FUTURE COMPUTING 2022

The Fourteenth International Conference on Future Computational Technologies and Applications

ISBN: 978-1-61208-949-2

April 24 - 28, 2022

Barcelona, Spain

FUTURE COMPUTING 2022 Editors

Claus-Peter Rückemann, Westfälische Wilhelms-Universität Münster (WWU) / DIMF / Leibniz Universität Hannover, Germany

FUTURE COMPUTING 2022

Forward

The Fourteenth International Conference on Future Computational Technologies and Applications (FUTURE COMPUTING 2022), held on April 24 - 28, 2022, continued a series of events targeting advanced computational paradigms and their applications. The target was to cover (i) the advanced research on computational techniques that apply the newest human-like decisions, and (ii) applications on various domains. The new development led to special computational facets on mechanism-oriented computing, large-scale computing and technology-oriented computing. They are largely expected to play an important role in cloud systems, on-demand services, autonomic systems, and pervasive applications and services.

Similar to the previous edition, this event attracted excellent contributions and active participation from all over the world. We were very pleased to receive top quality contributions.

We take here the opportunity to warmly thank all the members of the FUTURE COMPUTING 2022 technical program committee, as well as the numerous reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors that dedicated much of their time and effort to contribute to FUTURE COMPUTING 2022.

Also, this event could not have been a reality without the support of many individuals, organizations and sponsors. We also gratefully thank the members of the FUTURE COMPUTING 2022 organizing committee for their help in handling the logistics and for their work that made this professional meeting a success.

We hope FUTURE COMPUTING 2022 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in the area of future computational technologies and applications. We also hope that Barcelona provided a pleasant environment during the conference and everyone saved some time to enjoy the historic charm of the city

FUTURE COMPUTING 2022 Steering Committee

Hiroyuki Sato, The University of Tokyo, Japan
Sergio Ilarri, University of Zaragoza, Spain
Jay Lofstead, Sandia National Laboratories, USA

FUTURE COMPUTING 2022 Publicity Chair

Lorena Parra, Universitat Politecnica de Valencia, Spain
Javier Rocher, Universitat Politècnica de València, Spain

FUTURE COMPUTING 2022

Committee

FUTURE COMPUTING 2022 Steering Committee

Hiroyuki Sato, The University of Tokyo, Japan
Sergio Ilarri, University of Zaragoza, Spain
Jay Lofstead, Sandia National Laboratories, USA

FUTURE COMPUTING 2022 Publicity Chair

Lorena Parra, Universitat Politecnica de Valencia, Spain
Javier Rocher, Universitat Politècnica de València, Spain

FUTURE COMPUTING 2022 Technical Program Committee

Andrew Adamatzky, University of the West of England, Bristol, UK
Ehsan Atoofian, Lakehead University, Canada
Yadu Babuji, University of Chicago, USA
Bernhard Bandow, GWDG, Göttingen, Germany
Kaustav Basu, The Laboratory for Networked Existence (NetXT), USA
Rudolf Berrendorf, Bonn-Rhein-Sieg University, Germany
Christos J. Bouras, University of Patras, Greece
Massimiliano Caramia, University of Rome "Tor Vergata", Italy
Ryan Chard, Argonne National Laboratory, USA
Nan-Yow Chen, National Center for High-Performance Computing (NCHC), Taiwan
Sunil Choenni, Ministry of Justice and Security / Rotterdam University of Applied Sciences, Netherlands
Fabio D'Andreagiovanni, CNRS & UTC - Sorbonne, France
Leandro Dias da Silva, Universidade Federal de Alagoas, Brazil
Félix J. García Clemente, University of Murcia, Spain
Apostolos Gkamas, University Ecclesiastical Academy of Vella of Ioannina, Greece
Victor Govindaswamy, Concordia University - Chicago, USA
Francesc Guim, Intel Corporation, Spain
Tzung-Pei Hong, National University of Kaohsiung, Taiwan
Wei-Chiang Hong, School of Computer Science and Technology - Jiangsu Normal University, China
Sergio Ilarri, University of Zaragoza, Spain
Yuji Iwahori, Chubu University, Japan
Yasushi Kambayashi, Nippon Institute of Technology, Japan
Mehdi Kargar, Ted Rogers School of Management - Ryerson University, Toronto, Canada
Michihiro Koibuchi, National Institute of Informatics, Japan
Zbigniew Kokosinski, Cracow University of Technology, Poland
Carlos León-de-Mora, Universidad de Sevilla, Spain
Jay Lofstead, Sandia National Laboratories, USA

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

A Heuristic Approach to the Dihedral Hidden Subgroup Problem

Hachiro Fujita
Department of Computer Science
Tokyo Metropolitan University
Hino, Tokyo 191-0065, Japan
Email: hfujita@tmu.ac.jp

