Optimal measurements for the dihedral hidden subgroup problem

Andrew Childs
Caltech Institute for Quantum Information

joint work with

Dave Bacon
Santa Fe Institute

Wim van Dam
UC Santa Barbara

quant-ph/0501044

Quantum algorithms

Key question: What problems can be solved (asymptotically) faster by a quantum computer than by a classical computer?

- Factoring, discrete log [Shor 94]
- Unstructured search [Grover 96]

Quantum algorithms

Key question: What problems can be solved (asymptotically) faster by a quantum computer than by a classical computer?

- Factoring, discrete log [Shor 94]
- Unstructured search [Grover 96]
- Various hidden subgroup problems
- Pell's equation [Hallgren 02]
- Hidden shift problems [van Dam, Hallgren, Ip 03]
- Graph traversal [CCDFGS 03]
- Spatial search [AA 03, CG 03/04, AKR 04]
- Element distinctness [Ambainis 03]
- Various graph problems [DHHM 04, MSS 03, . . .]
- Testing matrix multiplication [Buhrman, Špalek 04]
- . . .

Quantum algorithms

Key question: What problems can be solved (asymptotically) faster by a quantum computer than by a classical computer?

Approaches:

- Fourier sampling
- Amplitude amplification
- Adiabatic evolution
- Quantum walk

The hidden subgroup problem

Problem: Fix a group $\mathcal{G}$ (known) and a subgroup $\mathcal{H} \leq \mathcal{G}$ (unknown). Given query access to a function $f : \mathcal{G} \to S$ that is

- Constant on any particular left coset of $\mathcal{H}$ in $\mathcal{G}$
- Distinct on different left cosets of $\mathcal{H}$ in $\mathcal{G}$

We say that f hides $\mathcal{H}$.

Goal: Find (a generating set for) $\mathcal{H}$.

Efficient algorithm: run time $\mathrm{poly}(\log |\mathcal{G}|)$.

Query complexity

The quantum query complexity of the HSP is polynomial: $O(\log |\mathcal{G}|)$ quantum queries of f are sufficient to determine $\mathcal{H}$.
[Ettinger, Høyer, Knill 99]

But the best known general algorithm uses $O(|\mathcal{G}|)$ time.

Efficient algorithms

- Abelian groups [Shor 94; Boneh, Lipton 95; Kitaev 95]
- $\mathbb{Z}_2^n \wr \mathbb{Z}_2$ [Püschel, Rötteler, Beth 98]
- Normal subgroups [Hallgren, Russell, Ta-Shma 00]
- “Almost abelian” groups [GSVV 01]
- $\mathbb{Z}_{p^k}^n \rtimes \mathbb{Z}_2$ [FIMMS 02]
- q-hedral groups [MRRS 04]
- “Near-Hamiltonian” groups [Gavinsky 04]
- $\mathbb{Z}_{p^k} \rtimes \mathbb{Z}_p$ [Inui, Le Gall 04]

Interesting instances

Symmetric group

$\Longrightarrow$ Graph isomorphism. [Boneh, Lipton 95]

Some evidence that it may be hard. [Kempe, Shalev 04; Moore, Russell 05]

Dihedral group

$\Longrightarrow$ $\mathrm{poly}(d)$ unique shortest vector in a lattice. [Regev 02]

$\Longleftarrow$ Trivial/order two subgroups. [Ettinger, Høyer 98]

$\Longleftarrow$ Subset sum. [Regev 02]

$2^{O(\sqrt{\log N})}$-time algorithm… [Kuperberg 03]

…with polynomial space. [Regev 04]

