УДК 373.5.016:004.4

QUANTUM PERIOD FINDING PROBLEM AS A DRIVER OF QUANTUM CRYPTANALYSIS

Yevgen Kotukh, Romain Murenzi, Aidan Zlotak

Abstract. The paper explores the foundational role of quantum period-finding algorithms, particularly in the context of cryptography. The work focuses on quantum algorithms that exploit periodicity, such as Shor's algorithm, which is central to efficient integer factorization. It emphasizes the challenges quantum algorithms face when applied to non-abelian groups like Suzuki, Hermitian, and Ree groups, which exhibit complex periodic structures that are difficult to solve with existing quantum techniques. The research delves into the structure and properties of these groups, explaining the complexity of their representations and the challenges quantum Fourier transform (QFT) presents in these cases. It contrasts the relative ease with which abelian groups can be addressed using quantum algorithms with the exponential complexity encountered with non-abelian groups. The study provides a comparative analysis of the computational complexity between classical and quantum approaches for period finding across various group types, highlighting that while quantum algorithms offer exponential speedup for abelian cases, non-abelian structures remain a frontier for further research. The conclusion calls for continued exploration in quantum representation theory and cryptanalysis, particularly for non-abelian groups, where current quantum techniques have not yet provided efficient solutions. The period-finding problem is identified as critical for advancing both quantum computing and cryptographic applications.

Keywords: quantum period finding problem, post-quantum security, hidden subgroup problem.

Introduction

Quantum Period Finding Algorithms are a central component of quantum computing, particularly in problems where periodicity plays a key role, such as Shor’s algorithm (for integer factorization) and other applications involving periodic functions over groups. These algorithms exploit the principles of quantum superposition and interference to find the period of a given function exponentially faster than classical algorithms. Below is an overview of the quantum period finding algorithm, its theoretical background, and a comparison with existing quantum and classical methods. To provide a comprehensive analysis of period-finding algorithms for different group types, including Suzuki, Hermitian, and Ree groups, we need to first understand the general structure and properties of these groups in relation to quantum algorithms, particularly period-finding.

Analysis on the literature

Quantum period-finding algorithms play a foundational role in quantum computing and cryptanalysis, particularly because of their application in Shor’s algorithm, which enables the efficient factorization of large integers and the computation of discrete logarithms. These tasks are critical to the security of many widely used cryptographic systems, such as RSA encryption. Peter Shor's groundbreaking work in 1994 demonstrated how a quantum computer could solve these problems exponentially faster than classical methods, posing a major challenge to classical cryptography [1]. Shor's algorithm uses the Quantum Fourier Transform (QFT) to identify the period of a given function, an approach that has become the basis for many quantum algorithms tackling cryptographic challenges. The period-finding algorithm is key to efficiently solving problems such as integer factorization, which is central to breaking RSA. This has sparked interest in quantum-resistant cryptographic systems [2-3].

Classical algorithms for period-finding, such as Pollard's Rho algorithm, have significant limitations when it comes to handling large inputs. Pollard's Rho algorithm, though effective for certain cyclic group structures, operates with an exponential time complexity, making it impractical for larger instances [4]. Classical brute-force methods are also infeasible for large periods, as they require checking every possible input until a repetition is found, with a complexity of O(T), where T is the period.

On the other hand, quantum algorithms like Shor's operate in polynomial time and offer an exponential speedup over classical methods. Shor's algorithm, in particular, has a time complexity of O((log N)^3), where N is the integer being factored, compared to the classical exponential complexity of O(exp(log N)^c) [1]. This dramatic speedup makes quantum period-finding a crucial tool in quantum cryptanalysis, where it can be applied to break classical cryptographic systems efficiently [5].

The Quantum Fourier Transform (QFT) is central to quantum period-finding algorithms, including Shor's algorithm. The QFT efficiently computes the frequency components of a periodic function, allowing for the identification of the period in logarithmic time relative to the size of the input. Shor's algorithm begins by initializing a superposition of states, applies a quantum oracle to compute the periodic function, and then uses the QFT to extract the period Nielsen2002. However, the application of QFT to non-abelian groups is significantly more complex. In cases involving non-abelian structures, such as Suzuki and Ree groups, the quantum Fourier transform is multi-dimensional and less straightforward, making period-finding in these groups an open research challenge [6]. These groups are critical to the study of Hidden Subgroup Problems (HSPs) in quantum cryptography, where current quantum algorithms fail to efficiently extract periodicity [7].

