QuIC Seminar 3

# More on Tensor Products and Measurements

## Contents



## 3.1 Multi-particle Quantum Systems

It is a fundamental postulate of quantum mechanics that multiple qubits (more generally multiple quantum states) combine in a way that we mathematically represent with the tensor product.

*Definition* 3.1 (State space of multi-particle quantum systems.). The **state space of a composite quantum system** is the tensor product of the state spaces of component quantum systems. If the systems are labeled 1 through $n$ and system $i$ is in the state $|i\rangle$, then the state of the total system is given by

$$|\psi\rangle = \bigotimes_{i=1}^{n} |i\rangle = |1\rangle \otimes |2\rangle \otimes \cdots \otimes |n\rangle. \tag{3.1}$$

This state lives in the composite space

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n \tag{3.2}$$

where $\mathcal{H}_i$ is the Hilbert space of system $i$.

We've seen one notable feature of tensor products already that "dimensions multiply with tensor product spaces" (namely Theorem 2.1). We've also computed tensor products element-wise and worked with implicit tensor products in ket notations like ($|00\rangle \equiv |0\rangle \otimes |0\rangle$) in the quantum teleportation algorithm. (It's generally better in analyzing quantum algorithms to stick to the latter inasmuch as possible.) The first topic of this seminar is to mathematically formalize tensor products. Doing so will allow us to master quantum algorithms faster and discuss further features of them without being confused by the mathematical details. We'll mention and discuss further important physical considerations (such as product states, entangled states, etc.) in our presentation as well.

### 3.1.1 Tensor Product Properties

Before formally stating a computational definition of the tensor product, we start with an example.

**Example 1: Tensor products of matrices.**
Let $A = [A_{ij}]$ and $B = [B_{ij}]$ be two-by-two matrices, explicitly

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}, \qquad B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}. \tag{3.3}$$

Then, we have

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B \\ A_{21}B & A_{22}B \end{bmatrix} \qquad \text{and} \qquad B \otimes A = \begin{bmatrix} B_{11}A & B_{12}A \\ B_{21}A & B_{22}A \end{bmatrix}. \tag{3.4}$$

In words, to compute $A \otimes B$, we take $A_{11}$ copies of $B$ as our new (1, 1) element, which is a scalar multiple of a two by two matrix (and again a two by two matrix). Similarly for the other entries. Written out explicitly in terms of all matrix elements, we have

$$A \otimes B = \begin{bmatrix} A_{11}B_{11} & A_{11}B_{12} & A_{12}B_{11} & A_{12}B_{12} \\ A_{11}B_{21} & A_{11}B_{22} & A_{12}B_{21} & A_{12}B_{22} \\ A_{21}B_{11} & A_{21}B_{12} & A_{22}B_{11} & A_{22}B_{12} \\ A_{21}B_{21} & A_{21}B_{22} & A_{22}B_{21} & A_{22}B_{22} \end{bmatrix} \tag{3.5}$$

Note that the dimension of $A \otimes B$ (four by four, sixteen elements) is the product of the dimensions of $A$ (two by two, four elements) and $B$ (two by two, four elements), as we have stated previously. Also note that $A \otimes B \neq B \otimes A$ in general. That is, the tensor product is not commutative.

**Exercise 22:** Write down $B \otimes A$ in the same way as (3.5).

The above example easily generalizes into the definition below. Note that we use the term *tensor* to be a generalization of the terms scalar, vector, matrix, etc. A *rank zero tensor* is a scalar, a *rank one tensor* is a vector, and a *rank two tensor* is a matrix. A *rank three tensor*, for which we have no other commonly-used name, is indexed by three dimensions, $[T = T_{ijk}]$, say. This can be thought of as "a book whose pages are matrices," or equivalently as a matrix whose entries are vectors. Generally, a tensor is just a multidimensional object (a *rank* $n$ tensor has $n$ dimensions) whose entries are in some field like $\mathbb{R}$ or $\mathbb{C}$. We use this to generally state the tensor product given below.

*Definition* 3.2 (Computing the Tensor Product). Let $u$ be a rank $m$ tensor and $v$ be a rank $n$ tensor. The **tensor product** $u \otimes v$ is a rank $mn$ tensor whose $i_1 i_2 \cdots i_m$th component is $u_{i_1 \cdots i_m} v$, a rank $n$ tensor.

