

## Lecture 2: Quantum computation review

*“I think that a particle must have a separate reality independent of measurements. That is, an electron has spin, location and so forth even when it is not being measured. I like to think the moon is there even if I am not looking at it.”*

— Albert Einstein

*“... experiments have now shown that what bothered Einstein is not a debatable point but the observed behaviour of the real world.”*

— N. David Mermin

### Contents

<b>1</b>	<b>Linear Algebra</b>	<b>1</b>
<b>2</b>	<b>Basic quantum computation</b>	<b>6</b>
2.1	Pure state quantum computation . . . . .	6
2.1.1	Individual systems . . . . .	6
2.1.2	Quantum gates . . . . .	6
2.1.3	Composite quantum systems . . . . .	7
2.1.4	Measurement . . . . .	9
2.2	Mixed state quantum computation . . . . .	10
2.2.1	Operations and measurements on mixed states . . . . .	11

**Introduction.** In Lecture 1, we reviewed the basics of classical complexity theory, including Turing machines, P, NP, reductions, and NP-completeness. We now move to the quantum realm and review the basics of quantum computation. Again, we shall move rather quickly, as a beginning background in quantum computation is assumed for this course.

### 1 Linear Algebra

In this course, we shall discuss quantum computation exclusively from a finite-dimensional linear algebraic perspective. For this, we begin with a quick review of linear algebraic terminology and definitions.

We denote  $d$ -dimensional complex column vectors  $|\psi\rangle \in \mathbb{C}^d$  using Dirac notation, i.e. as

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_d \end{pmatrix}, \tag{1}$$

for  $\psi_i \in \mathbb{C}$ . The term  $|\psi\rangle$  is read “ket  $\psi$ ”. Recall also that a complex number  $c \in \mathbb{C}$  can be written in two equivalent ways: Either as  $c = a + bi$  for  $a, b \in \mathbb{R}$  and  $i = \sqrt{-1}$ , or in its *polar form* as  $c = re^{i\theta}$  for  $r \in \mathbb{R}$  and  $\theta \in [0, 2\pi)$ . The *complex conjugate* of  $c$  is  $c = a - bi$ , or equivalently  $c = re^{-i\theta}$ .

**Exercise 1.** The *magnitude* or “length” of  $c \in \mathbb{C}$  is given by  $|c| = \sqrt{cc^*}$ . What is the magnitude of  $e^{i\theta}$  for any  $\theta \in \mathbb{R}$ ? How about the magnitude of  $re^{i\theta}$ ?

The *conjugate transpose* of  $|\psi\rangle$  is given by

$$\langle\psi| = (\psi_1^*, \psi_2^*, \dots, \psi_d^*), \quad (2)$$

where note  $\langle\psi|$  is a *row* vector. The term  $\langle\psi|$  is pronounced “bra  $\psi$ ”. This allows us to define how much two vectors “overlap” via the *inner product* function, defined as  $\langle\psi|\phi\rangle = \sum_{i=1}^d \psi_i^* \phi_i$ , which satisfies  $(\langle\psi|\phi\rangle)^* = \langle\phi|\psi\rangle$ . The “length” of a vector  $|\psi\rangle$  can then be quantified by measuring the overlap of  $|\psi\rangle$  with itself, which yields the *Euclidean norm*,  $\| |\psi\rangle \|_2 = \sqrt{\langle\psi|\psi\rangle}$ .

**Exercise 2.** Let  $|\psi\rangle = \frac{1}{\sqrt{2}}(1, i)^T \in \mathbb{C}^2$ , where  $T$  denotes the transpose. What is  $\langle\psi|$ ? How about  $\| |\psi\rangle \|_2$ ?

**Orthonormal bases.** A set of vectors  $\{|\psi\rangle_i\} \subseteq \mathbb{C}^d$  is *orthogonal* if for all  $i \neq j$ ,  $\langle\psi|_i|\psi\rangle_j = 0$ , and *orthonormal* if  $\langle\psi|_i|\psi\rangle_j = \delta_{ij}$ . Here,  $\delta_{ij}$  is the Kronecker delta, whose value is 1 if  $i = j$  and 0 otherwise. For the vector space  $\mathbb{C}^d$ , which has dimension  $d$ , it is necessary and sufficient to use  $d$  orthonormal vectors in order to form an orthonormal basis.

