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

Andrew Childs
Caltech Institute for Quantum Information

Dave Bacon
University of Washington

Wim van Dam
UC Santa Barbara

quant-ph/0501044, quant-ph/0504083, quant-ph/0507190

What are quantum computers good for?

What are quantum computers good for?

Practical question: Building a quantum computer will take a lot of resources. If we build one, can we use it to do anything useful other than factoring numbers?

What are quantum computers good for?

Practical question: Building a quantum computer will take a lot of resources. If we build one, can we use it to do anything useful other than factoring numbers?

Fundamental question: What is the computational power of quantum mechanics?

What are quantum computers good for?

Practical question: Building a quantum computer will take a lot of resources. If we build one, can we use it to do anything useful other than factoring numbers?

Fundamental question: What is the computational power of quantum mechanics?

Problems

- Simulating quantum dynamics
- Factoring
- Discrete log
- Pell's equation
- Abelian HSP
- Some nonabelian HSPs
- Estimating gauss sums
- Legendre symbol/polynomial reconstruction
- Graph traversal
- Approximating Jones polynomial
- Counting solutions of finite field equations

What are quantum computers good for?

Practical question: Building a quantum computer will take a lot of resources. If we build one, can we use it to do anything useful other than factoring numbers?

Fundamental question: What is the computational power of quantum mechanics?

Problems

- Simulating quantum dynamics
- Factoring
- Discrete log
- Pell's equation
- Abelian HSP
- Some nonabelian HSPs
- Estimating gauss sums
- Legendre symbol/polynomial reconstruction
- Graph traversal
- Approximating Jones polynomial
- Counting solutions of finite field equations

Techniques

- Fourier sampling
- Quantum walk
- Adiabatic optimization
- Trace estimation
- Optimal measurement

Outline

- The hidden subgroup problem (HSP)
- Optimal measurements for distinguishing quantum states
- Dihedral HSP
- Heisenberg HSP
- Unlabeled hidden shift problem
- Summary and open problems

The hidden subgroup problem

Problem: Fix a group G (known) and a subgroup H (unknown).
Given a black box that computes $f\colon G \to S$ that is

- Constant on any particular left coset of H in G
- Distinct on different left cosets of H in G

(We say that f hides H.)

Goal: Find (a generating set for) H.
An efficient algorithm runs in time $\mathrm{poly}(\log|G|)$.

The hidden subgroup problem

Problem: Fix a group G (known) and a subgroup H (unknown). Given a black box that computes $f\colon G \to S$ that is

- Constant on any particular left coset of H in G
- Distinct on different left cosets of H in G

(We say that f hides H.)

Goal: Find (a generating set for) H.
An efficient algorithm runs in time $\mathrm{poly}(\log|G|)$.

Even for very simple groups (e.g., $G = \mathbb{Z}_2^n$), a classical algorithm provably requires exponentially many queries of f to find H.

Most interesting cases of the HSP

- Abelian groups
  Applications to factoring, discrete log, Pell's equation, etc.
  Can be solved efficiently

- Dihedral group
  Applications to lattice problems [Regev 2002]
  Subexponential-time algorithm [Kuperberg 2003]

- Symmetric group
  Application to graph isomorphism
  No nontrivial algorithms

Efficient algorithms for the HSP

- Abelian groups [Shor 1994; Boneh, Lipton 1995; Kitaev 1995]
- Normal subgroups [Hallgren, Russell, Ta-Shma 2000]
- "Almost abelian" groups [Grigni, Schulman, Vazirani^2 2001]
- "Near-Hamiltonian" groups [Gavinsky 2004]
- $(\mathbb{Z}_2^n \times \mathbb{Z}_2^n) \rtimes \mathbb{Z}_2$ [Püschel, Rötteler, Beth 1998]
- $\mathbb{Z}_{p^k}^n \rtimes \mathbb{Z}_2$, smoothly solvable groups [Friedl, Ivanyos, Magniez, Santha, Sen 2002]
- p-hedral: $\mathbb{Z}_N \rtimes \mathbb{Z}_p$, $p{=}\phi(N)/\mathrm{poly}(\log N)$ prime, N prime [Moore, Rockmore, Russell, Schulman 2004]
- $\mathbb{Z}_{p^k} \rtimes \mathbb{Z}_p$ [Inui, Le Gall 2004]

Efficient algorithms for the HSP

- Abelian groups [Shor 1994; Boneh, Lipton 1995; Kitaev 1995]
- Normal subgroups [Hallgren, Russell, Ta-Shma 2000]
- "Almost abelian" groups [Grigni, Schulman, Vazirani[2] 2001]
- "Near-Hamiltonian" groups [Gavinsky 2004]
- ➡ $(\mathbb{Z}_2^n \times \mathbb{Z}_2^n) \rtimes \mathbb{Z}_2$ [Püschel, Rötteler, Beth 1998]
- $\mathbb{Z}_{p^k}^n \rtimes \mathbb{Z}_2$, smoothly solvable groups [Friedl, Ivanyos, Magniez, Santha, Sen 2002]
- ➡ p-hedral: $\mathbb{Z}_N \rtimes \mathbb{Z}_p$, $p{=}\phi(N)/\mathrm{poly}(\log N)$ prime, N prime [Moore, Rockmore, Russell, Schulman 2004], N arbitrary NEW!
- ➡ $\mathbb{Z}_{p^k} \rtimes \mathbb{Z}_p$ [Inui, Le Gall 2004]
- ➡ $\mathbb{Z}_p^r \rtimes \mathbb{Z}_p$, r constant (including Heisenberg, $r{=}2$) NEW!

