A Heuristic Approach to the Dihedral Hidden Subgroup Problem

Hachiro Fujita

Department of Computer Science
Tokyo Metropolitan University

E-mail: hfujita@tmu.ac.jp

FUTURE COMPUTING 2022

About Hachiro Fujita

- **Education:**
  - BS and MS in mathematics, Kyoto University, in 1994 and 1996, respectively;
  - PhD in communications, Tokyo Institute of Technology, in 2005.
- **Work experience:**
  - communications engineer at Mitsubishi Electric Corporation from 1996 to 2002;
  - postdoctoral at The University of Tokyo from 2005 to 2006;
  - since 2006 he has been with TMU and is currently Assistant Professor at the Dept. of CS.
- **Research interest:**
  - coding and information theory;
  - cryptography and information security;
  - quantum information.

The Dihedral Group D_N

- For $N \in \mathbb{N}$, let $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ denote a cyclic group of order N.

Definition

The **dihedral group** D_N is the symmetry group of an N-sided polygon, which is isomorphic to a semidirect product of $\mathbb{Z}_N$ by $\mathbb{Z}_2$ with the following product denoted by "$\circ$": for $(a, x), (b, y) \in D_N$ where $a, b \in \mathbb{Z}_2$ and $x, y \in \mathbb{Z}_N$,

$$(a, x) \circ (b, y) = (a + b, (-1)^b x + y).$$

For simplicity we may omit the notation "$\circ$".

Dihedral Hidden Subgroup Problem (DHSP)

- Let $\mathcal{X}$ be a finite set and let H be a subgroup of D_N. A function $f : D_N \to \mathcal{X}$ is said to **hide** H if the following condition holds: for any $g, g' \in D_N$,

$$f(g) = f(g') \iff Hg = Hg'.$$

Problem (DHSP)

Let a function f hiding a subgroup $H \leq D_N$ be given. The problem is to find H (or the generators of H) using evaluations of f.

- Exhaustive search takes time $O(N)$. No polynomial-time $(\mathrm{poly}(\log_2 N))$ algorithm for DHSP is known.
- DHSP has many applications in cryptanalysis.

Related Work in DHSP

- **Ettinger–Høyer, Adv. Appl. Math., 2000**
  present a quantum algorithm whose query complexity is polynomial (in fact, linear) in $\log_2 N$, but requires exponential time classical postprocessing to find the hidden subgroup.
- **Kuperberg, SIAM J. Comp., 2005**
  presents a subexponential-time quantum algorithm using a sieve method, which is the fastest algorithm known to date.
- **Bacon–Childs–van Dam, Chicago J. Theor. Comp. Sci., 2006**
  present the optimal measurement for DHSP using Pretty Good Measurement (PGM), whose implementation is equivalent to the solution of the random case subset sum problem.

From DHSP to Dihedral Coset Problem (DCP)

- Thanks to the Ettinger–Høyer reduction, we may assume that a hidden subgroup $H \leq D_N$ is of order 2: $H = \langle (1, s) \rangle = \{(0, 0), (1, s)\}$ for some $s \in \mathbb{Z}_N$.
- By using the so-called **coset sampling** we can reduce DHSP to the following:

Problem (DCP)

Given a large number of sample states of the form (called **coset states**)

$$|\psi_{s,x}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 |x\rangle_2 + |1\rangle_1 |x + s\rangle_2)$$

where $s \in \mathbb{Z}_N$ (resp. $x \in \mathbb{Z}_N$) is unknown but fixed (resp. unknown and random) for each sample state, the problem is to find the hidden s.

Further Reduction of DCP: The Chia–Hallgren reduction

- Below we restrict ourselves to the case $N = 2^n$. For $x \in \mathbb{Z}_N$ we write $x = \sum_{i=1}^{n} x_i 2^{i-1}$ (binary expansion)
- Using the binary expansions of s and x, we have

$$\begin{aligned} |\psi_{s,x}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_1 |x\rangle_2 + |1\rangle_1 |x+s\rangle_2) \\ &= \frac{1}{\sqrt{2}}(|0\rangle_1 |x_1\rangle_{2'} \left|x'\right\rangle_{2''} + |1\rangle_1 |x_1 + s_1\rangle_{2'} \left|x' + s' + c\right\rangle_{2''}). \end{aligned}$$

