The hidden subgroup problem, quantum state estimation, and phase transitions in computational problems

Andrew Childs
Caltech Institute for Quantum Information

joint work with

Dave Bacon
University of Washington

Wim van Dam
UC Santa Barbara

quant-ph/0501044, **quant-ph/0504083**

Outline

- Quantum computation
- The hidden subgroup problem
- Distinguishing quantum states:
  The ***pretty good measurement***
- Semidirect product groups
- The ***matrix sum problem***
- Implementing the measurement
- Applications

Quantum mechanics in a nutshell

- ***States*** are unit vectors in Hilbert space, $|\psi\rangle \in (\mathbb{C}^2)^n$

  One qubit: $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, $|\alpha_0|^2 + |\alpha_1|^2 = 1$

  n qubits: $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle$, $\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$

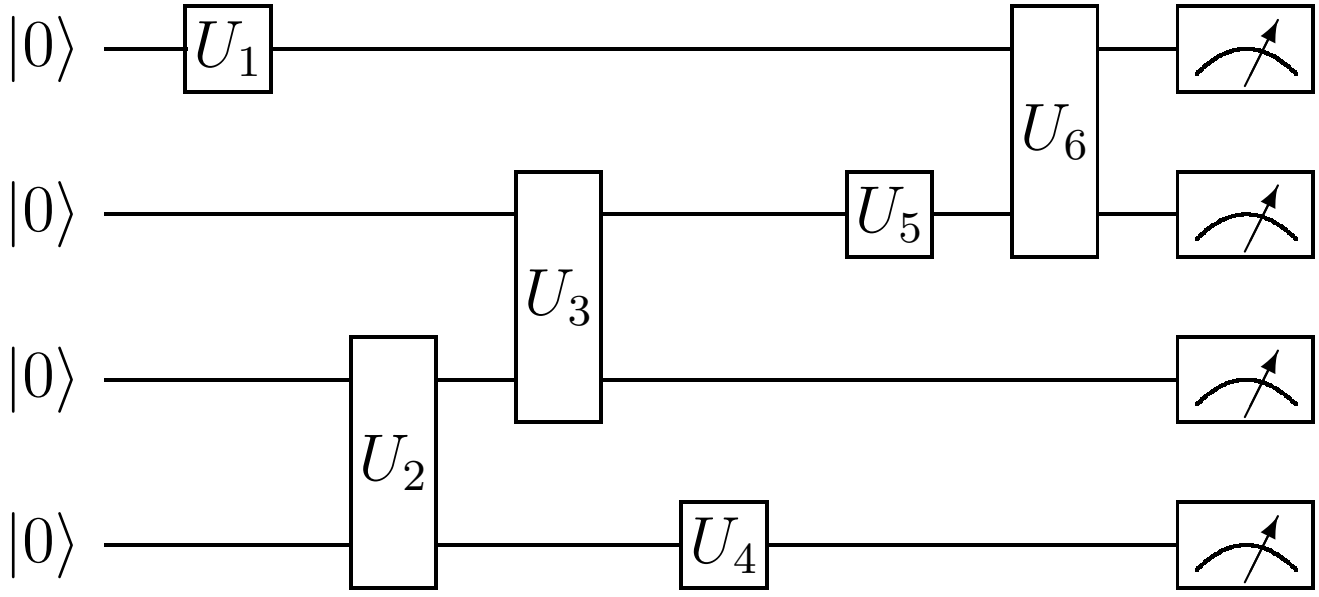
- ***Evolution*** is unitary: $|\psi\rangle \mapsto U|\psi\rangle$, $U^\dagger U = UU^\dagger = I$

- The quantum state is not directly observable (cf. a probability distribution). To get information from $|\psi\rangle$, we must perform a ***measurement***.

  Example: *Computational basis measurement*, $\Pr(x) = |\alpha_x|^2$

Quantum computation

- Prepare n qubits in the state $|\underbrace{0 \cdots 0}_{n}\rangle$.
- Apply a sequence of $\mathrm{poly}(n)$ unitary operations acting on one or two qubits at a time.
- Measure in the computational basis to get the result.



Mixed states and POVMs

- A statistical mixture of quantum states can be described by a ***density matrix*** ρ.