Standard approach to the HSP

Compute uniform superposition of function values:

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle \mapsto \frac{1}{\sqrt{|G|}}\sum_{g\in G}|g, f(g)\rangle$$

Standard approach to the HSP

Compute uniform superposition of function values:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, f(g)\rangle$$

Discard second register to get a *coset state*,

$$|gH\rangle := \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$$

with $g \in G$ (unknown) chosen uniformly at random.

Standard approach to the HSP

Compute uniform superposition of function values:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, f(g)\rangle$$

Discard second register to get a *coset state*,

$$|gH\rangle := \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$$

with $g \in G$ (unknown) chosen uniformly at random.

Equivalently, we have the *hidden subgroup state*

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

Standard approach to the HSP

Compute uniform superposition of function values:

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle \mapsto \frac{1}{\sqrt{|G|}}\sum_{g\in G}|g, f(g)\rangle$$

Discard second register to get a *coset state*,

$$|gH\rangle := \frac{1}{\sqrt{|H|}}\sum_{h\in H}|gh\rangle$$

with $g\in G$ (unknown) chosen uniformly at random.

Equivalently, we have the *hidden subgroup state*

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

Now we can (without loss of generality) perform a Fourier transform over G, and measure which irreducible representation the state is in (weak Fourier sampling).

Distinguishing quantum states

Problem: Given a quantum state ρ chosen from an ensemble of states ρ_i with a priori probabilities p_i, determine i.

This can only be done perfectly if the states are orthogonal. In general, we would just like a high probability of success: maximize $\Sigma_i \; p_i \, \mathrm{tr}(\rho_i E_i)$.

HSP as state estimation

State distinguishability problem: given the state ρ_H, determine H.

HSP as state estimation

State distinguishability problem: given the state ρ_H, determine H.

In general, we can use many copies of the coset states: make $\rho_H^{\otimes k}$ (equivalently, $|g_1 H, g_2 H, \ldots, g_k H\rangle$) for $k = \mathrm{poly}(\log |G|)$.

HSP as state estimation

State distinguishability problem: given the state ρ_H, determine H.

In general, we can use many copies of the coset states: make $\rho_H^{\otimes k}$ (equivalently, $|g_1 H, g_2 H, \ldots, g_k H\rangle$) for $k = \mathrm{poly}(\log|G|)$.

Good news: In principle $k = \mathrm{poly}(\log|G|)$ copies contain enough information to identify H. [Ettinger, Høyer, Knill 1999]

HSP as state estimation

State distinguishability problem: given the state ρ_H, determine H.

In general, we can use many copies of the coset states: make $\rho_H^{\otimes k}$ (equivalently, $|g_1 H, g_2 H, \ldots, g_k H\rangle$) for $k = \mathrm{poly}(\log|G|)$.

Good news: In principle $k = \mathrm{poly}(\log|G|)$ copies contain enough information to identify H. [Ettinger, Høyer, Knill 1999]

Bad news: For some groups, it is necessary to make joint measurements on $\Omega(\log|G|)$ copies. [Moore, Russell, Schulman 2005-6; Hallgren, Rötteler, Sen 2006]

HSP by optimal measurement

Question: What measurement maximizes the probability of successfully identifying the hidden subgroup?

HSP by optimal measurement

Question: What measurement maximizes the probability of successfully identifying the hidden subgroup?

[Ip 2003]: Shor's algorithm implements the optimal measurement for the abelian HSP.

HSP by optimal measurement

Question: What measurement maximizes the probability of successfully identifying the hidden subgroup?

[Ip 2003]: Shor's algorithm implements the optimal measurement for the abelian HSP.

Can we use this as a principle to find quantum algorithms?

Optimal measurement

Theorem. [Holevo 1973, Yuen-Kennedy-Lax 1975]
Given an ensemble of quantum states ρ_i with a priori probabilities p_i, the measurement with POVM elements E_i maximizes the probability of successfully identifying the state if and only if $R = R^\dagger$ and $R \geq p_i \rho_i$ for all i, where

$$R := \sum_i p_i \rho_i E_i \, .$$

Optimal measurement

Theorem. [Holevo 1973, Yuen-Kennedy-Lax 1975]
Given an ensemble of quantum states ρ_i with a priori probabilities p_i, the measurement with POVM elements E_i maximizes the probability of successfully identifying the state if and only if $R = R^\dagger$ and $R \geq p_i \rho_i$ for all i, where

$$R := \sum_i p_i \rho_i E_i \, .$$

In general, it is nontrivial to find a POVM that satisfies these conditions (although it is a semidefinite program!).

But for all the cases discussed in this talk, the optimal measurement is a particularly simple POVM, the *pretty good measurement*.

Pretty good measurement

Given states ρ_i with a priori probabilities p_i, define POVM elements

$$E_i := p_i \frac{1}{\sqrt{\Sigma}} \rho_i \frac{1}{\sqrt{\Sigma}} \qquad \text{where} \qquad \Sigma := \sum_i p_i \rho_i$$

(invert Σ over its support)

Pretty good measurement

Given states ρ_i with a priori probabilities p_i, define POVM elements

$$E_i := p_i \frac{1}{\sqrt{\Sigma}} \rho_i \frac{1}{\sqrt{\Sigma}} \qquad \text{where} \qquad \Sigma := \sum_i p_i \rho_i$$

(invert Σ over its support)

This is a POVM:

$$\sum_i E_i = \frac{1}{\sqrt{\Sigma}} \Big(\sum_i p_i \rho_i \Big) \frac{1}{\sqrt{\Sigma}} = 1$$

Pretty good measurement

Given states ρ_i with a priori probabilities p_i, define POVM elements

$$E_i := p_i \frac{1}{\sqrt{\Sigma}} \rho_i \frac{1}{\sqrt{\Sigma}} \qquad \text{where} \qquad \Sigma := \sum_i p_i \rho_i$$