One of the most common bases we use is the *computational* or *standard* basis, defined for  $\mathbb{C}^d$  as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \quad \dots \quad |d-1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \quad (3)$$

Since  $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$  is an orthonormal basis, any unit vector  $|\psi\rangle \in \mathbb{C}^d$  can be written as  $|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle$  for  $\alpha_i \in \mathbb{C}$  satisfying the *normalization* condition  $\| |\psi\rangle \|_2 = 1$ .

**Exercise 3.** What does  $\| |\psi\rangle \|_2 = 1$  mean in terms of a condition on the amplitudes  $\alpha_i$ ?

**Linear maps and matrices.** In this course, maps  $\Phi : \mathbb{C}^d \mapsto \mathbb{C}^d$  will typically be *linear*, meaning they satisfy for any  $\sum_i \alpha_i |\psi_i\rangle \in \mathbb{C}^d$  that  $\Phi(\sum_i \alpha_i |\psi_i\rangle) = \sum_i \alpha_i \Phi(|\psi_i\rangle)$ . The set of linear maps from vector space  $\mathcal{X}$  to  $\mathcal{Y}$  is denoted  $\mathcal{L}(\mathcal{X}, \mathcal{Y})$ . For brevity, we use shorthand  $\mathcal{L}(\mathcal{X})$  to mean  $\mathcal{L}(\mathcal{X}, \mathcal{X})$ .

Recall that linear maps have a *matrix* representation. A  $d \times d$  *matrix*  $A$  is a two-dimensional array of complex numbers whose  $(i, j)$ th entry is denoted  $A(i, j) \in \mathbb{C}$  for  $i, j \in [d]$ . To represent a linear map  $\Phi : \mathbb{C}^d \mapsto \mathbb{C}^d$  as a  $d \times d$  matrix  $A_\Phi$ , we use its action on a basis for  $\mathbb{C}^d$ . Specifically, define the  $i$ th column of  $A_\Phi$  as  $\Phi(|i\rangle)$  for  $\{|i\rangle\}$  the standard basis for  $\mathbb{C}^d$ , or

$$A_\Phi = [ \Phi(|0\rangle), \Phi(|1\rangle), \dots, \Phi(|d-1\rangle) ]. \quad (4)$$

In this course, we use both the matrix and linear map views interchangeably.

**Exercise 4.** Consider the linear map  $\Phi : \mathbb{C}^2 \mapsto \mathbb{C}^2$  with action  $\Phi(|0\rangle) = |1\rangle$  and  $\Phi(|1\rangle) = |0\rangle$ . What is the  $2 \times 2$  complex matrix representing  $\Phi$ ?

**Exercise 5.** Given any  $d \times d$  matrix  $A$ , what is  $A|i\rangle$  for  $|i\rangle \in \mathbb{C}^d$  a standard basis state?

The product  $AB$  of two  $d \times d$  matrices  $A$  and  $B$  is also a  $d \times d$  matrix with entries  $AB(i, j) = \sum_{k=1}^d A(i, k)B(k, j)$ . Note that unlike for scalars, for matrices it is *not* always true that  $AB = BA$ . In the special case where  $AB = BA$ , we say  $A$  and  $B$  *commute*.

**Exercise 6.** Do the following Pauli  $X$  and  $Z$  matrices commute:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}? \quad (5)$$

The *image* of a matrix  $A$  is the set of all possible output vectors under the action of  $A$ , i.e.  $\text{Im}(A) := \{|\psi\rangle \in \mathbb{C}^d \mid |\psi\rangle = A|\phi\rangle \text{ for some } |\phi\rangle \in \mathbb{C}^d\}$ . The *rank* of  $A$  is the dimension of its image, i.e.  $\dim(\text{Im}(A))$ . The set of all vectors sent to zero by  $A$  is called its *null space*, i.e.  $\text{Null}(A) := \{|\psi\rangle \in \mathbb{C}^d \mid A|\psi\rangle = 0\}$ . The *Rank-Nullity Theorem* says that these two spaces are related via  $\dim(\text{Null}(A)) + \dim(\text{Im}(A)) = d$ .

**Exercise 7.** Is the null space of matrix  $Z$  from Equation (5) non-empty? What is  $\text{rank}(Z)$ ?

**Matrix operations.** We will frequently apply the *complex conjugate*, *transpose* and *adjoint* operations to matrices in this course; they are defined, respectively, as

$$A^*(i, j) = (A(i, j))^* \quad A^T(i, j) = A(j, i) \quad A^\dagger = (A^*)^T. \quad (6)$$

Note that  $(AB)^\dagger = B^\dagger A^\dagger$ , and similarly for the transpose.

