# CPSC 436Q Project Proposal

Marcus Lai, Vincent Ling, Rain Zimin Yang
University of British Columbia

## 1 Topic

We will explore the hidden subgroup problem (HSP) and the quantum Fourier transform (QFT). Our focus will be on the methods used to solve the HSP for general abelian groups, and examine how the group structure allows for efficient quantum algorithms.

If time permits, we will extend our investigation to the HSP for non-abelian groups, specifically the dihedral group. This is significantly more complex, and it remains unsolved. Finally, we will explore its connection to the lattice problem, which is a key challenge in cryptography and computation complexity.

## 2 Timeline

Below is our proposed timeline.

**Now – Nov 1.** Go through resources on QFT, specifically pages 216-242 [1], pages 6-8 of [2], and [3]. Start writing about QFT in the paper.

**Nov 1. – Nov 15.** Explore the hidden subgroup problem. With focus on [2] (pages 8-16), [4] (chapter 6, 11-13), and [5].

**Nov 15. – End of Term** Write up learnings and findings. Explore the Lattice Problem if time permits [6] [7] [8] [9].

## References

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 1 2011. [p. 1]

[2] A. M. Childs and W. Van Dam, "Quantum algorithms for algebraic problems," *Reviews of Modern Physics*, vol. 82, pp. 6–8, 1 2010. [p. 1]

[3] P. Hoyer, "Efficient quantum transforms," 1997. [p. 1]

[4] A. Childs, "Lecture notes on Quantum algorithms." [p. 1]

[5] C. Lomont, "The hidden subgroup problem - review and open problems," 2004. [p. 1]

[6] Y.-K. Liu, "An uncertainty principle for the curvelet transform, and the infeasibility of quantum algorithms for finding short lattice vectors," 2023. [p. 1]

[7] Y. Chen, Q. Liu, and M. Zhandry, "Quantum algorithms for variants of average-case lattice problems via filtering," 2021. [p. 1]

[8] R. Cramer, L. Ducas, C. Peikert, and O. Regev, "Recovering short generators of principal ideals in cyclotomic rings.," *IACR Cryptology ePrint Archive*, vol. 2015, p. 313, 2015. [p. 1]

[9] Y. Chen, "Quantum algorithms for lattice problems.," *IACR Cryptol. ePrint Arch.*, vol. 2024, p. 555, 2024. [p. 1]