Chapter 2

Multipartite Quantum Systems

The formalism introduced in the previous chapter allows us to describe individual "quantum-mechanical objects" and predict their individual behavior. In this chapter, we extend the formalism so as to be able to capture *multiple* "quantum-mechanical objects" and predict their *joint* behavior. For instance, we may want to study how the respective polarizations of two photons behave in a certain experiment.

2.1 Multipartite Quantum Systems

Consider two labeled Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ (see Section 0.6) for distinct labels A and B. By default, we then understand A and B to refer to two quantum systems, and $\mathcal{H}_A$ and $\mathcal{H}_B$ as their respective state spaces. Following Section 0.6, the Hilbert space $\mathcal{H}_{AB}$ with label AB is then given by the tensor product

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B \,.$$

$\mathcal{H}_{AB}$ is then understood to be the state space of the **bipartite** quantum system that consists of the subsystems A and B. The corresponding holds for general **multipartite** systems, consisting of an arbitrary (finite) number of subsystems. The physical relevance should be clear: the state of two (or more) quantum systems is described by a state vector in the tensor product of the individual state spaces.

If the state of A is given by state vector $|\varphi\rangle \in \mathcal{S}(\mathcal{H}_A)$ and the state of B by $|\psi\rangle \in \mathcal{S}(\mathcal{H}_B)$ then the state of the bipartite system AB — sometimes also referred to as the **joint** state — is given by $|\Omega\rangle = |\varphi\rangle \otimes |\psi\rangle \in \mathcal{S}(\mathcal{H}_{AB})$. We refer to such a state (vector) $|\Omega\rangle$ that is a pure tensor $|\varphi\rangle \otimes |\psi\rangle$ as a **product state**. We emphasize though that in general, if A and B (i.e., the two quantum systems of concern) were not kept in isolation from each other but may have interacted, their joint state is described by an arbitrary state vector $|\Omega\rangle$ in $\mathcal{S}(\mathcal{H}_{AB})$. In this case, i.e., if $|\Omega\rangle$ is not a product state, we say that A and B are **entangled**; entanglement is another strange phenomenon of quantum physics.

By identifying any operator $R \in \mathcal{L}(\mathcal{H}_A)$ with $R \otimes \mathbb{I} \in \mathcal{L}(\mathcal{H}_{AB})$, we naturally recover the evolution of bipartite (or multipartite) quantum systems *when acting on a subsystem*. For instance, applying a unitary $U \in \mathcal{U}(\mathcal{H}_A)$ to subsystem A of a bipartite system AB has the effect that their joint state $|\Omega\rangle \in \mathcal{S}(\mathcal{H}_{AB})$ evolves to

$$U_A \, |\Omega\rangle_{AB} = (U \otimes \mathbb{I})|\Omega\rangle \in \mathcal{S}(\mathcal{H}_{AB}) \,.$$

Similarly, Definition 1.4 extends to measurements $\mathbf{M} \in \mathcal{M}eas_I(\mathcal{H}_A)$ and states $|\Omega\rangle \in \mathcal{S}(\mathcal{H}_{AB})$.

In the special case of rank-1 projective measurements, we then get the following. First, we observe that by elementary properties we have that for any $|\Omega\rangle \in \mathcal{S}(\mathcal{H}_{AB})$ and orthonormal basis $\{|i\rangle\}_{i\in I}$ of $\mathcal{H}_A$, we can write

$$|\Omega\rangle = \sum_{i\in I} \alpha_i |i\rangle|\psi_i\rangle$$

with $\alpha_i \in \mathbb{C}$ and $|\psi_i\rangle \in \mathcal{S}(\mathcal{H}_B)$ for all $i \in I$, and where $\sum_i |\alpha_i|^2 = 1$. For a rank-1 projective measurement $\{|i\rangle\langle i|\}_{i\in I} \in \mathcal{M}eas_I(\mathcal{H}_A)$ given by $\{|i\rangle\}_{i\in I}$, we then see that

$$p_i = \langle\Omega|(|i\rangle\langle i| \otimes \mathbb{I}_B)|\Omega\rangle = |\alpha_i|^2$$

and

$$|\Omega^i\rangle = \frac{1}{\sqrt{p_i}}(|i\rangle\langle i| \otimes \mathbb{I}_B)|\Omega\rangle = \frac{\alpha_i}{|\alpha_i|}|i\rangle|\psi_i\rangle \equiv |i\rangle|\psi_i\rangle\,.$$