The *trace* is a linear map  $\text{Tr} : \mathcal{L}(\mathbb{C}^d) \mapsto \mathbb{C}$  summing the entries on the diagonal of  $A$ , i.e.  $\text{Tr}(A) = \sum_{i=1}^d A(i, i)$ . A wonderful property of the trace is that it is *cyclic*, i.e.  $\text{Tr}(ABC) = \text{Tr}(CAB)$ .

**Exercise 8.** In a previous exercise, you showed that  $X$  and  $Z$  do not commute. What is nevertheless true about  $\text{Tr}(XZ)$  versus  $\text{Tr}(ZX)$ ?

**Outer products.** Whereas the inner product mapped a pair of vectors  $|\psi\rangle, |\phi\rangle \in \mathbb{C}^d$  to a scalar, the *outer product* produces a  $d \times d$  matrix  $|\psi\rangle\langle\phi| \in \mathcal{L}(\mathbb{C}^d)$ . For example,

$$|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad |1\rangle\langle 0| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}. \quad (7)$$

More generally, the matrix  $|i\rangle\langle j| \in \mathcal{L}(\mathbb{C}^d)$  has a 1 at position  $(i, j)$  and zeroes elsewhere. Thus, any matrix  $A \in \mathcal{L}(\mathbb{C}^d)$  written in the computational basis can be written  $\sum_{ij} A(i, j)|i\rangle\langle j|$ . We hence see that

$$\langle i|A|j\rangle = \langle i| \left( \sum_{i'j'} A(i', j')|i'\rangle\langle j'| \right) |j\rangle = \sum_{i'j'} A(i', j')\langle i|i'\rangle\langle j|j'\rangle = \sum_{i'j'} A(i', j')\delta_{ii'}\delta_{jj'} = A(i, j), \quad (8)$$

where the third equality follows since  $\{|i\rangle\}$  forms an orthonormal basis for  $\mathbb{C}^d$ . In other words,  $\langle i|A|j\rangle$  simply rips out entry  $A(i, j)$ .

**Exercise 9.** Observe that  $X$  from Equation 5 can be written  $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ . What is  $\langle 0|X|0\rangle$ ? How about  $\langle 0|X|1\rangle$ ? How can you rewrite  $\text{Tr}(X)$  in terms of expressions of the form  $\langle i|X|j\rangle$ ?

**Eigenvalues and eigenvectors.** Given any matrix  $A \in \mathcal{L}(\mathbb{C}^d)$ , an *eigenvector* is any non-zero vector  $|\psi\rangle \in \mathbb{C}^d$  satisfying the equation

$$A|\psi\rangle = \lambda|\psi\rangle, \quad (9)$$

for some  $\lambda \in \mathbb{C}$  which is the corresponding *eigenvalue*.

**Exercise 10.** Show that  $|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  and  $|-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$  are eigenvectors of  $X$  from Equation (5). What are their respective eigenvalues?

A matrix  $A \in \{\mathcal{L}(\mathbb{C}^d)\}$  is *normal* (i.e. satisfies  $AA^\dagger = A^\dagger A$ ) if and only if it is unitarily diagonalizable, meaning it has *spectral decomposition*

$$A = \sum_{i=1}^d \lambda_i |\lambda_i\rangle \langle \lambda_i|, \quad (10)$$

where  $\lambda_i$  and  $|\lambda_i\rangle$  are the eigenvalues and corresponding eigenvectors of  $A$ , respectively. Equivalently, there exists a unitary matrix (defined shortly)  $U$  such that  $UAU^\dagger$  is diagonal. Note that if the eigenvalues  $\lambda_i$  are all distinct, then the eigenvectors  $|\lambda_i\rangle$  are uniquely determined (and hence the spectral decomposition is unique). For normal operators, the eigenvectors form an orthonormal set. (Aside: It is worth noting that some non-normal matrices  $A$  may also be diagonalized, albeit with a similarity transformation more general than a unitary, i.e. by some invertible  $S$  such that  $SAS^{-1}$  is diagonal. In this case, the eigenvectors of  $A$  are no longer guaranteed to be orthonormal, but they are linearly independent. In this course, we will typically take “diagonalizable” to mean “unitarily diagonalizable”.)

