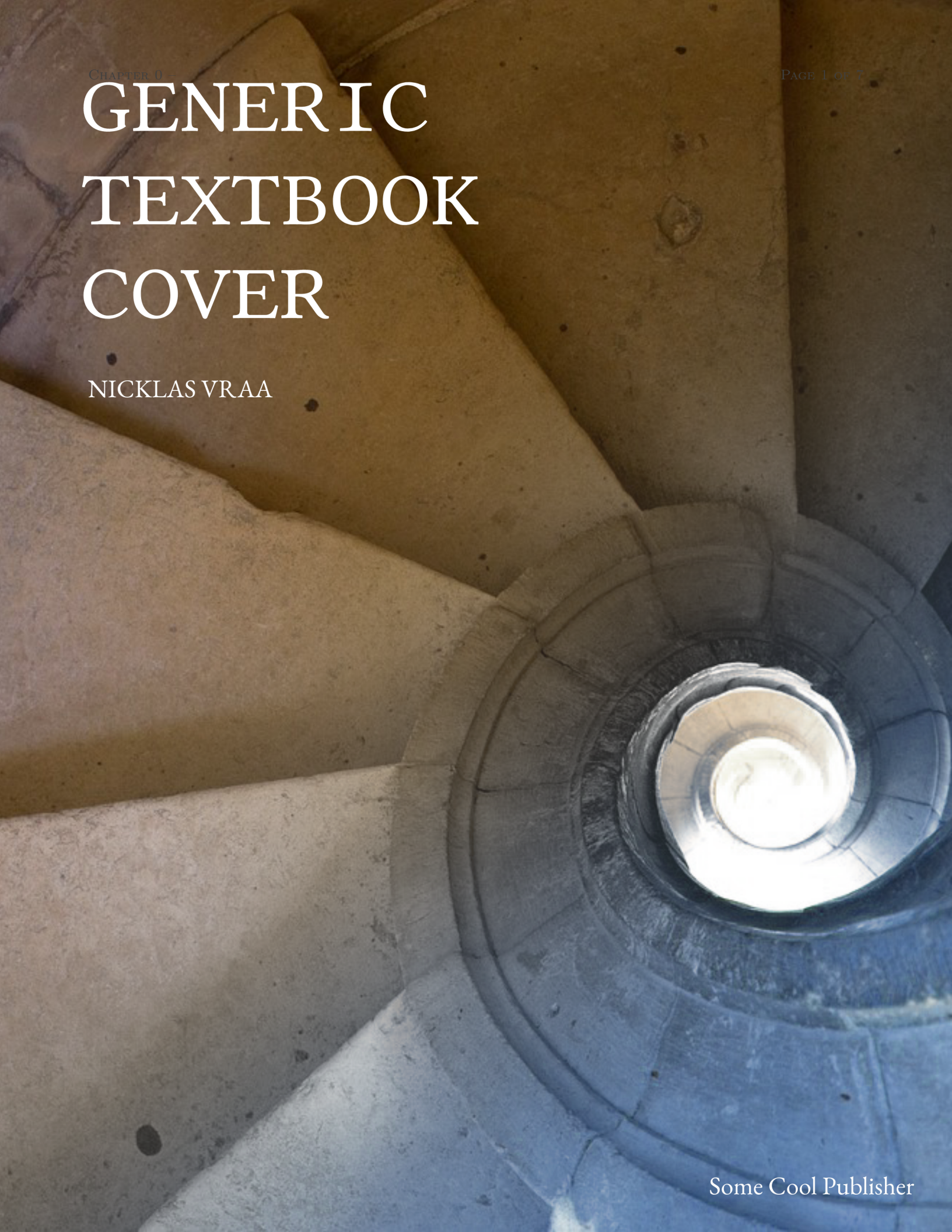
GENERIC TEXTBOOK COVER

NICKLAS VRAA



Some Cool Publisher

Publisher: Nobody, just me!
First edition, published in 2024.

Copyright 2022–2024
This work is licensed under a Creative Commons "Attribution-NonCommercial-ShareAlike 3.0 Unported" license.

Contents

1 Preliminaries **4**
1.1. Complex Numbers 4
1.1.1. Complex conjugate numbers 4
1.2. Euler's Identity 4
1.2.1. 4
1.3. The Stern-Gerlach experiment 4

2 Information in quantum systems. **5**
2.1. The Qubit 5
2.2. Measurements 5
2.3. Computational complexity 5

3 Classical problems done in Quantum ways **6**
3.1. The travelling salesman problem (TSP) 6

4 Qiskit and Quantum Simulations **7**

Preliminaries

There are a few things we might need to have in mind before we start working properly in quantum cryptography.