Thus, also here, as in Section 1.4, we can easily "read out" the statistics and the corresponding post-measurement states when the original state is expressed in the basis that determines the (rank-1 projective) measurement.

We point out that actions on different subsystems *commute*. For instance, for $U \in \mathcal{U}(\mathcal{H}_A)$ and $M_i \in \mathbf{M} \in \mathcal{M}eas_I(\mathcal{H}_B)$, it holds that

$$(\mathbb{I}_A \otimes M_i)(U \otimes \mathbb{I}_B)|\Omega\rangle = (U \otimes M_i)|\Omega\rangle = (U \otimes \mathbb{I}_B)(\mathbb{I}_A \otimes M_i)|\Omega\rangle\,.$$

This reads as follows. Whether we first apply U to A and then measure B, or we first measure B and then apply U to A, we get the same probability p_i to observe outcome i:

$$p_i = \langle\Omega|(U^\dagger \otimes M_i^\dagger)(U \otimes M_i)|\Omega\rangle = \langle\Omega|(\mathbb{I}_A \otimes M_i^\dagger M_i)|\Omega\rangle$$

and the same post-measurement state:

$$|\Omega^i\rangle = (U \otimes M_i)|\Omega\rangle\,.$$

2.2 No-Cloning

The goal of *cloning* is to turn an unknown quantum state into two copies of the original state. Clearly, if the state to be cloned is promised to be one out of two (or more) given states that are *perfectly distinguishable*, then the state *can* be (perfectly) cloned: simply perform a measurement that tells which state it is, and then prepare this state twice "from scratch". The no-cloning theorem tells us that this is *the only* case where cloning is possible.

Theorem 2.1 (No-cloning theorem)**.** *Let $V \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_A \otimes \mathcal{H}_{A'})$ be an isometry with $\mathcal{H}_A = \mathcal{H}_{A'}$, and let $|\varphi\rangle, |\psi\rangle \in \mathcal{S}(\mathcal{H}_A)$. Then, unless $\langle\varphi|\psi\rangle = 0$ or $|\varphi\rangle \equiv |\psi\rangle$, it is not possible that both*

$$V|\varphi\rangle \equiv |\varphi\rangle|\varphi\rangle \qquad \text{and} \qquad V|\psi\rangle \equiv |\psi\rangle|\psi\rangle\,.$$

Note that Theorem 2.1 considers cloning by means of an isometry, whereas above we speak of cloning in terms of measuring and preparing new states. We will later see that there is no loss of generality here.

Proof. We show the contraposition and thus assume that both equalities do hold. By taking the inner product of these two equalities, we obtain

$$\langle\varphi|\psi\rangle = \langle\varphi|V^\dagger V|\psi\rangle \equiv \langle\varphi,\varphi|\psi,\psi\rangle = \langle\varphi|\psi\rangle^2$$

from which it follows that either $\langle\varphi|\psi\rangle = 0$, and we are done, or $|\langle\varphi|\psi\rangle| = 1$. In case of the latter, by the tightness condition for Cauchy-Schwarz, $|\varphi\rangle$ and $|\psi\rangle$ must then be equal up to a scalar ω, which must then be in $\mathcal{S}(\mathbb{C})$. □

2.3 Naimark's Dilation Theorem

We show here that projective measurements are equally powerful as general measurements when allowing "pre-processing", in the sense that any general measurement $\mathbf{M}$ on a system A can be "simulated" by means of appending an ancilla system B to A, applying a unitary transformation to the joint system AB, and then doing a projective measurement, actually doing a rank-1 projective measurement on B.

