Conjugate Searching Problem vs. Hidden Subgroup Problem

Licheng Wang[1,2] and Lihua Wang[2]

1 Beijing University of Posts and Telecommunications, China
2 National Institute of Information and Communications Technology, Japan

Motivation

Whether braid-based cryptography is qualified the label of post quantum cryptography ?

Main Consideration

- CSP: plays a core role in braid-based cryptosystems.

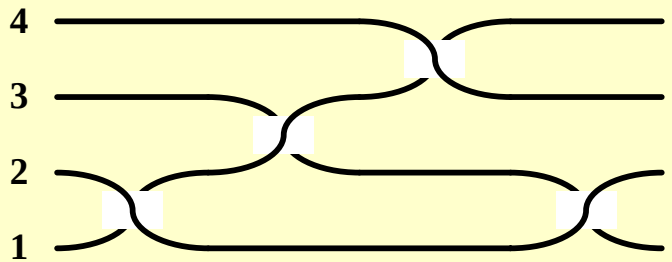
- HSP: provides a unified framework to study problems of group-theoretical nature in quantum computing.

Main Consideration (cont.)

- Complexity: Prasolov's newest negative answer for solving CSP over braid groups by using classical computers.
- Quantum Computation: Blank spot of HSP for the CSP over braid groups.
- Methodology: From braid groups to other non-commutative groups.

Braid, Braid Crypt and Assumptions

- Braid
  - Geometric illustration



  - Algebraic presentation

$$B_n = \left\langle \sigma_1,\ldots,\sigma_{n-1} \;\middle|\; \begin{array}{l} \sigma_i\sigma_j = \sigma_j\sigma_i \ \text{ if } |i-j|>1; \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \ \text{ if } |i-j|=1; \\ 1 \le i, j \le n-1. \end{array} \right\rangle$$

- Braid Crypt
  - Encrytion based on DHCP (Ko et al., 2000)
  - Encryption based on CSP (ePrint/Report 2009/566)

Conjugate searching problem (CSP)

- x~y (i.e. x conjugate y) if there exists z such that $y = z^{-1}xz$

- CSP: Find z in G such that $y = z^{-1}xz$ for a given instance (x,y) in G^2 with x~y

  (Here, G is a non-commutative group.)

DH protocol from intractable CSP

- $F_a(b) = a^{-1}ba$
  - Basic assumption: hard to extract a from $(b, F_a(b))$
- $F_{a^s}(F_{a^t}(b)) = F_{a^t}(F_{a^s}(b))$
  - Stronger assumption: hard to decide s from $(a, b, F_{a^s}(b))$ when s is large (e.g., more than 80 bits)

Can we efficiently solve CSP over braid groups by using

- classical computers?
- quantum computers?

Progress of Classical Algorithms for CSP over Braid Groups

- 1969, Garside method: Sumit Set (SS)
- 1994, ElRifai and Morton method: Super Summit Set (SSS-EM)
- 2003, Franco and Gonzalez-Meneses method: Super Summit Set (SSS-FM)
- 2005, Gebhardt method: Ultra Summit Set (USS)
- 2008, Birman, Gebhardt and Gonzalez-Meneses: We need to find a polynomial bound for the size of USS(X) when X is a rigid pseudo-Anosov braid.
- 2010, Prasolov: "Small braids having a big USS" --- a negative answer for BGM's project.

Prasolov's Results

Theorem 1: The braid $\alpha_n = \sigma_1\sigma_2^{-1}\sigma_3\sigma_4^{-1}...\sigma_n^{(-1)^{n-1}}$ on n strands is rigid and the size of its Ultra Summit Set is at least $2^{[(n-2)/2]}$.

Theorem 3: The braid α_n is pseudo-Anosov for odd number n>=3.

Theorem 2: USS of α_n in BKL presentation contains at least $2^{[(n-1)/2]}$ rigid braids for odd n.

Prasolov's Calculation: (for n=3,4,…,9)

$$|USS(\alpha_n)| = \frac{3-(-1)^n}{2} \cdot n \cdot 3^{n-3}$$

How about some heuristic attacks?

- Length based attacks
- Linear representation attacks

Both of them aim to break braid cryptosystems that are in fact not based on CSP directly.