Subset sum problem

Problem: Given k integers from $\mathbb{Z}_N = \{0, \ldots, N-1\}$ ($x \in \mathbb{Z}_N^k$) and a target $t \in \mathbb{Z}_N$.
Goal: Find a subset $b \in \mathbb{Z}_2^k$ such that

$$b \cdot x := \sum_{j=1}^{k} b_j x_j \bmod N = t\,.$$

Subset sum problem

Problem: Given k integers from $\mathbb{Z}_N = \{0, \ldots, N-1\}$ ($x \in \mathbb{Z}_N^k$) and a target $t \in \mathbb{Z}_N$.
Goal: Find a subset $b \in \mathbb{Z}_2^k$ such that

$$b \cdot x := \sum_{j=1}^{k} b_j x_j \bmod N = t\,.$$

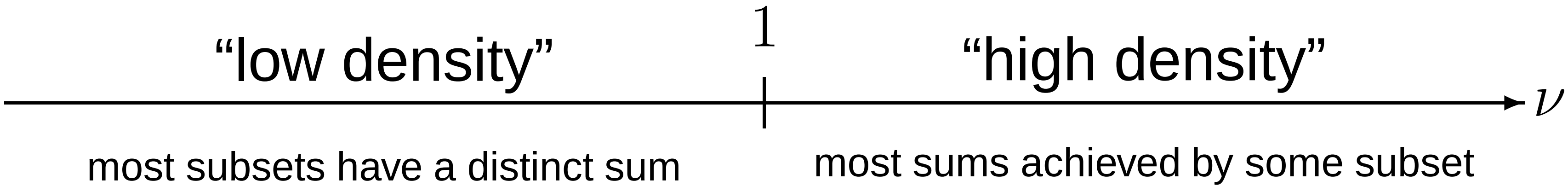
General problem is NP-hard. But average-case problem at a fixed density $\nu := k/\log_2 N$ may be much easier.

Subset sum problem

Problem: Given k integers from $\mathbb{Z}_N = \{0, \ldots, N-1\}$ ($x \in \mathbb{Z}_N^k$) and a target $t \in \mathbb{Z}_N$.
Goal: Find a subset $b \in \mathbb{Z}_2^k$ such that

$$b \cdot x := \sum_{j=1}^{k} b_j x_j \bmod N = t\,.$$

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



"low density"

1

"high density"

ν

most subsets have a distinct sum

most sums achieved by some subset

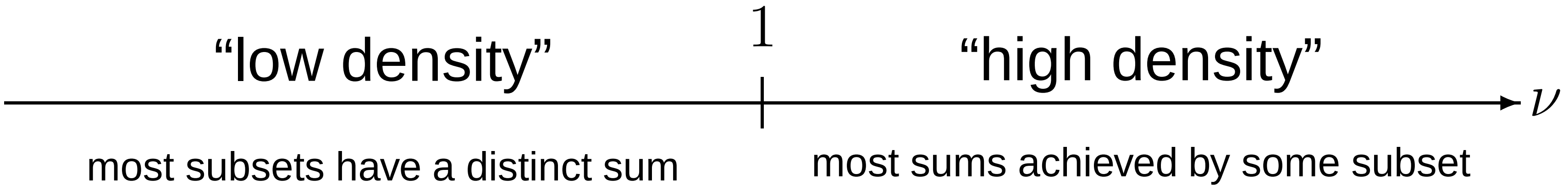
Subset sum problem

Problem: Given k integers from $\mathbb{Z}_N = \{0, \ldots, N-1\}$ ($x \in \mathbb{Z}_N^k$) and a target $t \in \mathbb{Z}_N$.

Goal: Find a subset $b \in \mathbb{Z}_2^k$ such that

$$b \cdot x := \sum_{j=1}^{k} b_j x_j \bmod N = t\,.$$

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



“low density”

1

“high density”

ν

most subsets have a distinct sum

most sums achieved by some subset

efficient algorithm
($k < c\sqrt{\log N}$)
[Lagarias, Odlyzko 85]

hard?