Theorem 2.2 (Naimark's dilation theorem)**.** *Let $\mathbf{M} = \{M_i\}_{i\in I} \in \mathcal{M}eas_I(\mathcal{H}_A)$, and let $\{|i\rangle\}_{i\in I}$ be an orthonormal basis of $\mathcal{H}_B = \mathbb{C}^{|I|}$. Then, there exists an isometry $V \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_{AB})$ such that for every $|\varphi\rangle \in \mathcal{S}(\mathcal{H}_A)$ and $i \in I$*

$$M_i|\varphi\rangle \otimes |i\rangle = (\mathbb{I}_A \otimes |i\rangle\langle i|)\, V|\varphi\rangle\,.$$

By basic properties of isometries, as discussed in Section 0.2, V can be chosen to be of the form $UV_\circ$, for $V_\circ$ the particular isometry $\mathcal{H}_A \to \mathcal{H}_{AB}$, $|\varphi\rangle \mapsto |\varphi\rangle|0\rangle$, and $U \in \mathcal{U}(\mathcal{H}_{AB})$; such a state $|0\rangle_B$ that is "appended" to a given state in this manner is called an **ancilla**. Naimark's dilation theorem then means that every general measurement is equivalent to appending an ancilla, applying a unitary (to the joint system), and performing a rank-1 projective measurement on the ancilla system (and ignoring the collapsed state of the ancilla).

Proof. Consider $V \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_{AB})$ defined by

$$V|\varphi\rangle = \sum_{i\in I} M_i|\varphi\rangle \otimes |i\rangle$$

for any $|\varphi\rangle \in \mathcal{H}_A$. It is then clear that $(\mathbb{I}_A \otimes |i\rangle\langle i|)\, V|\varphi\rangle = M_i|\varphi\rangle \otimes |i\rangle$. Furthermore, V is an isometry since for any $|\varphi\rangle, |\psi\rangle \in \mathcal{H}_A$ it holds that

$$\begin{aligned}\langle\psi|V^\dagger V|\varphi\rangle &= \sum_{i,j\in I} (\langle\psi|M_j^\dagger \otimes \langle j|)(M_i|\varphi\rangle \otimes |i\rangle) \\ &= \sum_{i,j\in I} \langle\psi|M_j^\dagger M_i|\varphi\rangle\langle j|i\rangle = \sum_{i\in I} \langle\psi|M_i^\dagger M_i|\varphi\rangle = \langle\psi|\varphi\rangle\,.\end{aligned}$$

This proves the claim. □

If one is merely interested in the measurement outcome (and its distribution), but not in the post-measurement state, then also the converse holds: applying an isometry V followed by a measurement, given by a POVM $\{E_i\}_{i\in I}$, gives rise to the same distribution as directly performing the measurement given by the POVM $\{V^\dagger E_i V\}_{i\in I}$.

2.4 Quantum Teleportation

By **teleportation**, we understand the process of transporting a physical system from one place to another, without actually moving the physical system through the intervening space, merely classical information is communicated. We capture this by the following theorem.

Theorem 2.3. *Let $\mathcal{H}_A = \mathcal{H}_B = \mathcal{H}_E = \mathbb{C}^2$, and let $|\Phi\rangle \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be an EPR pair. Then, there exists $\mathbf{M} \in \mathcal{M}eas_I(\mathcal{H}_E \otimes \mathcal{H}_A)$ and a family $\{U_i\}_{i\in I}$ of unitaries in $\mathcal{U}(\mathcal{H}_B)$, such that for every $|\varphi\rangle \in \mathcal{S}(\mathcal{H}_E)$ and $i \in I$ there exists $|\psi^i\rangle \in \mathcal{S}(\mathcal{H}_E)$ such that*

$$\big(\mathbb{I}_{EA} \otimes U_i\big)\big(\tfrac{1}{\sqrt{p_i}} M_i \otimes \mathbb{I}_B\big)|\varphi\rangle|\Phi\rangle = |\psi^i\rangle \otimes |\varphi\rangle\,.$$

In other words, Alice can teleport the state $|\varphi\rangle \in \mathcal{S}(\mathcal{H}_E)$ to Bob by measuring EA and sending the measurement outcome i to Bob, and Bob can recover $|\varphi\rangle$ by applying U_i to B (see Figure 2.1).