For us, we will almost always be concerned with tensor products of quantum states $|\psi\rangle$, unitary matrices $U$, and later the density matrix formalism of quantum states commonly denoted $\rho$. We can now compute tensor products of all of these using the above definition in terms of matrix elements. Often, it is the case that we *do not* explicitly want to do this, but rather work with properties of the tensor product, listed below.

*Theorem* 3.1 (Basic Properties of the Tensor Product). Let $u_i$, $v_i$ be tensors over the complex numbers and $c$ a complex scalar. Then, the following scalar multiple and distributive properties hold:

$$(cu) \otimes v = u \otimes (cv) = c(u \otimes v) \tag{3.6}$$

$$(u_1 + u_2) \otimes v = u_1 \otimes v + u_2 \otimes v \tag{3.7}$$

$$u \otimes (v_1 + v_2) = u \otimes v_1 + u \otimes v_2. \tag{3.8}$$

Further, tensor products multiply respectively as

$$(u_1 \otimes v_1)(u_2 \otimes v_2) = u_1 u_2 \otimes v_1 v_2 \tag{3.9}$$

where the operation on the right is tensor multiplication of $u_1$ ($v_1$) and $u_2$ ($v_2$).

*Proof.* The proof of these properties follows immediately from Definition 3.2. □

Consider tensors which are qubits $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. We now know that multiple qubits combine via the tensor product given above. We often have operators $U$ which act on qubits, however. How do operators work under the tensor product?

*Definition* 3.3 (Tensor Products of Operators). Let $U$ be an operator on a Hilbert space $\mathcal{H}_A$ and $V$ be an operator on another Hilbert space $\mathcal{H}_B$. If $|\psi\rangle_A \otimes |\phi\rangle_B$ is a quantum state on the composite space $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$, then $U \otimes V$ is an operator on the space $\mathcal{H}_{AB}$ and

$$(U \otimes V)(|\psi\rangle_A \otimes |\phi\rangle_B) := U|\psi\rangle_A \otimes V|\phi\rangle_B. \tag{3.10}$$

We have an important theorem about tensor products of unitary matrices:

*Theorem* 3.2 (Tensor Product of Unitary Operators is Unitary). Let $U$ and $V$ be as in Definition 3.3. If $U$ is unitary on $\mathcal{H}_A$ and $V$ is unitary on $\mathcal{H}_B$, then $U \otimes V$ is unitary on $\mathcal{H}_{AB}$.

*Proof.* This can be proved by noting (Theorem 2.1) that a basis for $\mathcal{H}_{AB}$ is $\{|i\rangle_A \otimes |j\rangle_B\}_{i,j}$. Then, since unitary operators map orthonormal bases to orthonormal bases, it is easy to see that $U \otimes V$ is unitary. □

**Example 2: Four by four Hadamard transform.**
Here we compute $H \otimes H$ ($H$ is the Hadamard gate) and verify that the resulting matrix is indeed unitary. We have that

$$H \otimes H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \tag{3.11}$$

It is easy to see that all four columns have norm one and are mutually orthogonal, which shows that the resulting matrix is indeed unitary as guaranteed by Theorem 3.2. This is an example of a more general class of *Hadamard transforms*, a set of unitary transforms which can be recursively defined via the tensor product as $H_m = H_1 \otimes H_{m-1}$ where $H_1 \equiv H$ and $m = 1, 2, 3, \ldots$.

Last, we note the following about tensor products and inner products, which is often useful for calculations with quantum algorithms.

*Definition* 3.4 (Inner Product of Product States). Let $|\psi\rangle_A \otimes |\phi\rangle_B$ and $|\omega\rangle_A \otimes |\gamma\rangle_B$ be states on $\mathcal{H}_A \otimes \mathcal{H}_B$. Then, the **inner product** of these states is

$$(|\psi\rangle_A \otimes |\phi\rangle_B)^\dagger (|\omega\rangle_A \otimes |\gamma\rangle_B) = (\langle\psi|_A \otimes \langle\phi|_B)(|\omega\rangle_A \otimes |\gamma\rangle_B) = \langle\psi|\omega\rangle\langle\phi|\gamma\rangle, \tag{3.12}$$

that is, the product of inner products on the respective Hilbert spaces.