  Pure state $|\psi\rangle$: $\rho = |\psi\rangle\langle\psi|$

  Mixture of states $|\psi_i\rangle$ with probabilities p_i:
  $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

- ***Positive operator-valued measure*** (POVM): positive matrices E_i satisfying $\sum_i E_i = I$

  $\Pr(i) = \mathrm{tr}(E_i \rho)$

  Example: For computational basis measurement, $E_x = |x\rangle\langle x|$

Quantum computation is powerful!

Strong Church-Turing Thesis: All physically reasonable models of computation are (essentially) equivalent in power to the computer on your desk.

Quantum computation is powerful!

Strong Church-Turing Thesis: All physically reasonable models of computation are (essentially) equivalent in power to the computer on your desk.

Quantum mechanics calls this into question!

[Shor 1994]: Polynomial-time quantum algorithm for factoring. Believed to be hard for classical computers; best known algorithm takes time $2^{O(n^{1/3}\log^{2/3} n)}$.

Quantum computation is powerful!

Strong Church-Turing Thesis: All physically reasonable models of computation are (essentially) equivalent in power to the computer on your desk.

Quantum mechanics calls this into question!

[Shor 1994]: Polynomial-time quantum algorithm for factoring. Believed to be hard for classical computers; best known algorithm takes time $2^{O(n^{1/3}\log^{2/3} n)}$.

Main open question: What problems can be solved faster on quantum computers than classical computers?

The hidden subgroup problem

Problem: Fix a group G (known) and a subgroup $H \leq G$ (unknown). Given a black box that computes a function $f : G \to S$ 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.
Efficient algorithm: run time $\mathrm{poly}(\log |G|)$.

Most interesting cases of the HSP

- Abelian groups ($\Rightarrow$ factoring, discrete log, Pell's equation)
- Dihedral group ($\Rightarrow$ shortest vector in a lattice [Regev 02])
  Subexponential-time algorithm [Kuperberg 03]
- Symmetric group ($\Rightarrow$ graph isomorphism)

Efficient algorithms for the HSP

- Abelian groups [Shor 94; Boneh, Lipton 95; Kitaev 95]
- Normal subgroups [Hallgren, Russell, Ta-Shma 00]
- “Almost abelian” groups [Grigni, Schulman, Vazirani[2] 01]
- “Near-Hamiltonian” groups [Gavinsky 04]
- $\mathbb{Z}_2^n \wr \mathbb{Z}_2$ [Püschel, Rötteler, Beth 98]
- $\mathbb{Z}_{p^k}^n \rtimes \mathbb{Z}_2$ [Friedl, Ivanyos, Magniez, Santha, Sen 02]
- $\mathbb{Z}_N \rtimes \mathbb{Z}_p$, N prime, $p = \frac{\phi(N)}{\mathrm{poly}(\log N)}$ prime (p-hedral) [Moore, Rockmore, Russell, Schulman 04]
- $\mathbb{Z}_{p^k} \rtimes \mathbb{Z}_p$ [Inui, Le Gall 04]

Efficient algorithms for the HSP

- Abelian groups [Shor 94; Boneh, Lipton 95; Kitaev 95]
- Normal subgroups [Hallgren, Russell, Ta-Shma 00]
- "Almost abelian" groups [Grigni, Schulman, Vazirani^2 01]
- "Near-Hamiltonian" groups [Gavinsky 04]

➡ $\mathbb{Z}_2^n \wr \mathbb{Z}_2$ [Püschel, Rötteler, Beth 98]

- $\mathbb{Z}_{p^k}^n \rtimes \mathbb{Z}_2$ [Friedl, Ivanyos, Magniez, Santha, Sen 02]

➡ $\mathbb{Z}_N \rtimes \mathbb{Z}_p$, N prime, $p = \frac{\phi(N)}{\mathrm{poly}(\log N)}$ prime (p-hedral) [Moore, Rockmore, Russell, Schulman 04], N arbitrary [BCD 05]

➡ $\mathbb{Z}_{p^k} \rtimes \mathbb{Z}_p$ [Inui, Le Gall 04]

➡ $\mathbb{Z}_p^r \rtimes \mathbb{Z}_p$, r constant (including the Heisenberg group, $r = 2$) [BCD 05]

Overview of the PGM approach

- Cast the HSP as a problem of distinguishing quantum states
- Express these states in terms of a ***matrix sum problem*** (MSP)
- Perform the ***pretty good measurement*** on k copies of the hidden subgroup states
- Show that the measurement succeeds if k is sufficiently large (MSP is in the phase where solutions exist with high probability)
- Implement the measurement by solving the MSP (***quantum sampling*** from the set of solutions)

Standard approach to the HSP

Compute uniform superposition of function values:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, 0\rangle \rightarrow \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, f(g)\rangle \, .$$

Standard approach to the HSP

Compute uniform superposition of function values:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, 0\rangle \rightarrow \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, f(g)\rangle \, .$$

Discard second register to get a **hidden subgroup state**,

$$\boxed{\rho_H := \frac{|H|}{|G|} \sum_{g \in \mathcal{K}} |gH\rangle\langle gH|}$$

(where

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

and $\mathcal{K}$ is a set of coset representatives).