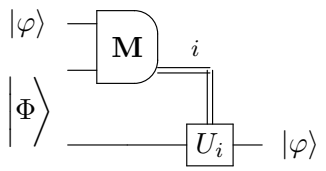

Figure 2.1: Quantum teleportation.

The measurement on Alice's side is given by the **Bell states**

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big) \qquad |\Psi^+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|1\rangle + |1\rangle|0\rangle\big)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle - |1\rangle|1\rangle\big) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|1\rangle - |1\rangle|0\rangle\big)\,,$$

which form a basis of the 2-qubit state space $\mathbb{C}^2 \otimes \mathbb{C}^2$. The first state vector, $|\Phi^+\rangle$, is called an **EPR pair**, named after Einstein, Podolsky and Rosen; $|\Psi^+\rangle$ is called a **singlet state**. As can easily be verified, the inverse basis transformation is given by

$$|0\rangle|0\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle) \qquad |1\rangle|0\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle)$$
$$|0\rangle|1\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle) \qquad |1\rangle|1\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle)\,.$$

Proof. **M** is the projective rank-1 measurement given by the Bell basis; the unitaries, we will fix later. Consider now an arbitrary qubit state $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathcal{H}_E$. The joint state is then given by the 3-qubit state

$$\begin{aligned}|\Omega\rangle = |\varphi\rangle \otimes |\Phi^+\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big) \\ &= \frac{\alpha}{\sqrt{2}}|0\rangle|0\rangle|0\rangle + \frac{\alpha}{\sqrt{2}}|0\rangle|1\rangle|1\rangle + \frac{\beta}{\sqrt{2}}|1\rangle|0\rangle|0\rangle + \frac{\beta}{\sqrt{2}}|1\rangle|1\rangle|1\rangle\,.\end{aligned}$$

To understand the effect of the Bell measurement, we rewrite the two qubits that Alice controls in the Bell basis, and obtain

$$|\Omega\rangle = \frac{1}{2}|\Phi^+\rangle\big(\alpha|0\rangle+\beta|1\rangle\big) + \frac{1}{2}|\Phi^-\rangle\big(\alpha|0\rangle-\beta|1\rangle\big) + \frac{1}{2}|\Psi^+\rangle\big(\beta|0\rangle+\alpha|1\rangle\big) + \frac{1}{2}|\Psi^-\rangle\big(-\beta|0\rangle+\alpha|1\rangle\big)\,.$$

Hence, depending on the measurement outcome, the state collapses to one of the following four states.

$$|\Phi^+\rangle\big(\alpha|0\rangle+\beta|1\rangle\big), \quad |\Phi^-\rangle\big(\alpha|0\rangle-\beta|1\rangle\big), \quad |\Psi^+\rangle\big(\beta|0\rangle+\alpha|1\rangle\big), \quad \text{or} \quad |\Psi^-\rangle\big(-\beta|0\rangle+\alpha|1\rangle\big)$$

Note the similarity of Bobs qubit to the original state $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$; in all cases, the qubit Bob controls can be transformed into the right state by a suitable unitary: in case of the first of the four possible measurement outcomes, it is simply the identity, in case of the second possible outcome, it is the unitary that maps $|0\rangle$ to $|0\rangle$ and $|1\rangle$ to $-|1\rangle$, etc. □

2.5 "Quantum" versus "Classical" Information

So far, and we will to a large extent continue doing so, we have carefully distinguished between *classical* and *quantum* information. Formally, "classical information", like the outcome of a measurement, is captured by an element x of some given non-empty finite set $\mathcal{X}$. On the other hand, "quantum information" is captured by a state vector $|\varphi\rangle$ in some given Hilbert space. We want to argue here that we may also use the quantum formalism to capture classical information, i.e., in other words, we may understand quantum information as a generalization of classical information.