(invert Σ over its support)

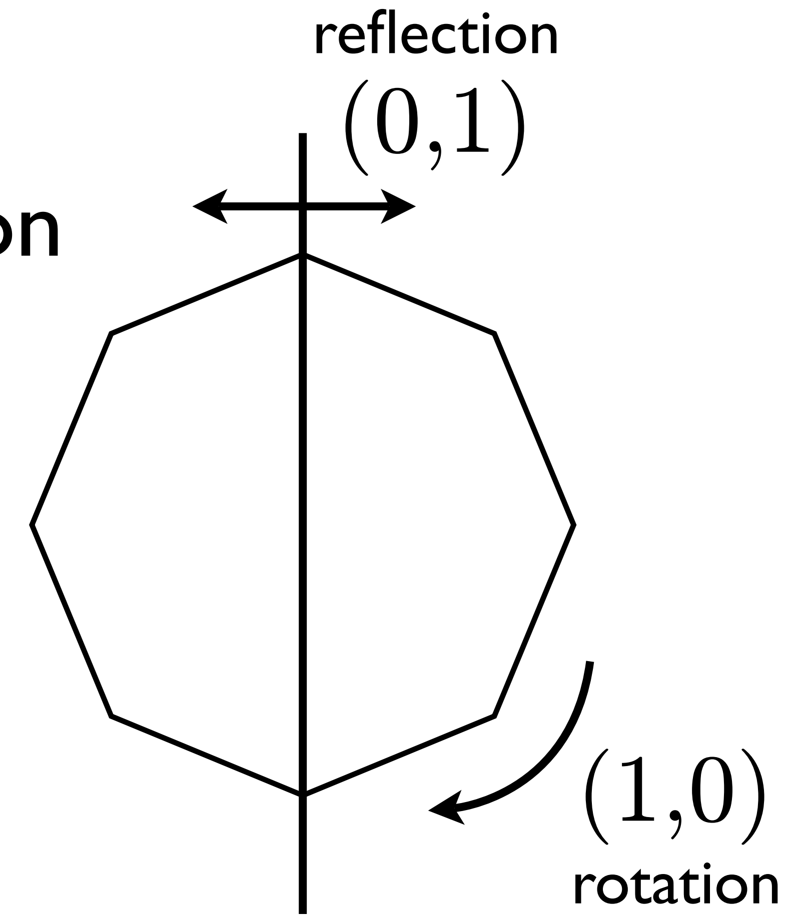
This is a POVM:

$$\sum_i E_i = \frac{1}{\sqrt{\Sigma}} \Big(\sum_i p_i \rho_i \Big) \frac{1}{\sqrt{\Sigma}} = 1$$

The PGM often does a pretty good job of distinguishing the ρ_i.
In fact, sometimes it is optimal! (Check Holevo/YKL conditions)

Dihedral group $(\mathbb{Z}_N \rtimes \mathbb{Z}_2)$

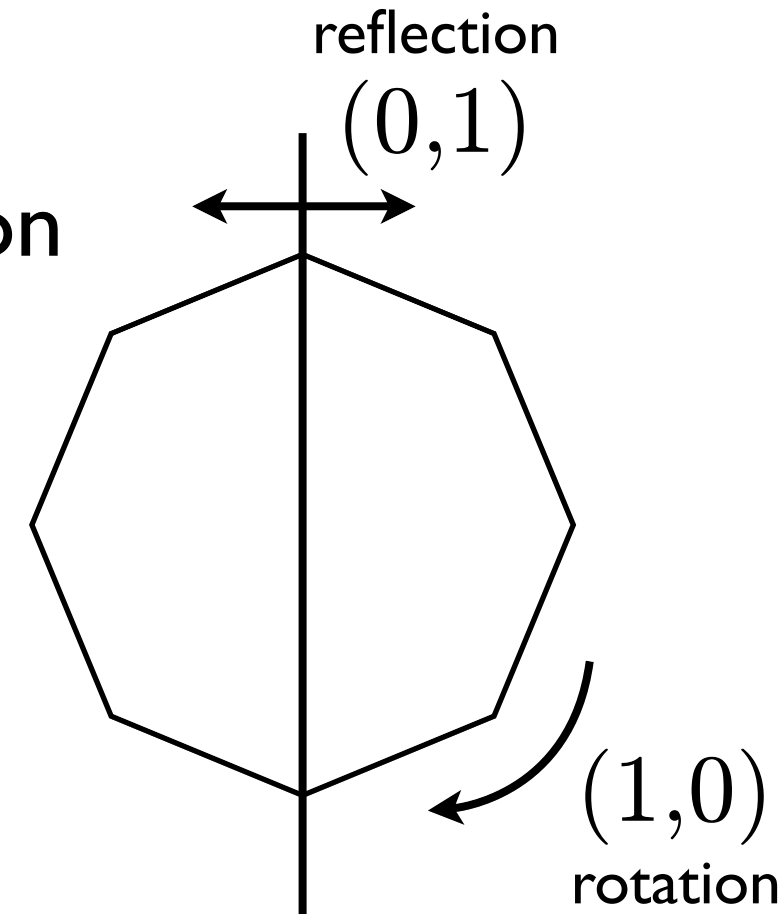
Symmetry group of an N-sided regular polygon