Whether they are suite for solve CSP over braid groups? (We do not know)

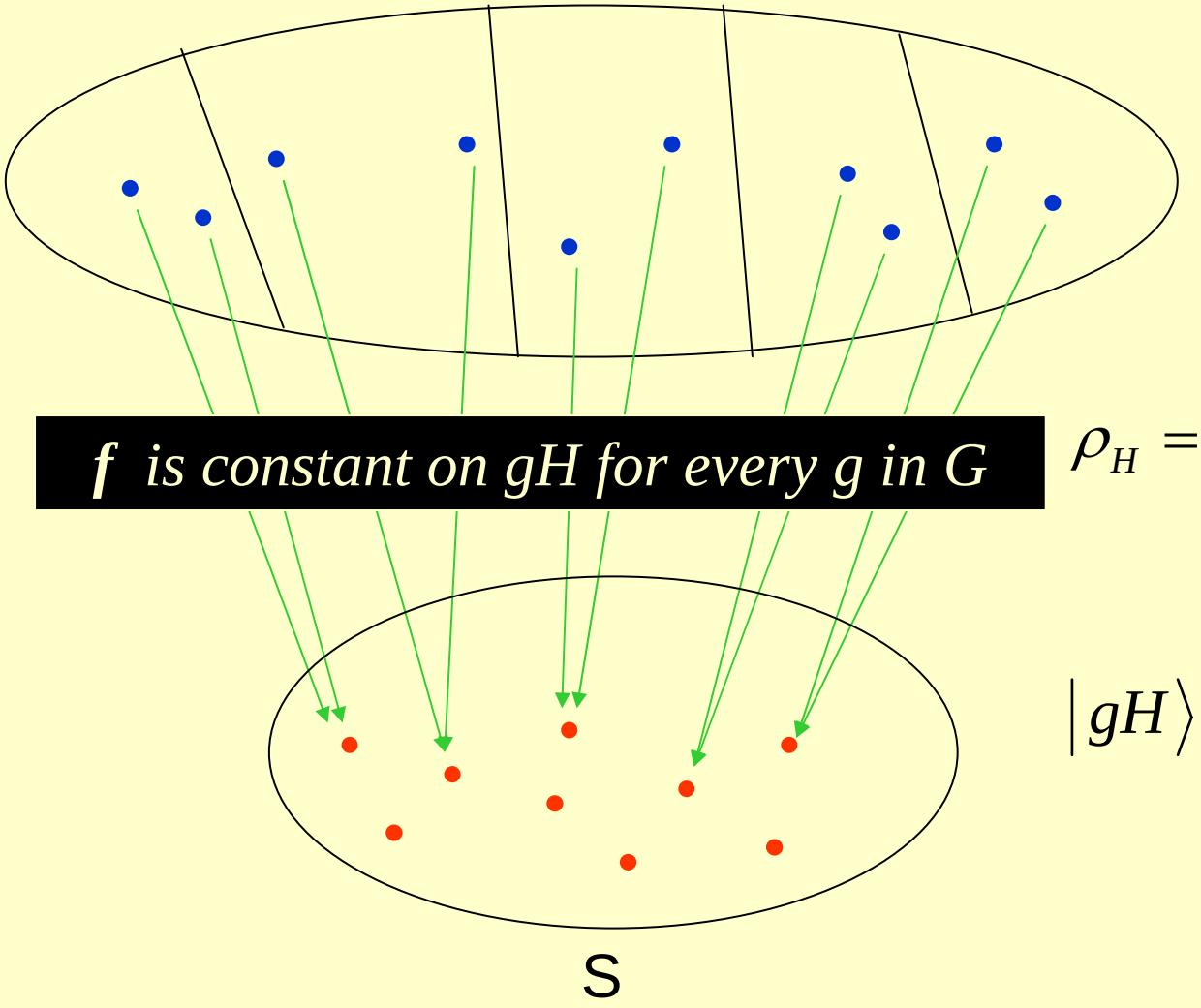
Can we solve CSP over braid groups quantumly?

Review on Quantum Algorithms

- amplitude amplification algorithms (AAA)
- hidden subgroup algorithms (HSA)

- can merely obtain polynomial speed-up ratios
- deals with the hidden subgroup problem (HSP) and has the promise to obtain exponential speed-up ratios.