Distinguishing quantum states

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

This can only be done perfectly if the states are orthogonal.

Distinguishing quantum states

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

This can only be done perfectly if the states are orthogonal.

Applications:

- Experiments
- Decoding information sent through a quantum channel
- Quantum algorithms

Pretty good measurement

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

Pretty good measurement: For $\Sigma := \sum_i p_i \rho_i$, let

$$E_i := p_i \frac{1}{\sqrt{\Sigma}} \rho_i \frac{1}{\sqrt{\Sigma}} .$$

This measurement often does a pretty good job of distinguishing the states.

Optimal measurement

Theorem [Holevo 73, Yuen-Kennedy-Lax 75]**.** 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!).

Optimal measurement for the HSP

Approach to the HSP: Find the optimal measurement for distinguishing states in the ensemble $\{\rho_H\}_{H \leq G}$ for the various possible subgroups (or some subset thereof).

Optimal measurement for the HSP

Approach to the HSP: Find the optimal measurement for distinguishing states in the ensemble $\{\rho_H\}_{H \leq G}$ for the various possible subgroups (or some subset thereof).

More generally, $\{\underbrace{\rho_H \otimes \cdots \otimes \rho_H}_{k}\}$.

Optimal measurement for the HSP

Approach to the HSP: Find the optimal measurement for distinguishing states in the ensemble $\{\rho_H\}_{H \leq G}$ for the various possible subgroups (or some subset thereof).

More generally, $\{\underbrace{\rho_H \otimes \cdots \otimes \rho_H}_{k}\}$.

[Ip 03]: Shor's algorithm implements the optimal measurement for the abelian hidden subgroup problem.

Optimal measurement for the HSP

Approach to the HSP: Find the optimal measurement for distinguishing states in the ensemble $\{\rho_H\}_{H \leq G}$ for the various possible subgroups (or some subset thereof).

More generally, $\{\underbrace{\rho_H \otimes \cdots \otimes \rho_H}_{k}\}$.

[Ip 03]: Shor's algorithm implements the optimal measurement for the abelian hidden subgroup problem.

For all the ensembles of (k copes of) hidden subgroup states considered in this talk, the pretty good measurement is optimal, as can be shown by explicitly verifying the Holevo/Yuen-Kennedy-Lax conditions.

Semidirect product

Definition. Let A, B be groups (written additively) and let $\varphi : B \to \mathrm{Aut}(A)$ be a homomorphism ($\varphi(b_1 b_2) = \varphi(b_1)\varphi(b_2)$). Then $A \rtimes_\varphi B$ is the group with elements (a, b) for $a \in A$ and $b \in B$, and group operation

$$(a, b)(a', b') = (a + \varphi(b)(a'), b + b') \,.$$

Semidirect product

Definition. Let A, B be groups (written additively) and let $\varphi : B \to \mathrm{Aut}(A)$ be a homomorphism ($\varphi(b_1 b_2) = \varphi(b_1)\varphi(b_2)$). Then $A \rtimes_\varphi B$ is the group with elements (a, b) for $a \in A$ and $b \in B$, and group operation

$$(a, b)(a', b') = (a + \varphi(b)(a'), b + b') \,.$$

Example: Let $B = \mathbb{Z}_2$ and let

$$\varphi(0)(a) = a$$
$$\varphi(1)(a) = -a \,.$$

Then

$$(a, b)(a', b') = (a + (-1)^b a', b + b') \,.$$

For $A = \mathbb{Z}_N$, this is the dihedral group D_N.

Reduction to cyclic subgroups

Lemma. If there is an efficient algorithm for the HSP over $G = A \rtimes \mathbb{Z}_p$ with p prime and with the promise that H is either trivial or $H = \langle (d, 1) \rangle$ for some (unknown) $d \in A$ such that $|\langle (d, 1) \rangle| = p$, then there is an efficient algorithm for the general case.