While quantum algorithms have shown great success with abelian groups, the non-abelian case remains much more difficult. Non-abelian groups, such as the Suzuki, Hermitian, and Ree groups, are more complex due to their multi-dimensional representations and the non-commutative nature of their elements. These properties make the application of quantum algorithms, particularly period-finding algorithms, exponentially harder [3].

For example, the Suzuki group is a non-abelian simple finite Lie-type group with twisted Chevalley structure. Quantum algorithms for period-finding struggle with these groups because their representation theory is much more involved, and no efficient QFT exists for such groups [6]. Similar challenges are observed with Hermitian (Unitary) and Ree groups, where the periodicity is tied to matrix eigenvalues or twisted automorphisms, and current quantum techniques do not offer efficient solutions [8].

The importance of period-finding algorithms in quantum cryptanalysis cannot be overstated. Quantum period-finding is at the core of many cryptographic attacks, most notably those that threaten the security of RSA and elliptic curve cryptography. Shor's algorithm, which uses period-finding to efficiently factor integers, directly undermines the RSA encryption scheme, as the security of RSA relies on the difficulty of factoring large integers [1]. Beyond RSA, quantum period-finding can also be applied to problems such as the discrete logarithm problem in both finite fields and elliptic curve groups. If efficient quantum algorithms for non-abelian groups were developed, it could lead to the breaking of cryptographic systems that rely on the hardness of these problems [9]. Despite the breakthroughs provided by quantum period-finding algorithms, significant challenges remain in applying these techniques to non-abelian group structures. Research continues into developing efficient quantum algorithms for the hidden subgroup problem (HSP) in non-abelian groups, which would allow quantum computers to solve a wider range of cryptographic problems [7]. The development of post-quantum cryptography, which aims to design cryptographic algorithms that are resistant to quantum attacks, is another critical area of ongoing research [10-11].

Purpose of the paper

The objective of this paper is to define the quantum period-finding problem, examine its current state with respect to non-abelian groups, and analyze the complexity criteria associated with the most prominent groups utilized in cryptographic applications.

Research results

The Suzuki, Hermitian, and Ree groups are specific examples of non-abelian groups, which adds a significant layer of complexity to quantum algorithms. While efficient period-finding algorithms exist for abelian groups and certain non-abelian cases (such as dihedral groups), the period-finding problem remains challenging in these more complex, Lie-type groups.

Suzuki Group is non-abelian, simple, finite, Lie-type, Twisted Chevalley Group. Its denoted as Sz(q), are part of the larger class of twisted Chevalley groups and are defined for fields of characteristic 2, where $q = 2^{2n+1}$. These groups are finite and non-abelian and arise from algebraic groups with certain automorphisms (field twisting). Suzuki groups exhibit highly symmetric, non-commutative structures. They exist for odd powers of 2, and they are classified as simple groups (groups with no non-trivial normal subgroups). The group has a complex internal structure, which involves field automorphisms and requires advanced techniques from Lie theory and algebraic geometry to describe. Order of Suzuki group $Sz(q): |Sz(q)| = q^2 (q-1)(q^2+1)$. Periodicity in Suzuki groups is extremely hard to analyze. Since Suzuki groups are non-abelian, their representation theory is much more complicated than that of abelian groups. Quantum algorithms that rely on Fourier sampling, such as Shor's algorithm, perform poorly for Suzuki groups because their structure leads to multi-dimensional representations. Quantum Fourier Transform (QFT) is not straightforward, and no efficient period-finding algorithms are known for Suzuki groups. Extracting subgroup information in Suzuki groups remains computationally challenging. Suzuki groups are studied in the context of finite simple groups and Lie-type groups, and solving the HSP for these groups would provide significant insights into the broader class of quantum problems. The lack of efficient algorithms reflects the general challenge of solving period-finding problems for non-abelian groups.