For this purpose, for any given (non-emtpy finite) set $\mathcal{X}$, we consider a fixed orthonormal basis $\{|x\rangle\}_{x\in\mathcal{X}}$ of the state space $\mathcal{H} = \mathbb{C}^{|\mathcal{X}|}$, and we identify $x \in \mathcal{X}$ with $|x\rangle \in \mathcal{S}(\mathcal{H})$. It is in this sense that the qubit states $|0\rangle$ and $|1\rangle$ represent the respective classical bits 0 and 1. We note that such an "encoding of classical information into a quantum state" can be "decoded" simply by measuring the "encoding" $|x\rangle$ in the considered basis $\{|x\rangle\}_{x\in\mathcal{X}}$: the classical measurement outcome x is observed with probability 1.

We can also use the quantum formalism to capture classical information *processing*, by identifying classical functions by unitary operators. For example, we see that the logical `not` function $\neg : \{0,1\} \to \{0,1\}$, $x \mapsto x \oplus 1$, where $\oplus$ is the addition modulo 2, is captured by the the Pauli-X unitary, as introduced in Section 1.2:

$$|\neg x\rangle = X|x\rangle$$

for any $x \in \{0,1\}$. Another example is the 2-qubit **SWAP** operator $SWAP \in \mathcal{U}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, defined by

$$SWAP|x\rangle|y\rangle = |y\rangle|x\rangle$$

for all $x, y \in \{0,1\}$, which captures the 2-bit function that swaps the input bits by means of a 2-qubit unitary. Another simple yet important example is the 2-qubit **control-NOT** operator $CNOT \in \mathcal{U}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, defined by

$$CNOT|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle$$

for all $x, y \in \{0,1\}$, which captures the 2-bit function that applies the logic `not` to the second bit if and only if the first is 1. We emphasize that this representation of a function by means of a unitary crucially depends on the choice of basis used for representing classical information by means of quantum states. Indeed, it is interesting to see how $CNOT$ acts on an input that is classical with respect to the Hadamard basis, i.e., what $CNOT(H|x\rangle \otimes H|y\rangle)$ evaluates to (when expressed in the Hadamard basis $\{H|0\rangle, H|1\rangle\}$ again). We leave this as an exercise.

We also emphasize that the above approach for representing a classical function f by means of the operator $|x\rangle \mapsto |f(x)\rangle$ only works if the function is *injective*, as otherwise the operator is not unitary. In order to deal with an arbitrary function, one uses the following approach.

Definition 2.1. *For any function $f : \mathcal{X} \to \mathcal{Y}$, we define $U_f \in \mathcal{U}(\mathcal{H}_X \otimes \mathcal{H}_Y)$ given by*

$$U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$$

so that

$$U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle\,.$$

Here, it is understood that fixed bases $\{|x\rangle\}_{x\in\mathcal{X}}$ and $\{|y\rangle\}_{y\in\mathcal{Y}}$ of $\mathcal{H}_X = \mathbb{C}^{|\mathcal{X}|}$ and $\mathcal{H}_Y = \mathbb{C}^{|\mathcal{Y}|}$ have been respectively chosen, and $\oplus$ is an operation that turns $\mathcal{Y}$ into an Abelian group with neutral element 0. Often, this group structure is naturally given.

In this light (and with the obvious way to understand the binary set $\{0,1\}$ as a group), we actually have that $CNOT = U_{id}$ for the identity function $id : \{0,1\} \to \{0,1\}$, $x \mapsto x$, but this is not how we think of $CNOT$.

2.6 Control Unitaries

The control-NOT operator $CNOT \in \mathcal{U}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ can also be understood in that it applies the Pauli X operator to the target qubit if (and only if) the control (qu)bit is set. This naturally generalizes.

