Unusual System Solving in Quantum Algorithms

Gábor Ivanyos
MTA SZTAKI

3rd de Brún Workshop, Galway, 30 November–10 December, 2009.

Contents

1. Introduction
2. Relaxed systems in quantum algorithms
   - Original systems
   - Examples in quantum algorithms
   - The relaxed systems
3. HSP and the Chevalley-Warning theorem
   - HSP in 2-step nilpotent groups of
   - The equations
   - Comparison with Chevalley's theorem
4. Unsolving
   - Hidden shift
   - Random linear disequations
   - Disequations and polynomials

Introduction

- Quantum computers can
  - factor integers
  - compute discrete log

  in polynomial time by Shor (1994).
- The approach can be formulated in terms of **HSP**.
- HSP also captures the **Graph Isomorphism problem**
- This talk: less usual computational algebraic tasks

  in quantum algorithms for the HSP and related problems

HSP - the hidden subgroup problem

- G (finite) group
- $f : G \longrightarrow \{\text{objects}\}$ **hides** the subgroup $H \leq G$, if

  $f(x) = f(y) \Leftrightarrow xH = yH$

  i.e., x and y are in the same left coset of H.

  f is constant on the left cosets of H and takes different values on different cosets
- f given by an oracle (or an efficient algorithm) for

  $x \mapsto f(x)$ in quantum: $|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle)$
- Task: find (generators for) H.

HSP - an example

- $b : V \otimes V \to W$ linear
- $G = \mathrm{GL}(V) \times \mathrm{GL}(W)$
- $f(g, h) = b^{(g,h)}$, where
- $b^{(g,h)}(u, v) = h^{-1} \cdot b(g \cdot u, g \cdot v)$
- $H =$

$$\{(g, h) | b(g \cdot u, g \cdot v) = h \cdot b(u, v)\} = \psi \mathrm{Isom}(b)$$

- In general: stabilizers

Outline

1. Introduction

Outline

1. Introduction
2. Relaxed systems in quantum algorithms
   - Original systems
   - Examples in quantum algorithms
   - The relaxed systems

Outline

1. Introduction
2. Relaxed systems in quantum algorithms
   - Original systems
   - Examples in quantum algorithms
   - The relaxed systems
3. HSP and the Chevalley-Warning theorem
   - HSP in 2-step nilpotent groups of
   - The equations
   - Comparison with Chevalley's theorem

Outline

1. Introduction
2. Relaxed systems in quantum algorithms
   - Original systems
   - Examples in quantum algorithms
   - The relaxed systems
3. HSP and the Chevalley-Warning theorem
   - HSP in 2-step nilpotent groups of
   - The equations
   - Comparison with Chevalley's theorem
4. Unsolving
   - Hidden shift
   - Random linear disequations
   - Disequations and polynomials

Contents

1 Introduction

2 Relaxed systems in quantum algorithms
- Original systems
- Examples in quantum algorithms
- The relaxed systems

3 HSP and the Chevalley-Warning theorem
- HSP in 2-step nilpotent groups of
- The equations
- Comparison with Chevalley's theorem

4 Unsolving
- Hidden shift
- Random linear disequations
- Disequations and polynomials

Original systems

- Polynomial matrix

$$Q(t) = (f_{ij}(t)) \in \mathbb{F}[t]^{n\times m}$$

  - variable(s) t: $t = (\tau_1, \dots, \tau_k)^T$ (this talk $k = 1$)
  - $Q(0) = 0$ (i.e., $f_{ij}(0) = 0$)
- Also given $y = (y_1, \dots, y_m)^T \in \mathbb{F}^m$, $z = (z_1, \dots, z_n)^T \in \mathbb{F}^n$
- Solve equation $Q(t)y = z$:
  - list $t \in \mathbb{F}^k$ s.t.

$$\sum_{j=1}^{m} f_{ij}(t)y_j = z_i, \ (i = 1, \dots, n)$$

- Spec case: $m = 1$, $y = 1$: $f_i(t) = z_i$ (usual systems)