HSP and Quantum HSA



H < G

f is constant on gH for every g in G

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

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

E.g.: HSP and Crypt. Problems

- [Shor'94] Factoring
  - ←Order finding: $f_y(x) := y^x \bmod N$
    - I.e., $f_y(x+r)=f_y(x)$, and the period r can be extracted using a DFT and post-processing in form of Diophatine approximation.

- [Regev'02] Reduction from $n^{\frac{1}{2}+2\varepsilon}$-GapSVP to the dihedral HSP.
  - ←Hidden reflection finding
    - A challengeing problem even for quantum computers --- the classical post-processing is very time-consuming

Quantum HSA for CSP?

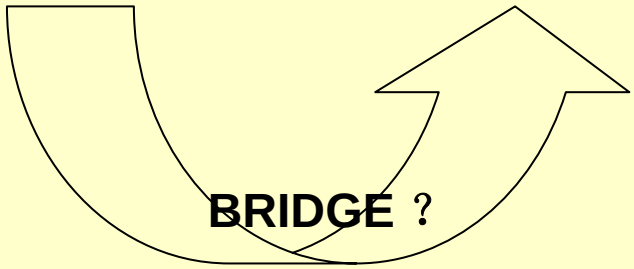
(1) Can we model CSP by using the framework of HSP?

(2) Can we solve the HSP obtained in (1) quantumly?

(3) Can we implement the quantum HSA obtained in (2) efficiently?

Map CSP to HSP ?

- Hidden Subgroup P.
  - Instance:
    - f: G→S, black-box
    - f constant on gH
  - Objective:
    - Find H
- Conjugator Search P.
  - Instance:
    - x
    - $y = zxz^{-1}$
  - Objective:
    - Find z (or z' s.t. $y=z'xz'^{-1}$)



Map CSP to HCSP⊂HSP ?

- Hidden Conjugate Subgroup P.
  - Instance:
    - f: G→S, black-box
    - H<G
    - f constant on $H^g=gHg^{-1}$
  - Objective:
    - Find H^g or.

    eq. find g

- Conjugator Search P.
  - Instance:
    - x
    - $y = zxz^{-1}$
  - Objective:
    - Find z (or z' s.t. $y=z'xz'^{-1}$)

Map CSP to HCSP⊂HSP ?

- Hidden Conjugate Subgroup P.
  - Instance:
    - f: G→S, black-box
    - H<G
    - f constant on $H^g=gHg^{-1}$
  - Objective:
    - Find H^g or.

      eq. find g

- Conjugator Search P.
  - Instance:
    - <x>
    - <y> = z<x>z^{-1}
  - Objective:
    - Find z (or z' s.t. y=z'xz'$^{-1}$)

CSP⊄ HCSP ?

⇑

Finding <y>≠ Finding z

-where if f?

-what is the obj.?

<y> is given!

Solve possible HSP in (1) ?

- We do not know how to create coset states in a braid group or in its finite sets such as $\mathrm{B}_n(l)$.

Efficient Impl. possible HSA in (2) ?

- The progress on HSP in S_n is so far dominated by negative results. (Rotteler, 2006)
- In 2009, Moore et al. speculated that HSP in the groups that contain S_n as a subgroup may be resistant to all known quantum techniques.
- There is a 1-to-1 correspondence between the set of the permutation braids in B_n and the set of the permutations in S_n.

Summary but not a conclusion

- Currently known quantum techniques cannot solve CSP over braid groups.