Definition 2.2. *For any $U \in \mathcal{U}(\mathcal{H})$, the corresponding* **control unitary** *$C(U) \in \mathcal{U}(\mathbb{C}^2 \otimes \mathcal{H})$ (w.r.t. $\{|0\rangle, |1\rangle\}$) is defined as*

$$C(U) := |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes U\,,$$

so that $C(U)|x\rangle|\varphi\rangle = |x\rangle \otimes U^x|\varphi\rangle$ for arbitrary $x \in \{0,1\}$ and $|\varphi\rangle \in \mathcal{H}$. More generally, for arbitrary $n \in \mathbb{N}$ the **multi-control unitary** *$C^n(U) \in \mathcal{U}(\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \otimes \mathcal{H})$ is defined to map*

$$C^n(U) : |x_1\rangle \cdots |x_n\rangle|\varphi\rangle \mapsto |x_1\rangle \cdots |x_n\rangle \otimes U^{x_1 \cdots x_n}|\varphi\rangle$$

for arbitrary $x_1, \ldots, x_n \in \{0,1\}$ and $|\varphi\rangle \in \mathcal{H}$.

We note that the above definition of $C(U)$ is so that the first qubit is the **control qubit** and the second qubit is the **target state**, but we also speak of a control unitary and write $C(U)$ if it is the other way round, or, in case of a multi-control unitary, if the target state is at an arbitrary position. For instance, one could consider labeled Hilbert spaces, say using "1" and "2" as labels, and $C_1(U_2)$ would then be controlled by (the system labeled with) "1" and have (the system labeled with) "2" as target, and vice versa for $C_2(U_1)$ then. However, we typically clarify this matter in an ad-hoc manner, or by means of picturing them appropriately as **gates** in a **quantum circuit** (see the upcoming figures)

We also emphasize that even though the definition of a (multi-)control unitary is in terms of how $C^n(U)$ acts when the control qubits are classical, i.e. $|0\rangle$ or $|1\rangle$, the action of the control unitary is well defined on the entire space, and thus may be applied to an *arbitrary* state. Furthermore, maybe somewhat counterintuitive, $C^n(U)$ may in such a case then actually modify the control qubits.

Obviously, we have $CNOT = C(X)$. Furthermore, $C^2(X)$ is referred to as **Toffoli gate**. Of course, we can also consider variations of (multi-)control unitaries, where the unitary U is applied conditioned on another setting of the control qubit(s) than being (all) one. Formally, for any $c = (c_1, \ldots, c_n) \in \{0,1\}^n$ we can consider

$$C^n[c](U) := (X^{c_1 \oplus 1} \otimes \cdots \otimes X^{c_n \oplus 1} \otimes \mathbb{I})\, C^n(U)\, (X^{c_1 \oplus 1} \otimes \cdots \otimes X^{c_n \oplus 1} \otimes \mathbb{I})\,,$$

which is such that

$$C^n[c](U)|x\rangle|\varphi\rangle = \begin{cases} |x\rangle \otimes U|\varphi\rangle & \text{if } x = c \\ |x\rangle|\varphi\rangle & \text{else} \end{cases}\,.$$

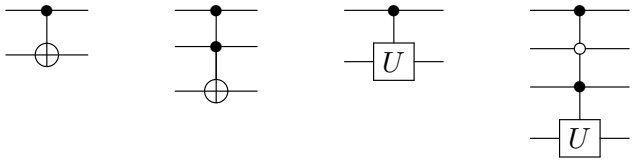

Figure 2.2: Pictorial gate representations of *CNOT*, the Toffoli gate, $C(U)$ and $C^3[1,0,1](U)$.

2.7 Decomposing Control Unitaries

Our goal here will be to show that for any *single-qubit* unitary $U \in \mathcal{U}(\mathbb{C}^2)$, the corresponding (multi-)control unitary $C^n(U)$ can be decomposed into *CNOT* and single-qubit unitaries.

First, we need the following technical result.

