Hidden Symmetry Subgroup Problems

Miklos Santha

CNRS, Université Paris Diderot, France
and
Centre for Quantum Technologies, NUS, Singapore

joint work with

Thomas Decker
CQT, Singapore

Gábor Ivanyos
SZTAKI, Budapest

Pawel Wocjan
U. of Central Florida

How to build quantum algorithms with exponential saving?

The success story in hidden structures:

Theorem[Shor'94]: The hidden subgroup problem can be solved in abelian groups in quantum polynomial time.

Post-abelian hidden structures finding:

- Hidden subgroups in non-abelian groups
- Hidden algebraic sets of higher degrees

Here:

- New proposal: Subgroups hidden by symmetries
- Generalizes the above problems
- In some cases reduces to solvable hidden subgroup problems

Hidden Subgroup Problem (HSP)

Hidden Subgroup Problem

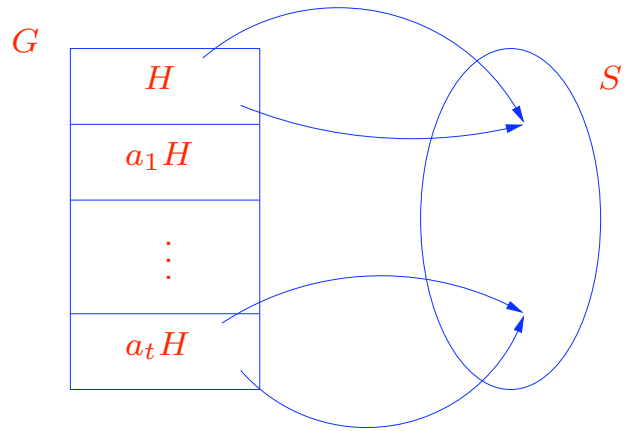
$\mathrm{HSP}(G;\mathcal{H})$ where G is finite group, $\mathcal{H}$ is a family of subgroups

Oracle Input: A function $f : G \to S$ (where S finite)

Promise: For some subgroup $H \in \mathcal{H}$, we have

$$f(x) = f(y) \iff Hx = Hy.$$

Output: Generators for H.



- Parameter: G and $\mathcal{H}$ are given explicitly
- Information: Partition π_f of G defined by the level sets
  $$f^{-1}(s) = \{x \in G : f(x) = s\}, \text{ for } s \in S$$
- Efficiency: Polynomial in $\log |G|$

HSP in non-abelian groups

Theorem: Can be solved in quantum $\mathrm{poly}(\log|G|)$-time when

– $G = \mathbb{Z}_2^k \wr \mathbb{Z}_2$ [Roetteler,Beth'98]

– H is normal and QFT_G is available [Hallgren,Russell,Ta-Shma'00]

– $\cap\{N(H) : H \leq G\}$ is large [Grigni,Schulman,Vazirani,Vazirani'01]

– $G = \mathbb{Z}_p \rtimes \mathbb{Z}_m$ if $m = \frac{p-1}{(\log p)^c}$ [Moore,Rockmore,Russell,Schulman'04]

– H is normal and G is solvable [Ivanyos,Magniez,Santha'01]

– G: is of constant exponent and constant length derived series [Friedl,Ivanyos,Magniez,Santha,Sen'03]

– G is the Heisenberg group [Bacon,Childs,van Dam'05]

– G is a nil-2 group [Ivanyos,Sanselme,Santha'08]

Non-linear hidden structure problems

HIDDEN POLYNOMIAL PROBLEM $\mathrm{HPP}(\mathbb{F}_q)$

Oracle Input: A function $f : \mathbb{F}_q^n \to S$

Promise: For some n-variate polynomial $\mathcal{P}$ of degree d over $\mathbb{F}_q$,

$$f(x) = f(y) \iff \mathcal{P}(x) = \mathcal{P}(y).$$

Output: $\mathcal{P}$.

HIDDEN QUADRATIC POLYNOMIAL PROBLEM $\mathrm{HQPP}(\mathbb{F}_q, n, d)$

Oracle Input: A function $f : \mathbb{F}_q \to S$

Promise: Let $\mathcal{P}_u(x) = x^2 - 2ux$. Then for some $u \in \mathbb{F}_q$,

$$f(x) = f(y) \iff \mathcal{P}_u(x) = \mathcal{P}_u(y),$$

Output: u.

