Quantum algorithms: Noisy intermediate-scale quantum (NISQ)

Yipeng Huang

Rutgers University

October 26, 2022

Table of contents

Quantum Fourier transform to obtain period

The task now is to use Fourier transform to obtain the period.

$$QFT\Big(|x\rangle\Big) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i}{2^n}xy} |y\rangle$$

$$QFT = \frac{1}{\sqrt{2^n}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{2^n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(2^n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{2^n-1} & \omega^{2(2^n-1)} & \cdots & \omega^{(2^n-1)(2^n-1)} \end{bmatrix}$$

Where

$$\omega = e^{\frac{2\pi i}{2^n}}$$

And recall that

$$e^{ix} = \cos x + i \sin x$$

Quantum Fourier transform to obtain period

The task now is to use Fourier transform to obtain the period.

$$QFT\left(|x\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i}{2^n} xy} |y\rangle$$

$$QFT\left(\frac{1}{\sqrt{A}} \sum_{a=0}^{A-1} |x_0 + ar\rangle \right)$$
$$= \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \left(\frac{1}{\sqrt{A}} \sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n}(x_0+ar)y} \right) |y\rangle$$
$$= \sum_{y=0}^{2^n-1} \left(\frac{1}{\sqrt{2^n A}} e^{\frac{2\pi i}{2^n} x_0 y} \sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n} ary} \right) |y\rangle$$

Quantum Fourier transform to obtain period

$$\text{Prob}(y) = \frac{A}{2^n}\left|\frac{1}{A}e^{\frac{2\pi i}{2^n}x_0 y}\sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n}ary}\right|^2$$
$$= \frac{A}{2^n}\left|\frac{1}{A}\sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n}ary}\right|^2$$

- Here, values of y such that $\frac{ry}{2^n}$ is close to an integer will have maximal measurement probability.
- In our case, only $\frac{ry}{2^n} = \frac{4 \cdot 4}{16}$, $|y\rangle = |4\rangle$ will have high measurement probability.
- To get a beautiful explanation of principle of least action, read Feynman, QED.

How to construct the Quantum Fourier transform

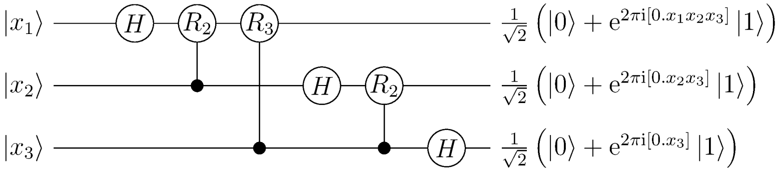


Figure: Credit: Wikimedia

How to construct the Quantum Fourier transform

- Cost of computing the FFT for functions encoded in n bits: $O(2^n n)$
- Cost of quantum Fourier transform for functions encoded in n qubits: $O(n^2)$ gates.

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^k} \end{bmatrix}$$

1. $$R_0 = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^0} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

2. $$R_1 = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z$$

3. $$R_2 = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = S$$

4. $$R_3 = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^3} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} \end{bmatrix} = T$$

Time cost and implementation

Factoring underpins cryptosystems.

For number represented as b bits:

- Classical algorithm: needs $O(2^{\sqrt[3]{b}})$ operations. Factoring 512-bit integer: 8400 years. 1024-bit integer: $13 \times 10^1 2$ years.
- Quantum algorithm: needs $O(b^2 log(b))$ operations. Factoring 512-bit integer: 3.5 hours. 1024-bit integer: 31 hours.

Source: Oskin et al. A Practical Architecture for Reliable Quantum Computers.

Time cost and implementation

Figure 1. Scaling the classical number field sieve (NFS) vs. Shor's quantum algorithm for factoring.[37]

The horizontal axis is the length of the number to be factored. The steep curve is NFS, with the marked point at $L = 768$ requiring 3,300 CPU-years. The vertical line at $L = 2048$ is NIST's 2007 recommendation for RSA key length for data intended to remain secure until 2030. The other lines are various combinations of quantum computer logical clock speed for a three-qubit operation known as a Toffoli gate (1Hz and 1MHz), method of implementing the arithmetic portion of Shor's algorithm (BCDP, D, and F), and quantum computer architecture (NTC and AC, with the primary difference being whether or not long-distance operations are supported). The assumed capacity of a machine in this graph is $2L^2$ logical qubits. This figure illustrates the difficulty of making pronouncements about the speed of quantum computers.