Hermitian (Unitary) Groups is non-abelian, classical group. Hermitian groups, also known as unitary groups, consist of matrices that preserve a Hermitian form (an inner product over complex vector spaces). A unitary group U(n, q) consists of n times n matrices over a field q, where each matrix satisfies the condition $U^{\dagger}U = I$ (preserving a Hermitian form). Hermitian groups are non-abelian when n > 1, making them part of the classical group family that preserves certain symmetries under transformations. These groups play an important role in quantum mechanics and quantum computing, as unitary transformations govern quantum evolution. Hermitian groups have complex eigenvalue structures, with periodicity tied to eigenvalue properties. Periodicity in Hermitian groups is connected to the behavior of eigenvalues. For example, the periodicity of unitary matrices involves rotational symmetries in complex vector spaces. The quantum Fourier transform (QFT) over unitary groups becomes more difficult to handle due to the multi-dimensional nature of the representations, especially as the matrix size n increases. Quantum algorithms that involve unitary matrices (such as quantum walk algorithms or HSP algorithms) must deal with periodicity that emerges from complex rotational symmetries. For period-finding algorithms, the challenge lies in efficiently identifying repeating eigenvalues or patterns in the matrix transformations, which is computationally intensive and requires significant post-processing. Hermitian groups are closely related to problems in quantum cryptography and quantum error correction, where unitary operations are fundamental. The HSP for unitary groups is not yet efficiently solvable, reflecting the broader difficulty of solving quantum problems for non-abelian groups. Periodicity extraction in such groups often requires techniques from representation theory and Lie algebras.

Ree Groups is non-abelian, simple, Lie-type, twisted Chevalley group. Its denoted $G_2(q)$ or $F_4(q)$, are finite simple groups defined over fields of characteristic 3 instead of 2 (as Suzuki does). Like the Suzuki groups, they belong to the class of twisted Chevalley groups and arise from specific automorphisms of algebraic groups. The order of Ree groups follows the structure of the underlying algebraic group (e.g., $G_2(q)$ and $F_4(q)$ certainly can be described using twisted field automorphisms. Order of Ree groups equal to $G_2(q) = q^3\left(q^3+1\right)(q-1)$, where $q = 3^n$. Periodicity in Ree groups is difficult to analyze due to their highly symmetric structure and the complexity of the twisted automorphisms that define them. Quantum algorithms struggle with the non-abelian nature of Ree groups, and there is no known efficient algorithm for solving period-finding or hidden subgroup problems in these groups. Ree groups' intricate structure leads to multi-dimensional representations that are not amenable to efficient Fourier sampling or the QFT, further complicating the extraction of periodic information. Like Suzuki groups, Ree groups are part of the classification of finite simple groups, and understanding how to solve the HSP for these groups is crucial for advancing quantum computing techniques. The complexity of periodicity in Ree groups reflects the broader difficulty of non-abelian groups in quantum algorithms. Solving period-finding problems for Ree groups would likely require breakthroughs in quantum representation theory and quantum information science.

Problem Definition. The quantum period-finding problem can be described as follows:
Given a function $f:\mathbf{Z}\to G$ where G is some group that is periodic with a period r (i.e. $f(x)=f(x+r)$ for all $x\in\mathbf{Z}$), the task is to determine the period r.

Steps in the Quantum Period Finding Algorithm

Step 1 Superposition. Initialize a quantum register in a superposition of all possible inputs $|x\rangle$, where $x\in\mathbf{Z}$:

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

Step 2. Function Evaluation. Apply a quantum oracle to compute the function $f(x)$, entangling the result with the input:

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|f(x)\rangle$$

The goal is to measure the period r of $f(x)$.

Step 3. Quantum Fourier Transform. Apply the QFT to the first register (which contains the superposition of inputs):

$$\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{2\pi ikx/r}|k\rangle$$

The QFT reveals the frequency components of the function, providing information about the periodicity.

Step 4. Measurement. After applying the QFT, measure the state of the system. With high probability, the result will yield a multiple of $1/r$, allowing you to deduce the period r.

The quantum period-finding algorithm runs in polynomial time, offering an exponential speedup compared to classical algorithms, which require exponential time in the worst case to determine the period. This is due to the fact that the QFT can be computed efficiently in $O\left(n^2\right)$ time, where n is the number of qubits used to represent the input space. There is an example of solving the problem is exist for 127 qubit IBM quantum computer. Period finding problem is the core of Shor's algorithm for factoring large integers. The period corresponds to the order of a number modulo N, and finding this period allows efficient factorization. Period finding is closely

related to the HSP in abelian groups, where identifying a hidden subgroup is equivalent to identifying the period of a function.

There are some classical approaches are existing. Classical brute force approaches for period finding require evaluating the function repeatedly for different inputs until a repetition is found. The complexity is $O(r)$, where r is the period. This method becomes infeasible for large periods. While Pollard's Rho algorithm offers a faster approach for finding periods in certain cyclic group structures (e.g., for discrete logarithms or integer factorization), it still operates in exponential time relative to the size of the input.

