{b \in \mathbb{Z}_p^k} \chi_x (\Phi (a)) \langle b \rangle \langle b \rangle$.

Matrix sum problem

$$S^x = \{ b \in \mathbb{Z}_p : \Phi (a) = x \}$$

Next the state is $\frac{1}{p} \sum_{a \in A} \chi_x (a) \langle \Phi \rangle (a) \langle b \rangle$. 

Then the state is $\frac{1}{p} \sum_{a \in A} \chi_x (a) \langle \Phi \rangle (a) \langle b \rangle$. 

As before, $\mathbf{1}^k \langle S \rangle$. 

$S^x = \{ b \in \mathbb{Z}_p : \Phi (a) = x \}$
The PGM calculations go through just as before. PGM is optimal, and is the projection into the states $|EF_a\rangle = \frac{1}{\sqrt{|A|}} \sum_{x \in A} \chi_w(x) |x\rangle$.

Success probability

Again, by the same calculations as for the standard group,

$$Pr(\text{success}) = tr\left( \rho_k \rho_n^k \right) = \frac{1}{\rho^k |A|^k} \left( \sum_{w \in \mathcal{E}} \sqrt{q(w)^k} \right)^2.$$ 

and averaging over the uniformly random $x \in A^k$,

$$Pr(\text{success}) = \frac{1}{\rho^k |A|^k} \sum_{x \in A^k} \left( \sum_{w \in \mathcal{E}} \sqrt{q(w)} \right)^2 = \frac{1}{|A|^k} \sum_{w \in \mathcal{E}} \left( \sum_{x \in A^k} \sqrt{q(w)} \right)^2.$$ 

Lemma 1. $Pr(\text{success}) \leq \frac{\rho^k}{|A|^k}$.

(iii) if $Pr(\eta^k \geq \alpha) \geq \beta$, then $Pr(\text{success}) \geq \beta \frac{\rho^k}{|A|^k}$.

Note: $E_{x \in A^k, w \in \mathcal{E}} \eta^k = \frac{1}{|A|^k} \sum_{x \in A^k} \sum_{w \in \mathcal{E}} \eta^k w^k = \frac{1}{|A|^k} \sum_{x \in A^k} \rho^k = \frac{\rho^k}{|A|^k}$, so $k = \log \rho |A|^k$ is the expected critical value.

Proof: (i) $Pr(\text{success}) \leq \frac{1}{\rho^k |A|^k} \sum_{x \in A^k} \left( \sum_{w \in \mathcal{E}} q(w) \right)^2 = \frac{1}{\rho^k |A|^k} \sum_{x \in A^k} \rho^k = \frac{\rho^k}{|A|^k}$.

(ii) using $\sum_{j=1}^N \frac{a_j^2}{j} \geq \frac{1}{N} \left( \sum_{j=1}^N a_j \right)^2$,

$$Pr(\text{success}) \geq \frac{1}{\rho^k |A|^k} \left( \sum_{x \in A^k} \sum_{w \in \mathcal{E}} \sqrt{q(w)} \right)^2$$

$$= \frac{|A|^k}{\rho^k |A|^k} \left( \sum_{x \in A^k} \sum_{w \in \mathcal{E}} \sqrt{q(w)} \right)^2$$

$$\geq \frac{1}{\rho^k} \beta \frac{\rho^k}{|A|^k}.$$

Implementation

Just as before, doing $|S^k\rangle \mapsto |w\rangle$ will implement the PGM. (Clear from form of $|EF_a\rangle$)

In fact, it is good enough to do it approximately:

$|w\rangle \mapsto \frac{1}{p} \sum_{x \in A^k} \chi_w(x) |x\rangle$

where $\langle S^k | S^k \rangle = 0$ (can be done if we can recognize bad instances).

Thus we have

$$\frac{1}{p} \sum_{w \in \mathcal{E}} \chi_w (x) |w\rangle$$

and if a constant fraction of instances were good, $\langle S^k | S^k \rangle \geq N \frac{1}{p} \sum_{w \in \mathcal{E}} \chi_w (x) |w\rangle^2$.

Fidelity with ideal state (averaged over $x$):

$$\frac{1}{pN} \sum_{w \in \mathcal{E}} \chi_w (x) \geq \frac{1}{p} \sum_{w \in \mathcal{E}} \chi_w (x) |w\rangle^2$$

since $\chi_w (x) \geq 1$ for $|x\rangle \in \mathcal{E}$, so fidelity $\geq \text{const.} \times \frac{N}{p}$.
Dihedral group

Consider \( G = A \times \mathbb{Z}_2 \) with \( \phi(a) = -a \). In particular, \( A = \mathbb{Z}_N \) is abelian.