**Exercise 23:** Compute $\langle 00|00\rangle$, $\langle 00|01\rangle$, and $\langle 00| + +\rangle$.

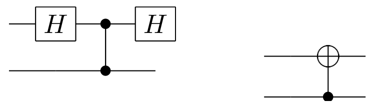


Figure 3.1: Two equivalent quantum circuits.

### 3.1.2 Controlled Operations

So far we have considered the tensor product from a very mathematical perspective. In the following three subsections, we'll successively get back to more and more physics. First we discuss controlled operations in quantum circuits, which have much to do with tensor products.

Let $U$ be an arbitrary unitary operation on one qubit. A controlled-$U$ operation involves two qubits. One serves as the *control*, and the other serves as the *target*. If the control qubit is in the $|0\rangle$ state, we do nothing to the target qubit. If the control qubit is in the $|1\rangle$ state, we perform $U$ on the target qubit. Mathematically, we can write this statement using tensor products.

*Definition* 3.5 (Controlled Operations). Let $C(U)$ denote a **controlled-$U$** operation. Then, we have

$$C(U) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U \tag{3.13}$$

where the first (left-most) qubit is the control and the second (right-most) qubit is the target.

**Exercise 24:** Using Definition 3.2, show that a matrix representation of $C(U)$ in the computational basis is

$$C(U) = \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix}. \tag{3.14}$$

Verify that this matrix is unitary.

**Exercise 25:** Let $U$ be the NOT gate (Pauli-$X$) and verify that (3.14) is the same as the matrix representation of CNOT in the computational basis (2.22).

**Exercise 26:** Using (3.14), prove that the control of a product is the product of controls. Explicitly, prove that

$$C(U_1 \cdots U_n) = C(U_1) \cdots C(U_n). \tag{3.15}$$

### 3.1.3 Tensor Products in Quantum Circuits

At this point we formalize the connection between tensor products and quantum circuits. Quantum computers themselves are like tensor product machines. Whenever we write a quantum circuit in a diagram, it's really just shorthand notation for a bunch of qubits combined via tensor products with unitary gates inserted at specified locations, as we saw in the mathematical analysis of the teleportation algorithm. Here we proceed with several examples to further illustrate this point.

**Example 3: Two Two-Qubit Circuit Analyses.**
Consider the two circuits shown in Figure 3.1. This example emphasizes the connection between quantum circuit diagrams and mathematical expressions involving tensor products. It also shows that the two circuits in this figure are equivalent, leading to one of many *circuit identities* that are important in quantum algorithms.

We omit input states in these circuits because they could be arbitrary. We can denote the input most generally as

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = [\alpha\,\beta\,\gamma\,\delta]^T. \tag{3.16}$$

Consider the circuit on the left in Figure 3.1. Reading the circuit from left to right, the first operation is a Hadamard gate on the first qubit and nothing—equivalently and identity gate—on the second qubit. Mathematically, this says perform $H \otimes I$ on $|\psi\rangle$. Next we perform a controlled-$Z$ ($C(Z)$ gate (note that this gate is symmetric with respect to control/target, as the circuit notation suggests). Applying $C(Z)$ then flips the sign of the second qubit if the first qubit is in the one state. Lastly we perform $H \otimes I$ on the resulting state. The entire circuit may thus be written

$$(H \otimes I)C(Z)(H \otimes I). \tag{3.17}$$

Using the matrix representations in the computational basis

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}, \qquad C(Z) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \tag{3.18}$$

it is easy to verify that

$$(H \otimes I)C(Z)(H \otimes I) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \tag{3.19}$$

Thus the entire effect of the circuit on the left in Figure 3.1 is

$$[\alpha\, \beta\, \gamma\, \delta] \longmapsto [\alpha\, \delta\, \gamma\, \beta]\,. \tag{3.20}$$

A matrix representation for the circuit on the right in Figure 3.1 is simply CNOT with the control as the second qubit and target as the first qubit. That is, this circuit has the effect

$$|00\rangle \mapsto |00\rangle, \qquad |01\rangle \mapsto |11\rangle, \qquad |10\rangle \mapsto |10\rangle, \qquad |11\rangle \mapsto |01\rangle. \tag{3.21}$$

Written as a matrix in the computational basis, this yields an identical matrix to (3.19). Thus, the effect of the two circuits is identical.