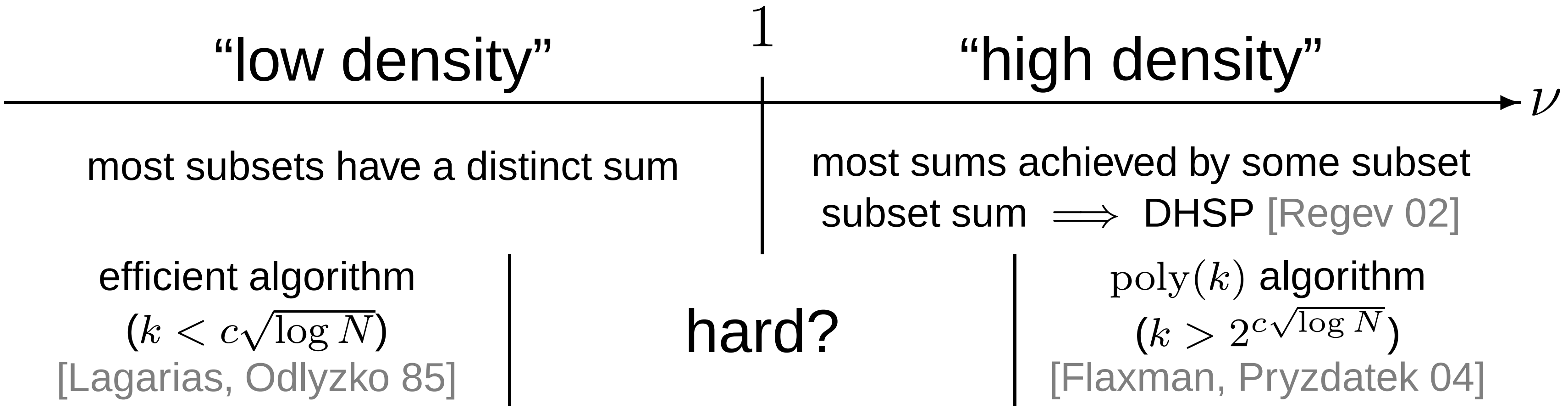
$\mathrm{poly}(k)$ algorithm
($k > 2^{c\sqrt{\log N}}$)
[Flaxman, Pryzdatek 04]

Subset sum problem

Problem: Given k integers from $\mathbb{Z}_N = \{0, \ldots, N-1\}$ ($x \in \mathbb{Z}_N^k$) and a target $t \in \mathbb{Z}_N$.
Goal: Find a subset $b \in \mathbb{Z}_2^k$ such that

$$b \cdot x := \sum_{j=1}^{k} b_j x_j \bmod N = t\,.$$

General problem is NP-hard. But 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 $\implies$ DHSP [Regev 02]

efficient algorithm
($k < c\sqrt{\log N}$)
[Lagarias, Odlyzko 85]

hard?

$\mathrm{poly}(k)$ algorithm
($k > 2^{c\sqrt{\log N}}$)
[Flaxman, Pryzdatek 04]

Standard approach to the HSP

Compute uniform superposition of function values:

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

Standard approach to the HSP

Compute uniform superposition of function values:

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

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

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

(where

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

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

Optimal measurement

Find the measurement with the highest possible success probability for distinguishing states in the ensemble $\{\rho_{\mathcal{H}}\}_{\mathcal{H}\leq\mathcal{G}}$ for the various possible subgroups.

Optimal measurement

Find the measurement with the highest possible success probability for distinguishing states in the ensemble $\{\rho_{\mathcal{H}}\}_{\mathcal{H} \leq \mathcal{G}}$ for the various possible subgroups.

More generally, $\{\underbrace{\rho_{\mathcal{H}} \otimes \cdots \otimes \rho_{\mathcal{H}}}_{k}\}$.

Optimal measurement

Find the measurement with the highest possible success probability for distinguishing states in the ensemble $\{\rho_{\mathcal{H}}\}_{\mathcal{H} \leq \mathcal{G}}$ for the various possible subgroups.

More generally, $\{\underbrace{\rho_{\mathcal{H}} \otimes \cdots \otimes \rho_{\mathcal{H}}}_{k}\}$.

Ip 03: Shor's algorithm implements the optimal measurement for the abelian hidden subgroup problem. $O(1)$ copies suffice.

Optimal measurement

Find the measurement with the highest possible success probability for distinguishing states in the ensemble $\{\rho_{\mathcal{H}}\}_{\mathcal{H}\leq\mathcal{G}}$ for the various possible subgroups.

More generally, $\{\underbrace{\rho_{\mathcal{H}} \otimes \cdots \otimes \rho_{\mathcal{H}}}_{k}\}$.