Reduction to cyclic subgroups

Lemma. If there is an efficient algorithm for the HSP over $G = A \rtimes \mathbb{Z}_p$ with p prime and with the promise that H is either trivial or $H = \langle (d, 1) \rangle$ for some (unknown) $d \in A$ such that $|\langle (d, 1) \rangle| = p$, then there is an efficient algorithm for the general case.

Ettinger-Høyer idea: Let $H_1 := H \cap (A \times \{0\})$. Can find H_1 by solving an abelian HSP. For $H_1 \trianglelefteq G$, we find

$$G/H_1 \cong A \rtimes \mathbb{Z}_p$$

$$H/H_1 \cong \langle (d, 1) \rangle .$$

Additional difficulty: We can have $H_1 \not\trianglelefteq G$. But this only occurs when $H = H_1$, and we can detect when it happens.

Form of cyclic subgroups

$$H = \langle (d,1) \rangle = \{(0,0), (d,1), (d,1)^2, (d,1)^3, \ldots\ (d,1)^{p-1}\}.$$

Form of cyclic subgroups

$$H = \langle (d,1) \rangle = \{(0,0), (d,1), (d,1)^2, (d,1)^3, \dots \ (d,1)^{p-1}\}.$$

$$(d,1)(d,1) = (d + \varphi(d), 2)$$

$$(d + \varphi(d), 2)(d,1) = (d + \varphi(d) + \varphi^2(d), 3)$$

$$\vdots$$

Form of cyclic subgroups

$H = \langle (d,1) \rangle = \{(0,0), (d,1), (d,1)^2, (d,1)^3, \ldots\ (d,1)^{p-1}\}.$

$$(d,1)(d,1) = (d + \varphi(d), 2)$$
$$(d + \varphi(d), 2)(d,1) = (d + \varphi(d) + \varphi^2(d), 3)$$
$$\vdots$$

In general, $(d,1)^b = (\Phi^{(b)}(d), b)$ where

$$\Phi^{(b)}(d) := \sum_{i=0}^{b-1} \varphi^i(d)\,.$$

$|H| = p \Leftrightarrow \Phi^{(p)}(d) = 0.$

Hidden subgroup states

$$\tilde{\rho}_d^{\otimes k} = \frac{1}{|G|^k} \sum_{x \in A^k} \sum_{w,v \in A} \chi_w(d)\, \bar{\chi}_v(d)\, \sqrt{\eta_w^x \eta_v^x}\, |x, S_w^x\rangle\langle x, S_v^x|$$

where

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

$$S_w^x := \{b \in \mathbb{Z}_p^k : \Phi^{(b)}(x) = w\}$$

$$\eta_w^x := |S_w^x|$$

Matrix sum problem

Given k elements $x_1, \ldots, x_k \in A$ and a target element $w \in A$, find $b \in \mathbb{Z}_p^k$ such that

$$\Phi^{(b)}(x) := \sum_{j=1}^{k} \sum_{i=0}^{b_j - 1} \varphi^i(x_j) = w \,.$$

$S_w^x := \{b \in \mathbb{Z}_p^k : \Phi^{(b)}(x) = w\}$ is the set of solutions and $\eta_w^x := |S_w^x|$ is the number of solutions.

Expected # of solutions: $\mathop{\mathbb{E}}_{x,w} \eta_w^x = \dfrac{1}{|A|^{k+1}} \displaystyle\sum_{x \in A^k} \sum_{w \in A} \eta_w^x = \dfrac{p^k}{|A|}$

Many solutions for $k \gg \log |A| / \log p$.
Few solutions for $k \ll \log |A| / \log p$.
$O(1)$ solutions for $k \sim \log |A| / \log p$.

Success probability

$$\Pr(\text{success}) := \operatorname{tr} E_d \rho_d^{\otimes k} \quad \text{(independent of } d\text{)}$$

$$= \frac{p}{|G|^{k+1}} \sum_{x \in A^k} \left(\sum_{w \in A} \sqrt{\eta_w^x} \right)^2$$

(Recall $\eta_w^x =$ # of solutions to matrix sum problem (x, w).)

Success probability

$$\Pr(\text{success}) := \operatorname{tr} E_d \rho_d^{\otimes k} \quad \text{(independent of } d\text{)}$$

$$= \frac{p}{|G|^{k+1}} \sum_{x \in A^k} \left(\sum_{w \in A} \sqrt{\eta_w^x} \right)^2$$

(Recall $\eta_w^x =$ # of solutions to matrix sum problem (x, w).)