Circuits that contain as few gates as possible are desirable when implemented on actual quantum computers because each additional gate adds a small amount of noise to the computation. Circuits with few gates, or *short-depth* circuits, are thus desirable.

Also, the only two-qubit gate that some quantum computers can implement is a CNOT gate, and other architectures are only able to implement a $C(Z)$ gate. To run an algorithm expressed in CNOT gates, the first type of quantum computers must translate these CNOT gates via Hadamard gates as in Figure 3.1. This type of problem falls into the realm of *quantum compiling*. Similar considerations exist in classical programming languages: compilers translate high-level language that humans can understand into low-level language that computers can understand. (By the way, any $n$-qubit unitary transformation can be written in terms of single qubit gates and CNOT gates up to arbitrary precision.)

### 3.1.4 More on Entanglement

Recall from previous seminars we defined entangled states to be any states that are not separable. A separable state is any state that can be written as a convex combination of product states. Before we argued that the Bell state

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right) \tag{3.22}$$

is an entangled state because it cannot be written as a product state. There is in fact a way to prove that (3.22) cannot be written as a product state, which we now go through.

**Example 4: Proof that $|\Phi^+\rangle$ is an Entangled State**

Suppose there exists states $\alpha|0\rangle + \beta|1\rangle$ and $\gamma|0\rangle + \delta|1\rangle$ such that

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle). \tag{3.23}$$

We can expand the right-hand side of this equation to write

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle. \tag{3.24}$$

By orthogonality, we can equate coefficients. This means that we must have complex numbers $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ such that

$$\alpha\gamma = \frac{1}{\sqrt{2}}, \qquad \alpha\delta = 0, \qquad \beta\gamma = 0, \qquad \beta\delta = \frac{1}{\sqrt{2}}. \tag{3.25}$$

By the middle two equations, it follows that at least two of these numbers must be zero, of which there are four cases: $\alpha = \beta = 0$, $\alpha = \gamma = 0$, $\delta = \beta = 0$, or $\delta = \gamma = 0$. In each of these cases, it is easy to see that at least one of the conditions of (3.25) is impossible to satisfy. Thus, the Bell state $|\Phi^+\rangle$ must be entangled.

This technique can be used in principle to find out if any given state is entangled. For states on many qubits, however, it is a very inefficient method since one would be dealing with many coefficients and many equations. More sophisticated methods based on Schmidt rank and reduced states, the theory of which we will develop later, are preferable in these cases.

**Exercise 27:** Generalize the argument in Example 3.1.4 to separable states, not just product states.

**Exercise 28:** Use the argument in Example 3.1.4 to show that the other three Bell states

$$|\Phi^-\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{3.26}$$

$$|\Psi^+\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{3.27}$$

$$|\Psi^-\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{3.28}$$

are entangled states.

## 3.2 Quantum Measurements

Measurements in quantum mechanics are what connects abstract quantum states (vectors in a Hilbert space) to physically observable quantities, like position, momentum, spin, etc. As if it weren't strange enough to represent physical systems by vectors in Hilbert space, quantum theory also imposes that measurement outcomes are probabilistic, as we have seen in the Born rule (Definition 1.10). In what follows we present a more systematic treatment of measurements in quantum systems. Our coverage only scratches the surface of a rich field—which has many connections to quantum foundations and the philosophy of quantum mechanics—but is sufficient for our focus on quantum algorithms.

For completeness, we repeat the measurement postulate of quantum mechanics here.

*Definition* 3.6 (Measurement Postulate in Quantum Mechanics)*.* **Quantum measurements** are described by a collection $\{M_m\}$ of *measurement operators* that act on the space of the quantum system being measured (e.g., $\mathbb{C}^2$ for qubits) and satisfy the *completeness equation*

$$\sum_m M_m^\dagger M_m = I. \tag{3.29}$$

The index $m$ refers to all measurement outcomes that may occur. If the state of the system is $|\psi\rangle$ immediately before the measurement, then the probability that result $m$ occurs is given by

$$p(m) := \langle\psi|M_m^\dagger M_m|\psi\rangle. \tag{3.30}$$

The state of the system immediately after the measurement is given by

$$\frac{M_m|\psi\rangle}{\sqrt{p(m)}}. \tag{3.31}$$

The two subsequent formalisms of POVMs and projective measurements are special cases of this postulate, as we will see, but are so commonly used and discussed that they warrant their own coverage. It may even be more appropriate to think of POVMs and Projective measurements as building blocks of the measurement postulate. In particular, POVMs are building blocks of projective measurements, and projective measurements are building blocks of the general measurement postulate. Because of this hierarchy, POVMs are the most general construction, and the one we will look at first.