Dihedral group $(\mathbb{Z}_N \rtimes \mathbb{Z}_2)$

Symmetry group of an N-sided regular polygon

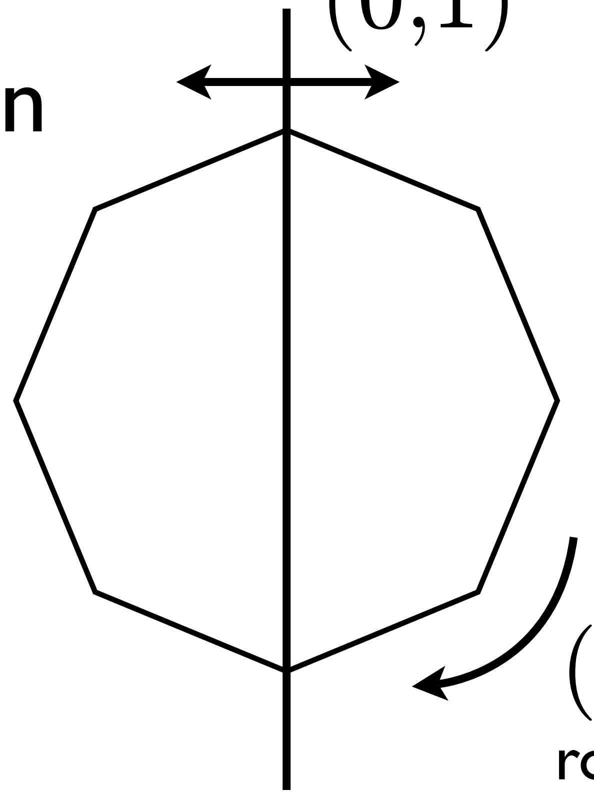
$$(a,b)(c,d) = (a + (-1)^b c, b + d)$$



Dihedral group $(\mathbb{Z}_N \rtimes \mathbb{Z}_2)$

Symmetry group of an N-sided regular polygon

$$(a,b)(c,d) = (a + (-1)^b c, b + d)$$

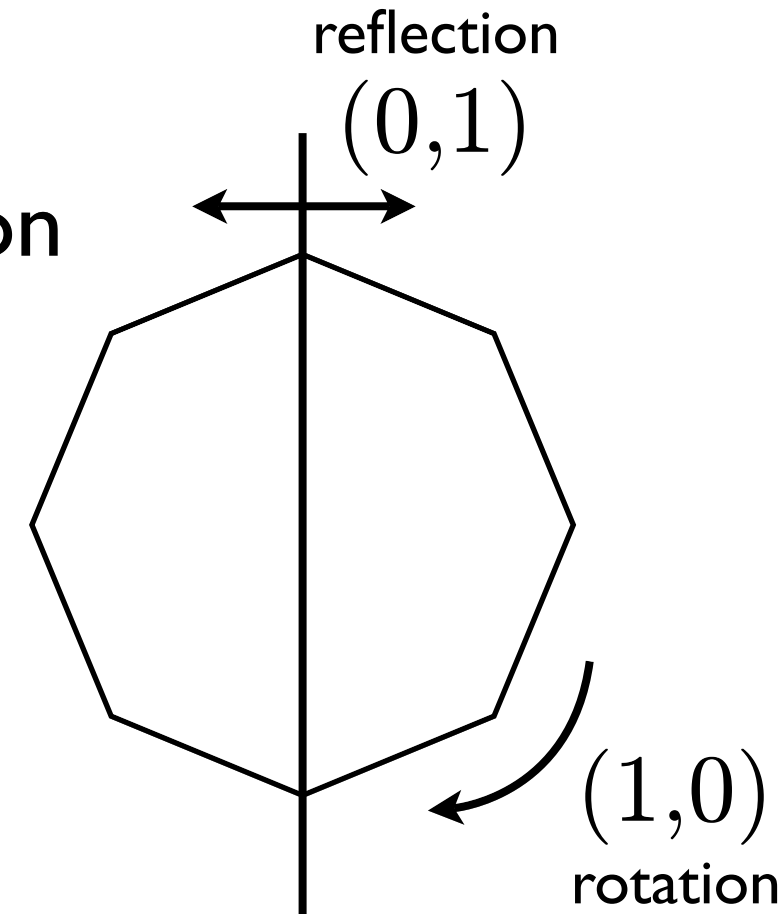


[Ettinger, Høyer 1998] To solve the HSP, it is sufficient to distinguish the order two subgroups $\{(0,0),(a,1)\}$ (hidden reflections)

Dihedral group $(\mathbb{Z}_N \rtimes \mathbb{Z}_2)$

Symmetry group of an N-sided regular polygon

$$(a,b)(c,d) = (a + (-1)^b c, b + d)$$



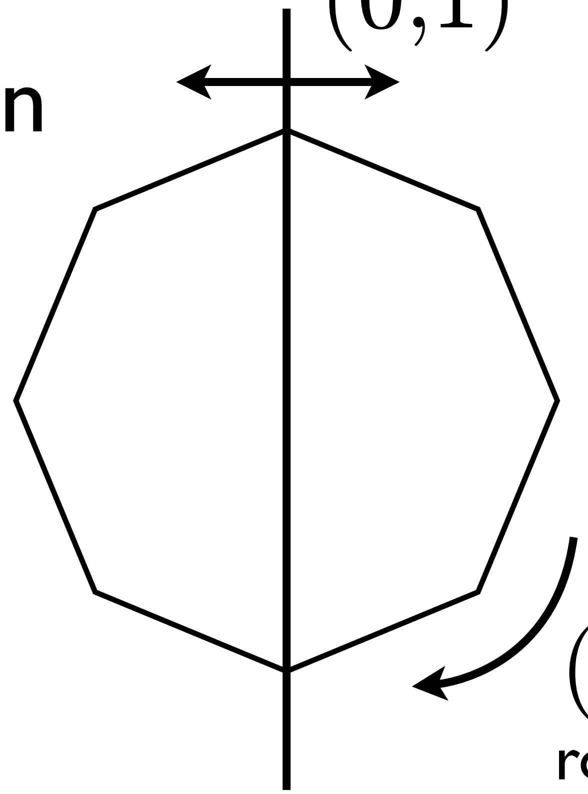
[Ettinger, Høyer 1998] To solve the HSP, it is sufficient to distinguish the order two subgroups $\{(0,0),(a,1)\}$ (hidden reflections)