Theorem[Childs,Schulman,Vazirani'07]: If n and d are constants, then for a $1 - o(1)$ fraction of the hidden polynomials, $\mathrm{HPP}(\mathbb{F}_q, n, d)$ has polylogarithmic query complexity.

HIDDEN POLYNOMIAL GRAPH PROBLEM $\mathrm{HPGP}(\mathbb{F}_q)$

Group actions

Definitions:

1. Permutation action of G on a set M:
$$\circ : G \times M \to M, \text{ where}$$
   - $g \circ (h \circ m) = (gh) \circ m$ for all $g, h \in G$
   - $e \circ m = m$ for the identity element e of G.
2. Stabilizer subgroup of $m \in M$:
$$G_m = \{g \in G : g \circ m = m\}$$
3. H-orbit of $m \in M$ for a subgroup H:
$$H \circ m = \{h \circ m : h \in H\}.$$

Subgroups and partitions

Notation: $(\mathcal{A}(G), \subseteq)$ is the lattice of all subgroups of G and $(\Pi(M), \leq)$ is the lattice of partitions of M

$$\begin{array}{rcl} (\mathcal{A}(G), \subseteq) & & (\Pi(M), \leq) \\ H & \to & H^* = \{H \circ m : m \in M\} \\ \pi^* = \{g \in G : \ \forall i \ \ g \circ \pi_i = \pi_i\} & \leftarrow & \pi = \{\pi_1, \ldots, \pi_\ell\} \end{array}$$

This is an order-reversing Galois connection between $(\mathcal{S}(G), \subseteq)$ and $(\Pi(M), \leq)$ (where $\pi \leq \pi'$ if π' is finer than π):

$H \leq \pi^*$ if and only if $\pi \subseteq H^*$.

Definition: The closure of H is H^{**}, and H is closed if $H = H^{**}$.

Facts:

- $H \subseteq H^{**}$
- H is closed if and only if $H = \pi^*$ for some partition π.

Subgroups and partitions: examples

1. Conjugation action: $G, M = G, g \circ h = ghg^{-1}$

   $H = \{e\} \implies H^* = \text{Equality} \implies H^{**} = Z(G)$

2. $G = S_n$, $M =$ labelled graphs on n vertices, $\sigma \circ G = \sigma(G)$

   $\pi =$ Total $\implies \pi^* = S_n \implies \pi^{**} =$ Isomorphism types

3. General affine group: invertible affine transformations over $\mathbb{F}_q$

$$\mathrm{Aff}_q = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\}.$$

   Natural action over $\mathbb{F}_q$:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} ax + b \\ 1 \end{pmatrix}.$$

   The stabilizer of $m \in \mathbb{F}_q$:

$$G_m = \left\{ \begin{pmatrix} a & (1-a)m \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_q^* \right\}.$$

   $G_m^* = \{\{m\}, \{x \in \mathbb{F}_q : x \neq m\}\}$ since

$$ax + (1-a)m = y \iff x = m + a^{-1}(y - m).$$

   $G_m = G_m^{**}$ is closed

Hidden symmetry subgroup problem

Hidden Symmetry Subgroup Problem

HSSP$(G, M, \circ; \mathcal{H})$, where G finite, $\mathcal{H}$ a set of closed subgroups

Oracle Input: A function $f : M \to S$

Promise: For some subgroup $H \in \mathcal{H}$, we have

$$f(x) = f(y) \iff H \circ x = H \circ y.$$

Output: H.

Remarks:

- For an arbitrary f there can be no or several subgroups H whose orbits are π_f
- Our promise: π_f is closed and $\pi_f^* \in \mathcal{H}$
- More general problem: Without any promise find π_f^*.
- HSP is a special case of HSSP for $M = G$ and $g \circ h = gh$

HSSP can have exponential query complexity

Theorem: The query complexity of $\mathrm{HSSP}(\mathrm{Aff}_q, \mathbb{F}_q, \circ, \mathcal{S})$ is $\Omega(q^{1/2})$, where $\mathcal{S} = \{G_m : m \in \mathbb{F}_q\}$.