### 3.2.1 Positive Operator Valued Measurements (POVMs)

The POVM formalism is commonly used when we only care about the outcome of a measurement and not the quantum state after measurement.

*Definition* 3.7 (POVMs). A **POVM** is a set of positive Hermitian operators $\{E_m\}$ such that

$$\sum_m E_m = I \tag{3.32}$$

and the probability of outcome $m$ is given by

$$p(m) = \langle\psi|E_m|\psi\rangle \tag{3.33}$$

when the state $|\psi\rangle$ is measured.

Note that we can define an observable $M_m$ for POVMs by $M_m := \sqrt{E_m}$. This enforces that $M_m^\dagger M_m = \sqrt{E_m}\sqrt{E_m} = E_m$. Thus, observables satisfy the completeness equation $\sum_m M_m^\dagger M_m = I$.

**Example 5: Heisenberg Uncertainty Principle**

The POVM formalism is enough to derive the famous Heisenberg uncertainty principle[a], which has to do with measuring separate observables simultaneously. Given the quantum state $|\psi\rangle$, suppose we are interested in two observables $A$ and $B$. Generally, we can say

$$\langle\psi|AB|\psi\rangle = x + iy \tag{3.34}$$

where $x, y \in \mathbb{R}$, from which it follows that

$$\langle\psi|BA|\psi\rangle = \langle\psi|AB|\psi\rangle^\dagger = x - iy. \tag{3.35}$$

Defining the commutator

$$[A, B] := AB - BA \tag{3.36}$$

and anticommutator

$$\{A, B\} := AB + BA, \tag{3.37}$$

it is easy to show that

$$\langle\psi|[A,B]|\psi\rangle = 2iy, \qquad \langle\psi|\{A,B\}|\psi\rangle = 2x. \tag{3.38}$$

By noting that

$$|\langle\psi|AB|\psi\rangle|^2 = \langle\psi|AB|\psi\rangle^\dagger\langle\psi|AB|\psi\rangle = (x-iy)(x+iy) = x^2+y^2, \tag{3.39}$$

we can equate combine (3.38) and (3.39) as

$$|\langle\psi|[A,B]|\psi\rangle|^2 + |\langle\psi|\{A,B\}|\psi\rangle|^2 = 4|\langle\psi|AB|\psi\rangle|^2. \tag{3.40}$$

Now, the key ingredient used in the derivation of the Heisenberg uncertainty principle is the Cauchy-Schwarz inequality

$$|\langle\psi|AB|\psi\rangle|^2 \leq \langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle. \tag{3.41}$$

Using this with (3.40), we may write

$$|\langle\psi|[A,B]|\psi\rangle|^2 \leq 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle. \tag{3.42}$$

If the operators are *centered*, i.e. $\langle A\rangle := \langle\psi|A|\psi\rangle = 0$ and similarly for $B$, then this is exactly the Heisenberg uncertainty principle

$$\boxed{\Delta(A)\Delta(B) \geq \frac{1}{2}|\langle\psi|[A,B]|\psi\rangle|} \tag{3.43}$$

where $\Delta(A) := \sqrt{\langle A^2\rangle - \langle A\rangle^2}$ is the standard deviation of $A$ (and similarly for $B$). If the operators are not centered, we can still permute $A \mapsto A - \langle A\rangle$ and $B \mapsto B - \langle B\rangle$ to obtain (3.43). (Note that $[A-\langle A\rangle, B-\langle B\rangle] = [A,B]$.)

[a] Which is really just the Cauchy-Schwarz inequality stated in the context of quantum mechanical measurements.

### 3.2.2 Projective Measurements

Projective measurements are more specific than POVMs via one additional orthogonality condition as well as a description of the quantum state immediately after measurement.

