Quantum Coset Multiplication and the Hidden Subgroup Problem in Dihedral Groups D_p

João R. Sarmento[1], **Leandro M. Zatesko**[1], **Abner F. B. Costa**[2]

[1]Federal University of Technology of Paraná – Curitiba (UTFPR-CT)

[2]Federal University of Paraná (UFPR)

{joaosarmento@alunos.,zatesko@}utfpr.edu.br, abnerfbcosta@gmail.com

Abstract. *The Hidden Subgroup Problem (*HSP*) generalises and is related to important computational problems, such as Integer Factorisation. A major breakthrough in the study of quantum algorithms is Shor's approach to solving* HSP *for abelian groups. Recently, one of the authors of this paper has proposed a quantum algorithm for coset multiplication, which seems to be promising for the* HSP *in some group classes, such as symmetric and alternating groups. We extend the result on symmetric groups to dihedral groups D_p when p is prime.*

1. Introduction

We assume throughout that the reader is familiar with the basics on Group Algebra, Computational Complexity, and Quantum Computing. We follow the standard definitions and notation of the textbooks of [Arora and Barak 2009, Nielsen and Chuang 2010, Rotman 2005] on these topics.

The hidden subgroup problem (HSP) is an important problem and a candidate to be NP-intermediate to which many other problems are reducible, like integer factorisation and graph isomorphism [Shor 1994, Jozsa 2001]. It is defined as: being a $G \subseteq \{0,1\}^n$ a group and given access to a function $f : G \to S$, where $S \subseteq \{0,1\}^s$ and f *hides* a subgroup $H \leq G$, find a generating set for H. In this context, f is given by a black-box unitary transformation U_f such that $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$. We say that f *hides* $H \leq G$ if for every $g_1, g_2 \in G$, we have $f(g_1) = f(g_2)$ if and only if the cosets g_1H and g_2H are the same.

In this article, we deal with the decision version of the HSP (dHSP), which is the problem of deciding whether the hidden subgroup H in G is the trivial group (positive instance) or not (negative instance). Equivalently, dHSP is the problem of deciding if $|H| = 1$ or $|H| \geq 2$, as any group with only one element (the neutral element), is isomorphic to the trivial group. This decision version of HSP is not the only one approached in the literature, but it is well studied [Ettinger et al. 2004, Sdroievski et al. 2019, Costa et al. 2023].

A polynomial quantum algorithm for abelian instances of HSP was shown by [Shor 1994], which was further generalised to all abelian groups [Kitaev 1995] and, using similar techniques, when the hidden subgroup is normal [Hallgren et al. 2000]. Since then, continuous work has been done aiming to generalise this result for non-abelian cases of the problem [Grigni et al. 2001, Gavinsky 2004, Gonçalves et al. 2017]. However, [Moore et al. 2008, Grigni et al. 2001, Gavinsky 2004] show that similar techniques used in [Shor 1994] might not work for the symmetric and dihedral HSP cases. The dihedral case of HSP is of particular interest, since [Regev 2002] presented solution for the

unique shortest vector problem (SVP) under the assumption that there exists an algorithm that solves the hidden subgroup problem on the dihedral group, and furthermore a polynomial solution for this problem could compromise lattice-based cryptography systems like [Hoffstein et al. 1998]. Currently, the best-known quantum algorithm for the dihedral HSP requires subexponential time $exp(O(\sqrt{\log N}))$ [Kuperberg 2003], and, with Regev's modification [Regev 2004], it can run in polynomial quantum space.

The dihedral group is the group that describes the symmetries of a regular polygon, including rotations (r) and reflections (s). A regular polygon with n sides has $2n$ symmetries: n rotations and n reflections. These rotations and reflections make up the dihedral group D_n of order $2n$. If n is odd, each axis of symmetry connects the midpoint of one side to the opposite vertex; if n is even, there are $n/2$ axis connecting opposite vertex and $n/2$ axis connecting opposite sides. Either way there are n reflections.

[Costa 2024] introduced a coset multiplication quantum algorithm that, for some cases of dHSP and under certain conditions, is capable of producing a state ρ^B such that:

- if H is trivial, ρ^B represents an element $g \in G$, that is, $\rho^B = |g\rangle \langle g|$ where $g = a_1 * a_2 * ... * a_m$, being $\{a_i\}$ the group elements sampled by the algorithm and $*$ the group operation (referred to as a multiplication);
- if $|H| \geq 2$, then ρ^B is likely a mixed state in which every element in the group G has probability close to $|G|^{-1}$ of being measured.

