Toward the Paradigm of Fault-Tolerant Quantum Computing

Shiro Tamiya

August 2020

The exponential performance improvement of modern computers is approaching the limits of semiconductor microfabrication. Meanwhile, computational demands from big data analysis, machine learning, and quantum simulation are increasing. Improving computational power through new computing paradigms is one of the central subjects of computational science. In this background, quantum computing is attracting attention from researchers, entrepreneurs, managers, and investors. Quantum computers are expected to efficiently solve problems that classical computers cannot, such as integer factoring, unstructured-database search, quantum simulation, and so on. The study of quantum computing is a subfield of quantum information science.

The field began in the early 1980s with proposals for a quantum mechanical model of Turing machines by Paul Benioff. Richard Feynman, one of the great physicists of the 20th century, later suggested that to simulate things that are intractable to classical computers (e.g., molecular dynamics), it should be quantum mechanical, and that quantum computers have such potential. The

following years saw sparse results, except for the development of quantum algorithms by Deutsch, Jozsa, and Simon. Tremendous attention in this field followed Peter Shor's surprising discovery in 1995 of a fast algorithm for solving integer factorization and discrete logarithm problems. Most modern cryptography is based on the difficulty of solving these two problems. Therefore, the discovery of Shor's algorithm meant that if a quantum computer is realized, it would efficiently break a current cryptography system such as RSA encryption. This discovery had a significant impact on people familiar with computer science and physics. After that, research on the physical implementation of quantum computers has made progress, and there are now a small number of noisy machines in existence. Recently, on 23 October 2019, the Google AI team demonstrated experimentally that quantum computers could outperform classical computers in a specific problem, Random Circuit Sampling, with a 54-qubit processor called Sycamore [1]. This achievement was a breakthrough in the decades-long development of quantum computers. However, the "Random Circuit Sampling"

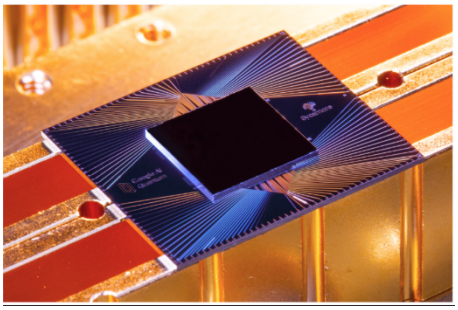

Figure 1: Photograph of Google's Sycamore processor, which demonstrates quantum supremacy[1]. (copyright: Erik Lucero)

problem, the task of taking a random quantum circuit of a specific class and generating samples from its output quantum state, is not practically and industrially as valuable as solutions to problems that involve integer factoring, quantum simulation, and machine learning that quantum computers could solve more efficiently than classical computers. The obstacle to performing such powerful algorithms on today's quantum computers is the lack of fault-tolerant systems required to protect information from noise.

In quantum computing, one encodes information of interest into quantum states. The fundamental information-carrying unit of a quantum computer is called a "qubit," which is a counterpart of a bit in a classical computer. Qubits can be realized physically in many ways, e.g., superconducting circuits, single photons, single atoms, nitrogen-vacancy centers in diamonds or silicones, etc. One of the features of qubits that are different from classical bits is that they are easily destroyed by noise, which makes it difficult to realize a quantum computer. This loss of quantum coherence of quantum states is called "decoherence", which is caused by vibrations, electromagnetic waves, interactions with neighboring nuclear spins, and other unknown interactions with the external environment. Therefore, the development of error correction

techniques will be required to overcome decoherence, although they are far more challenging to implement in quantum than in classical computers.

In classical error correction, redundancy plays an important role: making a lot of copies of the information. If an error occurs with low probability, it is possible to fix the information of a bit where the error occurs by taking a majority vote. On the other hand, in terms of qubits, copying the information is not allowed due to the no-cloning theorem of quantum mechanics, which states that it is impossible to make a copy of an arbitrary unknown quantum state. Moreover, it is not possible to check if errors occur since the quantum state is broken when observed. These properties seem to be an obstacle to developing quantum error correction codes, but Peter Shor discovered a way of formulating a quantum error-correcting code by embedding the information of one physical qubit into a highly entangled logical qubit consisting of nine qubits and retrieving information about errors that have happened without corrupting the quantum state [2]. If the error that occurs on physical qubits and the measurement error is small enough, one can suppress the errors in logical qubits by increasing the level of concatenating quantum error correction codes.

In practice, because of the strict demands on the classical computer and the classical controller of a quantum device, it is considered quite challenging to implement a fault-tolerant framework. In the case of superconducting qubits, one microwave controller is basically required for each physical qubit. If a logical qubit is represented by 1,000 physical qubits and 1024 logical qubits are prepared, one would need about one million microwave controllers. In addition, we require ultra-high-speed communication devices and classical computers with a performance comparable to or better than a supercomputer capable of sending the results of measurements, analyzing them, and deciding which recovery operation is to be carried out before the coherence of the superconducting qubit is lost. These requirements seem to be very demanding to enable practical performance of fault-tolerant quantum computation.

The challenge of realizing large-scale quantum computing with a fault-tolerant function is a battle against noise and scalability. First, to overcome these difficulties, we have to reduce the noise by identifying the kinds of noise and what is causing them. It will be helpful to decrease the number of concatenation levels in constructing the codes and thereby relax the requirements for classical devices. The benefits of building a balanced

framework for quantum devices, control devices, and classical computers will bring us one step closer to realizing fault-tolerant quantum computing.

In recent years, some interesting attempts have been made to explore practical applications with noisy quantum devices. However, it is widely agreed that transformative quantum technologies are going to have a fault-tolerant function by solving the extreme cost of error correction. Undoubtedly, the development of fault-tolerant quantum computing in realistic settings will be the central task of researchers in the coming decades.

References:

[1] F. Arute, *et al.*, Quantum supremacy using a programmable superconducting processor, Nature **574,** 505 – 510 (2019).

[2] J. Roffe, Quantum Error Correction: An Introductory Guide, arXiv:1907.11157 (2019).