***Abstract*—The Dihedral Hidden Subgroup Problem (DHSP) is a long-standing open problem in quantum computation. The best known quantum algorithm for the DHSP is Kuperberg's sieve algorithm which runs in subexponential time. Regev showed that the DHSP is related to a lattice problem on which the security of some public-key cryptosystems is based, and that an efficient solution to the DHSP would lead to breaking such cryptosystems. In this extended abstract, we present a simple quantum algorithm for the hidden subgroup problem over the dihedral group of order a power of two, which runs in polynomial time under some heuristic assumptions. We have implemented our algorithm in MATLAB and tested it with a small example. The simulation result shows evidence of the correctness of our algorithm.**

***Index Terms*—dihedral group; hidden subgroup problem; quantum algorithm; statistical test.**

I. INTRODUCTION

Since Shor's seminal work [1] on quantum algorithms for integer factorization and discrete logarithms, the Hidden Subgroup Problem (HSP) has been a hot research topic in the field of quantum information and computation. See, e.g., [2], for a survey on this topic. The HSP is classified into two categories: abelian and nonabelian. Many abelian HSPs have been well understood and a quantum computer can solve many abelian HSPs exponentially faster than a classical computer. On the other hand, nonabelian HSPs in general are difficult to solve and for some nonabelian groups (e.g., the symmetric group) negative results have been reported.

The Dihedral HSP (DHSP for short) stated in the next section is the first step towards understanding nonabelian HSPs. Ettinger and Høyer [3] were the first to consider the DHSP and showed that polynomial-time quantum computation provides enough information to solve the problem, but classical post-processing may take exponential time. At the time of writing, the best quantum algorithm known to date is due to Kuperberg [4] who shows a subexponential-time quantum algorithm for the DHSP (see also [5][6] for its improvements).

The DHSP is related to a lattice problem. Regev [7] shows that if an efficient algorithm exists for the DHSP then one can efficiently solve the unique Shortest Vector Problem (uSVP). Some lattice-based cryptosystems assume the hardness of the uSVP. In fact, no classical polynomial-time algorithm for the uSVP is known. However, since the periodic structure of a lattice is suited to quantum computation, many researchers have tried to solve lattice problems with a quantum computer, but no polynomial-time quantum algorithm for the uSVP is known to date.

A. Problem Statement and Our Main Result

In this paper, we restrict ourselves to dihedral groups of order a power of two. For a positive integer n, let D_{2^n} denote a dihedral group of order 2^{n+1} (see the next section for the definition of the dihedral group D_{2^n}). Let f be a function on D_{2^n} and H a subgroup of D_{2^n}. We say that the function f *hides* the subgroup H if the following holds: for all $g, g' \in D_{2^n}$, $f(g) = f(g')$ if and only if $Hg = Hg'$ for the right cosets of H. The DHSP is stated as follows.

Problem 1 (DHSP)**.** Given an efficiently computable function f on D_{2^n} that hides a subgroup H of D_{2^n}, find the generators of H by evaluating the function f.

In our paper [8], we present a simple quantum algorithm for the DHSP. Our approach to the DHSP is essentially the same as the one taken by Ettinger and Høyer [3]. Using the quantum Fourier transform, we reduce the DHSP to a problem of distinguishing (discrete) probability distributions. To solve the latter problem we propose a simple statistical test, which can be performed in polynomial time on a classical computer under some heuristic assumptions stated in Section 4.2 of [8], and so the DHSP can be solved in polynomial time on classical and quantum computers. The description and analysis of our quantum algorithm are given in Sections 3 and 4 of [8]. Our main result is summarized in the following (informal) theorem:

Theorem 2. *There exists a quantum algorithm for the DHSP over D_{2^n}, whose runtime is polynomial in n under some heuristic assumptions.*

See [8] for a *heuristic* proof.

B. Related Work

The related work includes [3]–[6], among others, as mentioned above. For a survey on the DHSP see [9]. We have to mention the work of Bacon *et al*. [10]. They show the optimal measurement for the DHSP using a Pretty Good Measurement (PGM) and a result about quantum hypothesis testing, which has a better query complexity than [3]. They also show the equivalence between the implementation of the optimal measurement in a restricted form and the solution of

 ISBN: 978-1-61208-949-2

the average-case subset sum problem. Since the average-case subset sum problem appears to be hard, the PGM approach seems unlikely to yield an efficient quantum algorithm for the DHSP. Chia and Hallgren [11] also consider a decision problem related to the DHSP and show its relation to the subset sum problem.

II. Outline of Our Solution to the DHSP

We will outline our quantum algorithm for the DHSP below.

A. Notation

For a positive integer N, let $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$. We denote modulo N addition and subtraction on $\mathbb{Z}_N$ by "$+$" and "$-$", respectively. Although we use the same notation as used in the field of real numbers, the meaning is clear from the context. Note that $\mathbb{Z}_N$ with respect to addition is a cyclic group of order N.

