Our generous universe comes equipped with the ability to compute.
—*Dave Bacon* [22]

CHAPTER 2

A Brief History of Quantum Computing

The possibility that we can leverage quantum mechanics to do computation in new and interesting ways has been hiding in plain sight since the field's early days; the principles of superposition and entanglement can form the basis of a very powerful form of computation. The trick is to build such a system that we can easily manipulate and measure.

While Richard Feynman is often credited with the conception of quantum computers, there were several researchers who anticipated this idea. In 1979, Paul Benioff, a young physicist at Argonne National Labs, submitted a paper entitled "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines" [30].[1] In this paper, Benioff demonstrated the theoretical basis for quantum computing and then suggested that such a computer could be built:

> That is, the whole computation process is described by a pure state evolving under the action of a given Hamiltonian. Thus all the component parts of the Turing machine are described by states which have a definite phase relation to one another as the calculation progresses...The existence of such models at least suggests that the possibility of actually constructing such coherent machines should be examined.

Yuri Manin also laid out the core idea of quantum computing in his 1980 book *Computable and Non-Computable* [181]. The book was written in Russian, however, and only translated years later.

[1]Note: Benioff completed and submitted the paper in 1979. It was published in the following year, 1980.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2021

J. D. Hidary, *Quantum Computing: An Applied Approach*,
https://doi.org/10.1007/978-3-030-83274-2_2

In 1981, Feynman gave a lecture entitled "Simulating Physics with Computers" [111].[2] In this talk, he argued that a classical system could not adequately represent a quantum mechanical system:

> ...nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy...

He then set out the features that a quantum computer should have to be useful. At the time of this lecture, however, it was unclear to Feynman and the physics community how one could build such a machine (for additional background see [225]).

2.1 *Early Developments and Algorithms*

Once Benioff, Manin and Feynman opened the doors, researchers began to investigate the nature of the algorithms that could be run on QCs. David Deutsch, a physicist at Oxford, suggested a more comprehensive framework for quantum computing in his 1985 paper [88]. In this work, he describes in detail what a quantum algorithm would look like and anticipates that "one day it will become technologically possible to build quantum computers."

Deutsch then went on to develop an example of an algorithm that would run faster on a quantum computer. He then further generalized this algorithm in collaboration with Richard Jozsa [90]. We will cover these and the other algorithms in more detail with code examples later on in this text.

In computer science and quantum computing, it is often important to evaluate how efficient an algorithm is — that is, how many steps would it take to run such an algorithm. We use big-O notation to represent the upper bound of the worst case of running an algorithm. The O in big-O notation comes from the "order" of the algorithm. We use big-Ω (Omega) notation to indicate the lower bound of the worst-case scenario. So, while Deutsch's problem takes at *worst* $O(n)$ steps to solve on a classical computer, Deutsch-Jozsa's algorithm solves the problem in one step on a quantum computer. Big-O notation will be helpful throughout this book in illuminating the difference between the classical and quantum algorithms.

Umesh Vazirani and his student Ethan Bernstein picked up where Deutsch and Jozsa left off. In 1993, Bernstein and Vazirani (BV) published a paper which described an algorithm that showed clear quantum-classical separation

[2] Note: Feynman gave his lecture in 1981 and submitted the lecture for publication in May of 1981. The lecture was published by IJTP in 1982.