Here \( \overline{\phi}(b)(x) = \sum_{i=0}^{b-1} \phi^i(x) = \begin{cases} 0 & b = 0 \\ b \cdot x & b \neq 0 \end{cases} \)

so \( S^x_w = \{ b \in \mathbb{Z}_2^k : \overline{\phi}(b)(w) = w \} = \{ b \in \mathbb{Z}_2^k : b \cdot x = w \} \).

The subset sum problem can be solved exactly by calculating the integer powers of \( \overline{\phi}(w) \) and using Chinese remainder theorem.

Metacyclic groups

\( G = \mathbb{Z}_N \rtimes \mathbb{Z}_p \) with \( \phi(a) = \mu a \) for some \( \mu \in \mathbb{Z}_N^\times \) with \( \mu \equiv 1 \mod N \)

then \( \overline{\phi}(w)(x) = \sum_{i=0}^{\mu^{-1}} \mu^i x \).

For simplicity, suppose \( \mu^{-1} \in \mathbb{Z}_N^\times \) (this is not necessary); then \( \frac{\mu^{b-1}}{\mu-1} x = w \).

For \( k = 1 \), we have \( S^x_w = \{ b \in \mathbb{Z}_p^k : \frac{\mu^{b-1}}{\mu-1} x = w \} \).

\((\mu^{b-1})x = (\mu-1)w \times \frac{\mu^{b-1}}{\mu-1} \) provided \( x \in \mathbb{Z}_p^k \).

This is a discrete log problem.

Now for uniformly random \( x \in \mathbb{Z}_N \), \( \Pr(x \in \mathbb{Z}_N^\times) = \frac{\phi(N)}{N} = \Omega(1/\log \log N) \)

and for uniformly random \( w \in \mathbb{Z}_N, \) \( \Pr(\phi(x) = \mu x) = \frac{1}{N} \)

so \( \Pr(\mu^b x = w) = p \frac{\phi(N)}{N} \), which is \( \frac{1}{p \cdot \text{poly}(\log N)} \) provided \( N/p = \text{poly}(\log N) \).

(Note this is exactly the condition from Moore et al.)

For \( k = 2 \), consider \( x \in \mathbb{Z}_p^2 \), \( \mu^{\frac{b_1-1}{\mu-1}} x_1 + \frac{b_2-1}{\mu-1} x_2 = w \).

\( \mu^{b_1} x_1 + \mu^{b_2} x_2 = x_1 x_2 + (\mu-1)w \) how to solve?
Stripped down version of the algorithm:

For hidden subgroup \( \langle (a, 1) \rangle \), the coset states are
\[
| (a, 0) \rangle \psi \rangle_{H_0} = \frac{1}{\sqrt{p}} \sum_{b \in \mathbb{Z}_p} | b \rangle \sum_{x \in \mathbb{Z}_p} \omega^{x(a+b)} | x \rangle | b \rangle
\]

Fourier transform 1st register over \( \mathbb{Z}_N \) (\( \omega = e^{2\pi i / N} \)):
\[
\frac{1}{\sqrt{N_\mathbb{Z}}} \sum_{x \in \mathbb{Z}_N} \sum_{b \in \mathbb{Z}_p} \omega^{x(x+b)} | x \rangle | b \rangle
\]

Measure \( x \) and post-select on \( x \in \mathbb{Z}_N^k \) (probability \( \Omega(1/\log \log N) \))

Compute \( \Gamma^{(b)}(1) \):
\[
\frac{1}{\sqrt{p}} \sum_{b \in \mathbb{Z}_p} \omega^{\Gamma^{(b)}(a)} | b \rangle | x \rangle
\]

Note \( \Gamma^{(b)} \) can be computed efficiently since \( \Gamma^{(b)} = (1 + \mu^b) \Gamma^{(a)} \)

Compute \( \mu^b \) from \( \Gamma^{(a)}(1) = 1 + \mu^a \)

-use Shor to erase \( b \) (discrete log)- then erase \( x \)

\[
\frac{1}{\sqrt{p}} \sum_{b \in \mathbb{Z}_p} \omega^{\Gamma^{(b)}(a)} | x \rangle | b \rangle
\]

new a Fourier transform gives a with probability \( \frac{1}{N} \).