Proof: Grover's search over $\mathbb{F}_q$ is trivially reducible to this HSSP. Recall that

$$G_m = \left\{ \begin{pmatrix} a & (1-a)m \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_q^* \right\},$$

and

$$G_m^* = \{\{m\}, \{x \in \mathbb{F}_q : x \neq m\}\}.$$

These are exactly the level sets of the Grover oracle $f_m(x) = \delta_{m,x}$.

If $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ generates G_m then $m = (1-a)^{-1}b$.

Reduction scheme of HSSP to HSP

Suppose $f : M \to S$ hides $H \leq G$ by symmetries.
How to construct $f_{\mathrm{HSP}} : G \to S$, which hides H?

Natural idea: Pick $B = \{m_1, \ldots, m_t\} \subseteq M$ and define

$$f_{\mathrm{HSP}}(g) = (f(g \circ m_1), \ldots, f(g \circ m_t)).$$

For $\{e\}$ it works if $\bigcap_{i=1}^{t} G_{m_i} = \{e\}$.
In general $\bigcap_{m \in B} HG_m = H$ is necessary.

Definition: B is an H-strong base if for every $g \in G$, we have

$$\bigcap_{m \in B} HG_{g \circ m} = H.$$

B is $\mathcal{H}$-strong for a family of subgroups if it is H-strong for $H \in \mathcal{H}$.

Lemma: If $f : M \to S$ hides some $H \in \mathcal{H}$ by symmetries and $B = \{m_1, \ldots, m_t\}$ is $\mathcal{H}$-strong, then H is hidden by f_{HSP}.

Remark M is strong for closed subgroups: $\bigcap_{m \in M} HG_m = H^{**}$.

Affine groups

The general affine group Aff_q is the semi-direct product $\mathbb{F}_q \rtimes \mathbb{F}_q^*$:

$$(b, a)(b', a') = (ab' + b, aa')$$

Definition For $\{1\} < H \leq \mathbb{F}_q^*$ let

$$G = \mathrm{Aff}_q(H) = \mathbb{F}_q \rtimes H.$$

The stabilizer of 0 is

$$G_0 = \{(0, a) : a \in H\} \cong H,$$

and its conjugates are the other stabilizers, for $m \in \mathbb{F}_q$:

$$G_m = (m, 1)G_0(-m, 1).$$

We consider the family of stabilizer subgroups of G:

$$\mathcal{S} = \{G_m : m \in \mathbb{F}_q\}$$

Aff_q doesn't have polynomial size $\mathcal{S}$-strong base.

Theorem: Let $G = \mathrm{Aff}_q(H)$ such that $H < \mathbb{F}_q^*$. If $B \subseteq \mathbb{F}_q$ is a uniformly random set of size $\Theta(\log q \cdot \log 1/\epsilon)$ then B is a $\mathcal{S}$-strong base with probability of at least $1 - \epsilon$.

Remark: The same is true in Frobenius groups for the Frobenius complements.

Small bases in affine groups

Outline of proof: Since $\mathcal{S}$ consists of H-conjugate subgroups, it suffices to show that B is H-strong.
For $b \neq b' \in \mathbb{F}_q$ we say that $m \in \mathbb{F}_q$ separates b and b' if

$$b' \circ m \notin H \circ (b \circ m).$$

Lemma 1: B is an H-strong base $\iff$ for all $b \neq b' \in \mathbb{F}_q$ there exists $m \in B$ which separates b and b'.

Lemma 2: For all $b \neq b' \in \mathbb{F}_q$ we have

$$|\{m \in \mathbb{F}_q : m \text{ does not separate } b \text{ and } b'\}| < q/2.$$

Proof: If m does not separate $b \neq b'$ then $\exists\ a_m \neq 1 \in H$ such that

$$b' + m = a_m(b + m).$$

For $m \neq m'$ we have $a_m \neq a_{m'}$ since otherwise

$$b' + m' = a_m(b + m')$$

which implies $a_m = 1$. Therefore

$$|\{m \in \mathbb{F}_q : m \text{ does not separate } b \text{ and } b'\}| \leq |H| - 1 < q/2.$$

The rest is just counting.