Coset states: $|(a',0)H\rangle = \frac{1}{\sqrt{2}}(|a',0\rangle + |a+a',1\rangle)$

Dihedral group $(\mathbb{Z}_N \rtimes \mathbb{Z}_2)$

Symmetry group of an N-sided regular polygon

$$(a,b)(c,d) = (a + (-1)^b c, b + d)$$

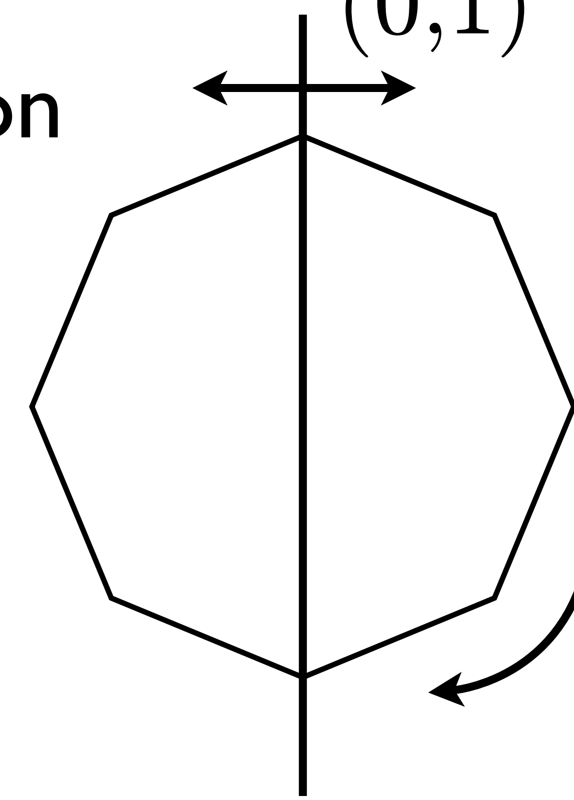


[Ettinger, Høyer 1998] To solve the HSP, it is sufficient to distinguish the order two subgroups $\{(0,0),(a,1)\}$ (hidden reflections)

Coset states: $|(a',0)H\rangle = \frac{1}{\sqrt{2}}(|a',0\rangle + |a+a',1\rangle)$

Fourier transform: $$\frac{1}{\sqrt{2N}} \sum_{x \in \mathbb{Z}_N} |x\rangle(|0\rangle + \omega^{xa}|1\rangle)$$

Dihedral group $(\mathbb{Z}_N \rtimes \mathbb{Z}_2)$



Symmetry group of an N-sided regular polygon

$$(a,b)(c,d) = (a + (-1)^b c, b + d)$$

[Ettinger, Høyer 1998] To solve the HSP, it is sufficient to distinguish the order two subgroups $\{(0,0),(a,1)\}$ (hidden reflections)

Coset states: $|(a',0)H\rangle = \frac{1}{\sqrt{2}}(|a',0\rangle + |a+a',1\rangle)$

Fourier transform: $\frac{1}{\sqrt{2N}} \sum_{x \in \mathbb{Z}_N} |x\rangle(|0\rangle + \omega^{xa}|1\rangle)$

By symmetry, we can measure x wlog (Fourier sampling: measure which irreducible representation)

Multiple dihedral coset states

$$\frac{|0\rangle + \omega^{x_1 a}|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + \omega^{x_k a}|1\rangle}{\sqrt{2}}$$

Multiple dihedral coset states

$$\frac{|0\rangle + \omega^{x_1 a}|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + \omega^{x_k a}|1\rangle}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2^k}} \sum_{\vec{b} \in \mathbb{Z}_2^k} \omega^{(\vec{b}\cdot\vec{x})a} |b\rangle$$

Multiple dihedral coset states

$$\frac{|0\rangle + \omega^{x_1 a}|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + \omega^{x_k a}|1\rangle}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2^k}} \sum_{\vec{b} \in \mathbb{Z}_2^k} \omega^{(\vec{b}\cdot\vec{x})a} |b\rangle$$

$$= \frac{1}{\sqrt{2^k}} \sum_{w \in \mathbb{Z}_N} \omega^{wa} \sqrt{\eta_w^{\vec{x}}} |S_w^{\vec{x}}\rangle$$

solutions of *subset sum problem*:

$$S_w^{\vec{x}} := \{\vec{b} \in \mathbb{Z}_2^k : \vec{b}\cdot\vec{x} = w\}$$

$$\eta_w^{\vec{x}} := |S_w^{\vec{x}}|$$

$$|S_w^{\vec{x}}\rangle := \frac{1}{\sqrt{\eta_w^{\vec{x}}}} \sum_{\vec{b} \in S_w^{\vec{x}}} |\vec{b}\rangle$$

Subset sum and DHSP

The PGM (which is optimal) can be implemented unitarily by doing the inverse of the *quantum sampling* transformation:

$$|w\rangle \mapsto |S_w^{\vec{x}}\rangle$$

Subset sum and DHSP

The PGM (which is optimal) can be implemented unitarily by doing the inverse of the *quantum sampling* transformation:

$$|w\rangle \mapsto |S_w^{\vec{x}}\rangle$$

Applying this to the coset state gives

$$\frac{1}{\sqrt{2^k}} \sum_{w \in \mathbb{Z}_N} \omega^{wa} \sqrt{\eta_w^{\vec{x}}} |S_w^{\vec{x}}\rangle \mapsto \frac{1}{\sqrt{2^k}} \sum_{w \in \mathbb{Z}_N} \omega^{wa} \sqrt{\eta_w^{\vec{x}}} |w\rangle$$

