Group Theoretic Overview of the Quantum Core in Shor's algorithm

Parthasarathi Nag

Black Hills State University

Quantum Partnership Workshop
SURF, July 21-24 2026

In this presentation we will discuss the application of group theory and Quantum Fourier Transform [QFT] for finite abelian groups in particular as it relates to Shor's algorithm. Then illustrate it with an example the hidden subgroup problem as it relates to Shor's algorithm.

Finite abelian Group preliminaries

A finite abelian group G is a set together with binary operation $\circ : G \times G \to G$ such that :(a) $g, h \in G$ then $g \circ h \in G$. (closure property), (b) $(g \circ h) \circ i = g \circ (h \circ i)$ (associativity), (c) there exist a identity element e such that $e \circ g = g \circ e = g$, (d) $g \in G$ there exists $g^{-1} \in G$ such that $g \circ g^{-1} = g^{-1} \circ g = e$, (e) $g, h \in G$ if $g \circ h = h \circ g$ then G is called abelian and finally (f) the order of the group $|G| < \infty$.

Example of finite abelian group $Z_n = Z/nZ$ a finite abelian group of whose operation $\circ$ is addition modulo n and the order of the group is n.

Finite abelian Group preliminaries

A subgroup $H \subset G$ is a subgroup if it is a group with the operation $\circ$. In particular if $a, b \in H$ then $a \circ b^{-1} \in H$.

Let's discuss the following subgroup of Z_n which we will denote as H_d where d is a divisor of n. Then
$H_d = \langle n/d \rangle = \{0, n/d, 2n/d, \ldots, (d-1)n/d\}$.

The structure theorem for finite abelian group states that G decomposes uniquely (up to ordering) as $G \cong Z_{p_1^{n_1}} \times \cdots Z_{p_k^{n_k}}$

Finite abelian Group preliminaries

Representation of an abelian group G is a group homomorphism $\chi : G \to \mathbf{C}^{\times}$.

In particular for the group Z_n there are at most n representations. Hence, for each $j \in Z_n$ and any $x \in Z_n$ we have the following representation $\chi_j(x) = exp(\frac{2\pi i}{n} jx)$

Note: $\chi(1)^n = \chi(n \cdot 1) = \chi(0) = 1$. Hence, $\chi_j(1) = exp(\frac{2\pi i}{n} j)$, for $j = 0, 1, \ldots (n-1)$. Hence, there are n representations. Thus, $\chi_j(x) = \chi_j(1 + \cdots + 1) = exp(\frac{2\pi i}{n} jx)$

Finally, for a subgroup $H \subset Z_n$ then $H^{\perp} = \{j \in Z_n \mid \chi_j(h) = 1, \forall h \in H\}$. Finally the Pontryagin dual is given by $H^{\perp\perp} = H$.

Remark: The subgroups H and $H^{\perp}$ are both unknown. Hence, it is a unknown subgroup problem which is solved by QFT

Shor's Factoring Algorithm in brief

Step 1: Consider factoring an integer M. Then, choose an integer $0 < a < M$ such that a, M are coprime.

Step 2a: Use Quantum parallelism to compute $f(x) = a^x \ (mod\ M)$ where $x \in \{0, \ldots, 2^n - 1\}$, where n is such that $M^2 \leq 2^n < 2M^2$. Essentially Quantum parallelism uses an unitary map $U_f(|x\rangle|0\rangle) = |x\rangle|f(x)\rangle$ to obtain the superposition $\frac{1}{\sqrt{2^n}} \Sigma_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$

Step 2b: Apply Quantum Fourier Transform to the superposition.

Step 3: Measure. With high probability a value v close to a multiple of $\frac{2^n}{r}$ will be obtained where $r > 0$ is unknown and $a^r = 1 \ (mod\ M)$.

Shor's Factoring Algorithm in brief

Step 4: Use classical algorithm to obtain a period r' from the value v.

Step 5: When r' is even, use the Euclidean algorithm to check whether $a^{r'/2} + 1$ or $a^{r'/2} - 1$ has a common factor with M.