Upper bound on the success probability:

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

So for example, if $k = \nu \log |A| / \log p$, then the success probability will be exponentially small in $\log |A|$ for any fixed $\nu < 1$.

Success probability

$$\Pr(\text{success}) := \operatorname{tr} E_d \rho_d^{\otimes k} \quad \text{(independent of } d\text{)}$$

$$= \frac{p}{|G|^{k+1}} \sum_{x \in A^k} \left(\sum_{w \in A} \sqrt{\eta_w^x} \right)^2$$

(Recall $\eta_w^x =$ # of solutions to matrix sum problem (x, w).)

Lower bound on the success probability:
If $\Pr(\eta_w^x \geq \alpha) \geq \beta$ for uniformly random x, w (i.e., if most instances have many solutions), then

$$\Pr(\text{success}) \geq \alpha \beta^2 \frac{|A|}{p^k} .$$

This will typically be the case for $k > \log |A| / \log p$

Implementing the measurement

Neumark's Theorem: Any POVM can be implemented by a unitary operation on the system (plus an ancilla), followed by a computational basis measurement. For a rank-one POVM, $E_j = |e_j\rangle\langle e_j|$,

$$U = \left(\begin{array}{ccc|c} | & & | & \\ e_1 & \cdots & e_n & A \\ | & & | & \\ \hline & & & \\ & B & & C \\ & & & \end{array}\right).$$

Implementing the measurement

The PGM for hidden subgroups $\langle (d,1) \rangle \leq A \rtimes \mathbb{Z}_p$ can be implemented efficiently if we can perform a transformation of the form

$$|x,w\rangle \mapsto \begin{cases} |x, S_w^x\rangle & \eta_w^x > 0 \\ |\xi_w^x\rangle & \eta_w^x = 0 \end{cases}$$

("quantum sampling" of matrix sum solutions).

Review of the PGM approach

- Cast the HSP as a problem of distinguishing quantum states
- Express these states in terms of a ***matrix sum problem*** (MSP)
- Perform the ***pretty good measurement*** on k copies of the hidden subgroup states
- Show that the measurement succeeds if k is sufficiently large (MSP is in the phase where solutions exist with high probability)
- Implement the measurement by solving the MSP (***quantum sampling*** from the set of solutions)

Application 1: Dihedral group

$G = Z_N \rtimes \mathbb{Z}_2$ with $\varphi(a) = -a$

So $\Phi^{(b)}(a) = ba$ ($a \in \mathbb{Z}_N$, $b = 0$ or 1)

Application 1: Dihedral group

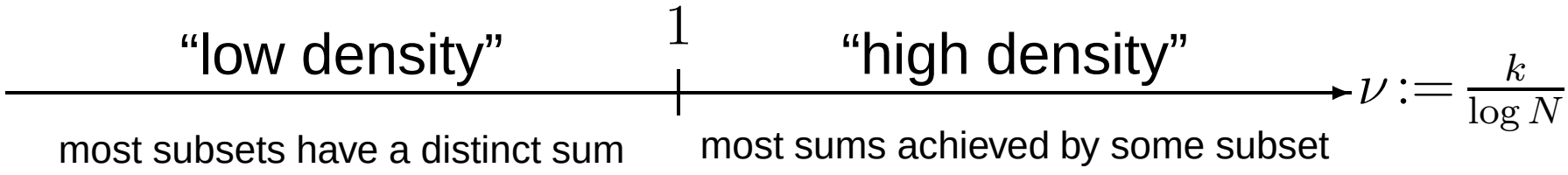
$G = Z_N \rtimes \mathbb{Z}_2$ with $\varphi(a) = -a$
So $\Phi^{(b)}(a) = ba$ ($a \in \mathbb{Z}_N$, $b = 0$ or 1)

Matrix sum problem: given $x \in \mathbb{Z}_N^k$ and $w \in \mathbb{Z}_N$ uniformly at random, find $b \in \mathbb{Z}_2^k$ such that $b \cdot x = w \bmod N$. This is the well-studied ***subset sum problem***.

