Quantum Computing: Report 1

Scott Schoeller

Feb 3, 2021

1 Origins of Quantum Computing

Richard Feynman, a nuclear physicist, and Yuri Manin, a mathematician, separately proposed the model of quantum computation in the 1980s [2]. Progress was made on theoretical algorithms in the 1990s. One of the first quantum computing companies, D-Wave Systems, was founded in 1999. In 2016, IBM brought the power of small quantum computers to the masses with the IBM Quantum Experience. The IBM machines made available to the public currently range from 1–15 qubits.

2 Types of Quantum Computing

There are three types of quantum computers that are commercially available – gate-based, adiabatic and quantum annealing [4].

2.1 Gate-Based

The newer quantum computing designs, such as those at IBM, are based off of quantum logic gates. These are analogous to classical logic gates.

2.2 Adiabatic & Quantum Annealing

Adiabatic and quantum annealing computation machines are considered analog [4]. These quantum computers are based on the energy states of qubits.

3 Implications of Quantum Mechanics

Quantum mechanics has two major implications for computing. Qubits can be in states of superposition and can be entangled.

3.1 Superposition

Superposition means that a qubit can hold more than one possible value until it is measured. At that point, the value for that qubit becomes part of a uniform distribution.

3.2 Entanglement

Entanglement is the effect of one qubit on another. If entanglement occurs on all qubits, the state of a quantum computer becomes exponential [4].

4 Types of Quantum Gates

There are a number of operations similar to logic gates in classical computing. Some are unique to the world of quantum computing.

4.1 HAD

At the core of quantum computing is the Hadamard Gate, also known as HAD for short. The HAD operation allows for a single qubit to be in a superposition of the $| 1 >$ and $| 0 >$ states.

4.2 NOT, CNOT and RNOT

The NOT operator is analagous to the respective classical operator. In contrast, there are operators not present in ordinary computers of today that act on more than one qubit. RNOT is the root of the quantum NOT Gate. CNOT, the conditional NOT, acts on two qubits. If a qubit is “on” then the affected qubit also turns “on.” A related operation is the Trifolli Gate, which is like CNOT, except it acts on three qubits. RNOT is short for the “Root of Not” operation, which is unique to quantum computing.

4.3 SWAP and CSWAP

The SWAP operation allows qubits to trade places. CSWAP is a conditional swap, much like CNOT is a conditional NOT.

4.4 PHASE and CPHASE

The phase angle with respect to the $| 1 >$ state matters in quantum computation. The phase can be thought of as a fraction of a qubit in the $| 1 >$ state. CHPASE is the conditional form of the PHASE operation.

5 Expected Implications of Quantum Computing

Quantum computing, like any technological breakthrough, is expected to have positive and negative effects. In particular, this computing paradigm is expected to have positive outcomes on scientific problems and negative impacts on current cryptography.

5.1 Science

Quantum computing has been applied to quantum systems problems in the physical sciences. Solutions to quantum chemistry problems have been accomplished with existing quantum computing and the application of this form of computing to the physical sciences is expected to expand [2].

5.2 Cryptography

Existing asymmetric cryptography is expected to be adversely affected by sufficiently large quantum computers. Peter Shor proposed an algorithm in 1994 that can break RSA. This algorithm can also be extended to discrete logarithm cryptosystems, including ECC [4]. The computing power to break 1024-bit RSA is already believed to be within the range of classical supercomputing [1]. NIST (the National Institute for Science and Technology) announced a post-quantum cryptography competition in 2016 [3]. NIST currently is examining seven candidates and eight alternates.

References

[1] Bos, J. W., Kaihara, M. E., Kleinjung, T., Lenstra, A. K., and Montgomery, P. L. On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography. Preprint, Sept. 2009.

[2] Cao, Y., Romero, J., Olson, J. P., Degroote, M., Johnson, P. D., Kieferová, Mária, Kivlichan, I. D., Menke, T., Peropadre, B., Sawaya, N. P., Sim, S., Veis, L., and Aspuru-Guzik, A. Quantum Chemistry in the Age of Quatum Computing. *Chemical Reviews 119*, 19 (2019), 10856–10915.

[3] Chen, L., Moody, D., and Liu, Y.-K. Post-Quantum Cryptography | CSRC.

[4] Grumbling, E., and Horowitz, M., Eds. *Quantum Computing Progress and Prospects*. The National Academies Press, Washington, DC, 2019.