*Definition* 3.8 (Projective Measurement). A **projective measurement** is a set of positive Hermitian operators $\{P_m\}$ such that

$$\sum_m P_m = I \tag{3.44}$$

and

$$P_m P_{m'} = \delta_{mm'} P_m. \tag{3.45}$$

Upon measuring the state $|\psi\rangle$, the probability of getting result $m$ is

$$p(m) = \langle\psi|P_m|\psi\rangle. \tag{3.46}$$

Given that outcome $m$ occurred, the state of the quantum system immediately after the measurement is given by

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}} \tag{3.47}$$

Note that the observable for projective measurements is $M = \sum_m mP_m$ where $m$ is the eigenvalue of the eigenspace associated with $P_m$.

Projective measurements can be seen as a special case of general measurements (Definition 3.6) with the additional constraint is that the $M_m$ in Definition 3.6 are mutually orthogonal. That is,

$$M_m M_l = \delta_{ml} M_m. \tag{3.48}$$

Why is this? Note that he only difference between Definition 3.6 and Definition 3.8 is $p(m)$. If we enforce that $\{M_m\}$ are mutually orthogonal, then

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|M_m^2|\psi\rangle = \langle\psi|M_m|\psi\rangle, \tag{3.49}$$

the same as Definition 3.8 with $M_m = P_m$. (Note that these $M_m$ operators have spectral decompositions because they are Hermitian.)

The relationship between POVMs and projective measurements is summarized in the table below.

| Formalism | **POVMs** | **Projective Measurements** |
|---|---|---|
| Conditions | (1) $\{E_m\}$ such that $\sum_m E_m = I$ | (1) $\{P_m\}$ such that $\sum_m P_m = I$, (2) $P_m P_{m'} = \delta_{mm'} P_m$ |
| Observable | $M_m = \sqrt{E_m}$ | $M_m = \sum_m m P_m$ |
| Statistics | $p(m) = \langle\psi|E_m|\psi\rangle$ | $p(m) = \langle\psi|P_m|\psi\rangle$ |
| State | — | $P_m|\psi\rangle/\sqrt{p(m)}$ |

Table 3.1: Summary of POVMs and projective measurements. Each operator $E_m$ and each operator $M_m$ is positive and Hermitian. Compare these formalisms the the measurement postulate of quantum mechanics given in Defintion 3.6.

**Example 6: Projective Measurements on Qubits**

For qubits, a set of projective measurements can be formed via the projection operators

$$P_0 := |0\rangle\langle 0|, \qquad P_1 := |1\rangle\langle 1|. \tag{3.50}$$

These operators are clearly positive (eigenvalues are zero and one) and Hermitian (since $(|0\rangle\langle 0|)^\dagger = |0\rangle\langle 0|$ and similarly for $P_1$). In the context of quantum algorithms, these are referred to as *computational basis measurements* or *measurements in the computational basis* or *projectors onto the computational basis states*.

It's also easy to verify that

$$P_0 + P_1 = |0\rangle\langle 0| + |1\rangle\langle 1| = I. \tag{3.51}$$

Let $|\psi\rangle = \alpha|0\rangle_\beta|1\rangle$ be an arbitary qubit state. Then, the probability of obtaining $m = 0$ is, from (3.46),

$$\begin{aligned} p(m=0) &= \langle\psi|P_0|\psi\rangle \\ &= \langle\psi|0\rangle\langle 0|\psi\rangle \\ &= (\langle 0|\psi\rangle)^\dagger\langle 0|\psi\rangle \\ &= |\langle 0|\psi\rangle|^2 \\ &= |\alpha|^2, \end{aligned}$$

as we have seen previously with Born's law.

**Exercise 29:** Is $\{P_0, P_1\}$ a POVM (for $P_0$ and $P_1$ as defined in (3.50) above)?

**Exercise 30:** Let $P_2 := |+\rangle\langle +|$. Verify that $P_2$ is positive and Hermitian. Is $\{P_0, P_1\}$ a POVM? Is it a projective measurement?

**Exercise 31:** Is $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ a POVM? Is it a projective measurement? What is the probability of obtaining $+$, $p(m = +)$ for the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$? What about $p(m = -)$?