1.1. Complex Numbers

A complex number is a numerical evaluation that has a part that is imaginary, and a part that is real.

1.1.1. Complex conjugate numbers

If $\alpha = a + ib$, then we can conjugate it as $\hat{\alpha} = a - ib$. This is interesting because if we multiply these numbers, we arrive to:

$$a \cdot \hat{a} = a^2 - i^2 b^2 = a^2 + b^2 \tag{1.1}$$

this is equal to the square of the magnitude a complex number has in representing both the real and the complex space.

1.2. Euler's Identity

Say for example we let the function $f(\theta) = (cos\theta + i \sin\theta)e^{-i\theta}$ where $\theta \in \mathbb{R}$

we can assume then from derivating this expression:

$$\frac{df(\theta)}{d\theta} \tag{1.2}$$

This equation is a constant because of this derivative, and therefore we can calculate f(0) and it will equal the same for all real values.

$$f(0) = (cos0 + i \sin 0)e^{-i*0} \tag{1.3}$$

$$e^{i\pi} + 1 = 0$$

This can also be proved through Taylor series or extend it to square matrices, however, as it stands right now, we just need to use it for working on imaginary numbers, so this is the result that happens to become relevant to us.

1.2.1.

1.3. The Stern-Gerlach experiment

We can prove a few quantum properties through this experiment, and it will theoretically fundament a bunch of our calculations. So, given an iron magnet, and macroscopic parcticles,

Information in quantum systems.

Quantum information is, in essence, a multidisciplinary field somewhere in the middle of physics, mathematics, and computer science. While mostly a theoretical field at this point, but in essence, we can think on it as a way to solve problems unsolvable by current systems, that are based on the Von Neumann architecture. Of course, this is a pretty versatile architecture that can be used for a lot of stuff, but it might have a few limitations we're slowly crawling towards.

A lot of complex calculations are intractable for Von Neumann computers, as for example is the case for factorization, which ends up happening to give us modern classical cryptography. In that same vein, there are different natural problems with such systems.

For example, Caffeine ($C_8H_{10}N_4O_2$) is a 24 atom molecule, and it requires for those 24 atoms, 10^{48} bits for describing all possible energy arrangements. And yet, 160 qubits can represent the model on it's completeness, as a $2^{160} = 1.46 \cdot 10^{48}$ system in the complex space.

For another application in chemistry, let's imagine a block of mineral Carbon (C), such material can be layered into layers to create graphite, or another form of such atoms, diamonds are also composed from carbon in molecules, and yet mineral Carbon has wildly different properties. This are problems that don't have structural forms that can be fully simulated in classical computers. Materials Science will probably find a lot of uses for quantum information in the realms of simulation and data modeling. We'll probably end up needing better quantum computers, but the important thing is we'll find that such technologies will become incredibly useful.

In layman's terms, quantum computers will:

- Make it possible to represent unrepresentable information
- Generate calculations at a much faster rate bit-to-qubit (we'll see what a qubit is later) per second
- ...probably break some cryptographic systems, we'll also get to that.

2.1. The Qubit

A qubit is a bit of a weird system, as it represents a quantum state somewhere between $|0\rangle$ and $|1\rangle$. As quantum computing tends to work, this is of a probabilistic variable, and won't be .

2.2. Measurements

In a lot of ways, quantum computers are inherently about measurements, Imperfect, unreliable and yet incredibly potent measurements. As it comes, quantum computers in essence depend on their measures

2.3. Computational complexity

When we talk about algorithms, there exists a window

this has important applications for cryptography, because of the inherent limitations of classical computers, for example, the multiplication of two numbers can be solved in $O(n^2)$ steps, but given a number, finding out the factors will be $O(e^{n^{\frac{1}{3}}})$ Therefore, the factors of a number are hard to calculate, but easy to verify.

In such systems, we can also talk about other problems with this same form of working,

Classical problems done in Quantum ways

3.1. The travelling salesman problem (TSP)

Qiskit and Quantum Simulations

For most practical purposes, we'll use the tools provided by Qiskit for simulating quantum systems. This is a tool developed by IBM to test quantum algorithms in classical computers, with the side effect of this tool being able to write circuits for actual quantum computers. as this document is being currently written, the cost of quantum compute is significantly higher than classical systems. Therefore, we'll be mostly simulating before we run in an actual quantum computer

The circuit

To mantain our qubits, we'll represent the state of our program as a circuit. So for example, we could write the following expression:

```
# Assuming qiskit already is installed
import qiskit
from qiskit import QuantumCircuit

qc0 = QuantumCircuit()
```

Snippet 4.1: Basic Quantum circuit declaration