Subset sum and DHSP

The PGM (which is optimal) can be implemented unitarily by doing the inverse of the *quantum sampling* transformation:

$$|w\rangle \mapsto |S_w^{\vec{x}}\rangle$$

Applying this to the coset state gives

$$\frac{1}{\sqrt{2^k}} \sum_{w \in \mathbb{Z}_N} \omega^{wa} \sqrt{\eta_w^{\vec{x}}} |S_w^{\vec{x}}\rangle \mapsto \frac{1}{\sqrt{2^k}} \sum_{w \in \mathbb{Z}_N} \omega^{wa} \sqrt{\eta_w^{\vec{x}}} |w\rangle$$

This is close to the FT of $|a\rangle$ if the $\eta_w^{\vec{x}}$ are nearly uniform in w

Subset sum and DHSP

The PGM (which is optimal) can be implemented unitarily by doing the inverse of the *quantum sampling* transformation:

$$|w\rangle \mapsto |S_w^{\vec{x}}\rangle$$

Applying this to the coset state gives

$$\frac{1}{\sqrt{2^k}} \sum_{w \in \mathbb{Z}_N} \omega^{wa} \sqrt{\eta_w^{\vec{x}}} |S_w^{\vec{x}}\rangle \mapsto \frac{1}{\sqrt{2^k}} \sum_{w \in \mathbb{Z}_N} \omega^{wa} \sqrt{\eta_w^{\vec{x}}} |w\rangle$$

This is close to the FT of $|a\rangle$ if the $\eta_w^{\vec{x}}$ are nearly uniform in w

Questions:

- How big must k be so that the solutions of the subset sum problem are nearly uniformly distributed?
- For such values of k, can we quantum sample from the subset sum solutions?

Subset sum problem

Problem: Given k integers $x_1,\ldots,x_k$ from $\mathbb{Z}_N$ and a target w from $\mathbb{Z}_N$, find a subset of the k integers that sum to the target (i.e., find $b_1,\ldots,b_k$ from $\mathbb{Z}_2$ so that $b \cdot x = w$).

Subset sum problem

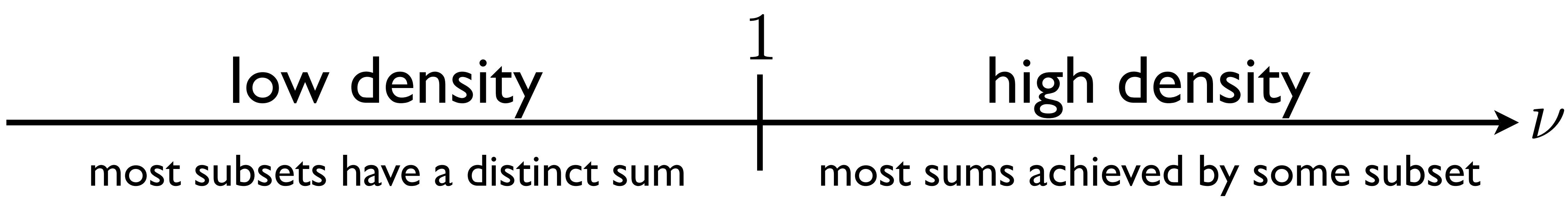
Problem: Given k integers $x_1,\ldots,x_k$ from $\mathbb{Z}_N$ and a target w from $\mathbb{Z}_N$, find a subset of the k integers that sum to the target (i.e., find $b_1,\ldots,b_k$ from $\mathbb{Z}_2$ so that $b{\cdot}x{=}w$).

In general, this problem is NP-hard. But the average-case problem at a fixed density $\nu{:=}k/\log_2 N$ may be much easier.

Subset sum problem

Problem: Given k integers $x_1,\ldots,x_k$ from $\mathbb{Z}_N$ and a target w from $\mathbb{Z}_N$, find a subset of the k integers that sum to the target (i.e., find $b_1,\ldots,b_k$ from $\mathbb{Z}_2$ so that $b \cdot x = w$).

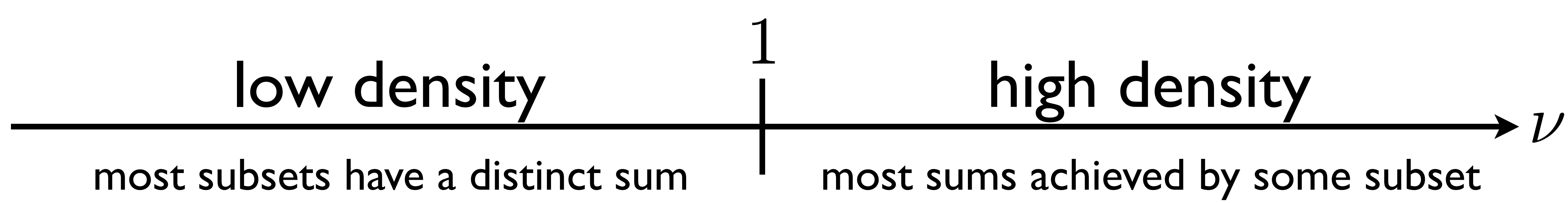
In general, this problem is NP-hard. But the average-case problem at a fixed density $\nu := k/\log_2 N$ may be much easier.