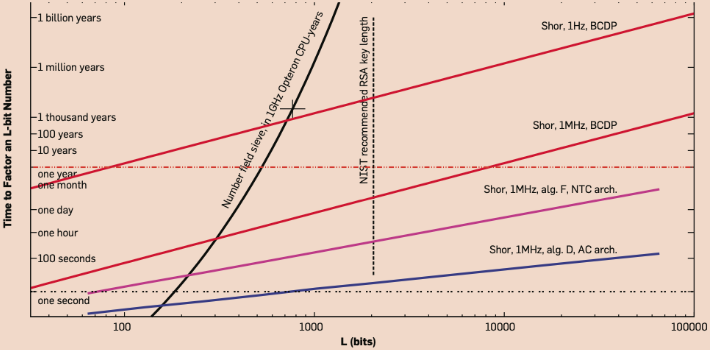


Figure: Credit: Van Meter and Horsman. A Blueprint for Building a Quantum Computer. Communications of the ACM. 2013.

Table of contents

Hardware noise

1. Decoherence error
2. Gate error (imprecise control of single qubit, two qubit gates)
3. Measurement error

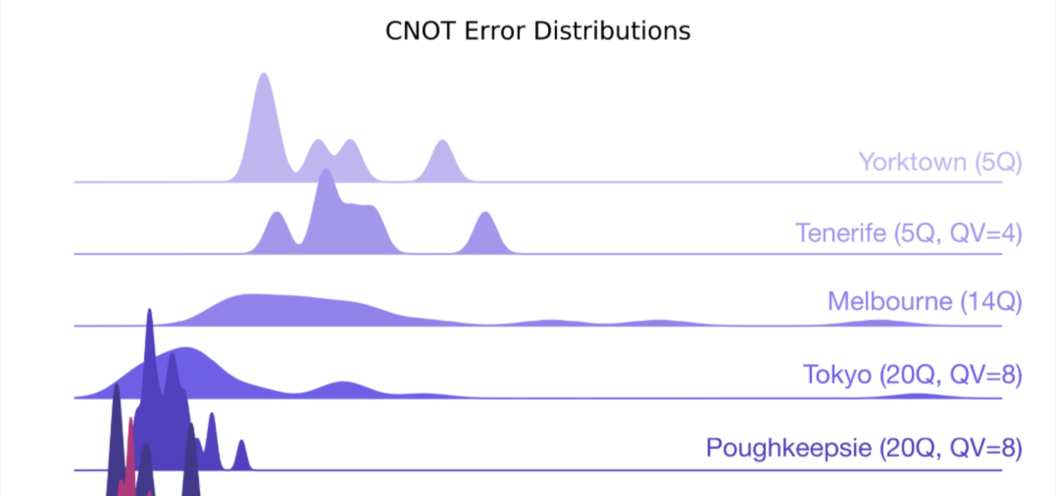
Technology	Coherence Time (s)	1-Qubit Gate Latency (s)	2-Qubit Gate Latency (s)	1-Qubit Gate Fidelity (%)	2-Qubit Gate Fidelity (%)	Mobile
Ion Trap	0.2 [165] - 0.5 [169]	1.6e-6 [166] - 2e-5 [169]	5.4e-7 [166] - 2.5e-4 [169]	99.1 [169] - 99.9999 [168]	97 [169] - 99.9 [165]	YES
Superconductors	7.0e-6 [182] - 9.5e-5 [178]	2.0e-8 [62, 177, 180] - 1.30e-7 [78, 169]	3.0e-8 [182] - 2.5e-7 [78, 169]	98 [179] - 99.92 [177]	96.5 [78, 169] - 99.4 [177]	NO
Solid State Nuclear spin	0.6 [183]	1.12e-4 [184] - 1.5e-4 [183]	1.2e-4 [185]*	99.6 - [184] - 99.95 [183]	89 [186] - 96 [185]*	NO
Solid State Electron spin	1e-3 [3]	3.0e-6 [183] - 2.3e-5 [184]	1.2e-4 [185]*	99.4 [184] - 99.93 [183]	89 [186] - 96 [185]*	NO
Quantum Dot	1e-6 [3, 187] - 4e-4 [173]	1e-9 [3] - 2e-8 [171]	1e-7 [174]	98.6 [171] - 99.9 [172]	90 [171]	NO
NMR	16.7 [158]	2.5e-4 [158] - 1e-3 [24]	2.7e-3 [158] - 1.0e-2 [24]	98.74 [24] - 99.60 [158]	98.23 [24] - 98.77 [158]	NO

Table 1. Metrics for various quantum technologies. * Nuclear/Electron Hybrid

Figure: Credit: [Resch and Karpuzcu, 2019]

Hardware noise

1. Decoherence error
2. Gate error (imprecise control of single qubit, two qubit gates)
3. Measurement error



Hardware noise

Stochastic, uncorrelated noise.