Ip 03: Shor's algorithm implements the optimal measurement for the abelian hidden subgroup problem. $O(1)$ copies suffice.

Natural questions:

- What is the optimal measurement for other HSPs?
- How many copies are necessary?
- Can the measurements be implemented efficiently?

Generalized measurement

POVM: Operators $\{E_j\}$ satisfying

- $E_j \geq 0$
- $\sum_j E_j = I$

Given a quantum state ρ, $\Pr(j) = \mathrm{tr}(E_j \rho)$.

Generalized measurement

POVM: Operators $\{E_j\}$ satisfying

- $E_j \geq 0$
- $\sum_j E_j = I$

Given a quantum state ρ, $\mathrm{Pr}(j) = \mathrm{tr}(E_j \rho)$.

Neumark's Theorem: Any POVM can be implemented by a unitary operation on the system (plus an ancilla), followed by a standard measurement. For a rank-one POVM, $E_j = e_j e_j^T$,

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

Pretty good measurement

Given an ensemble $\{\rho_j\}$, what is a good way to determine j?

Pretty Good Measurement: For $G := \sum_j \rho_j$, let

$$E_j := G^{-1/2} \rho_j G^{-1/2} \, .$$

(If the states do not have support on the whole Hilbert space, can add $E_{\mathrm{out}} := I - \sum_j E_j$.)

This measurement often does a pretty good job of distinguishing the states. It is known to be optimal (in terms of success probability) for certain kinds of ensembles.

In fact, we can prove that it is optimal for the dihedral hidden subgroup states.

Dihedral group

$\mathcal{G} = \mathcal{D}_N$: Symmetry group of an N-sided regular polygon.

- Rotation$= s$. $s^N = e$.
- Reflection$= r$. $r^2 = e$, $rsr = s^{-1}$.

Group elements: $r^t s^k$ where $t \in \mathbb{Z}_2$, $k \in \mathbb{Z}_N$.

Dihedral group

$\mathcal{G} = \mathcal{D}_N$: Symmetry group of an N-sided regular polygon.

- Rotation$= s$. $s^N = e$.
- Reflection$= r$. $r^2 = e$, $rsr = s^{-1}$.

Group elements: $r^t s^k$ where $t \in \mathbb{Z}_2$, $k \in \mathbb{Z}_N$.

Ettinger-Høyer 98: Sufficient to consider $\mathcal{H} = \{e\}$ or $\mathcal{H} = \{e, rs^d\}$ for some (unknown) d.

Dihedral group

$\mathcal{G} = \mathcal{D}_N$: Symmetry group of an N-sided regular polygon.

- Rotation$= s$. $s^N = e$.
- Reflection$= r$. $r^2 = e$, $rsr = s^{-1}$.

Group elements: $r^t s^k$ where $t \in \mathbb{Z}_2$, $k \in \mathbb{Z}_N$.

Ettinger-Høyer 98: Sufficient to consider $\mathcal{H} = \{e\}$ or $\mathcal{H} = \{e, rs^d\}$ for some (unknown) d.

We will focus on the order two subgroups $\{e, rs^d\}$. When the optimal measurement identifies d, it can also identify the trivial subgroup.

Dihedral hidden subgroup states

Standard approach gives

$$\rho_d = \frac{1}{N}\sum_{k\in\mathbb{Z}_N} |\phi_{k,d}\rangle\langle\phi_{k,d}| \qquad \left(|\phi_{k,d}\rangle := \frac{1}{\sqrt{2}}(|0,k\rangle + |1,-k+d\rangle)\right)$$

Dihedral hidden subgroup states

Standard approach gives

$$\rho_d = \frac{1}{N} \sum_{k \in \mathbb{Z}_N} |\phi_{k,d}\rangle\langle\phi_{k,d}| \qquad \left(|\phi_{k,d}\rangle := \frac{1}{\sqrt{2}}(|0,k\rangle + |1,-k+d\rangle) \right)$$

