Shor's Algorithm Does Not Factor Large Integers in the Presence of Noise

Jin-Yi Cai
University of Wisconsin - Madison

Primes ... and Prime Factorizations

The Prime Factorization problem is to factor an arbitrary integer N into its (unique) expression as a product of primes

$$N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

The dignity of science requires that every possible means be explored for the solution of a problem so elegant and so celebrated.
— C. F. Gauss

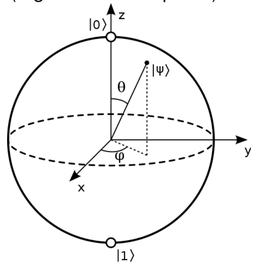
Theorem [Hadamard, de la Vallée]: There are about $\frac{N}{\ln N}$ primes up to integer N.
Theorem [Fouvry]: There is a positive density of primes p such that $p-1$ has a largest prime factor $> p^{2/3}$.

Shor's Factoring Algorithm

In 1994, Peter Shor [1] gave a **quantum** polynomial-time algorithm that can factor large integers. This is the **single most important** algorithm in quantum computing. If such algorithms can be realized in practice, then public-key cryptographic systems such as **RSA** can be broken. **Billions** of dollars have been spent in this quest, and many more billions are planned.
Billions and Billions ... — Carl Sagan

Qubits and quantum operations

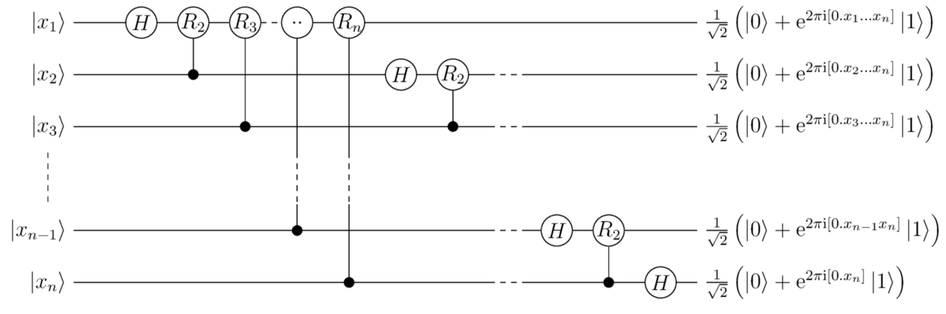
Unlike classical computing where the basic elements are the bits 0 and 1, quantum information processing is built on *qubits* which can be viewed as a unit length vector on the sphere (Figure from Wikipedia).



Quantum operations are rotations and reflections in these spheres. Multiple qubits reside in *superpositions* in a tensor product space, called a **Hilbert** space.
An important quantum operation is a (controlled-)rotation $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$, with angle $\frac{2\pi}{2^k}$. This is **tiny** for large k.

Quantum Fourier Transform

The magic step in Shor's algorithm is the following Quantum Fourier Transform (Figure from Wikipedia)



But, in any physical realization, one can expect some noise to be present. What happens to Shor's algorithm when a little bit of noise is introduced?
Consider an error model, where the operator R_k is substituted by

$$\widetilde{R_k} = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i(1+\epsilon r)/2^k} \end{bmatrix},$$

where $r \sim N(0,1)$ is an *independent* normally distributed noise random variable, and ϵ is a global magnitude parameter.

Main Results

Theorem 1 *[2] If each controlled-R_k-gate in the quantum Fourier transform circuit is replaced by controlled-$\widetilde{R_k}$-gate, even with a vanishingly small amount of noise $\epsilon(n) \to 0$, Shor's algorithm* **does not** *factor n-bit integers of the form pq, where p and q are Fouvry primes, with high probability over quantum measurements.*

The level of noise where failure provably occurs is when $\epsilon = \epsilon(n)$ exceeds

$$\epsilon_0 \approx O(n^{-1/3}).$$

The failure is with probability exponentially close to 1, as $n \to \infty$.