  where $x' = \sum_{i=2}^{n} x_i 2^{i-2}$, $s' = \sum_{i=2}^{n} s_i 2^{i-2}$, and $c = s_1 \cdot x_1$.
- We measure register $2'$ in the $\{|0\rangle_{2'}, |1\rangle_{2'}\}$ basis:
  - If $s_1 = 0$, we obtain $|\psi_{s',x'}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 |x'\rangle_{2''} + |1\rangle_1 |x' + s'\rangle_{2''})$.
  - If $s_1 = 1$, we obtain $|a\rangle_1 |x''\rangle_{2''} = |0\rangle_1 |x'\rangle_{2''}$ or $|1\rangle_1 |x' + s' + c\rangle_{2''}$.
- Chia–Hallgren called the problem of distinguishing coset states $\left|\psi_{s',x'}\right\rangle$ from random basis states the **Dihedral Coset Space Problem**.

Further Reduction of DCP: The QFT approach of Ettinger–Høyer (1/3)

- The **Quantum Fourier Transform (QFT)** F_{2^n} over $\mathbb{Z}_{2^n}$ is defined for each basis state $|x\rangle$, $x \in \mathbb{Z}_{2^n}$, as

$$\boxed{F_{2^n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{Z}_{2^n}} \omega_{2^n}^{xy} |y\rangle}$$

  where $\omega_{2^n} = e^{2\pi\sqrt{-1}/2^n}$.
- We apply the QFT to the register $2'$ measurement outcome. We have to consider two cases:
  - *Case 1:* $s_1 = 1$. We have $|a\rangle_1 |x''\rangle_{2''}$.
  - *Case 2:* $s_1 = 0$. We have $|\psi_{s',x'}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 |x'\rangle_{2''} + |1\rangle_1 |x' + s'\rangle_{2''})$.

Further Reduction of DCP: The QFT approach of Ettinger–Høyer (2/3)

- *Case 1:* $s_1 = 1$. Applying the QFT, we have

$$(F_2 \otimes F_{2^{n-1}}) \left|a\right\rangle_1 \left|x''\right\rangle_{2''} = \frac{1}{\sqrt{2^n}} \sum_{b \in \mathbb{Z}_2} \sum_{y' \in \mathbb{Z}_{2^{n-1}}} (-1)^{ab} \omega_{2^{n-1}}^{x''y'} \left|b\right\rangle_1 \left|y'\right\rangle_{2''} .$$

  - Measurement of register 1 in the $\{\left|0\right\rangle_1, \left|1\right\rangle_1\}$ basis gives the outcomes 0 and 1 with equal probability 1/2. Assume that the outcome 0 is obtained. Then, discarding register 1, the system is in the state

$$\frac{1}{\sqrt{2^{n-1}}} \sum_{y' \in \mathbb{Z}_{2^{n-1}}} \omega_{2^{n-1}}^{x''y'} \left|y'\right\rangle_{2''} .$$

  - Measuring register $2''$ in the $\{\left|y'\right\rangle_{2''}\}_{y' \in \mathbb{Z}_{2^{n-1}}}$ basis, we obtain the outcome y' with equal probability

$$\boxed{P(y') = \frac{1}{2^{n-1}}.}$$

Further Reduction of DCP: The QFT approach of Ettinger–Høyer (3/3)

- *Case 2:* $s_1 = 0$. Applying the QFT, we have

$$(F_2 \otimes F_{2^{n-1}}) \left|\psi_{s',x'}\right\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{b \in \mathbb{Z}_2} \sum_{y' \in \mathbb{Z}_{2^{n-1}}} \omega_{2^{n-1}}^{x'y'} \cdot \left(1 + (-1)^b \omega_{2^{n-1}}^{s'y'}\right) |b\rangle_1 \left|y'\right\rangle_{2''}.$$

  - Measurement of register 1 in the $\{|0\rangle_1, |1\rangle_1\}$ basis gives the outcomes 0 and 1 with equal probability 1/2. Assume that the outcome 0 is obtained. Then, discarding register 1, the system is in the state

$$\frac{1}{\sqrt{2^n}} \sum_{y' \in \mathbb{Z}_{2^{n-1}}} \omega_{2^{n-1}}^{x'y'} (1 + \omega_{2^{n-1}}^{s'y'}) |y'\rangle_{2''}.$$

  - Measuring register $2''$ in the $\{|y'\rangle_{2''}\}_{y' \in \mathbb{Z}_{2^{n-1}}}$ basis, we obtain the outcome y' with probability

$$\boxed{Q(y') = \frac{1}{2^{n-2}} \cos^2\left(\pi \frac{s'y'}{2^{n-1}}\right).}$$