Efficient solution for the HSSP in some affine groups

Theorem: Let $H \leq \mathbb{F}_q^*$ such that $1 < |H| < q-1$. Then the following results hold for $\mathrm{HSSP}(\mathrm{Aff}_q(H), \mathbb{F}_q, \circ, \mathcal{S})$:

1. It has polynomial quantum query complexity.
2. It can be solved in quantum polynomial time when $q = p$ is prime and $|H| = \Omega(p/\mathrm{polylog}(p))$.
3. It can be solved in quantum polynomial time when $q = p^n$ is the power of a fixed prime p.

Proof: By the reduction scheme to $\mathrm{HSP}(\mathrm{Aff}_q(H), \mathcal{S})$.

Special case: Generalized dihedral group, for $p \neq 2$

$$\mathrm{Aff}_{p^n}(\{\pm 1\}) \cong \mathbb{Z}_p^n \rtimes \mathbb{Z}_2$$

HQPP and HSSP in generalized dihedral groups

Theorem: $\mathrm{HQPP}(\mathbb{F}_q)$ and $\mathrm{HSSP}(\mathrm{Aff}_q(\{\pm 1\}), \mathbb{F}_q, \circ, \mathcal{S})$ are polynomially equivalent.

Proof: The level sets of $\mathcal{P}_u(x) = x^2 - 2ux$ are $\{x, -x + 2u\}$ since

$$x^2 - 2ux = y^2 - 2uy$$

exactly when $y \in \{x, -x + 2u\}$.

The $G_u = \{(0,1)(2u,-1)\}$-orbits: $G_u^* = \{\{x, -x + 2u\} : x \in \mathbb{F}_q\}$

Therefore

$$\begin{aligned} f \text{ hides } \mathcal{P}_u &\iff \pi_f = G_u^* \\ &\iff \pi_f^* = G_u \\ &\iff f \text{ hides } G_u. \end{aligned}$$

Theorem $\mathrm{HQPP}(\mathbb{F}_q)$ can be solved in quantum polynomial time over fields of constant characteristic ($q = p^n$ and p constant).

Remark: $\mathrm{HQPP}(\mathbb{F}_q)$ and $\mathrm{HSP}(\mathrm{Aff}_q(\{\pm 1\}), \mathcal{S})$ are equivalent.

Multivariate quadratic polynomials

Theorem: $\mathrm{HPP}(\mathbb{F}_q, n, 2)$ can be computed in time $(n + \log q)^{O(1)}$ using an oracle for $\mathrm{HQPP}(\mathbb{F}_q)$.

Classical reduction

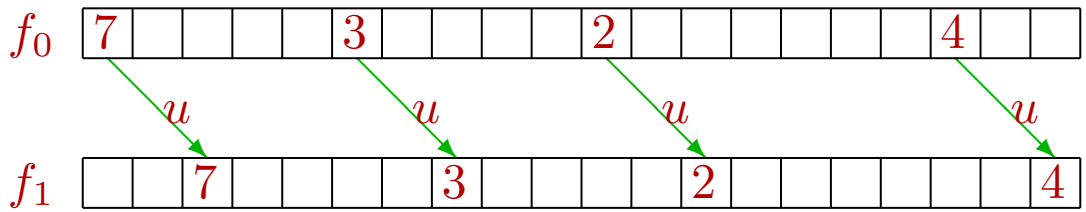
Corollary:$\mathrm{HPP}(\mathbb{F}_q, n, 2)$ can be solved by a polynomial time quantum algorithm if q is a power of a fixed prime.

Input: G finite group.

$f_0, f_1 : G \to S$ injective functions having a translation $u \in G$:

$$\forall x \in G, \quad f_0(x) = f_1(xu).$$

Output: u.



Theorem. [Ettinger-Høyer'00]. If G finite Abelian group then HIDDEN TRANSLATION on $G \simeq$ HIDDEN SUBGROUP on $G \rtimes \mathbb{Z}_2$.