Application 1: Dihedral group

$G = Z_N \rtimes \mathbb{Z}_2$ with $\varphi(a) = -a$
So $\Phi^{(b)}(a) = ba$ ($a \in \mathbb{Z}_N$, $b = 0$ or 1)

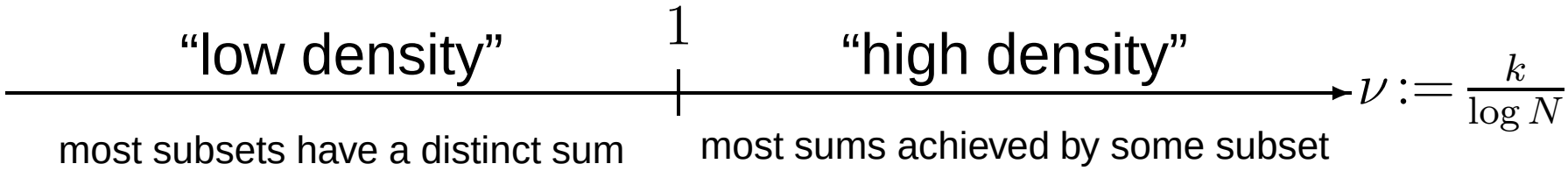
Matrix sum problem: given $x \in \mathbb{Z}_N^k$ and $w \in \mathbb{Z}_N$ uniformly at random, find $b \in \mathbb{Z}_2^k$ such that $b \cdot x = w \bmod N$. This is the well-studied ***subset sum problem***.



Application 1: Dihedral group

$G = Z_N \rtimes \mathbb{Z}_2$ with $\varphi(a) = -a$
So $\Phi^{(b)}(a) = ba$ ($a \in \mathbb{Z}_N$, $b = 0$ or 1)

Matrix sum problem: given $x \in \mathbb{Z}_N^k$ and $w \in \mathbb{Z}_N$ uniformly at random, find $b \in \mathbb{Z}_2^k$ such that $b \cdot x = w \bmod N$. This is the well-studied ***subset sum problem***.

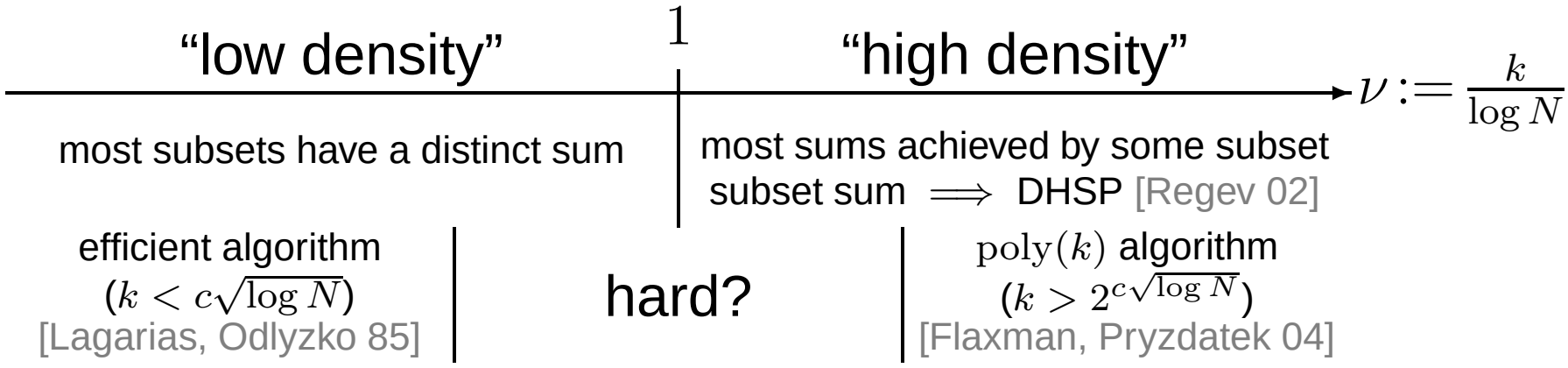


efficient algorithm ($k < c\sqrt{\log N}$) [Lagarias, Odlyzko 85]	hard?	$\mathrm{poly}(k)$ algorithm ($k > 2^{c\sqrt{\log N}}$) [Flaxman, Pryzdatek 04]

Application 1: Dihedral group

$G = Z_N \rtimes \mathbb{Z}_2$ with $\varphi(a) = -a$
So $\Phi^{(b)}(a) = ba$ ($a \in \mathbb{Z}_N$, $b = 0$ or 1)