From DCP to a Distribution Testing Problem

- Hereafter $N = 2^{n-1}$.
- We may assume that the s' is a nonzero element of $\mathbb{Z}_N$, which is denoted by s below.
- Thanks to Chia–Hallgren + Ettinger–Høyer, we have reduced DCP to the problem of distinguishing probability distributions P and Q on $\mathbb{Z}_N$:

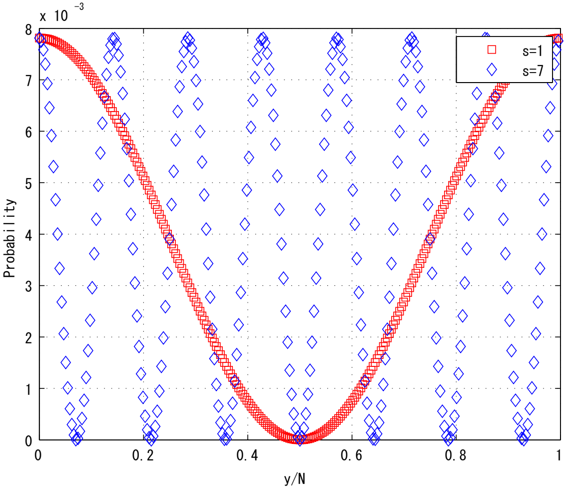
$$P(y) = \frac{1}{N} \quad \text{and} \quad Q(y) = \frac{2}{N}\cos^2\left(\pi\frac{sy}{N}\right)$$

for $y \in \mathbb{Z}_N$.
- Our main result is the following:

Theorem

Using a **simple statistical test**, *we can distinguish P and Q with high probability in time polynomial in $\log N$ under some heuristic assumptions (which are too technical to state here).*

- Let $N = 2^8 = 256$. Below is the plot of Q for $s = 1$ and $s = 7$.



Simple Statistical Test

1. (i) From coset states we obtain Y_j, $j = 1, \ldots, M$, samples from unknown distribution (P or Q).
   (ii) Compute $S_M = \sum_{j=1}^{M} g(Y_j)$ where g is the test function defined on $\mathbb{Z}_N$:
   $$g(y) = \left(-\ln\left(1 - \frac{y}{N}\right)\right)^K, \quad y \in \mathbb{Z}_N,$$
   where $M = \mathrm{poly}(n)$ and $K = \mathrm{poly}(n)$.
   (iii) Continue the above steps to obtain many S_M's.
2. (i) Generate Y'_j, $j = 1, \ldots, M$, by sampling from the uniform distribution P.
   (ii) Compute $S_M^P = \sum_{j=1}^{M} g(Y'_j)$.
   (iii) Continue the above steps to obtain many S_M^P's.
3. Compute $(S_M)^{1/K}$'s and $(S_M^P)^{1/K}$'s, and construct the **histograms** of these data.
4. Conclude that the distribution in question is P if two histograms are close in ℓ_1 metric, and Q otherwise.

Continuous Approximations to P and Q

Using continuous approximations to P and Q, we investigate **probability density functions** of S_M^P and S_M^Q.

- Replacing P with uniform distribution U on $(0,1)$, we obtain $X = g(U)$ (called a **Weibull variate**) with PDF

$$f_X(x) = \frac{1}{K} x^{-1+1/K} \exp(-x^{1/K}), \quad x > 0.$$

- Q has a continuous counterpart V with PDF

$$f_V(v) = 2\cos^2(\pi s v), \quad v \in (0,1)$$

from which we obtain $Z = g(V)$ with PDF

$$f_Z(z) = \frac{2}{K} z^{-1+1/K} \exp(-z^{1/K}) \cos^2(\pi s \exp(-z^{1/K})).$$

PDF of the Sum of Random Variables: Convolution

- We use a basic result in probability theory:

Fact

- Let X and Y be two independent continuous RVs with PDF f_X and f_Y, respectively, and let $Z = X + Y$ be the sum of X and Y. Then the PDF f_Z of Z is given by **convolution** of f_X and f_Y (denoted by $f * g$):

$$f_Z(z) = (f_X * f_Y)(z) = \int_{-\infty}^{\infty} f_X(z-y) f_Y(y) dy.$$

- Let $\{X_j\}_{j=1}^m$ be i.i.d. RVs with PDF f_X and let $S_m = \sum_{j=1}^m X_j$. Then the PDF of S_m is given by the m-th convolution power $f_X^{*m} = \underbrace{f_X * f_X * \cdots * f_X}_{m \text{ times}}$.