Lemma 2.4. *For any $U \in \mathcal{U}(\mathbb{C}^2)$ there exist $A, B, C \in \mathcal{U}(\mathbb{C}^2)$ and $\alpha \in \mathbb{R}$ so that*

$$ABC = \mathbb{I} \qquad \text{and} \qquad e^{i\alpha} AXBXC = U\,.$$

Proof. By means of the Z-Y decomposition (Theorem 1.4) and introducing a factor 2 for convenience, we can write U as $U = e^{i\alpha} R_Z(2\beta) R_Y(2\gamma) R_Z(2\delta)$. Setting

$$A := R_Z(2\beta) R_Y(\gamma) \quad , \qquad B := R_Y(-\gamma) R_Z(-\beta - \delta) \qquad \text{and} \qquad C := R_Z(-\beta + \delta)\,,$$

we then immediately see that $ABC = \mathbb{I}$, but also, by basic properties of X, R_Y and R_Z,

$$AXBXC = R_Z(2\beta) R_Y(\gamma) X R_Y(-\gamma) X X R_Z(-\beta-\delta) X R_Z(-\beta+\delta) = R_Z(2\beta) R_Y(2\gamma) R_Z(2\delta)\,,$$

which proves the claim. □

Theorem 2.5. *For any $U \in \mathcal{U}(\mathbb{C}^2)$ there exist $A, B, C \in \mathcal{U}(\mathbb{C}^2)$ and $\alpha \in \mathbb{R}$ so that*

$$C(U) = (S_\alpha \otimes A)\, CNOT\, (\mathbb{I} \otimes B)\, CNOT\, (\mathbb{I} \otimes C)$$

See Figure 2.3 below for the representation of the claimed decomposition of $C(U)$ in the form of a (pictorially represented) **quantum circuit**.

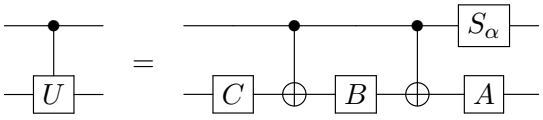

Figure 2.3: Computing $C(U)$ with *CNOT* and single qubit gates.

Remark 2.1. Note that, by convention, such a circuit acts on any input state vector by sequentially applying the **gates** starting from the *left*, while e.g. the corresponding term in Theorem 2.5 acts by sequentially applying the unitaries starting from the *right*.

Proof. Choosing the unitaries A, B, C and $\alpha \in \mathbb{C}$ as promised by Lemma 2.4, it is clear that $(\mathbb{I} \otimes A)\, CNOT\, (\mathbb{I} \otimes B)\, CNOT\, (\mathbb{I} \otimes C)$, where the phase shift gate S_α is omitted, maps

$$|0\rangle|\varphi\rangle \mapsto |0\rangle \otimes ABC|\varphi\rangle = |0\rangle|\varphi\rangle \qquad \text{and} \qquad |1\rangle|\varphi\rangle \mapsto |1\rangle \otimes AXBXC|\varphi\rangle\,.$$

It remains to show that S_α, acting on the first qubit, leaves $|0\rangle|\varphi\rangle$ untouched and maps the other into $|1\rangle \otimes e^{i\alpha} AXBXC|\varphi\rangle$, but this holds by definition of S_α. □

Arbitrary double-control unitaries can be computed from single-control unitaries as follows; the proof is left as an exercise.

Proposition 2.6. *Let $U \in \mathcal{U}(\mathcal{H})$, and let $V \in \mathcal{U}(\mathcal{H})$ be so that $V^2 = U$. Then $C^2(U)$ decomposes into CNOT, $C(V)$ and $C(V^\dagger)$ operations, as given in Figure 2.4.*

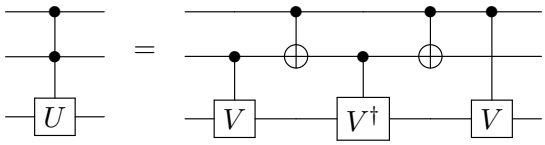

Figure 2.4: Computing $C^2(U)$ with *CNOT* and single-control unitaries.

Remark 2.2. We could circumvent the representation of the claimed decomposition by means of a quantum circuit by labelling the three qubits as $1, 2$ and 3, say, and then express the claimed operator equality as

$$C^2_{12}(U_3) = C_1(V_3)\, CNOT_{12}\, C_2(V_3^\dagger)\, CNOT_{12}\, C_2(V_3)\,.$$

However, such an expression seems harder to parse than a quantum circuit.