Subset sum problem

Problem: Given k integers $x_1,\ldots,x_k$ from $\mathbb{Z}_N$ and a target w from $\mathbb{Z}_N$, find a subset of the k integers that sum to the target (i.e., find $b_1,\ldots,b_k$ from $\mathbb{Z}_2$ so that $b \cdot x = w$).

In general, this problem is NP-hard. But the average-case problem at a fixed density $\nu := k/\log_2 N$ may be much easier.



$k < c\sqrt{\log N}$
efficient classical algorithm
[Lagarias, Odlyzko 1985]

hard?

$k > 2^{c\sqrt{\log N}}$
$\mathrm{poly}(k)$ classical algorithm
[Flaxman, Przydatek 2004]

Subset sum problem

Problem: Given k integers $x_1,\ldots,x_k$ from $\mathbb{Z}_N$ and a target w from $\mathbb{Z}_N$, find a subset of the k integers that sum to the target (i.e., find $b_1,\ldots,b_k$ from $\mathbb{Z}_2$ so that $b \cdot x = w$).

In general, this problem is NP-hard. But the average-case problem at a fixed density $\nu := k/\log_2 N$ may be much easier.

1

low density | high density → ν

most subsets have a distinct sum

most sums achieved by some subset

subset sum $\Rightarrow$ DHSP [Regev 2002]

PGM succeeds

$k < c\sqrt{\log N}$		$k > 2^{c\sqrt{\log N}}$
efficient classical algorithm [Lagarias, Odlyzko 1985]	hard?	$\mathrm{poly}(k)$ classical algorithm [Flaxman, Przydatek 2004]

Subset sum problem

Problem: Given k integers $x_1,\ldots,x_k$ from $\mathbb{Z}_N$ and a target w from $\mathbb{Z}_N$, find a subset of the k integers that sum to the target (i.e., find $b_1,\ldots,b_k$ from $\mathbb{Z}_2$ so that $b\cdot x = w$).

In general, this problem is NP-hard. But the average-case problem at a fixed density $\nu := k/\log_2 N$ may be much easier.

1

low density | high density → ν

most subsets have a distinct sum

most sums achieved by some subset

subset sum $\Rightarrow$ DHSP [Regev 2002]

PGM succeeds

$k < c\sqrt{\log N}$

efficient classical algorithm

[Lagarias, Odlyzko 1985]

hard?

$k > 2^{c\sqrt{\log N}}$

$\mathrm{poly}(k)$ classical algorithm

[Flaxman, Przydatek 2004]

$\mathrm{poly}(k)$ quantum DHSP algorithm

[Kuperberg 2003]

General approach

- Cast problem as a state distinguishability problem (e.g., coset states for HSP)
- Express the states in terms of an average-case algebraic problem (e.g., subset sum for dihedral HSP)
- Perform the pretty good measurement on k copies of the states:
  - Choose k large enough that the measurement succeeds with reasonably high probability (this happens if the average-case problem typically has many solutions)
  - Implement the measurement by solving the problem on average (quantum sampling from the set of solutions)

The Heisenberg group

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

Semidirect product $\mathbb{Z}_p^2 \rtimes_\varphi \mathbb{Z}_p$

$$\varphi : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_p^2) \quad \text{with} \quad \varphi(c)(a,b) = (a + bc, b)$$

$$(a,b,c)(a',b',c') = (a + a' + b'c, b + b', c + c')$$

Group of $p \times p$ unitary matrices

$\langle X, Z \rangle = \{\omega^a X^b Z^c : a, b, c \in \mathbb{Z}_p\}$ where

$$X := \sum_{x \in \mathbb{Z}_p} |x+1\rangle\langle x| , \quad Z := \sum_{x \in \mathbb{Z}_p} \omega^x |x\rangle\langle x| , \quad \omega := e^{2\pi \mathrm{i}/p}$$

Heisenberg subgroups

Fact: To solve the HSP in the Heisenberg group, it is sufficient to distinguish the order p subgroups $\langle(a,b,1)\rangle = \{(a,b,1)^j : j \in \mathbb{Z}_p\}$

$$(a,b,1)^2 = (a,b,1)(a,b,1) = (2a+b, 2b, 2)$$
$$(a,b,1)^3 = (a,b,1)(2a+b, 2b, 2) = (3a+3b, 3b, 3)$$
$$(a,b,1)^4 = (a,b,1)(3a+2b, 3b, 3) = (4a+6b, 4b, 4)$$
$$\vdots$$
$$(a,b,1)^j = (ja + \tbinom{j}{2} b, jb, j)$$

Average-case problem: Two quadratic equations in k variables.

Heisenberg HSP algorithm

Two copies of the coset states are sufficient to distinguish these subgroups. The optimal measurement can be implemented by solving a pair of quadratic equations in two variables.

Heisenberg HSP algorithm

Two copies of the coset states are sufficient to distinguish these subgroups. The optimal measurement can be implemented by solving a pair of quadratic equations in two variables.

More generally, for $\mathbb{Z}_p^r \rtimes \mathbb{Z}_p$, the optimal measurement on r copies solves the HSP, and can be implemented by solving rth order equations (use Buchberger's algorithm to compute a Gröbner basis; efficient for r constant).

Heisenberg HSP algorithm

Two copies of the coset states are sufficient to distinguish these subgroups. The optimal measurement can be implemented by solving a pair of quadratic equations in two variables.

More generally, for $\mathbb{Z}_p^r \rtimes \mathbb{Z}_p$, the optimal measurement on r copies solves the HSP, and can be implemented by solving rth order equations (use Buchberger's algorithm to compute a Gröbner basis; efficient for r constant).