Examples in quantum algorithms

- Hidden polynomial (Decker, Draisma, Wocjan 2009)
  $m = 1$, $Q(t) = (t, t^2, \ldots, t^n)^T$ (n constant, field $\mathbb{F}_q$, $q \to \infty$)
- HSP in Heisenberg group order p^3 (Bacon, Childs, van Dam 2005)
  - Remark: Lazard-correspondence
    $$G = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$
    $m = n = 2$, (field $\mathbb{F}_p$, $p \to \infty$) $Q(t) = \begin{pmatrix} t & \frac{t(t-1)}{2} \\ 0 & t \end{pmatrix}$
  - similar for $G = \mathbb{Z}_p^n \rtimes \mathbb{Z}_p$ (constant n) (BCvD 2005)

The relaxed systems

- Original: $Q(t)y = z$
- Relaxation: can choose ℓ, $t \to T = (t_1, \ldots, t_\ell)^T$,
  $y \to Y = (y^1, \ldots, y^\ell)^T, \; y_i \to (y_i^1, \ldots, y_i^\ell)$
- Relaxed system:

$$\sum_{j=1}^{\ell} Q(t_j)y^j = z,$$

$$\begin{pmatrix} Q(t_1) & Q(t_2) & \ldots & Q(t_\ell) \end{pmatrix} \begin{pmatrix} y^1 \\ y^2 \\ \vdots \\ y^\ell \end{pmatrix} = z,$$

$$\sum_{j=1}^{\ell} \sum_{s=1}^{m} f_{is}(t_j) y_s^j = z_i, \quad (i = 1, \ldots, n).$$

Requirements

- Should be able to solve relaxed system
  - for reasonably many pairs Y, z
  - s.t. #solutions reasonably close to average
- In the examples $\ell = n$ (#vars = #eqs, generically zero-dim)
  - hidden polynomial

$$\begin{pmatrix} t_1 & t_2 & \dots & t_n \\ t_1^2 & t_2^2 & \dots & t_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ t_1^n & t_2^2 & \dots & t_n^n \end{pmatrix} \begin{pmatrix} y^1 \\ y^2 \\ \vdots \\ y^n \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix}$$

  - Heisenberg HSP

$$\begin{pmatrix} t_1 & \frac{t_1(t_1-1)}{2} & t_2 & \frac{t_2(t_2-1)}{2} \\ 0 & t_1 & 0 & t_2 \end{pmatrix} \begin{pmatrix} y_1^1 \\ y_2^1 \\ y_1^2 \\ y_2^2 \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$

Results for examples and open problems

- In the examples

  for a constant fraction of pairs
  - $0 < \#$solutions $<$ const
  - efficiently (time $\mathrm{poly}\log q$) listed
  - (except: Hidden polynomial in bad characteristics)
- Open problems:
  - Hidden polynomial in bad characteristics
  - Further applications ?

Contents

1. Introduction
2. Relaxed systems in quantum algorithms
   - Original systems
   - Examples in quantum algorithms
   - The relaxed systems
3. HSP and the Chevalley-Warning theorem
   - HSP in 2-step nilpotent groups of
   - The equations
   - Comparison with Chevalley's theorem
4. Unsolving
   - Hidden shift
   - Random linear disequations
   - Disequations and polynomials

HSP in 2-step nilpotent groups

Result from ∼, Sanselme, Santha (2008)

- G Nilpotent of class 2: $G' \leq Z(G)$
- Interesting instances:
  - G p-group of exponent p
  - $|H| = p$
- Special case: Heisenberg group
- Strategy:
  1. Find HG'
  2. Abelian HSP in HG'
- For (1), need: sampling from irreps of G/G'
- Have: random irreps of G

Sampling for finding HG'

- Secret: $X \in \mathbb{C}G$ hidden subgroup state
- Sampling: $\rho(X)$, ρ representation of G
- For HG' need: $\rho(X)$ for random one-dimensional irreps.
- Have $\rho(X)$ for typically $>$ 1-dim irreps
- Idea: tensor product of irreps may become
  multiple of regular rep of G/G'
- Can also use twists for "tuning".