As mentioned earlier, Shor's algorithm uses quantum period finding as its core subroutine. It finds the period of a modular exponentiation function, which leads to efficient integer factorization. Complexity is equal to $O\left((\log N)^2\right)$ for factoring an N -bit integer.

Simon's Algorithm finds the period (or hidden XOR mask) of a function that is periodic under the XOR operation. It runs in polynomial time but solves a different type of periodicity problem compared to Shor's algorithm. Complexity is equal to $O(n^2)$, where n is the number of bits in the input.

Many quantum algorithms for the HSP rely on period-finding principles. For abelian groups, the complexity remains polynomial, but for non-abelian groups, the complexity increases significantly (often becoming exponential), as the quantum Fourier transform becomes harder to interpret. While Shor's and Simon's algorithms offer efficient period finding for specific types of periodicities (modular and XOR, respectively), their complexity remains polynomial. However, for non-abelian groups or other complex structures, quantum algorithms may not offer the same advantage.

Conclusion

Quantum period finding is one of the most significant breakthroughs in quantum computing, enabling efficient solutions to problems that are intractable classically. While these algorithms perform exceptionally well for abelian groups, non-abelian groups pose significant challenges. Further research is needed to unlock the full potential of quantum algorithms for non-abelian structures, but for now, quantum algorithms like Shor's and Simon's remain the most powerful tools for period finding in abelian settings. Comparison analysis results are presented in Table 1.

Table 1 – Comparison analysis

Group type	Periodicity	QFT application	Other quantum algorithms	Complexity	Quantum complexity	Remarks
Abelian	Definitely exists	Efficient, one-dimensional QFT is exist	Shor, Simon, Period Finding	$O(r)$ for brute-force period funding	$O\left((\log N)^2\right)$ for Shor algorithm	No challenges: Simple structure, clear periodicity, easy QFT.
Cyclic	Well-defined periodicity as order of group	Efficient, works similarly to abelian case.	Shor, Simon,	$O(N)$	$O\left((\log N)^2\right)$ for Shor algorithm	No challenges: most of problems solvable efficiently with QFT
Dihedral	Periodicity includes both rotation and reflection symmetry.	Challenging QFT due to non-abelian structure.	Sub-exponential algorithms for HSP	$O(r)$	Sub-exponential	Challenge: Non-abelian nature complicates subgroup finding.
Symmetric	Permutation-based	Exponentially complex QFT	No efficient	$O(n!)$	Exponential	Challenge: Multidimensional

	periodicity in cycle structures		algorithms known			QFT is required and remains an open problem.
Non-abelian	Complex periodicity, often difficult to identify	Multi-dimensional QFT, very complex	No efficient algorithms known	Exponential	Exponential	Challenge: Non-commutative nature of groups
Suzuki	Highly symmetric, non-abelian, twisted periodicity	Very challenging, no efficient QFT	No efficient algorithms known	Exponential	Exponential	Challenge: belongs to twisted Lie-type groups, difficult to analyze.
Ree	Highly symmetric, non-abelian, twisted periodicity	Very challenging, no efficient QFT	No efficient algorithms known	Exponential	Exponential	Challenge: belongs to twisted Lie-type groups, difficult to analyze.
Hermitian	Periodicity tied to matrix eigenvalue structure	Difficult due to matrix-based representations	No efficient algorithms known	Exponential	Exponential	Challenge: eigenvalue-based periodicity and QFT
Wreath product	Periodicity comes from product of cyclic and other groups	Multi-dimensional QFT, very complex	No efficient algorithms known	Exponential	Exponential	Challenge: complex combination of cyclic and dihedral structures.
Finite simple	Complex periodicity due to structure of simple groups	QFT generally infeasible for non-abelian	No efficient algorithms known	Exponential	Exponential	Challenge: same to Suzuki, Ree and other groups
Finite fields	Periodicity easy to define due to well-structured field	Efficient QFT for abelian subfields	Shor algorithm for finite fields	$O(q)$	$O\left((\log q)^2\right)$	Challenge: only abelian subgroups have efficient periodicity funding solution

