Contents

3 SHOR'S ALGORITHM

This chapter is dedicated to two central algorithms in quantum computing — quantum teleportation and Shor's algorithm — which exemplify the practical and theoretical strengths of quantum computation over classical methods. These algorithms demonstrate not only the principles of superposition and entanglement but also their applications in secure communication and cryptography, highlighting the distinct capabilities of quantum technologies.

The first of these, the quantum teleportation protocol, provides a secure method for transferring quantum information through entanglement, bypassing the need for direct physical transmission. This protocol is essential for advancing quantum communication and could play a pivotal role in the development of future quantum networks.

The second, Shor's algorithm, represents a major breakthrough in computational complexity, as it can factor large integers in polynomial time — a task that classical computers cannot achieve efficiently. This capability exposes vulnerabilities in widely – used cryptographic systems and emphasizes the transformative power of quantum computation.

In the following we'll examine these algorithms in detail, explaining their mechanisms, their implications for computational security, and their significance in the broader landscape of quantum information science.

3.1 SHOR'S ALGORITHM

When the number of logical qubits grows, it is customary to use different bases. A very important orthonormal basis defined for two logical qubits is the **Bell basis**: starting from the computational basis,

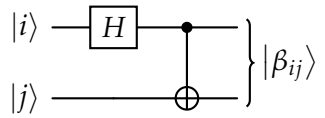
$$\mathcal{B}^{(c)} \equiv \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

we define

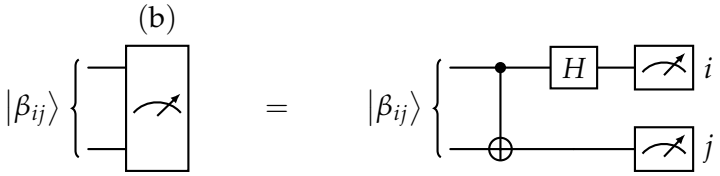
$$
\begin{aligned}
|\beta_{00}\rangle &\equiv \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\
|\beta_{01}\rangle &\equiv \frac{|01\rangle + |10\rangle}{\sqrt{2}} \\
|\beta_{10}\rangle &\equiv \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\
|\beta_{11}\rangle &\equiv \frac{|01\rangle - |10\rangle}{\sqrt{2}}
\end{aligned}
\qquad \mathcal{B}^{(\mathrm{b})} \equiv \{|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle\}
$$

Bell states are entangled by definition; they become immensely useful, seen as shared resources, in protocols like the **Quantum Teleportation Protocol**.

Bell states can be generated from computational states as follows,



being $i, j \in \{0, 1\}$. We refer to this architecture as a "Bell initializer". Equivalently, to perform a "Bell measurement" over a 2-qubits state means precisely



Final measurements gives back two classical bits, i and j.

In order to get to Shor's algorithm, we need to discuss first the features of quantum communication.

3.2 NO-CLONING THEOREM AND QUANTUM TELEPORTATION PROTOCOL

This section is seemingly unrelated, but treats some essential concepts of Quantum Mechanics. To problem is simple: given two quantum subsystems physically separated, how do they exchange information? Which means: if information is stored *here* in a qubit, how do we end up having the same information stored *there* in another qubit?

3.2.1 No-cloning Theorem

We start off by a seemingly unrelated

Theorem 2 (No-cloning). *Let $\mathcal{H}^{(\mathrm{ab})}$ be the shared Hilbert space of two subsystems* a *and* b,

$$\mathcal{H}^{(\mathrm{ab})} \equiv \mathcal{H}^{(\mathrm{a})} \otimes \mathcal{H}^{(\mathrm{b})}$$

Let $|\psi\rangle \in \mathcal{H}^{(a)}$ (any generic pure state of subsystem a) at the beginning. Similarly, let $|e\rangle \in \mathcal{H}^{(b)}$ be the "blank" state of the second subsystem. Then, no unitary operator U exists such that

$$U|\psi\rangle \otimes |e\rangle = e^{i\alpha(\psi,e)}|\psi\rangle \otimes |\psi\rangle$$

(with $\alpha(\psi, e)$ a phase) for any $|\psi\rangle$ and $|e\rangle$.

In other words, **no quantum copier exists**. This does not mean no specific state can be cloned; instead, no machine can exists able to clone any state from one subsystem to another.