Comparing the PDFs of S_M^P and S_M^Q

By choosing M and K properly and making certain assumptions, we can show the following:

- PDF of S_M^P: $f_X^{*M}(z) = a_M^X(x) b_M^X(x)$ where

$$a_M^X(x) = \frac{2^M}{\kappa^M K} x^{-1+1/K}.$$

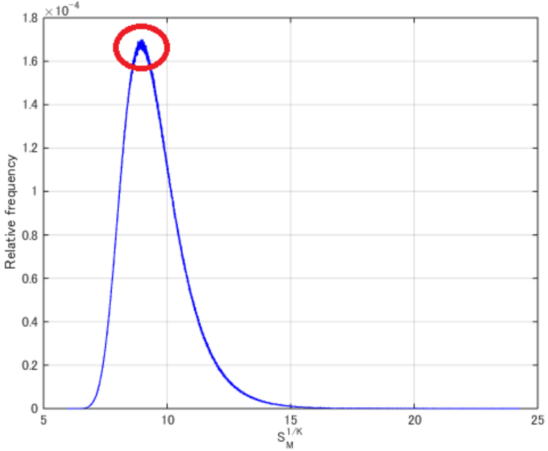
- PDF of S_M^Q: $f_Z^{*M}(z) = a_M^Z(z) b_M^Z(z)$ where

$$a_M^Z(z) \approx \frac{2^M}{\kappa^M K} z^{-1+1/K} \times \left(1 + \underbrace{\frac{\cos(2\pi n^{c_1} z^{1/K}) \sin(2\pi n^{c_1} \delta z^{1/K})}{2\pi n^{c_1} \delta z^{1/K}}}_{\text{oscillatory term!}} \right)$$

  - $c_1 = O(1)$ and $\delta = o(1)$.

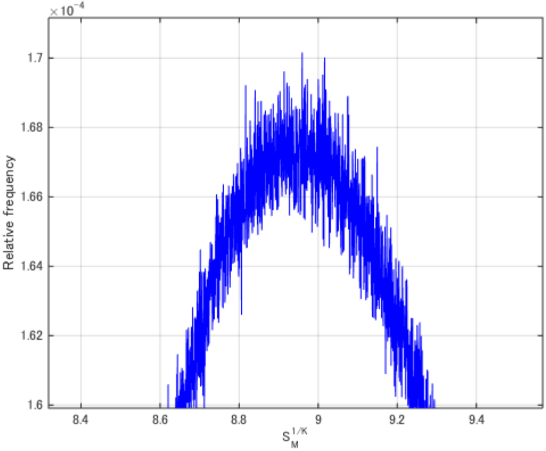
Simulation Result (1/3): Big Picture of the Histogram

- Histogram looks like an **extreme value distribution**. We zoom in on the summit of the mountain.



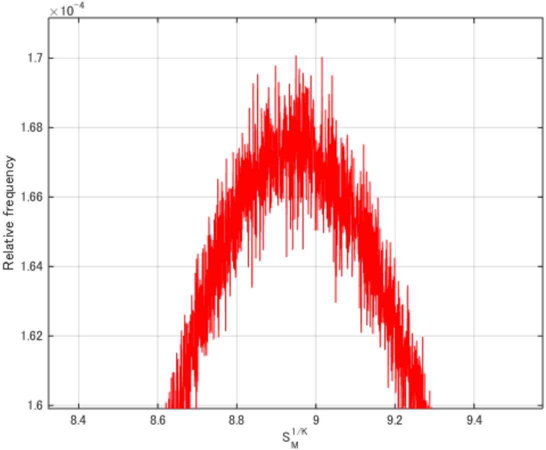
Simulation Result (2/3): The P Case

- Here is the histogram of $(S_M^P)^{1/K}$'s with $N = 2^{35}$, $M = 7652$, $K = 2000$, and bin width 4.55×10^{-4}:



Simulation Result (3/3): The Q Case

- Here is the histogram of $(S_M^Q)^{1/K}$'s with the same parameters as in the P case and $s = 7794178885$:



For More Information

- Please see EasyChair-Preprint-3475 (version 2) available at EasyChair.
- Any comments are welcome! E-mail: `hfujita@tmu.ac.jp`
  - A simulation program (MATLAB code) is available on request.

Thank you for your attention!