CPSC 436Q Project

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

Abstract

Next Steps and Updated Timeline

The focus of our project is meant to be on the hidden subgroup problem. Since we hope to minimize the overlap between this report and the material in lectures, we decide to only introduce QFT briefly and consider one application (phase estimation). From here, our plans were to explore the solution for the hidden subgroup problem for abelian groups and considering more specific problems for which the hidden subgroup problem is a generalization. Further directions could also include exploring 1) progress on the hidden subgroup problem for nonabelian groups, 2) QFT implementational speedups. What remains to be done is the following:

1. clean up and formalize the QFT introduction and phase estimation
2. discuss the proof of the hidden subgroup problem for abelian groups (we have already gone through the proof, just need to internalize put it down)
3. find and go through more references for the hidden subgroup problem (we have mainly focused on [CVD10], [Lom04], [NC11])
4. explore applications such as Pell's Equations

Below is our updated timeline.
Nov 11. - Nov 18. Find and go through more references about the hidden subgroup problem and QFT to get a more well-rounded understanding. Start exploring 2, 3 applications of the hidden subgroup problem, noting down new papers and references.
Nov 18. - Nov 25. By this point, put down the proof of the hidden subgroup problem for albelian groups. Finish exploring the 2, 3 chosen applications of the hidden subgroup problem and start writing findings. Find resources on the hidden subgroup problem for nonabelian groups.
Nov 25. - Dec 2. Explore the hidden subgroup problem for nonabelian groups. Write about findings.
Dec 2. - Dec 6. Finalize paper.

1 Introduction

2 The Quantum Fourier Transform

The Fourier Transform classifcally.... Turns out, the discrete fourier transform is something that could be implemented efficiently with a quantum circuit... Furthermore, it serves as the foundation for many applications...

Definition 2.1 (the quantum Fourier Transform)**.** *Given an orthonormal basis* $|0\rangle, |1\rangle, ..., |N-1\rangle$ *for some* $N \in \mathbb{N}$*, the quantum Fourier Transform (QFT) is the unitary matrix* Q *such that* $\forall j \in [N]$*,*

$$Q|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle . \tag{1}$$

(a comment on why it's unitary). More generally, we can define the QFT over abelian groups G

$$F_G := ....$$

We also introduce an alternate form to *Eq.* (1).

Proposition 2.2 (alternate representation of the QFT)**.** *Given an orthonormal basis* $|0\rangle, |1\rangle, ..., |2^n-1\rangle$*,* $\forall j \in [2^n]$ *and let* $j_1 j_2 ... j_n$ *be the binary representation of* j*. Then Eq.* (1) *(for* $N = 2^n \in \mathbb{N}$*) is equivalent to*

$$\frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.j_1 j_2 ... j_n}|1\rangle)}{2^{n/2}}$$

where $0.j_l j_{l-1} ... j_m = j_l/2 + j_{l-1}/2^2 + ... + j_m/2^{l-m+1}$*.*

Proof. We follow the approach of Nielsen and Chuang.

$$Q|j\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_n=0}^{1} \sum_{k_2=0}^{1} ... \sum_{k_1=0}^{1} e^{2\pi ij(\sum_{l=1}^{n} k_l 2^{n-l})/2^n} |k_1 k_2 ... k_n\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_n=0}^{1} \sum_{k_2=0}^{1} ... \sum_{k_1=0}^{1} e^{2\pi ij(\sum_{l=1}^{n} k_l 2^{-l})} |k_1\rangle |k_2\rangle ... |k_n\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_n=0}^{1} \sum_{k_2=0}^{1} ... \sum_{k_1=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi ij(k_l 2^{-l})} |k_l\rangle$$

Invoke the mixed-product property to get

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \sum_{k_l=0}^{1} e^{2\pi ij(k_l 2^{-l})} |k_l\rangle$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} (|0\rangle + e^{2\pi ij2^{-l}} |1\rangle)$$

Finally, we note that $j2^{-l}$ can be seen as shifting the binary representation of j down l positions. We also recognize that the integral part of $j2^{-l}$ generates integer multiples of $2\pi i$ in the exponent of e. So we have

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} (|0\rangle + e^{2\pi i 0.j_{n-l+1}...j_n} |1\rangle)$$

$$= \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.j_1 j_2 ... j_n}|1\rangle)}{2^{n/2}}$$

as required. □

2.1 Phase Estimation

Phase Estimation is an elementary but important application of the quantum Fourier Transform. Given a unitary matrix U with eigenvector $|u\rangle$, the algorithm seeks to find the eigenvalue $e^{2\pi i\psi}$ of $|u\rangle$. Note that it is well known that eigenvalues of unitary matrices have norm 1, thus any eigenvalue $v \in \mathbb{C}$ of U is expressible as $e^{2\pi i\psi_v}$ for some $\psi_v \in [0, 1)$.