**Exercise 11.** Suppose  $A$  is unitarily diagonalizable and has two matching eigenvalues, e.g.  $\lambda_1 = \lambda_2$ . (We then say  $A$  is *degenerate*.) Prove that there are infinitely many eigenvectors  $|\psi\rangle$  such that  $A|\psi\rangle = \lambda_1|\psi\rangle$ .

Using the spectral decomposition, we see that  $\text{Tr}(A)$  has a simple expression in terms of  $A$ 's eigenvalues for diagonalizable  $A$ , namely  $\text{Tr}(A) = \sum_i \lambda_i$ . Let us quickly prove this claim:

$$\text{Tr}(A) = \text{Tr} \left( \sum_i \lambda_i |\lambda_i\rangle \langle \lambda_i| \right) = \sum_i \lambda_i \text{Tr}(|\lambda_i\rangle \langle \lambda_i|) = \sum_i \lambda_i \text{Tr}(\langle \lambda_i | \lambda_i \rangle) = \sum_i \lambda_i. \quad (11)$$

Here, the second equality follows since the trace is linear, the third by the cyclic property of the trace, and the last since the eigenvectors  $|\lambda_i\rangle$  are unit vectors.

**Exercise 12.** Prove that for diagonalizable  $A$ ,  $\text{rank}(A)$  equals the number of non-zero eigenvalues of  $A$ .

**Important classes of matrices.** The following classes of matrices are ubiquitous in quantum information.

1. *Unitary matrices:* A matrix  $U \in \mathcal{L}(\mathbb{C}^d)$  is *unitary* if  $UU^\dagger = I$  (equivalently,  $U^\dagger U = I$ ). Thus, all unitary matrices are invertible. The set of unitary matrices acting on space  $\mathcal{X}$  is denoted  $\mathcal{U}(\mathcal{X})$ .

**Exercise 13.** Prove that any eigenvalue of a unitary matrix  $U$  is of form  $e^{i\theta}$  for some  $\theta \in \mathbb{R}$ . Thus, unitaries are high-dimensional generalizations of unit complex numbers.

2. *Hermitian matrices:* A matrix  $M \in \mathcal{L}(\mathbb{C}^d)$  is *Hermitian* if  $M = M^\dagger$ . The set of Hermitian matrices acting on space  $\mathcal{X}$  is denoted  $\text{Herm}(\mathcal{X})$ .

**Exercise 14.** Prove that any eigenvalue of a Hermitian matrix  $M$  is in  $\mathbb{R}$ . Thus, Hermitian matrices are high-dimensional generalizations of real numbers.

3. *Positive (semi-)definite matrices:* A Hermitian matrix with only positive (resp., non-negative) eigenvalues is called *positive definite* (resp., positive semidefinite). Thus, positive matrices generalize the positive (resp., non-negative) real numbers. We use  $M \succ 0$  (resp.,  $M \succeq 0$ ) to specify that  $M$  is positive definite (resp. positive semidefinite). The set of positive semi-definite matrices acting on space  $\mathcal{X}$  is denoted  $\text{Pos}(\mathcal{X})$ .

**Exercise 15.** Prove that the  $X$  and  $Z$  matrices are not positive semi-definite.

4. *Orthogonal projections:* A Hermitian matrix  $\Pi \in \mathcal{L}(\mathbb{C}^d)$  is an *orthogonal projection* (or projector for short) if  $\Pi^2 = \Pi$ .

**Exercise 16.** Prove a Hermitian matrix  $\Pi \in \mathcal{L}(\mathbb{C}^d)$  is a projector if and only if all its eigenvalues are from set  $\{0, 1\}$ . Thus, projectors are high-dimensional generalizations of bits.

Since a projector  $\Pi$ 's eigenvalues are 0's and 1's, its spectral decomposition must take the form  $\Pi = \sum_i |\psi_i\rangle\langle\psi_i|$ , where  $\{|\psi_i\rangle\}$  are an orthonormal set. Conversely, summing any set of orthonormal  $\{|\psi_i\rangle\}$  in this fashion yields a projector. A projector  $\Pi$  has rank 1 if and only if  $\Pi = |\psi\rangle\langle\psi|$  for some  $|\psi\rangle \in \mathbb{C}^d$ .

**Exercise 17.** Let  $\{|\psi_i\rangle\} \subseteq \mathbb{C}^d$  be an orthonormal set. Prove that  $\Pi = \sum_i |\psi_i\rangle\langle\psi_i|$  is a projector.

