ISSN 2464-4617 (print)
ISSN 2464-4625 (online)
Quantum Informatics, Computing & Technology 2025
QC-Horizon 2025
https://www.qc-horizon.eu/

Introducing the hidden subgroup problem in discrete mathematics class

Sehee Kim, Jiwoo Seo, Minju Kim, Yerak Kim, Seohyeon Baek, Seongbin Park*
Korea University, Sungbuk-ku, Anam-ro 145, Seoul, 02841, Korea
{sehee020512, jw3124, mim0924, yerak213, beth0508, hyperspace}@korea.ac.kr

ABSTRACT

Discrete mathematics is a branch of mathematics that deals with discrete structures, where a discrete structure is defined as either a finite nonempty set or a countably infinite set over which various relations, operations are defined. For computer science students, this is a class where fundamental subjects such as logic, number theory, relation, set theory, graph theory, algorithms are introduced in such a way that these subjects can be understood without much mathematics[Sandefur22]. In this poster, we describe our ongoing research that aims to introduce quantum computing to students without technical backgrounds[Jkim23, Slee23, Sjeong24]. More specifically, we argue that the hidden subgroup problem[Hallgren03] is a good subject that can be taught in discrete mathematics class because the problem deals with a simple discrete structure that can be easily explained to the students of discrete mathematics class. In addition, since it is well known that the famous quantum algorithms such as Simon's algorithm and Shor's algorithm solve the instances of the hidden subgroup problem[Nielsen16], we believe that introduction to the hidden subgroup problem can help students gain insights into the structural properties of computational problems in a wide perspective.

Keywords

Discrete mathematics, Hidden subgroup problem, Quantum computing

1 INTRODUCTION

The field of quantum computing has been progressing rapidly recently and it is expected to revolutionize a lot of technologies in the future[Alil22]. As is argued in[Bacon10], we believe that important ideas of quantum computing such as superposition, entanglement, reversibility, etc. can be introduced to students without backgrounds in mathematics and quantum mechanics.

In this poster, we describe our ongoing project that aims to introduce well-known quantum algorithms to the students in discrete mathematics class using the hidden subgroup problem(HSP).

The motivations of our research are as follows.

First, HSP can be defined using the concepts that students in discrete mathematics are already familiar with. For example, to define HSP, we need the concepts of a function, an equivalence class, a closure property, a binary operation, and a set and all of these are explained in discrete mathematics class.

Second, HSP naturally fits with the themes of discrete mathematics because HSP asks to find a certain structure (a subgroup) in a bigger structure (a group) that is discrete while discrete mathematics deals with various examples of discrete structures that we encounter in computing such as algorithms, computational problems, data structures, number theory, etc.

Finally, knowledge about HSP can serve as a window through which students can see a different world (that is, the world of quantum computing) than the world of classical computing since well-known quantum algorithms such as Simon's algorithm and Shor's algorithm solve instances of HSP more efficiently than classical algorithms.

This poster is structured as follows. In section 2, we explain how HSP can be introduced to the students in discrete mathematics with simple instances of HSP. Then, this poster concludes with research perspectives.

2 INSTANCES OF HSP

To introduce HSP to the students in discrete mathematics, we can start with a definition for HSP. Then, two different instances of HSP are explained so that their structural common denominator can be easily recognized.

HSP is defined as follows. We are given a finite group G and a function f from G to a finite set A such that f has the following property: (1) for all elements in the same coset of a subgroup H of G, the function values are the same, and (2) for elements x, y each of which belongs to a different coset of H, $f(x)$ and $f(y)$ are different. We say that the subgroup H is hidden by the function f and the problem is to find H.

Then, we can explain a simple example with a group G that consists of a set Z_6=$\{0,1,2,3,4,5\}$ with a binary operation that is addition mod 6. For this structure, there is a subgroup H that consists of a set B=$\{0,3\}$.

Now, there are 3 cosets of H which are $\{0,3\}$, $\{1,4\}$, and $\{2,5\}$.

We can point out that Z_6 is divided into 3 cosets so that when a function is defined, it can be interpreted as assigning 3 different colors to the members of Z_6 depending on the membership against the cosets.

