Quantum Computing

Summary

Fabian Damken

July 13, 2022

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Contents

List of Figures

List of Tables

List of Algorithms

1 Preliminaries

In this chapter we discuss the groundwork for the upcoming topics. Along with these subjects, basic knowledge from linear algebra is required.

1.1 Complex Numbers

One of the underlying principles of quantum mechanics (QM) and therefore quantum computing (QC), too, are complex numbers. This section summarizes some results for them *very briefly*.

Let $z = a + ib \in \mathbb{C}$ be a complex number with the real and imaginary components $\mathrm{Re}(z) = a, \mathrm{Im}(z) = b \in \mathbb{R}$. Its magnitude is

$$|z| := \sqrt{a^2 + b^2} = \sqrt{zz^*}$$

with the *complex conjugate* $z^* = a - ib$. The complex conjugate is distributive over addition and multiplication[1], i.e., $(z_1 + z_2)^* = z_1^* + z_2^*$ and $(z_1 z_2)^* = z_1^* z_2^*$ holds for two complex numbers $z_1, z_2 \in \mathbb{C}$. Any complex number can also be written in polar form $z = re^{i\varphi}$ with magnitude

$$|z| = \sqrt{zz^*} = \sqrt{re^{i\varphi} re^{-i\varphi}} = \sqrt{r^2 e^{i\varphi - i\varphi}} = \sqrt{r^2} = |r|.$$

Definition 1 (n-th Root of Unity)**.** We call the special complex number $\omega_n = e^{2\pi i/n}$ the *n-th root of unity.*

Theorem 1 (Power Sum of n-th Roots of Unity)**.** *Let ω_n be the n-th root of unity with $n > 1$. Then $\sum_{k=0}^{n-1} \omega_n^k = 0$.*

Proof.

$$\sum_{k=0}^{n-1} \omega_n^k = \frac{1 - \omega_n^n}{1 - \omega_n} = \frac{1 - e^{2i\pi}}{1 - \omega_n} = \frac{1 - 1}{1 - \omega_n} = \frac{0}{1 - \omega_n} = 0$$

□

1.2 Continued Fraction Expansion

Let $x \in (0, 1)$ be a real number[2]. Then we can express this number as its *continued fraction expansion (CFE)*

$$x = \frac{1}{a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}}$$

where $a_0, a_1, \dots \in \mathbb{N}^+$. The CFE of x is finite iff x is rational. The sums

$$\frac{1}{a_0} \qquad \frac{1}{a_0 + \frac{1}{a_1}} \qquad \frac{1}{a_0 + \frac{1}{a_1 + \frac{1}{a_2}}} \qquad \dots$$

[1]For other useful properties, see `https://en.wikipedia.org/wiki/Complex_conjugate#Properties`.

[2]Note that the restriction on the interval $(0, 1)$ is purely for convenience as we only have x's between zero and one down the line. It is also possible to extend continued fraction expansions to $\mathbb{R}$.

are called *partial sums*. For calculating $a_0, a_1, \ldots$, let

$$x_0 := \frac{1}{a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}} \qquad x_1 := \frac{1}{a_1 + \frac{1}{a_2 + \cdots}} \qquad x_2 := \frac{1}{a_2 + \cdots} \qquad \cdots$$

then the coefficients are $a_i = [1/x_i]$, where the brackets indicate the integral part, i.e., the part in front of the decimal. If for any j, $x_j = 0$, the CFE terminates and the number is exactly represented.

Example 1. *Let* $x = 11\,490/2^{14} \approx 0.701294$*. Then the CFE is calculated as follows:*

i	x_i	$1/x_i$	a_i
0	0.701 294	1.425 94	1
1	0.425 94	2.347 77	2
2	0.347 77	2.875 44	2
3	0.875 44	1.142 28	1
4	0.142 28	7.028 30	7
5	0.028 30	35.3333	35
6	0.333 33	3	3
7	0		

The final CFE is therefore

$$x = \frac{1}{1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{7 + \frac{1}{35 + \frac{1}{3}}}}}}}$$

with the coefficients $(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (1, 2, 2, 1, 7, 35, 3)$.

2 Postulates of Quantum Mechanics

2.1 States

2.2 Evolution

2.2.1 Gates

2.3 Measurement

2.4 Composite Systems and Tensor Products

2.4.1 Entanglement

Multipartite

Graph States

2.4.2 Multi-Qubit Gates

2.5 Protocols

2.5.1 No-Cloning

2.5.2 Quantum Teleportation

Concatenated Teleportation

2.5.3 Dense-Coding

2.6 Why these postulates?

3 Computational Complexity

4 Universal Computation

4.1 Classical Analogy

4.2 Universal Quantum Gates

4.2.1 Proof

Part 1/3: Unitaries as Two-Level Unitaries

Part 2/3: Decomposition of Two-Level Unitaries

Part 3/3: Approximation of Single-Qubit Gates

4.2.2 Final Gate Count

5 Algorithms

5.1 Quantum Parallelism

5.1.1 Interference

5.1.2 The Query Unitary

5.1.3 Deutsch's Approach

5.2 Deutsch-Josza Algorithm

5.3 Bernstein-Vazirani Algorithm

5.4 Simon's Algorithm

5.4.1 Problem

5.4.2 Classical Approach

5.4.3 Quantum Approach

Circuit

Post-Processing

Remarks

5.5 Quantum Fourier Transform

5.5.1 Binary Fraction Expansion

5.5.2 Quantum Circuit

5.5.3 Remarks

5.6 Shor's Algorithm

5.6.1 Period Finding

Using Quantum Fourier Transform

Post-Processing

Maximizing the $P(y)$

Recovering the Period

Remarks

5.6.2 From Period Finding to Factoring

Remarks

5.6.3 Summary

5.7 Grover's Algorithm

5.7.1 Classical Approach

5.7.2 Quantum Approach

Circuit

Illustration

Algebraic Proof

Multiple Solutions

Remarks

6 Quantum Error Correction

6.1 Tackling Bit-Flips

6.2 Tackling Phase-Flips

6.3 Shor's Code

6.3.1 Universal Error Correction

6.4 Steane Code

6.5 Fault-Tolerance and Transversality

6.6 Threshold Theorem

7 Quantum Nonlocality

7.1 Elements of Reality

7.2 CHSH Inequality

7.3 Quantum Violation of the CHSH Inequality

7.4 Tsirelson's Bound and Quantum Key Distribution

8 Measurement-Based Quantum Computing

8.1 Identity

8.2 Arbitrary Rotations

8.3 CNOT

8.4 Cluster States

8.5 Handling Errors

8.6 Important Gates