Hersenberg group and friends

Hersenberg group:

(i) subgroups of \( \mathrm{GL}_3 (\mathbb{F}_p) \):
\[
\left\{ \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ c & b & 1 \end{pmatrix} : a, b, c \in \mathbb{F}_p \right\}
\]

(ii) group of \( p \times p \) unitary matrices:
\[
\langle X, Z \rangle = \{ X^a Z^b : a, b \in \mathbb{Z}_p \}
\]
\[
X = \sum_{x \in \mathbb{Z}_p} | x \rangle \langle x | \quad Z = \sum_{x \in \mathbb{Z}_p} x^a | x \rangle \langle x | \quad \omega = e^{2\pi i / p}
\]

(iii) semidirect product \( \mathbb{Z}_p^2 \rtimes \mathbb{Z}_p \):
\[
(a, b) (a', b') = (a + a', b + b', c + c')
\]

Thus \( \Gamma^{(a)}(1) = \sum_{i=0}^{p-1} (\begin{pmatrix} i & 1 \\ 0 & 1 \end{pmatrix} \Gamma^{(a)}(1) \begin{pmatrix} i & 1 \\ 0 & 1 \end{pmatrix}^{-1}) = (\begin{pmatrix} i & 1 \\ 0 & 1 \end{pmatrix} \Gamma^{(a)}(1) \begin{pmatrix} i & 1 \\ 0 & 1 \end{pmatrix}^{-1}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\]

\[
\mathrm{MSP} = \sum_{j=1}^{p} (\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Gamma^{(j)}(1) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\]

with \( k=1 \) probability of having a solution is \( O(1/p) \) \( (p \text{ values of } b, \ p^2 \text{ values of } (v)) \)

but with \( k=2 \) probability is \( \approx \frac{1}{2} \). That there are 2 solutions:
\[
\begin{align*}
\omega &= b_x x_1 + b_2 x_2 + \frac{(b_3)}{2} y_2 \\
v &= b_y y_1 + b_2 y_2 + \frac{(b_3)}{2} y_2
\end{align*}
\]

\[
\Rightarrow \begin{align*}
&b_x y_1 + b_2 x_1 - x_1 y_2 = \sqrt{-1} y_1 (y_1 + y_2) \\
&b_y y_2 + b_2 y_1 - x_2 y_2 = \sqrt{-1} y_2 (y_1 + y_2)
\end{align*}
\]
More generally: recall \( \mathbb{F} \in \text{Aut} \mathbb{A} \) with \( \mathbb{F}^n \neq \mathbb{1} \). Consider \( \mathbb{A} = \mathbb{Z}_p^n \).

Now \( \mathbb{A} \in \text{GL}_n \left( \mathbb{F}_p \right) \) defined by \( \mathbb{U} \in \text{GL}_n \left( \mathbb{F}_p \right) \) put a Jordan canonical form:

\[ J = \begin{pmatrix}
1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 \\
\vdots & \vdots & \ddots & \vdots \\
1 & 1 & \cdots & 1
\end{pmatrix}
\]

and:

\[ \bar{a} = \bar{b} \begin{pmatrix}
a_1 \\
a_2 \\
\vdots \\
a_n
\end{pmatrix} = \begin{pmatrix}
b_1 \\
b_2 \\
\vdots \\
b_n
\end{pmatrix}
\]

1. \( \mathbb{F} \in \text{Aut} \mathbb{A} \) with \( \mathbb{F}^n \neq \mathbb{1} \). Consider \( \mathbb{A} = \mathbb{Z}_p^n \).

2. Now \( \mathbb{A} \in \text{GL}_n \left( \mathbb{F}_p \right) \) defined by \( \mathbb{U} \in \text{GL}_n \left( \mathbb{F}_p \right) \) put a Jordan canonical form:

\[ J = \begin{pmatrix}
1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 \\
\vdots & \vdots & \ddots & \vdots \\
1 & 1 & \cdots & 1
\end{pmatrix}
\]

and:

\[ \bar{a} = \bar{b} \begin{pmatrix}
a_1 \\
a_2 \\
\vdots \\
a_n
\end{pmatrix} = \begin{pmatrix}
b_1 \\
b_2 \\
\vdots \\
b_n
\end{pmatrix}
\]

3. \( \mathbb{F} \in \text{Aut} \mathbb{A} \) with \( \mathbb{F}^n \neq \mathbb{1} \). Consider \( \mathbb{A} = \mathbb{Z}_p^n \).

4. Now \( \mathbb{A} \in \text{GL}_n \left( \mathbb{F}_p \right) \) defined by \( \mathbb{U} \in \text{GL}_n \left( \mathbb{F}_p \right) \) put a Jordan canonical form:

\[ J = \begin{pmatrix}
1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 \\
\vdots & \vdots & \ddots & \vdots \\
1 & 1 & \cdots & 1
\end{pmatrix}
\]

and:

\[ \bar{a} = \bar{b} \begin{pmatrix}
a_1 \\
a_2 \\
\vdots \\
a_n
\end{pmatrix} = \begin{pmatrix}
b_1 \\
b_2 \\
\vdots \\
b_n
\end{pmatrix}
\]

5. \( \mathbb{F} \in \text{Aut} \mathbb{A} \) with \( \mathbb{F}^n \neq \mathbb{1} \). Consider \( \mathbb{A} = \mathbb{Z}_p^n \).