An instance of HSP here is as follows. Assume that we are given a function f that maps Z_6 to A=$\{a,b,c\}$ such that $f(0) = f(3)$=a, $f(1) = f(4)$=b, and $f(2) = f(5)$=c, respectively. What is the hidden subgroup?

Once this example is understood by the students, we can explain the problem that Simon's algorithm addresses.

The problem is defined as follows: We are given a function f from $\{0,1\}^n$ to $\{0,1\}^n$ such that for all $x,y \in \{0,1\}^n$, $f(x)$=$f(y)$ if and only if x=$y \oplus s$, for some $s \in \{0,1\}^n$, where $\oplus$ is the bitwise exclusive or operation. The problem is to find s.

The underlying structure of Simon's problem is HSP because if we let the group as the set, $\{0,1\}^n$ with the binary operation $\oplus$, then the hidden subgroup is the set $\{0^n$,$s\}$.

3 CONCLUSION

In this poster, we report our ongoing project that aims to introduce well-known quantum algorithms to the students in discrete mathematics class.

When mathematical structures are taught, it is important that the teacher should know more about structures than can be discussed in class[Taylor65]. We believe that introduction of HSP as a way to open students' eyes about applications of discrete structures is something that achieves this guideline because it connects a structure with a way to exploit it for solving a problem. This is similar to a matroid that can be exploited when an optimization problem posesses it[Edmonds71].

Introduction of HSP as well as an instance of the problem such as Simon's problem may help students get interested in a subtle subject such as what makes quantum computers more powerful than classical computers. In addition, students may ask whether there exists a general theorem that states the existence of a structural property that makes quantum computation more powerful compared to classical computation[Aaronson11].

Currently, we are working on intuitive ways to introduce instances of HSP such as Shor's period finding problem as well as graph isomorphism problem to students in discrete mathematics class. In addition, we are investigating ways by which visualization tools can be used to introduce quantum algorithms.

4 REFERENCES

[Sandefur22] E. Hart, G. Greefrath, J. Sandefur, E. Lockwood, Teaching and learning discrete mathematics, ZDM - Mathematics Education, Volume 54, pp. 753-775, 2022.

[Jkim23] Teaching an Elective Course about Quantum Computing, J. Kim, C. Lee, J. Song, C. Sim, S. Park, Poster, The 16th International Conference on Informatics in Schools, October 2023, HEP Vaud, Lausanne, Switzerland, https://zenodo.org/records/8431971 (PDF).

[Slee23] Introduction to Quantum Computing for Middle School Students, S. Lee, J. Kim, Y. Kim, C. Sim, S. Jeong, S. Park, Poster, The 16th International Conference on Informatics in Schools, October 2023, HEP Vaud, Lausanne, Switzerland, https://zenodo.org/records/8432008 (PDF).

[Sjeong24] An approach to introduce entanglement to novices, S. Jeong, S. Oh, S. Song, S. Park, Short paper, QC Workshop 2024: GI Quantum Computing Workshop September 24, Germany, 2024, https://dl.gi.de/server/api/core/bitstreams/77f9cb92-3e70-40d6-92b0-bd4b2882880a/content (PDF).

[Hallgren03] A. Russell, A. Ta-shma, S. Hallgren, The hidden subgroup problem and quantum computation using group representations, SIAM Journal on Computing, Volume 32, No 4, pp. 916-934, 2003.

[Nielsen16] I. L. Chuang, M. A. Nielsen, Quantum commputation and quantum information, Cambridge University Press, 2016.

[Alil22] T. Yue, R. Abreu, S. Ali, When software engineering meets quantum computing, Communications of the ACM, Volume 85, No 4, pp. 84-88, 2022.

[Bacon10] D. Bacon, W. van Dam, Recent progress in quantum algorithms, Communications of the ACM, Volume 53, No 2, pp. 84-93, 2010.

[Taylor65] T. L. Wade, H. E. Taylor, On the meaning of structure in mathematics, The mathematics teacher, Volume 58, No 3, pp. 226-231, 1965.

[Edmonds71] J. Edmonds, Matroids and the greedy algorithm, Mathematical Programming, Volume 1, pp. 127-136, 1971.

[Aaronson11] A. Ambainis, S. Aaronson, The need for structure in quantum speedups, Proceedings of Innovations in Theoretical Computer Science (ITCS), arXiv:0911.0996, 2011.