Group operation on $G \rtimes \mathbb{Z}_2$: $(x_1, b_1) \cdot (x_2, b_2) = (x_1 + (-1)^{b_1} x_2, b_1 \oplus b_2)$.

Fact. $f(x, b) = f_b(x)$ hides $H = \{(0, 0); (u, 1)\}$ on $G \rtimes \mathbb{Z}_2$.

Theorem. For every prime p, HIDDEN TRANSLATION can be solved on $\mathbb{Z}_p^n$ by a quantum algorithm with query complexity $O(p(n+p)^{p-1})$ and time complexity $(n+p)^{O(p)}$.

Idea of [EH'00]: Apply QFT on the direct product $\mathbb{Z}_p^n \times \mathbb{Z}_2$.

State: $\frac{1}{2p^n} \sum_{x\in\mathbb{Z}_p^n} \sum_{b=0}^{1} \sum_{y\in\mathbb{Z}_p^n} \sum_{c=0}^{1} \omega_p^{x\cdot y}(-1)^{bc}|y\rangle|c\rangle|f_b(x)\rangle$

Rewrite using the hidden translation:

$$\frac{1}{2p^n} \sum_{x\in\mathbb{Z}_p^n} \sum_{y\in\mathbb{Z}_p^n} \sum_{c=0}^{1} \left(\omega_p^{x\cdot y} + \omega_p^{(x+u)\cdot y}(-1)^c\right)|y\rangle|c\rangle|f_0(x)\rangle$$

For all x, y the amplitude of $|y\rangle|1\rangle|f_0(x)\rangle$ is:

$$\frac{1}{2p^n}\omega_p^{x\cdot y}(1-\omega_p^{y\cdot u})$$

After observation:

$$\Pr[\text{output} = (y,1)] = \frac{1}{4p^{2n}}|1-\omega_p^{y\cdot u}|^2.$$

Properties of the output distribution:

- $\Pr[c=1] = \frac{1}{2}$
- depends only on $y\cdot u$
- for every $(y,1)$ observed: $y\cdot u \neq 0 \mod p$.

Sample $(y, 1)$ such that $y \cdot u \neq 0 \mod p$ (*i.e.* $y \notin u^{\perp}$)

Linear inequations $\mapsto$ polynomial equations

$$y \cdot u \neq 0 \mod p \iff (y \cdot u)^{p-1} = 1 \mod p$$

Fact. Solving polynomial equations is NP-complete.

Idea: 'Linearize' the system in the symmetric power of $\mathbb{Z}_p^n$

Definition. $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ is the vector space of homogeneous polynomials in n-variables of degree $(p-1)$ over $\mathbb{Z}_p$.

- A basis: Monomials of degree $(p-1)$
- Dimension: $\binom{n+p-2}{p-1}$

Transfer from $\mathbb{Z}_p^n$ via $(\mathbb{Z}_p^n)^*$ to $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$:

Definition. For $y = (a_1, \ldots, a_n) \in \mathbb{Z}_p^n$ let $y^{(p-1)} = (\sum_j a_j x_j)^{p-1}$.

$$y \cdot u \neq 0 \mod p \implies y^{(p-1)} \cdot u^* = (y \cdot u)^{p-1} = 1 \mod p,$$

where in $u^* \in \mathbb{Z}_p^n$ the monomial $x_1^{e_1} \cdots x_n^{e_n}$ has coordinate $u_1^{e_1} \cdots u_n^{e_n}$.

End of the algorithm:

- Hopefully the linear system in $\mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ has unique solution
- Find the solution $U = u^*$
- Try the $(p-1)$ candidates v such that $v^* = u^*$

Example. $p = 3$, $n = 3$, $u = (1, 2, 0)$.