The main challenge in applying quantum algorithms for the Hidden Subgroup Problem (HSP) in non-abelian groups stems from the complexity of efficiently extracting subgroup information using quantum Fourier transforms. In the case of abelian groups, Shor's algorithm and related methods succeed due to the ability to perform efficient quantum Fourier sampling, which captures enough information to identify the hidden subgroup. However, in non-abelian groups, the quantum Fourier transform becomes significantly more complex because the group representations are no longer one-dimensional. This complexity leads to difficulties in efficiently computing or interpreting the quantum Fourier samples, which are spread across higher-dimensional spaces. As a result, existing quantum algorithms struggle to pinpoint hidden subgroups in non-abelian groups, particularly when the subgroup is not normal or easily distinguishable. Moreover, the non-abelian HSP includes famously difficult problems like graph isomorphism, where the hidden subgroup problem for symmetric groups is notoriously hard. Attempts to generalize successful abelian methods to non-abelian cases often result in incomplete or suboptimal solutions, requiring new quantum algorithmic techniques or insights into representation theory. Additionally, non-abelian groups may exhibit more intricate and unpredictable behavior when sampling quantum states, complicating efforts to design effective algorithms.

References

1. Shor, P. W. (1997). *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM Journal on Computing, 26(5), 1484–1509. https://epubs.siam.org/doi/10.1137/S0097539795293172
2. Nielsen, M. A., & Chuang, I. L. (2002). *Quantum Computation and Quantum Information*. Cambridge University Press. https://shorturl.at/09toE
3. Watrous, J. (2009). Quantum Computational Complexity. In: Meyers, R. (eds) Encyclopedia of Complexity and Systems Science. Springer, New York, NY. https://doi.org/10.1007/978-0-387-30440-3_428
4. Pollard, J. M. (1975). *A Monte Carlo method for factorization*. BIT Numerical Mathematics, 15(3), 331-334. https://link.springer.com/article/10.1007/BF01933667
5. Simon, D. R. (1994). *On the Power of Quantum Computation*. Proceedings of the 35th Annual Symposium on Foundations of Computer Science. https://ieeexplore.ieee.org/document/365701
6. Roetteler, M., & Beth, T. (1998). *Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups*. arXiv preprint quant-ph/9812070. https://arxiv.org/abs/quant-ph/9812070
7. Kuperberg, G. (2005). *A subexponential-time quantum algorithm for the dihedral hidden subgroup problem*. SIAM Journal on Computing, 35(1), 170–188. https://epubs.siam.org/doi/10.1137/S0097539703436345
8. Hallgren, S., Russell, A., & Ta-Shma, A. (2003). *The hidden subgroup problem and quantum computation using group representations*. SIAM Journal on Computing, 32(4), 916–934. https://epubs.siam.org/doi/abs/10.1137/S0097539701391800
9. Bernstein, D. J., & Lange, T. (2017). *Post-quantum cryptography*. Nature, 549(7671), 188-194. https://www.nature.com/articles/nature23461
10. Regev, O. (2005). *On lattices, learning with errors, random linear codes, and cryptography*. Journal of the ACM, 56(6), 1-40. https://dl.acm.org/doi/10.1145/1568318.1568324
11. Peikert, C. (2016). *A decade of lattice cryptography*. Foundations and Trends in Theoretical Computer Science, 10(4), 283–424. https://shorturl.at/0CFgn
12. Y. Kotukh, G. Khalimov. *Hard Problems for Non-abelian Group Cryptography*. Fifth International Scientific and Technical Conference" Computer and Information systems and technologies". https://doi.org/10.30837/csitic52021232176
13. Y. Kotukh, G. Khalimov. *Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures*. INFORMATION SECURITY: PROBLEMS AND PROSPECTS". https://shorturl.at/IaByX
14. Y. Kotukh, G. Khalimov. *Advantages of logarithmic signatures in the implementation of crypto primitives*. Challenges and Issues of Modern Science. https://cims.fti.dp.ua/j/article/download/119/158
15. Y. Kotukh. *Quantum cryptoanalysis of prospective asymmetric cryptosystems*. Proceedings of conference “Cybersecurity in energy sector”. https://shorturl.at/1pbcK

Відомості про авторів:

Котух Євген Володимирович - кандидат технічних наук, доцент, професор кафедри безпеки інформації та телекомунікацій Національного Технічного Університету «Дніпровська Політехніка», тел. +380503382693, e-mail: yevgenkotukh@gmail.com

Romain Murenzi – доктор філософії в фізиці, професор фізики в Вустерському Технологічному Інституті, Вустер, Массачусетс, США, тел. +1 (508) 8316960, email: rmurenzi@wpi.edu

Aidan Zlotak – асистент, аспірант кафедри фізики, в Вустерському Технологічному Інституті, Вустер, Массачусетс, США, тел. +19548548727, email: ahzlotak@wpi.edu