By replacing U with $C^{n-2}(U)$ and V with $C^{n-2}(V)$, and applying induction to compute $C\big(C^{n-2}(V)\big) = C^{n-1}(V)$, we obtain the following.

Corollary 2.7. *For any unitary $U \in \mathcal{U}(\mathcal{H})$, the multi-control unitary $C^n(U)$ decomposes into a sequence of CNOT's and control unitaries $C(V)$ with $V \in \mathcal{U}(\mathcal{H})$, all acting on $(\mathbb{C}^2)^{\otimes n} \otimes \mathcal{H}$.*

Using Theorem 2.5 to further decompose the control unitaries (in case $\mathcal{H} = \mathbb{C}^2$), we obtain the following.

Corollary 2.8. *For any single-qubit unitary $U \in \mathcal{U}(\mathbb{C}^2)$, the multi-control unitary $C^n(U)$ decomposes into CNOT's and single-qubit unitaries, all acting on $(\mathbb{C}^2)^{\otimes(n+1)}$.*

We point out that the number of gates to be computed in the above recursive construction for $C^n(U)$ is exponential in n. The following gives a more efficient way. First, note that applying Proposition 2.6 to $V \in \mathcal{U}(\mathbb{C}^2)$ with $V^2 = X$ gives us the means to compute the Toffoli gate with a single-qubit unitary and *CNOT*. Then, Figure 2.5 illustrates how a multi-control unitary $C^n(U)$ can be computed by means of the single-control unitary $C(U)$ and Toffolis, using $n-1$ "work qubits" that start off and end up again in state $|0\rangle$.

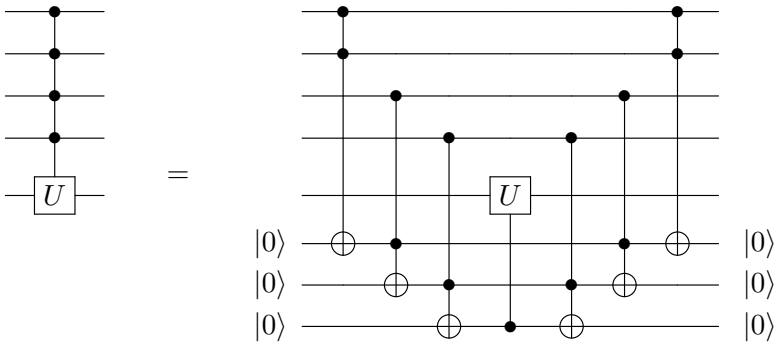

Figure 2.5: Computing $C^n(U)$ with Toffolis and $C(U)$, for the case $n = 4$.

Formally, we have the following.

Proposition 2.9. *For any $U \in \mathcal{U}(\mathcal{H})$ and for $V \in \mathcal{U}\big((\mathbb{C}^2)^{\otimes n} \otimes \mathcal{H} \otimes (\mathbb{C}^2)^{\otimes(n-1)}\big)$ defined by (the obvious generalization to an arbitrary n of) the right hand side in Figure 2.5, we have*

$$V|x\rangle|\varphi\rangle|\mathbf{0}\rangle = C^n(U)|x\rangle|\varphi\rangle \otimes |\mathbf{0}\rangle$$

for any $x \in \{0,1\}^n$ *and* $|\varphi\rangle \in \mathcal{H}$*, and where* $|\mathbf{0}\rangle = |0\rangle^{\otimes(n-1)}$.

Remark 2.3. In order for the above equality to extend to *any* $|\Omega\rangle \in (\mathbb{C}^2)^{\otimes n} \otimes \mathcal{H}$, not necessarily $|\Omega\rangle = |x\rangle|\varphi\rangle$, it is crucial that the "work qubits" end up again in state $|\mathbf{0}\rangle$, and not in something that, say, depends on x.