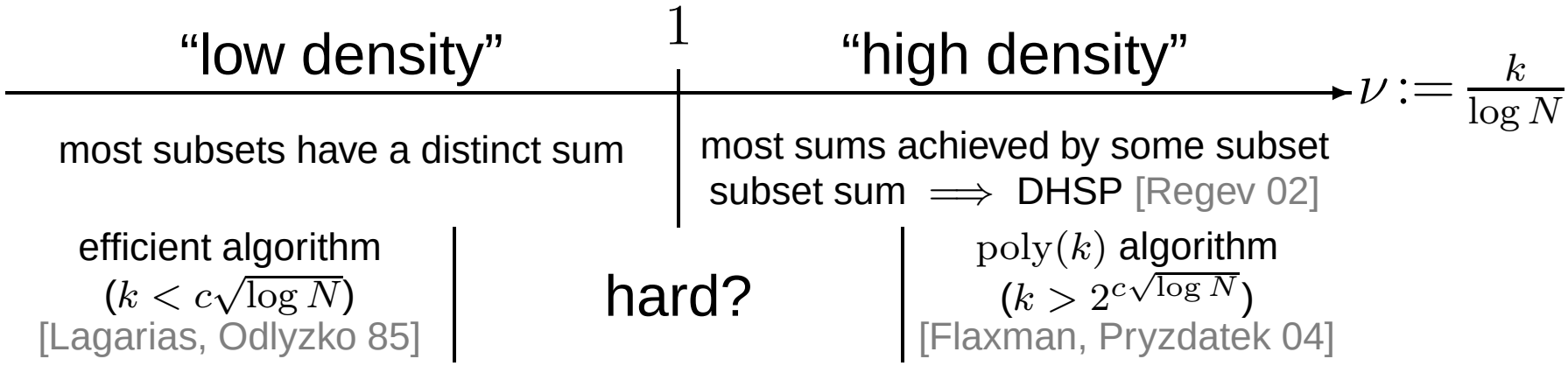
Matrix sum problem: given $x \in \mathbb{Z}_N^k$ and $w \in \mathbb{Z}_N$ uniformly at random, find $b \in \mathbb{Z}_2^k$ such that $b \cdot x = w \bmod N$. This is the well-studied ***subset sum problem***.



Application 1: Dihedral group

$G = Z_N \rtimes \mathbb{Z}_2$ with $\varphi(a) = -a$
So $\Phi^{(b)}(a) = ba$ ($a \in \mathbb{Z}_N$, $b = 0$ or 1)

Matrix sum problem: given $x \in \mathbb{Z}_N^k$ and $w \in \mathbb{Z}_N$ uniformly at random, find $b \in \mathbb{Z}_2^k$ such that $b \cdot x = w \bmod N$. This is the well-studied ***subset sum problem***.



PGM requires $k > 1 \cdot \log_2 N$ hidden subgroup states to succeed. Since it is optimal, *any* strategy requries this many states.

Application 2: Metacyclic groups

$G = Z_N \rtimes \mathbb{Z}_p$ with $\varphi(a) = \mu a$ for some $\mu \in \mathbb{Z}_N^\times$

So $\Phi^{(b)}(a) = \left(\sum_{i=0}^{b-1} \mu^i \right) a = \frac{\mu^b - 1}{\mu - 1}$ if $\mu - 1 \in \mathbb{Z}_N^\times$ (for simplicity)

Application 2: Metacyclic groups

$G = Z_N \rtimes \mathbb{Z}_p$ with $\varphi(a) = \mu a$ for some $\mu \in \mathbb{Z}_N^\times$

So $\Phi^{(b)}(a) = \left(\sum_{i=0}^{b-1} \mu^i\right) a = \frac{\mu^b - 1}{\mu - 1}$ if $\mu - 1 \in \mathbb{Z}_N^\times$ (for simplicity)

Matrix sum problem ($k = 1$): given $x, w \in \mathbb{Z}_N$ uniformly at random, find $b \in \mathbb{Z}_p$ such that $\frac{\mu^b - 1}{\mu - 1} x = w$. This can be solved by calculating a discrete logarithm (using Shor's algorithm!). $\Pr(\text{solution exists}) = p/N$, so this is efficient for $N/p = \text{poly}(\log N)$.