	Quantum noise mixtures (Pauli errors)	Quantum noise channels
Pauli-X type	Bit flip noise	Amplitude damping noise (related to T1 time)
Pauli-Z type	Phase flip noise	Phase damping noise (related to T2 time)
Combinations	Symmetric / asymmetric depolarizing noise	Generalized amplitude damping
Simulation technique	Can model as probabilistic ensembles of state vectors	Requires density matrix representation

Table: Summary of canonical quantum noise models.

Bit flip noise channel

$$|0\rangle \rightarrow BitFlip(0.64) \rightarrow \begin{cases} P(|0\rangle) = 0.64 \\ P(|1\rangle) = 0.36 \end{cases}$$

We represent such a mixture of quantum states as a density matrix:

$$\begin{aligned} & 0.64\,|0\rangle\langle 0| + 0.36\,|1\rangle\langle 1| \\ &= 0.64 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} + 0.36 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} \\ &= 0.64 \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + 0.36 \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 0.64 & 0 \\ 0 & 0.36 \end{bmatrix} \end{aligned}$$

(Conventions from [Nielsen and Chuang, 2011, Chapter 8.3])

Density matrix representation

$$0.64\,|0\rangle\langle 0| + 0.36\,|1\rangle\langle 1| = \begin{bmatrix} 0.64 & 0 \\ 0 & 0.36 \end{bmatrix}$$

More general representation:
$\rho = \sum_j p_j \,|\psi_j\rangle\langle\psi_j|$

Quantum (noise) channel

A quantum channel $\mathcal{E}(\rho)$ acts on mixed state ρ:

$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$

Bit flip noise channel

The bit flip channel flips the state of a qubit with probability $1 - p$. It has two elements:

$$E_0 = \sqrt{p}I = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$E_1 = \sqrt{1-p}X = \sqrt{p}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Bit flip noise channel

The bit flip noise channel $\mathcal{E}_{bitflip}(0.64)$ acts on the $|0\rangle$ state like so:

$$\mathcal{E}_{bitflip}(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix})$$

$$= \sum_k E_k \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} E_k^\dagger$$

$$= 0.8 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} 0.8 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + 0.6 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} 0.6 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0.64 & 0 \\ 0 & 0.36 \end{bmatrix}$$

Phase flip noise channel

The phase flip channel flips the phase of a qubit with probability $1 - p$. It has two elements:

$$E_0 = \sqrt{p}I = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$E_1 = \sqrt{1-p}Z = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Hardware noise

	Quantum noise mixtures (Pauli errors)	Quantum noise channels
Pauli-X type	Bit flip noise	Amplitude damping noise (related to T1 time)
Pauli-Z type	Phase flip noise	Phase damping noise (related to T2 time)
Combinations	Symmetric / asymmetric depolarizing noise	Generalized amplitude damping
Simulation technique	Can model as probabilistic ensembles of state vectors	Requires density matrix representation

Table: Summary of canonical quantum noise models.

Amplitude damping noise channel

The amplitude damping channel leaves $|0\rangle$ alone while probabilistically flipping $|1\rangle$. It has two elements:

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}$$
$$E_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}$$

γ represents probability that $|1\rangle$ decays to $|0\rangle$

Hardware noise

1. Decoherence error
2. Gate error (imprecise control of single qubit, two qubit gates)
3. Measurement error

Technology	Coherence Time (s)	1-Qubit Gate Latency (s)	2-Qubit Gate Latency (s)	1-Qubit Gate Fidelity (%)	2-Qubit Gate Fidelity (%)	Mobile
Ion Trap	0.2 [165] - 0.5 [169]	1.6e-6 [166] - 2e-5 [169]	5.4e-7 [166] - 2.5e-4 [169]	99.1 [169] - 99.9999 [168]	97 [169] - 99.9 [165]	YES
Superconductors	7.0e-6 [182] - 9.5e-5 [178]	2.0e-8 [62, 177, 180] - 1.30e-7 [78, 169]	3.0e-8 [182] - 2.5e-7 [78, 169]	98 [179] - 99.92 [177]	96.5 [78, 169] - 99.4 [177]	NO
Solid State Nuclear spin	0.6 [183]	1.12e-4 [184] - 1.5e-4 [183]	1.2e-4 [185]*	99.6 - [184] - 99.95 [183]	89 [186] - 96 [185]*	NO
Solid State Electron spin	1e-3 [3]	3.0e-6 [183] - 2.3e-5 [184]	1.2e-4 [185]*	99.4 [184] - 99.93 [183]	89 [186] - 96 [185]*	NO
Quantum Dot	1e-6 [3, 187] - 4e-4 [173]	1e-9 [3] - 2e-8 [171]	1e-7 [174]	98.6 [171] - 99.9 [172]	90 [171]	NO
NMR	16.7 [158]	2.5e-4 [158] - 1e-3 [24]	2.7e-3 [158] - 1.0e-2 [24]	98.74 [24] - 99.60 [158]	98.23 [24] - 98.77 [158]	NO