The idea of the algorithm is to exploit the properties of eigenvalues to construct the post Fourier transformation of a particular basis vector, then perform the inverse Fourier transform (which we know exist since the QFT is invertible as an unitary operation).

Consider first applying a Hadamard gate to $|0\rangle$ then performing a controlled-U operation from this bit to $|u\rangle$. Then

$$|0\rangle |u\rangle \xrightarrow{H} \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} |u\rangle = \frac{(|0\rangle |u\rangle + |1\rangle |u\rangle)}{\sqrt{2}}$$

$$\xrightarrow{controlled-U} \frac{(|0\rangle |u\rangle + |1\rangle U |u\rangle)}{\sqrt{2}} = \frac{(|0\rangle |u\rangle + e^{2\pi i\psi} |1\rangle |u\rangle)}{\sqrt{2}} = \frac{(|0\rangle + e^{2\pi i\psi} |1\rangle)}{\sqrt{2}} |u\rangle .$$

In particular, we note that applying controlled-U does not transform $|u\rangle$, allowing us to reuse $|u\rangle$ throughout our procedure. By reproducing this sequence with U^{2^j} for $j \in [n]$, we get

$$\frac{(|0\rangle + e^{2\pi ij\psi} |1\rangle)}{\sqrt{2}} |u\rangle .$$

By aggregating the result of this sequence for all $j \in [n]$, we obtain (excluding the $|u\rangle$ register which stays constant)

$$(\frac{(|0\rangle + e^{2\pi i2^{n-1}\psi} |1\rangle)}{\sqrt{2}})(\frac{(|0\rangle + e^{2\pi i2^{n-2}\psi} |1\rangle)}{\sqrt{2}})...(\frac{(|0\rangle + e^{2\pi i2^{0}\psi} |1\rangle)}{\sqrt{2}}) \tag{2}$$

$$= \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ik\psi} |k\rangle$$

To see the last equality, notice when we distribute the products in Eq. (2), the jth term multiplied yields $|0\rangle$ or $e^{2\pi j2^j\psi}$. So .... We notice this is precisely the quantum Fourier Transform of $|j\rangle$ such that $j/2^n = \psi$. So we can simply invert the transformation, measure to obtain j, and infer ψ. Notice however since $j \in [n]$, there only exist a finite number of ψ that we can infer. Namely, given a fixed n, we do not have arbitrary precision on ψ. To appreciate this more analytically, we consider the alternative representation of QFT.

3 The Hidden Subgroup Problem

Before stating the statement of the problem, we need some notation and definitions.

3.1 Mathematical Foundations

Definition 3.1 (Abstract Group). *A group is an ordered pair $(G, *)$ where G is a set and $* : G \times G \to G$ is a binary operation on G that satisfies the following:*

1. *Associativity: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$,*

2. *Identity: there exists an element $e \in G$ such that $g * e = e * g = g$ for all $g \in G$,*

3. Inverse: for every $g \in G$, there exists is an element g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

We say $(H, *)$ is a subgroup of $(G, *)$ if $H \subseteq G$, and $(H, *)$ is a group.

Note that an abstract group doesn't have to be commutative, that is, for $a, b \in G$, we don't necessarily have $a * b = b * a$. When $a * b = b * a$ for all $a, b \in G$, we say $(G, *)$ is abelian.

Definition 3.2. *(Coset) Let H be a subgroup of G, we define the **left cosets** of G with respect of H as the sets $gH = \{gh, h \in H\}$, note that we could define **right cosets** in similar fahsion*

For more information about groups, we refer to the textbook [DF03].

We will mainly focus on finite groups, that is, when $|G|$ is finite.

Theorem 3.3 (Fundamental Theorem of Finite Abelian Group)**.**

We now present the general definition of the Hidden Subgroup Problem.

Definition 3.4 (The Hidden Subgroup Problem)**.** *A function $f : G \to X$ from a group G to a finite set X is said to hide a subgroup H of G if $f(x) = f(y) \Leftrightarrow x$ and y are in the same coset of H, that is, $x - y \in H$. Given this function f, find a subset of H such that every element of H is a finite product of elements from this set, i.e., find a generating subset of H.*

The finite abelian hidden subgroup problem has been completely solved.

3.2 Classical Approach

3.3 Quantum Approach

4 Solving Pell's Equation

References

[CVD10] Andrew M. Childs and Wim Van Dam. Quantum algorithms for algebraic problems. *Reviews of Modern Physics*, 82(1):6–8, 1 2010. doi:10.1103/revmodphys.82.1. [p. 1]

[DF03] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2003. URL: https://books.google.ca/books?id=KJDBQgAACAAJ. [p. 4]

[Lom04] Chris Lomont. The hidden subgroup problem - review and open problems, 2004. URL: https://arxiv.org/abs/quant-ph/0411037, arXiv:quant-ph/0411037. [p. 1]

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 1 2011. URL: https://dl.acm.org/citation.cfm?id=1972505. [p. 1]