Proof. The proof is utterly simple. Suppose said U exists and take two states $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}^{(a)}$. Then

$$\begin{aligned}\langle\psi_1|\psi_2\rangle &= \langle\psi_1|\psi_2\rangle\langle e|e\rangle \\ &= \langle\psi_1 e|U^\dagger U|\psi_2 e\rangle \\ &= e^{-i\left[\alpha(\psi_1,e)-\alpha(\psi_2,e)\right]}\langle\psi_1|\psi_2\rangle^2\end{aligned}$$

Taking its absolute value,

$$|\langle\psi_1|\psi_2\rangle| = |\langle\psi_1|\psi_2\rangle|^2 \quad \Longrightarrow \quad |\langle\psi_1|\psi_2\rangle| \in \{0,1\}$$

which means: either $|\psi_1\rangle \perp |\psi_2\rangle$ or $|\psi_1\rangle = |\psi_2\rangle$ (up to a phase). So if U is able to copy one particular state, it is not true that it can clone any other state. This is contradiction with the assumptions, thus U does not exist. □

Other "no-go" theorems

The "no-cloning" theorem, along with several others, belongs to the class of so-called *no-go* theorems. To provide a more comprehensive view and for the sake of completeness, we present a brief preview of each one:

- No Teleportation. *An arbitrary quantum state cannot be fully represented using classical information. In other words, converting quantum information into classical form is an irreversible process: classical channels are incapable of transmitting quantum information.*
- No Broadcasting. *A single copy of a quantum state cannot be shared with two or more parties.* Since we cannot duplicate a (non-pure) state we cannot share it simoulta; indeed, this theorem does not apply if we are given more than one copy.
- No Deleting. *Given two copies of an arbitrary quantum state, it is impossible to delete one.* This can be thought of as the "time-dual" of no-cloning.
- No Communication. *An entangled state cannot be used to transmit information by measuring a subsystem.* This result is even stronger than no-cloning, as the latter can be derived from it.
- No Hiding. *Quantum information cannot be permanently lost, even through decoherence.* This demonstrates the robustness of quan-

tum states: although quantum information may appear lost, it remains conserved by nature.

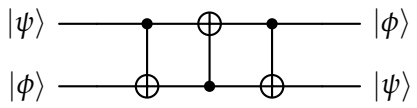
These mutually counterintuitive theorems may seem confusing at first. Rather than being discouraged, we encourage further exploration into their details. This collection of results exemplifies how the quantum world often exceeds the sum of its parts. For instance, the quantum teleportation protocol enables the transfer of quantum information by leveraging both "no-teleportation" and "no-communication."

Now that we know this, it seems that in order to communicate any possible quantum state we cannot clone it. In other words, to get information travel from one subsystem to another the price we pay is the information loss in the "communicating" system. This is of course not true for classical architectures: the ability of copying a string of classical bit without destroying it lies at the very basics of classical computation devices.

3.2.2 Preliminaries to quantum teleportation

Two enjoyers of quantum communication, Alice and Bob, want to share quantum information. Alice owns another "private" qubit in state $|\psi\rangle$. She wants to apply some protocol ending up with Bob having his qubit in state $|\psi\rangle$. What does she do?

Consider first a 2-qubits system. A quantum SWAP is efficiently performed by the circuit



since:

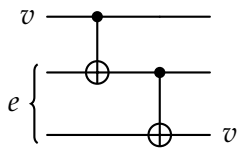
$$\Big[\,|0\rangle\langle 0|\otimes\mathbb{1}+|1\rangle\langle 1|\otimes X\Big]\Big[\mathbb{1}\otimes|0\rangle\langle 0|+X\otimes|1\rangle\langle 1|\Big]\Big[\,|0\rangle\langle 0|\otimes\mathbb{1}+|1\rangle\langle 1|\otimes X\Big]$$
$$=|00\rangle\langle 00|+|01\rangle\langle 10|+|10\rangle\langle 01|+|11\rangle\langle 11|$$

in matrix form (in the computational basis)

$$[\mathrm{SWAP}]=\begin{bmatrix}1&&&\\&&1&\\&1&&\\&&&1\end{bmatrix}$$

This is a swap indeed. It does not clone states and moves information as requested. There is a problem, though: Alice and Bob cannot be separated. The protocol works because 2-qubits quantum gates are applied over the collective state. But we need to *communicate*.

We draw inspiration from a classical probabilistic communication protocol. Take the classical circuit,



with

$$v \equiv \begin{bmatrix} p \\ 1-p \end{bmatrix} \qquad \text{and} \qquad e \equiv \begin{bmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{bmatrix}$$

The bit v is in state 0 with probability p and in state 1 with probability $1-p$. The two correlated bits e are in state 00 with probability $1/2$ and in state 11 with probability $1/2$. Now, let Alice read the first line and Bob read the last line. The intermediate communication line is **ancillary**. Bob ends up reading its bit with the same probability distribution as the original bit of Alice.