Twists

- Useful endomorphisms
$$\sigma^j(x) = x^{j^2} \text{ for } x \in G'.$$
- Have $\rho_1, \ldots, \rho_\ell > 1$-dim. irreps of G
- find $j_1, \ldots, j_\ell$ not all 0 s.t.:

$$R = \rho_1\sigma^{j_1} \otimes \cdots \otimes \rho_\ell\sigma^{j_\ell}$$

$$R_{|G'} = \text{identity}$$

- Decomposing $R \longrightarrow$ sample from irresp of G/G'
- system of $\log_p |G'|$ linear equations in $j_1^2, \ldots, j_r^2$
- $+$ have some lin. eq's in $j_1, \ldots, j_r$ (technical)

The equations

- $A = (a_{ij}) \in \mathbb{F}_p^{n\times\ell}$
- Find nonzero $x = (x_1, \dots, x_\ell)^T \in \mathbb{F}^\ell$:

$$\sum_{j=1}^{\ell} a_{ik} x_k^2 = 0 \ \ (i = 1, \dots, n)$$

  - $x_k \leftrightarrow j_k$
  - ρ_k on $G' \leftrightarrow (a_{1k}, \dots, a_{nk}) \in \mathrm{Hom}(G' \mapsto \mathbb{F}_p)$
- similar to relaxed systems:

  we can choose ℓ

  main difference: only one solution enough
- Result: efficient solution for $n \to \infty$

Efficient solution

- Result If $\ell \geq \frac{n(n+1)}{2}$, then

  a nonzero solution to

$$\sum_{j=1}^{\ell} a_{ij}x_j^2 = 0 \quad (i = 1, \ldots, n)$$

  found in time poly$(n + \ell)$

- Method: induction (recursion) in n

  using Gaussain elimination

The recursion

- Gaussian elimination

  $+$ solving 1-2 quadratic equations in 1-2 vars
- Eliminates first $n+1$ coefficients from $n-1$ equations
- Leaves only 2 nonzero of the first $n+1$ coeffs

  in one equation
- Solve the $n-1$ equations by recursion
- Substitute recursive solution

  in the remaining equation
- Becomes solve 2-variate
- Need quadratic non-residue in $\mathbb{F}$
- de Woestijne (2008) has unconditional deterministic version for $\ell \geq \frac{n(n+3)}{2}$

Allowing linear equations

- if $\ell \geq (m+1)\frac{n(n+1)}{2}$ then

$$\sum_{j=1}^{\ell} a_{ij}x_j^2 = 0 \;\; (i = 1, \ldots, n)$$

$$\sum_{j=1}^{\ell} b_{ij}x_j = 0 \;\; (i = 1, \ldots, m)$$

efficiently solvable.

- Method: replace quadratic part with $(m+1)n$ equations

  variables partitioned into $m+1$ blocks

Have $m+1$-dimensional space of solution of the quadratic part

Comparison with Chevalley's theorem

- Extension: n (at most) quadratic eq's with 0 constant term

  in $\ell \geq n(n+1)^2$ variables

  a nonzero solution found in time $poly(n\ell)$
- Chevalley's theorem
  - ℓ variables n polynomials with 0 constant term
  - degrees $d_1, \dots, d_n$
  - if $\ell > \sum_{i=1}^{n} d_i$ then $\exists$ nonzero solution

Comparison with Chevalley's theorem 2

- Presented result
  - polynomial time version of Chevalley for $d_i \leq 2$, $\ell = \Omega(n^3)$
  - Chevalley grants solution for $\ell = \Omega(n)$
- **Open problems:** poly time solution
  - for $\ell = \Omega(n)$ or $\ell = \Omega(n^2)$?
  - for $\ell = \text{poly}(n)$ in other degrees?
  - already $\sum a_{ij} x_j^3$ (HSP in certain class 3 groups)
  - average case ????