B. Reducing the DHSP to a Distribution Testing Problem

We first recall the definition of the dihedral group D_{2^n} of order 2^{n+1}, where n is a positive integer. The dihedral group D_{2^n} is defined by $\mathbb{Z}_2 \ltimes \mathbb{Z}_{2^n}$, a semidirect product of $\mathbb{Z}_2$ and $\mathbb{Z}_{2^n}$ both of which are considered as cyclic groups with respect to addition. The product operation on $D_{2^n} = \mathbb{Z}_2 \ltimes \mathbb{Z}_{2^n}$, denoted by "$\circ$", is defined by

$$(a, x) \circ (b, y) = (a + b, (-1)^b x + y) \tag{1}$$

for $(a, x), (b, y) \in D_{2^n}$. For simplicity we omit the notation "$\circ$".

We may assume that the hidden subgroup H is of order 2 (see [3]). Using the so-called standard method (see, e.g., [2] [9]), the DHSP for the above H is reduced to the following *Dihedral Coset Problem (DCP)* which is equivalent to the *hidden shift problem over the cyclic group* $\mathbb{Z}_{2^n}$ (see, e.g., [2]).

Problem 3 (DCP)**.** For $s \in \mathbb{Z}_{2^n} \setminus \{0\}$ and $x \in \mathbb{Z}_{2^n}$, let

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

The state above is called a *coset state*. Given a (polynomial size) sample of coset states in Eq. (2) with fixed s and varying x both of which are unknown, the problem is to find the shift s (or equivalently, its binary representation $(s_1, \ldots, s_n)$ with $s = \sum_{i=1}^{n} s_i 2^{i-1}$).

If we determine the least significant bit s_1 of the hidden shift s, then the DCP over D_{2^n} reduces to a smaller one over $D_{2^{n-1}}$. By using such a reduction we can solve the DCP iteratively. See [8] for more details.

To determine the s_1 we use the Quantum Fourier Transform (QFT). Using the QFT, we reduce the problem of determining s_1 to that of distinguishing between the discrete probability distributions P and Q on $\mathbb{Z}_N$ defined below, where $N = 2^{n-1}$. For $y \in \mathbb{Z}_N$,

$$P(y) = \frac{1}{N} \quad \text{and} \quad Q(y) = \frac{2}{N} \cos^2\left(\pi \frac{s'y}{N}\right), \tag{3}$$

where s' is a nonzero element of $\mathbb{Z}_N$. See [8] for more details.

C. Distinguishing the Distributions P and Q

To solve the above distribution testing problem we propose the following statistical test:

1) (a) From coset states we obtain Y_j, $j = 1, \ldots, M$, samples from unknown distribution (P or Q).
   (b) Compute $S_M = \sum_{j=1}^{M} g(Y_j)$ where g is the test function defined on $\mathbb{Z}_N$:
   $$g(y) = \left(-\ln\left(1 - \frac{y}{N}\right)\right)^K, \quad y \in \mathbb{Z}_N, \tag{4}$$
   where $M = \mathrm{poly}(n)$ and $K = \mathrm{poly}(n)$.
   (c) Continue the above steps to obtain many S_M's.
2) (a) Generate Y'_j, $j = 1, \ldots, M$, by sampling from the uniform distribution P.
   (b) Compute $S_M^P = \sum_{j=1}^{M} g(Y'_j)$.
   (c) 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.

We implemented the above statistical test in MATLAB and performed a Monte Carlo simulation. The simulation result can be found in [8].

III. Conclusion

In this extended abstract, we outlined our solution to the DHSP for the case D_{2^n}. For lack of space we omitted a heuristic analysis of the statistical test given in the previous section, which can be found in [8]. It remains open to give a rigorous proof of correctness of our quantum algorithm.

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[2] A. M. Childs and W. van Dam, "Quantum algorithms for algebraic problems," *Reviews of Modern Physics*, vol. 82, 2010.

[3] M. Ettinger and P. Høyer, "On quantum algorithms for noncommutative hidden subgroups," *Advances in Applied Mathematics*, vol. 25, no. 3, pp. 239–251, 2000.

[4] G. Kuperberg, "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem," *SIAM Journal on Computing*, vol. 35, no. 1, pp. 170–188, 2005.

[5] G. Kuperberg, "Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem," *Proc. 8th Conference on the Theory of Quantum Computation, Communication and Cryptography*, pp. 20–34, 2013.

[6] O. Regev, "A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space," arXiv:quant-ph/0406151, 2004.

[7] O. Regev, "Quantum computation and lattice problems," *SIAM Journal on Computing*, vol. 33, no. 3, pp. 738–760, 2004.

[8] H. Fujita, "A heuristic approach to the dihedral hidden subgroup problem," EasyChair-Preprint-3475, version 2, 2022.

[9] H. Kobayashi and F. Le Gall, "Dihedral hidden subgroup problem: A survey," *IPSJ Journal*, vol. 46, no. 10, pp. 2409–2416, 2005.

[10] D. Bacon, A. M. Childs, and W. van Dam, "Optimal measurements for the dihedral hidden subgroup problem," *Chicago Journal of Theoretical Computer Science*, 2006.

[11] N.-H. Chia and S. Hallgren, "How hard is deciding trivial versus nontrivial in the dihedral coset problem?" *Proc. 11th Conference on the Theory of Quantum Computation, Communication and Cryptography*, pp. 6:1–6:16, 2016.

 ISBN: 978-1-61208-949-2