Theorem 2 *[2] With the same level of noise, Shor's algorithm* **fails**, *with probability close to 1, to factor $N = pq$ for uniformly randomly chosen n-bit primes p and q, as $n \to \infty$.*

The theorems actually go further, so that failure happens even if we only introduce noisy quantum gates at level R_b, as long as

$$b + \log_2(1/\epsilon) < \frac{1}{3}\log_2 m - c.$$

A Taste of the Proof

With independent random noise present starting with controlled-R_b-gates, we need to analyse the quantity

$$\frac{1}{2^n K}\left|\sum_{k=0}^{K-1} \exp\left\{2\pi i\left[\sum_{t=1}^{n} \frac{\sum_{s=0}^{n-t} u_{n-t-s}^{(k)} v_s}{2^t} + \frac{\epsilon}{2^b}\left\{\left(u_{n-b}^{(k)} r_0^{(0)} + \cdots + \frac{u_0^{(k)} r_{n-b}^{(0)}}{2^{n-b}}\right) v_0 + \left(u_{n-b-1}^{(k)} r_0^{(1)} + \cdots + \frac{u_0^{(k)} r_{n-b-1}^{(1)}}{2^{n-b-1}}\right) v_1 + \ldots + u_0^{(k)} r_0^{(n-b)} v_{n-b}\right\}\right]\right\}\right|^2 \quad (1)$$

where

$$r_0^{(0)}, \ldots, r_{n-b}^{(0)}, r_0^{(1)}, \ldots, r_{n-b-1}^{(1)}, \ldots, r_0^{(n-b-1)}, r_1^{(n-b-1)}, r_0^{(n-b)}$$

are random variables i.i.d. $\sim N(0,1)$. After some work it turns out that the crux is to analyse the following sum

$$\frac{\epsilon}{2^b}\left(u_{n-b}^{(k)} v_0 r_0^{(0)} + u_{n-b-1}^{(k)} v_1 r_0^{(1)} + \ldots + u_0^{(k)} v_{n-b} r_0^{(n-b)}\right) = \frac{\epsilon}{2^b}\sum_{i=b}^{n} u_{i-b}^{(k)} v_{n-i} r_0^{(n-i)}. \quad (2)$$

This quantity appears as a subsum in the exponent in $\exp\{2\pi i[\ldots]\}$ in (1).
The main proof is to establish that, the sum (2) in the exponent in the exponential sum (1), behaves sufficiently randomly, **in the typical case** among exponentially many terms.
Then we use the following lemma
Lemma [2] Let $\sigma > 0$ and $\xi_m = e^{2\pi i/m}$. Let $X_i \sim N(0,1)$, i.i.d. for $i = 1, 2, \ldots, n$, and let $\{S_k \subseteq [n] \mid 1 \le k \le K\}$ be a finite collection of sets. Assume, all except at most δ fraction of pairwise symmetric differences $S_j \Delta S_k$ have cardinality $\ge (m/\sigma)^2 t$ for $j \ne k$. Let $\Sigma_k = \varphi_k + \sigma \sum_{i \in S_k} X_i$, where $\varphi_k \in [0, 2\pi)$. Then, the expectation

$$\mathbf{E}[|\xi_m^{\Sigma_1} + \xi_m^{\Sigma_2} + \ldots + \xi_m^{\Sigma_K}|^2] \le K + 2\delta\binom{K}{2} + 2(1-\delta)\binom{K}{2} e^{-2\pi^2 t}.$$

What does this mean?

Quantum mechanics is unquestionably an accurate model of microscopic physical reality.
But, despite being very accurate, it is not **infinitely** accurate. I believe the $\mathrm{SU}(2)$ description of possible operations of a qubit to be only approximately true. Specifically, I don't believe arbitrarily small angle rotations permitted by $\mathrm{SU}(2)$ have physical meaning.
The Schrödinger equation $i\hbar\frac{d}{dt}|\Psi(t)\rangle = \hat{H}|\Psi(t)\rangle$ suggests that small angles are related to small time periods. But physicists have suggested that time ultimately is also discrete. (Planck time is only about 5.39×10^{-44}).
It is unknown whether quantum error correction can save this. But if arbitrarily small angle rotations lack physical meaning, then it is doubtful quantum error correction code can correct to something that does not exist.

References

[1] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[2] Jin-Yi Cai. "Shor's Algorithm Does Not Factor Large Integers in the Presence of Noise". In: *CoRR* abs/2306.10072 (2023). DOI: 10.48550/arXiv.2306.10072. arXiv: 2306.10072. URL: https://doi.org/10.48550/arXiv.2306.10072.