Sample in $\mathbb{Z}_3^3$	Inequation in $\mathbb{Z}_3^3$	Equation in $\mathbb{Z}_3^{(2)}[x_1, x_2, x_3]$
$y_1 = (0, 1, 0)$	$x_2 \cdot u \neq 0$	$x_2^2 \cdot U = 1$
$y_2 = (0, 2, 1)$	$(2x_2 + x_3) \cdot u \neq 0$	$(x_2^2 + x_3^2 + x_2 x_3) \cdot U = 1$
$y_3 = (0, 2, 2)$	$(2x_2 + 2x_3) \cdot u \neq 0$	$(x_2^2 + x_3^2 + 2x_2 x_3) \cdot U = 1$
$\vdots$	$\vdots$	$\vdots$

where $x_1 = (1, 0, 0)$, $x_2 = (0, 1, 0)$, $x_3 = (0, 0, 1)$,
$x_1^2 = (1, 0, 0, 0, 0, 0)$, $\ldots$

System of full rank $\implies$ unique solution $U = x_1^2 + x_2^2 + 2x_1 x_2$.
Try the 2 possible translations $(1, 2, 0)$ and $(2, 1, 0) \rightsquigarrow u = (1, 2, 0)$.

Translation finding$^f(\mathbb{Z}_p^n)$

0. If $f_0(0) = f_1(0)$ then return 0.
1. $N \leftarrow 13p\binom{n+p-2}{p-1}$.

2. For $i = 1, \ldots, N$ do $(z_i, b_i) \leftarrow$ **Fourier sampling**$^f(\mathbb{Z}_p^n \times \mathbb{Z}_2)$.
3. $\{y_1, \ldots, y_m\} \leftarrow \{z_i : b_i = 1\}$.

4. For $i = 1, \ldots, m$ do $Y_i \leftarrow y_i^{(p-1)}$.
5. Solve $Y_1 \cdot U = 1, \ldots, Y_m \cdot U = 1$.
6. If several solutions then abort.

7. Let j be such that the coefficient of x_j^{p-1} in U is 1.
8. Let $v \in \mathbb{Z}_p^n$ be such that $v_k v_j$ is the coefficient of $x_k x_j^{p-2}$ in U.

9. Find $0 < a < p$ such that $f_0(0) = f_1(av)$.
10. Return av.

Line Lemma. Let $L_{z,y} = \{(z+ay)^{(p-1)} : 0 \le a \le p-1\}$ for $y, z \in \mathbb{Z}_p^n$. Then $y^{(p-1)} \in \mathrm{Span}(L_{z,y})$.

Proof. Let $M_{z,y} = \{\binom{p-1}{k} z^{(k)} y^{(p-1-k)} : 0 \le k \le p-1\}$.
Claim: $\mathrm{Span}(L_{z,y}) = \mathrm{Span}(M_{z,y})$.

	$z^{(p-1)}$	$(z+y)^{(p-1)}$	$(z+2y)^{(p-1)}$	$\dots$	$(z+(p-1)y)^{(p-1)}$
$\binom{p-1}{0} z^{(p-1)}$	1	1	1	$\dots$	1
$\binom{p-1}{1} z^{(p-2)} y^{(1)}$	0	1	2	$\dots$	$(p-1)$
$\binom{p-1}{2} z^{(p-3)} y^{(2)}$	0	1	2^2	$\dots$	$(p-1)^2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
$\binom{p-1}{p-1} y^{(p-1)}$	0	1	$(p-1)^2$	$\dots$	$(p-1)^{(p-1)}$

Corollary. $\mathbb{Z}_p^{(p-1)}[x_1, \dots, x_n]$ is spanned by $\{y^{(p-1)} : y \in \mathbb{Z}_p^n\}$.

Lemma. Let $W \leq \mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ and $R = \{y \in \mathbb{Z}_p^n : y^{(p-1)} \in W\}$.
Set $V_k = \{y \in \mathbb{Z}_p^n : y \cdot u = k\}$, and $R_k = R \cap V_k$.
If $W \neq \mathbb{Z}_p^{(p-1)}[x_1, \ldots, x_n]$ then $\frac{|R_k|}{|V_k|} \leq \frac{p-1}{p}$ for $k = 1, \ldots, p-1$.

Proof. Corollary $\implies R \neq \mathbb{Z}_p^n$.
Case 1: $R_0 = V_0$. Then $R_k \neq V_k$ for $k = 1, \ldots, p-1$. Let $y \in V_1 - R_1$.
Line Lemma $\implies$ in each coset of $<y>$ an element is outside R.