Step 6: Repeat all steps if necessary.

It is important to note Quantum computation is required only in Steps 2a, 2b and 3. All other steps can be carried out on a classical computation device.

Quantum Core on finite abelian group Z_n

Assume that $G = Z_n$ and let us apply the Shor's algorithm to finding the period of a function $f(x+r) = f(x)$. Also, assume that $r|n$.

This defines the subgroup $H = \{kr \mid k \in [0, \ldots, n/r)\}$. The problem is to find the generator r of the subgroup H.

Now, find the representations for Z_n and it is given by $\chi_j(h) = exp(\frac{2\pi i}{n} jh),\ h \in H$.

Then, $H^{\perp} = \{y \mid exp(\frac{2\pi i}{n} yh) = 1, \forall h \in H\}$. Hence, $H^{\perp} = \{y \mid yh = 0\ (mod\ n)\} = \{y \mid ykr = 0\ (mod\ n), \forall k \in [0, \ldots, n/r)\}$

Quantum Core on finite abelian group Z_n

Now for $k = 1$ we have $yr = 0 \ (mod \ n)$, hence $n|yr$ or $n/r|y$. Thus, $y = 0 \ (mod \ n/r)$, therefore $y \in \{0, n/r, 2n/r, \ldots, (r-1)n/r\}$. Thus, $H^{\perp}$ is a subgroup of order r with generator n/r.

We apply the quantum parallelism with U_f to the first register $\frac{1}{\sqrt{n}}\Sigma_{x=0}^{n-1}|x\rangle|0\rangle$ to obtain $\frac{1}{\sqrt{n}}\Sigma_{x=0}^{n-1}|x\rangle|f(x)\rangle$. Note: $f(x)$ is stored in the second register.

Measure the second register where the outcome is $y_0 = f(x_0)$ where $x_0 \in \{0, 1, \ldots, r-1\}$. The first register collapses to a **uniform coset superposition** $|\psi\rangle = \frac{1}{\sqrt{n/r}}\Sigma_{k=0}^{n/r-1}|x_0 + kr\rangle$.

Quantum Core on finite abelian group Z_n

Now, the apply Quantum Fourier Transform or $QFT(|\psi\rangle) = QFT(\frac{1}{\sqrt{n/r}}\Sigma_{k=0}^{n/r-1}|x_0 + kr\rangle) = \frac{1}{\sqrt{n/r}}\Sigma_{k=0}^{n/r-1}QFT(|x_0 + kr\rangle)$

$$QFT(|\psi\rangle) = \frac{1}{\sqrt{n/r}}\Sigma_{k=0}^{n/r-1}\frac{1}{\sqrt{n}}\Sigma_{y=0}^{n-1}(exp(\frac{2\pi i}{n}))^{(x_0+kr)y}|y\rangle$$

$$QFT(|\psi\rangle) = \frac{1}{\sqrt{n/r}}\Sigma_{k=0}^{n/r-1}exp(\frac{2\pi ikry}{n})\frac{1}{\sqrt{n}}\Sigma_{y=0}^{n-1}(exp(\frac{2\pi i}{n}x_0y))|y\rangle$$

Now, if $y \in H^{\perp}$ then $\Sigma_{k=0}^{n/r-1}exp(\frac{2\pi ikry}{n}) = n/r$. Hence,
$QFT(|\psi\rangle) = \frac{1}{\sqrt{r}}\Sigma_{y=0}^{(r-1)n/r}(exp(\frac{2\pi i}{n}x_0y))|y\rangle$.

The measurement outcome y is drawn uniformly at random with probability $1/r$ from $H^{\perp}$.

$H^{\perp} = \{outcomes\ with\ constructive\ interference\} = \{outcomes\ with\ non-zero\ probability\}$. Since the interference is perfect $(r|n)$ the only non-zero probability $P(y) = 1/r, y \in H^{\perp}$.