Application 2: Metacyclic groups

$G = Z_N \rtimes \mathbb{Z}_p$ with $\varphi(a) = \mu a$ for some $\mu \in \mathbb{Z}_N^\times$

So $\Phi^{(b)}(a) = \left(\sum_{i=0}^{b-1} \mu^i\right) a = \frac{\mu^b - 1}{\mu - 1}$ if $\mu - 1 \in \mathbb{Z}_N^\times$ (for simplicity)

Matrix sum problem ($k = 1$): given $x, w \in \mathbb{Z}_N$ uniformly at random, find $b \in \mathbb{Z}_p$ such that $\frac{\mu^b - 1}{\mu - 1} x = w$. This can be solved by calculating a discrete logarithm (using Shor's algorithm!). $\Pr(\text{solution exists}) = p/N$, so this is efficient for $N/p = \text{poly}(\log N)$.

Same condition as in [Moore, Rockmore, Russell, Schulman 04], but generalizes to N composite, and no nonabelian Fourier transforms are required.

Application 2: Metacyclic groups

$G = Z_N \rtimes \mathbb{Z}_p$ with $\varphi(a) = \mu a$ for some $\mu \in \mathbb{Z}_N^\times$

So $\Phi^{(b)}(a) = \left(\sum_{i=0}^{b-1} \mu^i\right) a = \frac{\mu^b - 1}{\mu - 1}$ if $\mu - 1 \in \mathbb{Z}_N^\times$ (for simplicity)

Matrix sum problem ($k = 1$): given $x, w \in \mathbb{Z}_N$ uniformly at random, find $b \in \mathbb{Z}_p$ such that $\frac{\mu^b - 1}{\mu - 1} x = w$. This can be solved by calculating a discrete logarithm (using Shor's algorithm!). $\Pr(\text{solution exists}) = p/N$, so this is efficient for $N/p = \text{poly}(\log N)$.

Same condition as in [Moore, Rockmore, Russell, Schulman 04], but generalizes to N composite, and no nonabelian Fourier transforms are required.

What happens with $k > 1$?

Application 3: Heisenberg et al.

$G = \mathbb{Z}_p^r \rtimes \mathbb{Z}_p$ with $\varphi(a) = \mu a$ for some $\mu \in \mathbb{Z}_p^{r \times r}$

Application 3: Heisenberg et al.

$G = \mathbb{Z}_p^r \rtimes \mathbb{Z}_p$ with $\varphi(a) = \mu a$ for some $\mu \in \mathbb{Z}_p^{r \times r}$

Example: $r = 2$, $\mu = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is the *Heisenberg group*, a discrete analog of the group generated by the position and momentum operators x, p

Then $\mu^i = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$, so $\sum_{i=0}^{b-1} \mu^i = \begin{pmatrix} b & \frac{b(b-1)}{2} \\ 0 & b \end{pmatrix}$.

Application 3: Heisenberg et al.

$G = \mathbb{Z}_p^r \rtimes \mathbb{Z}_p$ with $\varphi(a) = \mu a$ for some $\mu \in \mathbb{Z}_p^{r \times r}$

Example: $r = 2$, $\mu = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is the *Heisenberg group*, a discrete analog of the group generated by the position and momentum operators x, p

Then $\mu^i = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$, so $\sum_{i=0}^{b-1} \mu^i = \begin{pmatrix} b & \frac{b(b-1)}{2} \\ 0 & b \end{pmatrix}$.

Matrix sum problem: a system of r equations in k variables of degree r over the finite field $\mathbb{Z}_p$. Likely to have 1 or 2 solutions if $k = r$. Solutions can be found using Buchberger's algorithm to compute a Gröbner basis (or can be written down explicitly when $r = 2$), which is efficient for r constant.

Application 4: Generalized hidden shift

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

Application 4: Generalized hidden shift

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

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

Application 4: Generalized hidden shift

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

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

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

Application 4: Generalized hidden shift

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

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

Matrix sum problem: given $x \in \mathbb{Z}_N^k$ and $w \in \mathbb{Z}_N$ uniformly random, find $b \in \{0, \ldots, M-1\}^k$ 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 $\epsilon > 0$.

Conclusions

- The pretty good measurement is a powerful tool for solving hidden subgroup (and related) problems.
- This approach has produced new efficient quantum algorithms for the nonabelian hidden subgroup problem, e.g. for the Heisenberg group.
- Using only abelian Fourier transforms and classical algorithms, one can implement entangled measurements on many copies of a hidden subgroup state (which is necessary for some instances of the HSP).