6. Now \( \mathbb{A} \in \text{GL}_n \left( \mathbb{F}_p \right) \) defined by \( \mathbb{U} \in \text{GL}_n \left( \mathbb{F}_p \right) \) put a Jordan canonical form:

\[ J = \begin{pmatrix}
1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 \\
\vdots & \vdots & \ddots & \vdots \\
1 & 1 & \cdots & 1
\end{pmatrix}
\]

and:

\[ \bar{a} = \bar{b} \begin{pmatrix}
a_1 \\
a_2 \\
\vdots \\
a_n
\end{pmatrix} = \begin{pmatrix}
b_1 \\
b_2 \\
\vdots \\
b_n
\end{pmatrix}
\]

The success probability, need to show variance of \( \mu \) of solutions is small.

\[ E_{x \in K} \mu_x = \frac{1}{p^{n-1}} \sum_{x \in K} \mu_x = \frac{1}{p^{n-1}} \sum_{x \in K} \mu_x = \frac{1}{p^{n-1}} \cdot k = \frac{1}{p^{k-1}}
\]

\[ E_{x \in K} (\mu_x)^2 = \frac{1}{p^{n-1}} \sum_{x \in K} (\mu_x)^2 = \frac{1}{p^{n-1}} \sum_{x \in K} (\mu_x)^2 = \frac{1}{p^{n-1}} \cdot \frac{1}{k \cdot c} = \frac{1}{p^{k-1}} \cdot \frac{1}{c} = \frac{1}{p^{k-1}} \cdot \frac{1}{c}
\]

\[ E_{x \in K} \mu_x \mu_x = \frac{1}{p^{n-1}} \sum_{x \in K} \mu_x \mu_x = \frac{1}{p^{n-1}} \sum_{x \in K} \mu_x \mu_x = \frac{1}{p^{n-1}} \cdot \frac{1}{k \cdot c} = \frac{1}{p^{k-1}} \cdot \frac{1}{c} = \frac{1}{p^{k-1}} \cdot \frac{1}{c}
\]

\[ E_{x \in K} (\mu_x)^2 = \frac{1}{p^{n-1}} \sum_{x \in K} (\mu_x)^2 = \frac{1}{p^{n-1}} \sum_{x \in K} (\mu_x)^2 = \frac{1}{p^{n-1}} \cdot \frac{1}{k \cdot c} = \frac{1}{p^{k-1}} \cdot \frac{1}{c} = \frac{1}{p^{k-1}} \cdot \frac{1}{c}
\]

\[ E_{x \in K} \mu_x \mu_x = \frac{1}{p^{n-1}} \sum_{x \in K} \mu_x \mu_x = \frac{1}{p^{n-1}} \sum_{x \in K} \mu_x \mu_x = \frac{1}{p^{n-1}} \cdot \frac{1}{k \cdot c} = \frac{1}{p^{k-1}} \cdot \frac{1}{c} = \frac{1}{p^{k-1}} \cdot \frac{1}{c}
\]

\[ E_{x \in K} (\mu_x)^2 = \frac{1}{p^{n-1}} \sum_{x \in K} (\mu_x)^2 = \frac{1}{p^{n-1}} \sum_{x \in K} (\mu_x)^2 = \frac{1}{p^{n-1}} \cdot \frac{1}{k \cdot c} = \frac{1}{p^{k-1}} \cdot \frac{1}{c} = \frac{1}{p^{k-1}} \cdot \frac{1}{c}
\]

\[ E_{x \in K} \mu_x \mu_x = \frac{1}{p^{n-1}} \sum_{x \in K} \mu_x \mu_x = \frac{1}{p^{n-1}} \sum_{x \in K} \mu_x \mu_x = \frac{1}{p^{n-1}} \cdot \frac{1}{k \cdot c} = \frac{1}{p^{k-1}} \cdot \frac{1}{c} = \frac{1}{p^{k-1}} \cdot \frac{1}{c}
\]
Stripped down algorithm
\[ \frac{1}{P} \sum_{b_1, b_2 \in \mathbb{Z}_2^P} \sigma \left( \omega (a + b) \right) \]
and similarly:
\[ \frac{1}{P} \sum_{b_1, b_2 \in \mathbb{Z}_2^P} \sigma \left( \omega (a + b) \right) \]
now unitarily erase \( \frac{1}{\sqrt{2}} (|b_1, b_{21} \rangle + |b_{12}, b_{22} \rangle) \) (2 solutions \( n_r = 2 \))
\[ \frac{1}{P} \sum_{b_1, b_2 \in \mathbb{Z}_2^P} \sigma \left( \omega (a + b) \right) \]