Eliminating linear and mixed terms

n at most quadratic equations in ℓ variables

eliminate mixed terms containing N variables

by substituting linear terms into $\leq N$ other variables
e.g. $\sum_{j=1}^{s} \alpha_{1j} x_1 x_{i_j}$: $x_{i_1} \leftarrow -\alpha_{1j}^{-1} \sum_{j=2}^{s} \alpha_{1j} x_1 x_{i_j}$
need $\ell \geq 2N$

set remaining variables to zero

eliminate linear terms

by adding $\leq n$ linear equations

Result:

$\leq n$ diagonal quadratic $\leq n$ linear equations in N variables

efficiently solvable if $N \geq \frac{n(n+1)^2}{2}$

means $\ell \geq n(n+1)^2$.

Contents

1. Introduction
2. Relaxed systems in quantum algorithms
   - Original systems
   - Examples in quantum algorithms
   - The relaxed systems
3. HSP and the Chevalley-Warning theorem
   - HSP in 2-step nilpotent groups of
   - The equations
   - Comparison with Chevalley's theorem
4. Unsolving
   - Hidden shift
   - Random linear disequations
   - Disequations and polynomials

Hidden shift

- In this part: #variables fixed,

  draw random (dis)equations until unsoluble.

- **Hidden shift**

  Given f_0, f_1 : finite abelian group $G \longrightarrow$ finite set X such that

  f_0, f_1 are injective, and
  $\exists u \in G$ s.t.

  $$f_1(x) = f_0(x+u); \quad \text{for every } x \in G.$$

  Task: find u

Background

- an important induction tool for HSP
- itself a HSP in $G \rtimes \mathbb{Z}_2$

  $\mathbb{Z}_2$ acts on G by flipping sign
- polynomial quantum query complexity
- Kuperberg (2005) in time $2^{O(\sqrt{\ell})}$ where $\ell = \log |G|$.
- Friedl, $\sim$, Magniez, Santha, Sen 2003 in time $\ell^{O(rp_r \log p_r)}$,

  the exponent of G is $p_1 \cdots p_r$, with primes $p_1 \leq p_2 \ldots \leq p_r$.
- implies quasi-polynomial quantum complexity of the HSP in solvable groups of constant exponent.

Reduction to systems of linear disequations

- $G = \mathbb{Z}_p^n$
- Strategy
  (1) Find the "direction" of u: subgroup $\langle u \rangle$
  (2) Find u in $\langle u \rangle$
- In (1), so-called Fourier Sampling gives
  random $v \in \mathbb{Z}_p^n \setminus u^\perp$
  (nearly) uniform distribution

Random linear disequations

- Search version:
  - Can query samples of vectors from $\mathbb{Z}_p^n \setminus u^\perp$
  - (nearly) uniformly
  - Find direction of u
- Reducible to the **decision version:**
  - Can query samples from a distribution over $\mathbb{Z}_p^n$,
  - the distribution is either (nearly) uniform,
  - or (nearly) uniform on $\mathbb{Z}_p^n \setminus u^\perp$
    for a certain u
  - Which is the case?
- Method:

  Draw as many vectors v_i until $\bigcup v_i^\perp$ should become $\mathbb{Z}_p^n$ in the first case

Query complexity

- If the distribution is uniform, $O(np\log p)$ random linear disequations have no common solution.
  - one slope is excluded by $\approx 1/p$ of the linear disequations
  - $O(p\log 1/\epsilon)$ random disequations exclude a slope with probability at least $1-\epsilon$.
  - $O(np\log p) = O(p\log p^n)$ random exclude all the slopes with probability at least 99%.
- checking if a system of linear disequations have a solution is **NP-complete** for $p > 2$.

  Obvious reduction from 3-colorability of graphs.
- **Fortunately,** $\exists$ easier witness if $\#\mathit{equation}$ very large

Disequations and polynomials 1.

- disequations $\longrightarrow$ equations
  - $(u, w) \neq 0 \Leftrightarrow (u, w)^{p-1} = 1$

$$f(x) = f(x_1, \ldots, x_n) = (u, x)^{p-1} - 1 = \left(\sum_{i=1}^{n} u_i x_i \right)^{p-1} - 1 :$$

polynomial in $x = x_1, \ldots, x_n$ of degree at most $p - 1$.

- Reformulation of the problem
  - either uniform distribution
  - or $\exists$ a nonzero polynomial $f \in \mathbb{Z}_p[x] = \mathbb{Z}_p[x_1, \ldots, x_n]$ of degree at most $p - 1$ such that $Prob(w) = 0$ for every w s.t. $f(w) = 0$

Disequations and polynomials 2.