Change of basis:

$$\rho_d = \frac{1}{N} \sum_{x \in \mathbb{Z}_N} |\tilde{\phi}_{x,d}\rangle\langle\tilde{\phi}_{x,d}| \qquad \left(|\tilde{\phi}_{x,d}\rangle := \frac{1}{\sqrt{2}}(|0\rangle + \omega^{xd}|1\rangle)|x\rangle \right)$$

$$= \frac{1}{2N} \sum_{b,c \in \mathbb{Z}_2} \sum_{x \in \mathbb{Z}_N} \omega^{(b-c)xd} |b,x\rangle\langle c,x|$$

Dihedral hidden subgroup states (k copies)

$$\rho_d^{\otimes k} = \frac{1}{(2N)^k} \sum_{b,c \in \mathbb{Z}_2^k} \sum_{x \in \mathbb{Z}_N^k} \omega^{[(b-c)\cdot x]d} |b, x\rangle\langle c, x|$$

$$= \frac{1}{(2N)^k} \sum_{x \in \mathbb{Z}_N^k} \sum_{p,q \in \mathbb{Z}_N} \omega^{d(p-q)} \sqrt{\eta_p^x \eta_q^x} |S_p^x, x\rangle\langle S_q^x, x|$$

where

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

$$S_t^x := \{b \in \mathbb{Z}_2^k : b \cdot x = t\}$$

$$\eta_t^x := |S_t^x|$$

Dihedral PGM

We have

$$\begin{aligned} G &:= \sum_{j \in \mathbb{Z}_N} \rho_j^{\otimes k} \\ &= \frac{N}{(2N)^k} \sum_{x \in \mathbb{Z}_N^k} \sum_{t \in \mathbb{Z}_N} \eta_t^x \left| S_t^x, x \right\rangle \left\langle S_t^x, x \right| \end{aligned}$$

so

$$\begin{aligned} E_j &:= G^{-1/2} \rho_j^{\otimes k} G^{-1/2} \\ &= \frac{1}{N} \sum_{x \in \mathbb{Z}_N^k} \sum_{p,q \in \mathbb{Z}_N} \omega^{j(p-q)} \left| S_p^x, x \right\rangle \left\langle S_q^x, x \right| . \end{aligned}$$

The PGM is optimal

Theorem [Holevo 73]. Given an ensemble of quantum states ρ_i with a priori probabilities p_i, the measurement with POVM elements E_j maximizes the probability of successfully identifying the state if and only if

$$\Big(\sum_i p_i \rho_i E_i - \rho_j\Big) E_j = E_j \Big(\sum_i p_i \rho_i E_i - \rho_j\Big) = 0$$

The PGM is optimal

Theorem [Holevo 73]. Given an ensemble of quantum states ρ_i with a priori probabilities p_i, the measurement with POVM elements E_j maximizes the probability of successfully identifying the state if and only if

$$\Big(\sum_i p_i \rho_i E_i - \rho_j\Big) E_j = E_j \Big(\sum_i p_i \rho_i E_i - \rho_j\Big) = 0$$

Plugging in the expressions for the dihedral hidden subgroup states and the corresponding PGM in the $|S_t^x\rangle$ basis, one can verify these conditions.

Success probability

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

$$= \frac{1}{2^k N^{k+1}} \sum_{x \in \mathbb{Z}_N^k} \left(\sum_{t \in Z_N} \sqrt{\eta_t^x} \right)^2$$

(Recall $\eta_t^x =$ # of subsets of x summing to t.)

Success probability

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

$$= \frac{1}{2^k N^{k+1}} \sum_{x \in \mathbb{Z}_N^k} \left(\sum_{t \in Z_N} \sqrt{\eta_t^x} \right)^2$$

(Recall $\eta_t^x =$ # of subsets of x summing to t.)

Theorem. For any fixed $\nu > 1$, $p = O(1)$. For any fixed $\nu < 1$, p is exponentially small in $\log N$.

Success probability

$$p := \mathrm{tr}\, E_d \rho_d^{\otimes k} \quad \text{(independent of } d\text{)}$$

$$= \frac{1}{2^k N^{k+1}} \sum_{x \in \mathbb{Z}_N^k} \left(\sum_{t \in Z_N} \sqrt{\eta_t^x} \right)^2$$

(Recall $\eta_t^x =$ # of subsets of x summing to t.)