Proof. Applying the first CNOT operator, with probability p the first of the correlated bits is confirmed ($00 \to 00$ and $11 \to 11$), and with probability $1-p$ is negated ($00 \to 01$ and $11 \to 10$):

$$\text{CNOT}(1,2): \begin{bmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{bmatrix} \quad \to \quad \frac{1}{2} \begin{bmatrix} p \\ 1-p \\ 1-p \\ p \end{bmatrix}$$

Here $\text{CNOT}(1,2)$ indicates the control (first bit) and the target (second bit). The second CNOT acts only for the last two entries of the above vector, 10 and 11, and inverts them

$$\text{CNOT}(2,3): \frac{1}{2} \begin{bmatrix} p \\ 1-p \\ 1-p \\ p \end{bmatrix} \quad \to \quad \frac{1}{2} \begin{bmatrix} p \\ 1-p \\ p \\ 1-p \end{bmatrix}$$

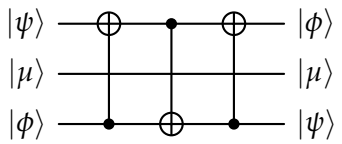
then the probability of measuring 0 on Bob's bit is $p/2 + p/2 = p$, the probability of measuring 1 is $(1-p)/2 + (1-p)/2 = 1-p$. Bob reads a bit identical to v, which is, has received v (notice also that Alice still has her copy of v). □

In this classical protocol the main feature is the presence of an ancillary bit, shared by the parts, in a state which can be mapped easily on its entangled quantum analog – the Bell state $|\beta_{00}\rangle$.

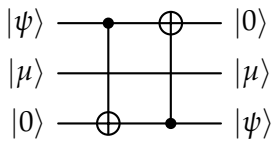
3.2.3 Shared resources

In order to perform quantum teleportation, a very important conceptual step is to look to entanglement as a *resource*. Entanglement cannot be used by itself for communication, as it is commonly known; but it establishes correlations between subsystems we can exploit.

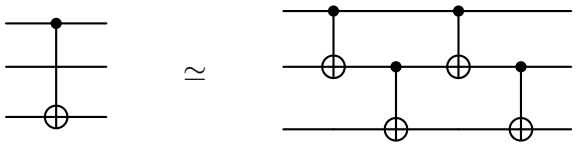
First thing, let us look to the immediate extension of the classical probabilistic teleportation protocol. There we introduced an *ancillary system*: could we use it in a quantum architecture to make the SWAP act "at distance"?



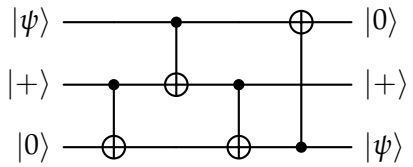
with $|\mu\rangle$ the ancillary qubit. If we initialize $|\phi\rangle = |0\rangle$, we can as well ignore the first CNOT,



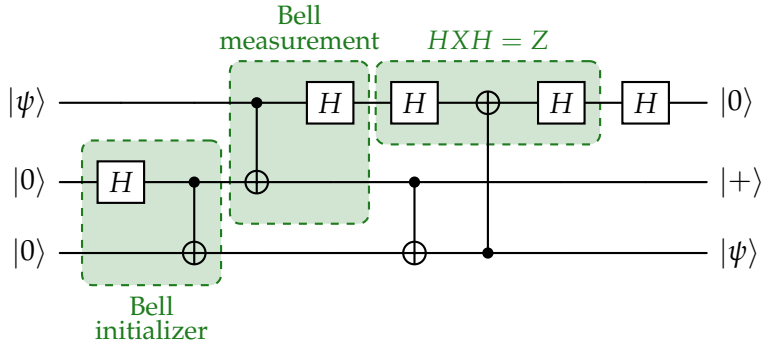
We now exploit the identity



Insert it inside the precedent circuit. Also, initialize $|\mu\rangle = |+\rangle$; the first CNOT (acting from the top wire on the middle wire) is ineffective over this state, being $X|+\rangle = |+\rangle$ and we may ignore it. Then the circuit is reduced to



To initialize the ancillary state we need an Hadamard gate; moreover, we may insert two identities $H^2 = \mathbb{1}$. Then



As highlighted in the circuit, we can exploit the identity $HXH = Z$ on the top wire. The last Hadamard gate can be ignored on the same wire by taking the output as $|+\rangle$. Moreover, we recognize a Bell measurement architecture on the top and ancillary wires. Finally, see the ancillary and bottom wires to be initialized in the $|\beta_{00}\rangle$ Bell state. Then the above circuit gets reduced to: Go on...

3.2.4 Quantum Teleportation Protocol