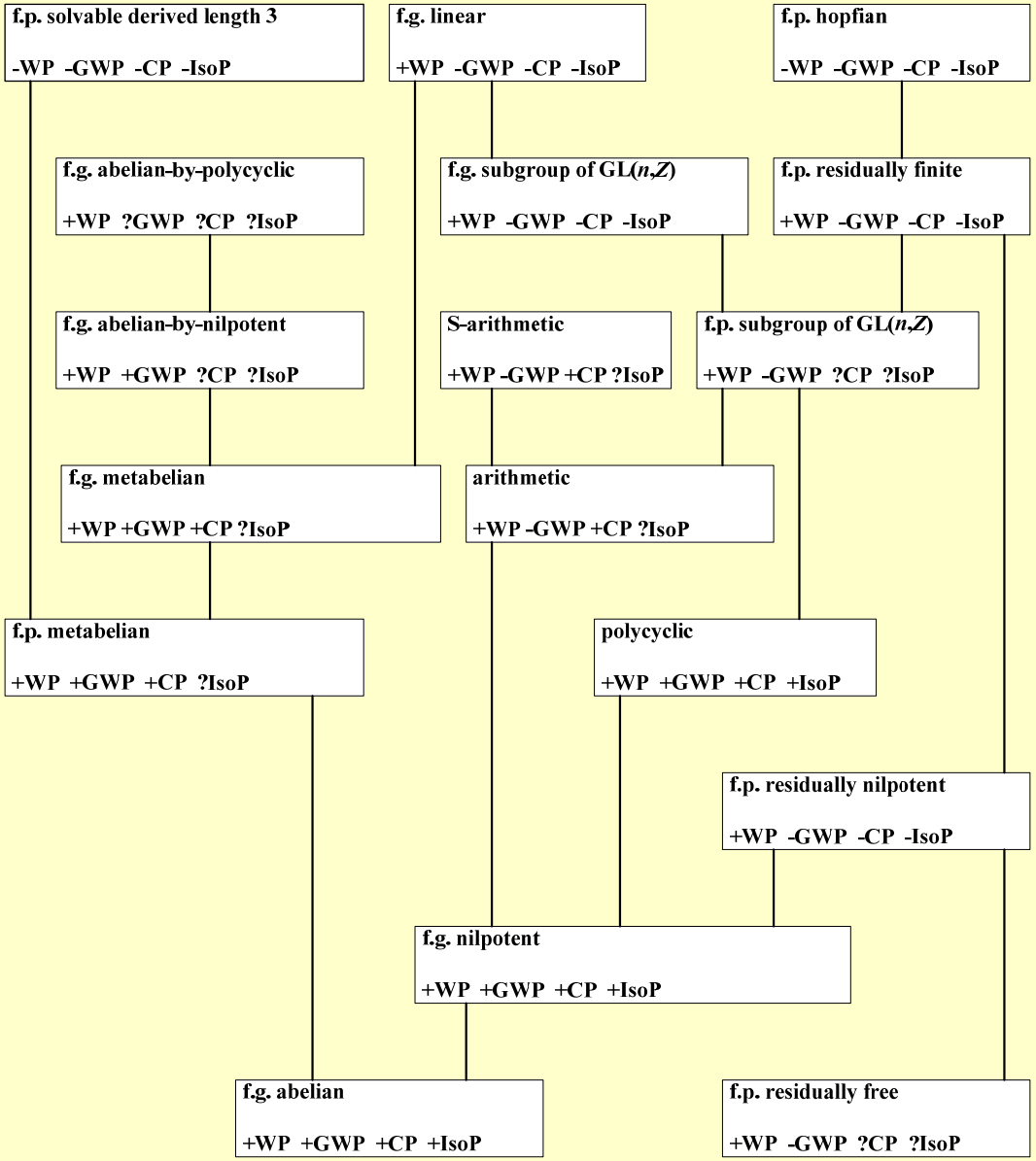
- Blank spot or infertile soil?

Methodology of Braid Crypt.

- Instructive for cryptosystems based on other non-commutative groups

- Other groups in which CSP is unsolvable. (Miller 1992)
  - How to representation these groups in computer?
  - How to generating hard instances?

Miller's Survey



Methodology of Braid Crypt.

- Can we use the methods from braid crypt to design other post-quantum cryptosystems?
  - E.g., in MPKCs, we usually set $P=S \circ F \circ T$.

    What would happen if we set $S=T^{-1}$?
    - Is this setting meaningful?
      - If so, can we derive S from P and F? This leads to new CSP problem.
      - If not, is there case in which this setting meaningful?
        - » If so, we might reach some non-trivial point.

What we want to do?

- To design a secure cryptosystem?
  - If so, braid crypt might be a bad choice at present.

Or

- To make clear a problem: why it is (in)secure?
  - Not to announce the death of braid crypt imprudently
  - Not to deceive ourselves

Acknowledgements

- Thank you for your attention!
- Any suggestion is deeply appreciated!