Shor's Algorithm and the Quantum Fourier Transform

Samar A. Aseeri

April 15, 2026

Overview of Shor's Algorithm

- Developed by Peter Shor in 1994.
- A quantum algorithm for integer factorization.
- Efficiently factors large integers in polynomial time.
- Key application: Breaking RSA encryption.

Classical vs Quantum Factorization

- Classical algorithms (e.g., Pollard's rho) take exponential time.
- Shor's algorithm runs in polynomial time:
  $O\left((\log N)^2(\log\log N)(\log N)\right)$
- Utilizes quantum parallelism and interference.

Steps of Shor's Algorithm

1. Choose a random integer a such that $1 < a < N$.
2. Compute the greatest common divisor (GCD): $r = \gcd(a, N)$
3. If r is even, proceed; otherwise, repeat.
4. Use the Quantum Fourier Transform to find the order r of a modulo N.
5. Use r to find factors of N.

Quantum Fourier Transform

- The QFT for N qubits is defined as: $\mathrm{QFT}_N = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} e^{\frac{2\pi i}{N} jk} |j\rangle$
- It transforms the state $|x\rangle$ into a superposition of frequency components.

Matrix Representation of QFT

- The QFT can be represented as a unitary matrix U: $U_{jk} = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N} jk}$
- For $N = 4$: $U = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{\frac{2\pi i}{4}} & e^{\frac{2\pi i \cdot 2}{4}} & e^{\frac{2\pi i \cdot 3}{4}} \\ 1 & e^{\frac{2\pi i \cdot 2}{4}} & e^{\frac{2\pi i \cdot 4}{4}} & e^{\frac{2\pi i \cdot 6}{4}} \\ 1 & e^{\frac{2\pi i \cdot 3}{4}} & e^{\frac{2\pi i \cdot 6}{4}} & e^{\frac{2\pi i \cdot 9}{4}} \end{pmatrix}$

Role of QFT in Shor's Algorithm

- QFT is used to efficiently find the period r of the function: $f(x) = a^x \mod N$
- The transformation is performed on $O(\log N)$ qubits.
- The output of QFT helps in determining the order r with high probability.

Conclusion

- Shor's algorithm demonstrates the power of quantum computing.
- The Quantum Fourier Transform is a critical component enabling efficient factorization.
- Potential implications for cryptography and security.

References

- Aseeri, S. (2025). Distributed Memory Fast Fourier Transforms. *IEEE*.
- Leu, B., Aseeri, S., & Muite, B. K. (2021). A comparison of parallel profiling tools for programs utilizing the FFT. *International Conference on High Performance Computing in Asia-Pacific Region*.
- Muite, B. K., & Aseeri, S. (2019). Benchmarking solvers for the one dimensional cubic nonlinear klein gordon equation on a single core. *International Symposium on Benchmarking, Measuring and Optimization*, 172-184.
- Aseeri, S., Muite, B. K., & Takahashi, D. (2019). Data for figures in "Reproducibility in Benchmarking Parallel Fast Fourier Transform based Applications".