Although, for those cases, this polynomial-time algorithm does not solve dHSP, it differentiates the instances of dHSP in a unique way, for which analysis could provide valuable insights into the non-abelian hidden subgroup problem. A particular case wherein the algorithm produces the state ρ^B as desired is the symmetric group [Costa 2024]. In this paper, we adapt the result concerning symmetric groups to dihedral groups.

The quantum circuit for Costa's algorithm is depicted in Figure 1, wherein $|G\rangle$ denotes the pure state given by superposition of the elements of G, i.e. $|G\rangle := (1/\sqrt{|G|}) \sum_{g \in G} |g\rangle$. Naturally, the number of qubits in the registers is the input lenght for HSP, i.e. the number n of bits necessary to represent the elements of G. Also, $U_{*,m}$ is the quantum circuit that implements the multiplication of m elements of the group.

Further preliminaries

An important metric for determining the distance between two mixed quantum states ρ, ρ' is the *trace distance*, which is defined as $D(\rho, \rho') = (1/2)\text{tr}(\sqrt{(\rho - \rho')^\dagger (\rho - \rho')})$. The *maximally mixed state* of a set S is defined and given by $I/S = (1/|S|) \sum_{g \in S} |g\rangle \langle g|$. The *normal closure* of a subgroup $H \leq G$ is the smallest normal subgroup of G that contains H and is denoted $ncl_G(H)$.

Given a sequence $(g_1, \ldots, g_m)$ of elements in G, let W be a random walk in the Cayley graph $\Gamma(ncl_G(H), H^G)$ that starts at the identity and at the ith step randomly chooses an element of H^{g_i}. The probability of the random walk W ending in an element g is given by

$$\frac{1}{|H|^m} \sum_{h_1 \in H^{g_1}} \cdots \sum_{h_1 \in H^{g_m}} 1 \tag{1}$$

if $h_1 * \cdots * h_m = g$, and 0 otherwise (in (1), $H^g = \{h^g : h \in H\}$ denotes the *conjugate* of H by g, being $h^g := ghg^{-1}$). A sequence $(g_1, \ldots, g_m)$ is said to be ε-*good* for Costa's

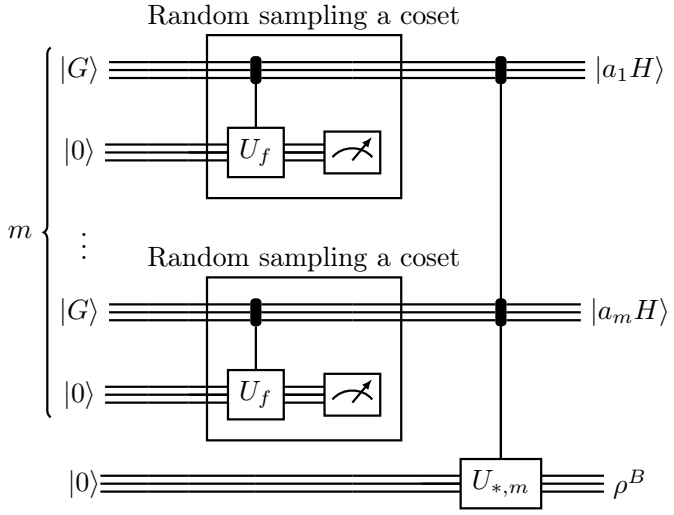

Figure 1. Coset multiplication quantum circuit.

coset multiplication quantum algorithm if the random walk W generates a distribution X_W close to uniform under the distance L_1, that is, $L_1(X_W, U_{ncl_G(H)}) \leq \epsilon$. Costa's algorithm requires $2/3$ of the sequences to be ϵ-good, which is a reasonable hypothesis to assume.