This algorithm implements an entangled measurement across r coset states. This is encouraging, since entangled measurements are information-theoretically necessary for some groups!*

*But not for the Heisenberg group [Radhakrishnan, Rötteler, Sen 2005], although no *efficient* single-register algorithm is known for this case.

Generalized abelian hidden shift problem

Problem: Given a function $f : \{0, 1, \ldots, M-1\} \times \mathbb{Z}_N \to S$ satisfying $f(b, x) = f(b+1, x+s)$ for $b = 0, 1, \ldots, M-2$, find the value of the *hidden shift* $s \in \mathbb{Z}_N$.

Generalized abelian hidden shift problem

Problem: Given a function $f : \{0, 1, \ldots, M-1\} \times \mathbb{Z}_N \to S$ satisfying $f(b, x) = f(b+1, x+s)$ for $b = 0, 1, \ldots, M-2$, find the value of the *hidden shift* $s \in \mathbb{Z}_N$.

$M{=}2$: equivalent to dihedral HSP
$M{=}N$: an instance of abelian HSP (efficiently solvable)

Generalized abelian hidden shift problem

Problem: Given a function $f : \{0, 1, \ldots, M-1\} \times \mathbb{Z}_N \to S$ satisfying $f(b, x) = f(b+1, x+s)$ for $b = 0, 1, \ldots, M-2$, find the value of the *hidden shift* $s \in \mathbb{Z}_N$.

$M=2$: equivalent to dihedral HSP
$M=N$: an instance of abelian HSP (efficiently solvable)

Average-case problem: Given $x \in \mathbb{Z}_N^k$ and $w \in \mathbb{Z}_N$ chosen uniformly at random, find $b \in \{0, 1, \ldots, M-1\}^k$ such that $b \cdot x = w \bmod N$.

Generalized abelian hidden shift problem

Problem: Given a function $f : \{0, 1, \ldots, M-1\} \times \mathbb{Z}_N \to S$ satisfying $f(b, x) = f(b+1, x+s)$ for $b = 0, 1, \ldots, M-2$, find the value of the *hidden shift* $s \in \mathbb{Z}_N$.

$M{=}2$: equivalent to dihedral HSP
$M{=}N$: an instance of abelian HSP (efficiently solvable)

Average-case problem: Given $x \in \mathbb{Z}_N^k$ and $w \in \mathbb{Z}_N$ chosen uniformly at random, find $b \in \{0, 1, \ldots, M-1\}^k$ such that $b \cdot x = w \bmod N$.

This is an instance of integer programming in k dimensions. Lenstra's algorithm (based on LLL lattice basis reduction) solves this efficiently for k constant. $k{=}\log N / \log M \Rightarrow$ efficient algorithm for any $M{=}N^\epsilon$ for fixed $\epsilon{>}0$.

Original problem	k	Average-case problem	Solution
Abelian HSP	1	Linear equations	Easy
Metacyclic HSP $\mathbb{Z}_N \rtimes \mathbb{Z}_p,\ p = \phi(N)/\operatorname{poly}(\log N)$	1	Discrete log	Shor's algorithm
$\mathbb{Z}_p^r \rtimes \mathbb{Z}_p$ (r=2 is Heisenberg)	r	Polynomial equations	Buchburger's algorithm, elimination
Generalized abelian hidden shift problem, $M{=}N^\epsilon$	$1/\epsilon$	Integer programming	Lenstra's algorithm
Dihedral HSP	$\log N$	Subset sum	?
Symmetric group HSP	$n \log n$	?	?

Open questions

Open questions

- Can we find better solutions of average-case problems that arise from this approach?

Open questions

- Can we find better solutions of average-case problems that arise from this approach?
  - Metacyclic group with $k{=}1$: $a\mu^x = b$, discrete log

    with $k{=}2$: $a\mu^x + b\mu^y = c$, how to solve?

Open questions

- Can we find better solutions of average-case problems that arise from this approach?
  - Metacyclic group with $k{=}1$: $a\mu^x = b$, discrete log
    with $k{=}2$: $a\mu^x + b\mu^y = c$, how to solve?
  - Faster solution of random subset sum problems/random integer programs (quantum algorithms?)

Open questions

- Can we find better solutions of average-case problems that arise from this approach?
  - Metacyclic group with $k{=}1$: $a\mu^x = b$, discrete log
    with $k{=}2$: $a\mu^x + b\mu^y = c$, how to solve?
  - Faster solution of random subset sum problems/random integer programs (quantum algorithms?)
- Is there a problem that is not even information theoretically reconstructible from *single*-register measurements, but for which there is an *efficient*, *multi*-register algorithm?

Open questions

- Can we find better solutions of average-case problems that arise from this approach?
  - Metacyclic group with $k{=}1$: $a\mu^x = b$, discrete log
    with $k{=}2$: $a\mu^x + b\mu^y = c$, how to solve?
  - Faster solution of random subset sum problems/random integer programs (quantum algorithms?)
- Is there a problem that is not even information theoretically reconstructible from *single*-register measurements, but for which there is an *efficient*, *multi*-register algorithm?
- Find new algorithms for the hidden subgroup problem. (Beyond the standard approach?)

Open questions

- Can we find better solutions of average-case problems that arise from this approach?
  - Metacyclic group with $k{=}1$: $a\mu^x = b$, discrete log
    with $k{=}2$: $a\mu^x + b\mu^y = c$, how to solve?
  - Faster solution of random subset sum problems/random integer programs (quantum algorithms?)
- Is there a problem that is not even information theoretically reconstructible from *single*-register measurements, but for which there is an *efficient*, *multi*-register algorithm?
- Find new algorithms for the hidden subgroup problem. (Beyond the standard approach?)
- Are there other hidden subgroup problems (besides dihedral & symmetric groups) with practical applications?