	$<y>$	$\ldots$	$z + <y>$	$\ldots$
V_0	0	$\ldots$	z	$\ldots$
V_1	y	$\ldots$	$z + y$	$\ldots$
$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$
V_{p-1}	$(p-1)y$	$\ldots$	$z + (p-1)y$	$\ldots$

$\implies \frac{|R|}{|Z_p^n|} \leq \frac{p-2}{p-1} \implies \frac{|R_k|}{|V_k|} \leq \frac{p-2}{p-1}$.

Case 2: $R_0 \neq V_0$. Let $y \in V_0 - R_0$, then V_k is union of cosets of $<y>$.
Line Lemma $\implies \frac{|R_k|}{|V_k|} \leq \frac{p-1}{p}$.

Non-linear hidden structure problems

HIDDEN POLYNOMIAL GRAPH PROBLEM $\mathrm{HPGP}(\mathbb{F}_q)$

Oracle Input: A function $f : \mathbb{F}_q^n \times \mathbb{F}_q \to S$

Promise: For some n-variate polynomial Q of degree d over $\mathbb{F}_q$,

$$f(x, y) = f(x', y') \iff y - Q(x) = y' - Q(x').$$

Output: Q.

Theorem[Decker, Draisma and Wocjan'09]:

- For every d and for every constant n, $\mathrm{HPGP}(\mathbb{F}_q, n, d)$ can be reduced in polynomial time to $\mathrm{HPGP}(\mathbb{F}_q, 1, d)$.
- For every d there exists a finite set E_d of primes such that when d is constant and the characteristic of $\mathbb{F}_q$ is not from E_d then $\mathrm{HPGP}(\mathbb{F}_q, 1, d)$ can be solved in quantum polynomial time.

Function graph groups

Consider $n = 1$ and $q = p$. Level sets of $f : \mathbb{F}_p \times \mathbb{F}_p \to S$:

$$f(x, y) = f(x', y') \iff \exists t \in \mathbb{Z}_p : \ (x', y') = (x + t, y + Q(x + t) - Q(x)).$$

Let $\mathbb{F}_p^{(d)}[x]$ be the group of univariate polynomials of degree d.

Definitions Shift map a_t, for every $t \in \mathbb{Z}_p$:

$$(a_t Q)(x) = Q(x - t).$$

Function graph group $\mathrm{Fg}(\mathbb{F}_p^{(d)}[x])$: semidirect product

$$\mathrm{Fg}(\mathbb{F}_p^{(d)}[x]) \rtimes_{t \mapsto a_t} \mathbb{Z}_p.$$

Multiplication rule:

$$(Q_1, t_1)(Q_2, t_2) = (Q_1 + a_{t_1} Q_2, t_1 + t_2).$$

Shifting action $\circ$ of $\mathrm{Fg}(\mathbb{F}_p^{(d)}[x])$ on $M = \mathbb{Z}_p \times \mathbb{Z}_p$:

$$(Q, t) \circ (x, y) = (x + t, y + Q(x + t)).$$

Standard complements: Conjugates of $\{(0, t) : t \in \mathbb{Z}_p\}$ by $(Q, 0)$:

$$A_Q = \{(Q - a_t Q, t) : t \in \mathbb{Z}_p\}.$$

Claim: Level sets of f hiding Q are the orbits of A_Q.

Results for HPGP

Lemma: There exists an easily computable basis of size $d+1$ for

$$\mathcal{H} = \{A_Q : Q \in \mathbb{F}_q^{(d)}[x]\}.$$

Theorem: For n and d constants, and for fixed characteristic, $\mathrm{HPGP}(\mathbb{F}_q, n, d)$ can be solved in quantum polynomial time.

Conclusion

- This work:
  - A new paradigm: HSSP
  - Generic reduction to HSP
  - HPP and HPGP are reducible to HSSP

- Open problems:
  - Multivariate HPP of higher degree
  - Study of HSP inspired by HSSP
  - Find for $\mathrm{HSP}(\mathbb{Z}_p^n \rtimes \mathbb{Z}_2)$ quantum algorithm polynomial in n and p.