- $L = \{g \in \mathbb{Z}_p[x] | \deg g \leq p-1\}$ vector space
  $\dim L = O((n+p)^{p-1})$.
- $w \in \mathbb{Z}_p^n$, $\mathrm{Eval}_w : L \to \mathbb{Z}_p$ linear

$$\mathrm{Eval}_w(g) = g(w)$$

- A generalized Reed-Muller code: Image of L under

$$\bigoplus_{w \in \mathbb{Z}_p^n} \mathrm{Eval}_w$$

- For $w_1, \ldots, w_j \in \mathbb{Z}_p^n$,
  $K = K(w_1, \ldots, w_j) = \{g \in L | g(w_1) = \ldots = g(w_j) = 0\}$
  subspace of L:

$$K = \bigcap_{i=1}^{j} \ker \mathrm{Eval}_{w_i}$$

Disequations and polynomials 3.

Schwartz-Zippel lemma:

- Relative distance of the code is $\frac{p-1}{p}$:
  If $0 \neq g \in L$ then
  $Prob_w(g(w) = 0) \leq \frac{p-1}{p}$

Consequence of Schwartz-Zippel:

$w_1, \ldots, w_j \in \mathbb{Z}_p^n$, $K = \{g \in L | g(w_1) = \ldots = g(w_j) = 0\}$.
Assume that $K \neq 0$. Then

$$Prob_{w \in \mathbb{Z}_p^n}(g(w) = 0 \text{ for every } g \in K) \leq \frac{p-1}{p}.$$

(Proof: let $0 \neq g \in K$. Then $Prob_w(g(w) = 0) \leq \frac{p-1}{p}$.)

Disequations and polynomials 4.

Corollary:

When $\ell = O(p \dim L) = O(p(n+p)^{p-1})$,

in the uniform case $K_{w_1,\ldots,w_\ell} = 0$ with high prob.
Otherwise $K_{w_1,\ldots,w_\ell}$ never 0.

Disequations - the algorithm

$\ell = O(p \dim L)$, take sample $w_1 \ldots, w_\ell$.
Compute $K = \{g \in L | g(w_1) = \ldots = g(w_\ell) = 0\}$.

System of linear equations in the coefficients of g.

If $K = 0$: uniform ; If $K \neq 0$: there exists u.
Costs: Polynomial in $p \dim L = O(p(n+p)^{p-1})$.

Open problems

- Efficient generalization for $\mathbb{Z}_{p^k}^n$?
  - Existing method ($\sim$ 2008) complexity $(pnk)^{O((2p)^k))}$: poly in n, exponential in p^k.
  - Quantum algorithm for hidden shift in $\mathbb{Z}_{p_k}^n$: poly in n, exp in pk.
- Polynomial time algorithm for $\mathbb{Z}_m^n$, where m constant but not power of a prime?

  Open already for $m = 6$
- Improved algorithm for $\mathbb{Z}_p^n \longrightarrow$ progress in HSP
  - trivial method: $2^{0(n \log p)}$
  - presented method: $2^{0((\log n) p \log p)}$

Generalization to $Z_{p^k}^n$

Encoding $\mathbb{Z}_{p^k}$ by p-expansion: $Z_{p^k} \to Z_p^k$.

Digits of sum of T elements: polynomials of degree $\leq (2p-2)^{k-1}$ of the summands.

If the sample $\perp u$ then $\exists$ a polynomial $F = F_u$ in nk variables of degree at most $D = (p-1)(2p-2)^k - 1)/(2p-3) = O((2p)^k)$ s.t. every sample element is a zero of F.

Otherwise we have a nearly uniform distribution over $\mathbb{Z}_p^{nk}$.

$\sim$ Generalized Reed-Muller code of degree D, rel. distance at least $p^{\lceil D/(p-1) \rceil}$.

Sample size $O((pnk)^D = (pnk)^{O((2p)^k))}$ sufficient.

Complexity $(pnk)^{O((2p)^k))}$.