Theorem. For any fixed $\nu > 1$, $p = O(1)$. For any fixed $\nu < 1$, p is exponentially small in $\log N$.

In particular, $k > \log N$ hidden subgroup states are necessary to solve the dihedral HSP.

Success probability

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

$$= \frac{1}{2^k N^{k+1}} \sum_{x \in \mathbb{Z}_N^k} \left(\sum_{t \in Z_N} \sqrt{\eta_t^x} \right)^2$$

(Recall $\eta_t^x = \#$ of subsets of x summing to t.)

Theorem. For any fixed $\nu > 1$, $p = O(1)$. For any fixed $\nu < 1$, p is exponentially small in $\log N$.

In particular, $k > \log N$ hidden subgroup states are necessary to solve the dihedral HSP.

Note: A straightforward information-theoretic argument only gives $k \geq p \log_2 N$.

Determining the least significant bit

Can one determine the least significant bit of d using fewer hidden subgroup states?

Determining the least significant bit

Can one determine the least significant bit of d using fewer hidden subgroup states?

No! Again, the PGM is optimal. The success probability is exponentially close to $\frac{1}{2}$ for $\nu < 1$.

$$\tilde{p} = \frac{1}{2}\Big[1 + \frac{1}{(2N)^k}\Big(\sum_{x\in\mathbb{Z}_N^k}\sum_{t\in\mathbb{Z}_N}\sqrt{\eta_t^x\eta_{-t}^x} + 2\eta_0^x + 2\eta_{N/2}^x\Big)\Big]$$

Implementing the measurement

The optimal measurement is

$$E_j = \sum_{x \in \mathbb{Z}_N^k} E_j^x \otimes |x\rangle\langle x|$$

where

$$E_j^x := \frac{1}{N} \sum_{p,q \in \mathbb{Z}_N} \omega^{j(p-q)} |S_p^x\rangle\langle S_q^x| \,.$$

It is natural to implement the measurement in particular way: first measure x, then implement the POVM $\{E_j^x\}_{j \in \mathbb{Z}_N}$ with an x-dependent quantum circuit. Each E_j^x is rank one, so the upper left submatrix of the Neumark matrix is unambiguous:

$$U^x = \begin{pmatrix} V^x & A^x \\ B^x & C^x \end{pmatrix} , \quad V^x = \frac{1}{\sqrt{N}} \sum_{j,t \in \mathbb{Z}_N} \omega^{-jt} |j\rangle\langle S_t^x| \,.$$

Implementing the measurement

Fourier transform on left (i.e., on the index j): $U^x \to \tilde{U}^x$ with

$$\tilde{V}^x = \sum_t |t\rangle\langle S_t^x| \,.$$

In other words, the measurement can be implemented efficiently iff we can perform a transformation of the form

$$|t,x\rangle \mapsto \begin{cases} |S_t^x, x\rangle & \eta_t^x > 0 \\ |\psi_t^x\rangle & \eta_t^x = 0 \end{cases}$$

(“quantum sampling” of subset sum solutions).

Summary of results

- The PGM is the optimal measurement for distinguishing dihedral hidden subgroup states.
- The success probability of this measurement has a sharp transition near $\nu \sim 1$.
- In particular, $\log N$ hidden subgroup states are necessary to determine the answer (or even the least significant bit).
- Quantum sampling for subset sum solutions at density ν allows us to implement the measurement at that density.
- Conversely, if the optimal measurement is implemented by first measuring the block x, then an implementation of the measurement can be used to solve the subset sum problem at the corresponding density.

Open questions

- Can we implement the optimal measurement at high (but subexponential) density, e.g. at the Kuperberg-Flaxman-Pryzdatek density, $k = 2^{O(\sqrt{\log N})}$?
  Can we even generate uniformly random subset sum solutions at this density?
- Can we implement the optimal measurement at lower density?
  Without solving subset sum?
- What are the optimal measurements for other non-abelian HSPs?
  Can they be implemented efficiently for the cases where efficient algorithms are known?
  Or for any cases where no efficient algorithm is known?