2. Result

Theorem 1. *If G is the dihedral group D_p of order $2p$ and p is a prime number, and there are $m = poly(n)$ and ϵ such that at least $2/3$ of the sequences are ϵ-good, then with probability at least $2/3$ we can produce a state ρ^B such that:*

- *if $|H| = 1$, then $D(\rho^B, I/G) = 1 - 1/|G|$;*
- *if $|H| \geq 2$, then $D(\rho^B, I/G) \leq 1/2 + \epsilon$.*

Proof. Costa has shown that, if there is an $m = poly(n)$ and an ϵ such that at least $2/3$ of sequences are ϵ-good, then with probability at least $2/3$ the coset multiplication quantum algorithm produces a state ρ^B such that

- if $|H| = 1$, then $D(\rho^B, I/G) = 1 - 1/|G|$
- if $|H| \geq 2$, then $D(\rho^B, I/G) \leq 1 - |ncl_G(H)|/|G| + \epsilon$

It suffices to consider only $|H| \geq 2$. [Conrad 2013] showed that the dihedral group D_k of order $2k$ has normal subgroups $\langle r^d \rangle$ for every $d \mid k$ with index $2d$, which are all proper normal subgroups of D_k when k is odd, and additionally the subgroups $\langle r^2, s \rangle$ and $\langle r^2, rs \rangle$ when k is even. Since $k = p$ is prime by hypothesis, the only non-trivial normal subgroup of D_p is $\langle r \rangle$ with index 2, and thus, order k. So $|ncl_G(H)|/|D_p| = 1/2$. Therefore,

$$D(\rho^B, I/G) \leq 1 - |ncl_G(H)|/|G| + \epsilon \leq 1/2 + \epsilon\,,$$

as desired. □

Remark that the same proof does not work when k is not prime, since $|ncl_G(H)|/|D_k|$ can get arbitrarily small as k grows if H is small enough.

3. Final remarks

Costa's quantum coset multiplication algorithm introduced a new heuristic approach to the decision version of the hidden subgroup problem, which we have extended to the dihedral group D_p when p is prime. Although this does not suffice to solve the problem, it at least provides new insights for future research on the topic. It is important to note that this algorithm is polynomial-time, in contrast to Kuperberg's subexponential algorithm for the same problem.

References

Arora, S. and Barak, B. (2009). *Computational Complexity: A Modern Approach*. Princeton.

Conrad, K. (2013). Dihedral groups II. course handout.

Costa, A. F., Hepp, H., da Silva, M. V., and Zatesko, L. M. (2023). The hidden subgroup problem and non-interactive perfect zero-knowledge proofs. In *Encontro de Teoria da Computação (ETC)*, pages 99–103. SBC.

Costa, A. F. B. (2024). Um algoritmo quântico para casos não abelianos de hsp. Dissertação de mestrado, Universidade Federal do Paraná.

Ettinger, M., Høyer, P., and Knill, E. (2004). The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letters*, 91(1):43–48.

Gavinsky, D. (2004). Quantum solution to the hidden subgroup problem for poly-near-hamiltonian groups. *Quantum Information & Computation*, 4(3):229–235.

Gonçalves, D. N., Fernandes, T. D., and Cosme, C. (2017). An efficient quantum algorithm for the hidden subgroup problem over some non-abelian groups. *TEMA (São Carlos)*, 18(2):215–223.

Grigni, M., Schulman, L., Vazirani, M., and Vazirani, U. (2001). Quantum mechanical algorithms for the nonabelian hidden subgroup problem. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 68–74.

Hallgren, S., Russell, A., and Ta-Shma, A. (2000). Normal subgroup reconstruction and quantum computation using group representations. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 627–635.

Hoffstein, J., Pipher, J., and Silverman, J. H. (1998). Ntru: A ring-based public key cryptosystem. In *International algorithmic number theory symposium*, pages 267–288. Springer.

Jozsa, R. (2001). Quantum factoring, discrete logarithms, and the hidden subgroup problem. *Computing in Science & Engineering*, 3(2):34–43.

Kitaev, A. Y. (1995). Quantum measurements and the abelian stabilizer problem. *arXiv preprint quant-ph/9511026*.

Kuperberg, G. (2003). A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *arXiv preprint quant-ph/0302112*.

Moore, C., Russell, A., and Schulman, L. J. (2008). The symmetric group defies strong fourier sampling. *SIAM Journal on Computing*, 37(6):1842–1864.

Nielsen, M. A. and Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press, 1 edition.

Regev, O. (2002). Quantum computation and lattice problems. In *Proc. 43rd Annual IEEE Symposium on Foundations of Comput. Sci.*, pages 520–529. IEEE.

Regev, O. (2004). A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space. *arXiv preprint quant-ph/0406151*.

Rotman, J. J. (2005). *A First Course in Abstract Algebra*. Pearson, 3 edition.

Sdroievski, N. M., da Silva, M. V., and Vignatti, A. L. (2019). The hidden subgroup problem and MKTP. *Theoretical Computer Science*, 795:204–212.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. IEEE.