Quantum Core on finite abelian group Z_n

Thus, from the measurement, we obtain $y = jn/r$ for some $j \in \{0, \ldots, r-1\}$

Compute $y/n = j/r$. Then apply the continued fraction algorithm which takes the best rational approximations p/q with small denominator q. When $gcd(j, r) = 1$, the fraction j/r is already in lowest terms and the algorithm return $q = r$, the period.

Finally, in summary what QFT does is establish the Pontryagin duality between H and $H^{\perp}$. In other words the QFT maps $\frac{1}{\sqrt{n}}\Sigma_k|x_0 + kr\rangle$ to $\frac{1}{\sqrt{r}}\Sigma_{y \in H^{\perp}} exp(2\pi i x_0 y/n)|y\rangle$.

An example: Factor $M = 21$ using Shor's algorithm

Step 1: Let $a = 2$ since $gcd(2, 21) = 1$

Step 2a: Then, $f(x) = 2^x \ (mod\ 21)$ where $M^2 = 21^2 \leq 2^9 < 2M^2 = 2 \times 21^2$. Then, $x \in \{0, 1, 2, \ldots, 2^9 - 1\}$ Then, Register 1: $|x\rangle, x \in \{0, 1, \ldots, 511\}$ and Register 2: $|f(x)\rangle = |2^x \ (mod\ 21)\rangle$. Applying, the unitary map to obtain Quantum parallelism to obtain the superposition $\frac{1}{\sqrt{512}} \Sigma_{x=0}^{511} |x\rangle |2^x \ (mod\ 21)\rangle$
Note: Here the **finite abelian group is** Z_{512}

Thus, the two registers are as follows: Register 1:$|x\rangle, x \in \{0, 1, 2, 3, 4, 5 \ldots, 511\}$ and Register 2:$|f(x)\rangle, f(x) \in \{0, 1, 4, 8, 16, 11, \ldots, \}$. This sequence repeats with period $r = 6$.

Thus, $H = \{6k \mid k \in [0, \ldots, \lfloor 512/6 \rfloor] = \langle 6 \rangle$.

An example: Factor $M = 21$ using Shor's algorithm

Step 2a: Measure the second register $y_0 = 4 = f(x_0) = f(2)$ Then, Register 1 collapses to the coset $x_0 + H = 2 + \langle 6 \rangle$ Thus, $|\psi\rangle = \frac{1}{\sqrt{85}} \Sigma_{k=0}^{84} |2 + 6k\rangle$.

Step 2b: We apply QFT as follows: $H^{\perp} = \{0, 85.33, 170.67, 256, 341.33, 426.67\}$. Thus, the output of QFT peaks at multiples of $512/6$ similar to standard Fourier transform.

Step 3: Suppose we measure $v = 171$.

Step 4: We apply the continued fraction algorithm to $v/n = 171/512$ Approximately, this is a continued fraction expansion of $171/512$ with certain ϵ error bound. We obtain $171/512 \approx 2/6 = 1/3$.

Step 5: Thus, $r = 6$ which is even and $q = 3$. Hence, the factor of $21 = 3 \times 7$!!!

Key take away is that QFT is essentially an operator that computes the Pontryagin dual of H which is $H^{\perp}$.

Afterwords: Hardware

The Quantum computer hardware which enables solving this hidden subgroup problem consist of Quantum gates which are Hadamard Gates, CNOT, controlled phase rotations, SWAP gates to reverse the output qubit order similar to the classical computer Logic gates which are AND, OR, NOT.

The QFT circuit which consists of Hadamard Gates and controlled phase rotations to produce the constructive interference, similar to arithmetic unit in classical computer like ADD, MUL.

Then, we have the qubit measurement, similar to the memory read from a classical computer.

The output is the classical bit string y

Bibliography

Quantum Computation and Quantum Information, Michael Nielsen and Issac Chuang

Quantum Computing since Democritus, Scott AAroson

Quantum Quantum Computing For everyone, Chris Bernhardt

Abstract Algebra, John Beachy and William Blair

Quantum Computing A Gentle Introduction, by Eleanor Rieffel and Wolfgang Polak