Table 1. Metrics for various quantum technologies. * Nuclear/Electron Hybrid

Figure: Credit: [Resch and Karpuzcu, 2019]

But what about correlated noise events?

Table of contents

Near-term and far-future quantum computing

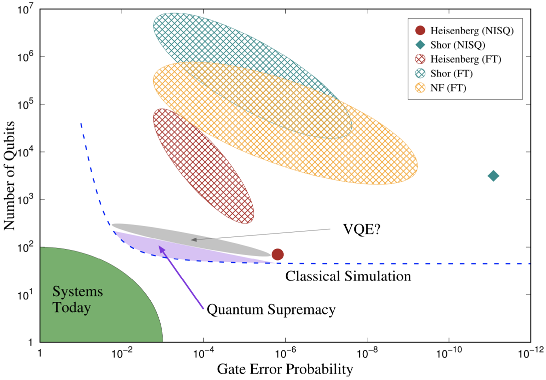
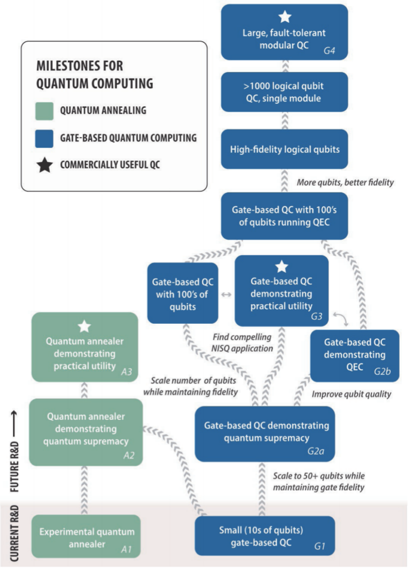


Fig. 2. *Performance space of quantum computers, measured by the error probability of each entangling gate in the horizontal axis (roughly inversely proportional to the total number of gates that can be executed on a NISQ machine), and the number of qubits in the system in the vertical axis. Blue dotted line approximately demarcates quantum systems that can be simulated using best classical computers, while the green colored region shows where the existing quantum computing systems with verified performance numbers lie (as of September 2018). Purple shaded region indicates computational tasks that accomplish the so-called "quantum supremacy," where the computation carried out by the quantum computer defies classical simulation regardless of its usefulness. The different shapes illustrate resource counts for solving various problems, with solid symbols corresponding to the exact entangling gate counts and number of qubits in NISQ machines, and shaded regions showing approximate gate error requirements and number of qubits for an FT implementation (not pictured are the regions where the error gets too close to the known fault-tolerance thresholds): cyan diamond and shaded region correspond to factoring a 1024-bit number using Shor's algorithm [14], magenta circle and shaded region represent simulation of a 72-spin Heisenberg model [20], and orange shaded region illustrates NF simulation [21].*

Figure: Credit: Maslov, Nam, and Kim. An Outlook for Quantum Computing. Proceedings of the IEEE. 2019.

Steps toward useful quantum computing



An illustration of potential milestones of progress in quan-

Figure: Credit: National Academies of Sciences, Engineering, and Medicine. Quantum Computing: Progress and Prospects. 2019.

Córcoles, A. D., Kandala, A., Javadi-Abhari, A., McClure, D. T., Cross, A. W., Temme, K., Nation, P. D., Steffen, M., and Gambetta, J. M. (2020).
Challenges and opportunities of near-term quantum computing systems.
Proceedings of the IEEE, 108(8):1338–1352.

Nielsen, M. A. and Chuang, I. L. (2011).
Quantum Computation and Quantum Information: 10th Anniversary Edition.
Cambridge University Press, USA, 10th edition.

Resch, S. and Karpuzcu, U. R. (2019).
Quantum computing: An overview across the system stack.