As for what a projector intuitively *does* — for any projector  $\Pi = \sum_i |\psi_i\rangle\langle\psi_i|$  and vector  $|\phi\rangle$ ,

$$\Pi|\phi\rangle = \left( \sum_i |\psi_i\rangle\langle\psi_i| \right) |\phi\rangle = \sum_i |\psi_i\rangle(\langle\psi_i|\phi\rangle) = \sum_i (\langle\psi_i|\phi\rangle)|\psi_i\rangle \in \text{Span}(\{|\psi_i\rangle\}),$$

where note  $\langle\psi_i|\phi\rangle \in \mathbb{C}$ . Thus,  $\Pi$  projects us down onto the span of the vectors  $\{|\psi_i\rangle\}$ .

**Exercise 18.** Consider three-dimensional vector  $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \in \mathbb{C}^3$  and  $\Pi = |0\rangle\langle 0| + |1\rangle\langle 1|$ . Compute  $\Pi|\phi\rangle$ , and observe that the latter indeed lies in the two-dimensional space  $\text{Span}(\{|0\rangle, |1\rangle\})$ .

**Operator functions.** A key idea used repeatedly in quantum information is that of an *operator function*, or in English, “how to apply real-valued functions to matrices”. To apply function  $f : \mathbb{R} \mapsto \mathbb{R}$  to a Hermitian matrix  $H \in \text{Herm}(\mathbb{C}^d)$ , we take the spectral decomposition  $H = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|$ , and define  $f(H)$  as

$$H = \sum_i f(\lambda_i) |\lambda_i\rangle\langle\lambda_i|,$$

i.e. we apply  $f$  to the eigenvalues of  $H$ . Why does this “work”? Let us look at the Taylor series expansion of  $f$ , which for e.g.  $f = e^x$  is (the series converges for all  $x$ )

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \quad (12)$$

The naive idea for defining  $e^H$  would be to substitute  $H$  in the right hand side of the Taylor series expansion of  $e^x$ :

$$e^H := I + H + \frac{H^2}{2!} + \frac{H^3}{3!} + \dots \quad (13)$$

Indeed, this leads to our desired definition; that to generalize the function  $f(x) = e^x$  to Hermitian matrices, we apply  $f$  to the eigenvalues of  $H$ , as you will now show.

**Exercise 19.** Let  $H$  have spectral decomposition  $H = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|$ . Show that in Equation (13),

$$e^H = \sum_i e^{\lambda_i} |\lambda_i\rangle\langle\lambda_i|.$$

**Exercise 20.** Let  $f(x) = x^2$ . What is  $f(X)$ , for  $X$  the Pauli  $X$  operator? Why does this yield the same results as multiplying  $X$  by itself via matrix multiplication?

**Exercise 21.** Let  $f(x) = \sqrt{x}$ . For any pure state  $|\psi\rangle \in \mathbb{C}^d$ , define rank one density operator  $\rho = |\psi\rangle\langle\psi|$ . What is  $\sqrt{\rho}$ ?

**Exercise 22.** What is  $\sqrt{Z}$  for  $Z$  the Pauli  $Z$  operator? Is it uniquely defined?

## 2 Basic quantum computation

We now review the basics of quantum computation. Recall here there are two successively more general notions of quantum states we utilize. The first, *pure* states, are the quantum analogue of “perfect knowledge” about our state; in the classical world, a “pure state” means your computer’s state is described by a fixed string  $x \in \{0, 1\}^n$ . The second, and more general notion, is that of *mixed* states, which model the notion of “uncertainty” about our state. The classical analogue here would be a computer whose state is described by some *distribution* over  $n$ -bit strings  $x$ .

### 2.1 Pure state quantum computation

We begin by discussing pure state quantum computation.

#### 2.1.1 Individual systems

Recall that an arbitrary  $d$ -dimensional pure quantum state is represented by a unit vector

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle \in \mathbb{C}^d.$$

If we interpret quantum mechanics *literally* (i.e. adopt the “Copenhagen interpretation” of quantum mechanics), we take  $|\psi\rangle$  to mean that our quantum system is in all  $d$  basis states  $|i\rangle$  *simultaneously*, with some appropriate *amplitudes*  $\alpha_i \in \mathbb{C}$ . Typically, in this course we will work with  $d = 2$ , i.e. qubit systems.

#### 2.1.2 Quantum gates

In the pure state setting, the set of allowable operations or *gates* on  $|\psi\rangle \in \mathbb{C}^d$  is the set of  $d \times d$  unitary matrices  $U \in \mathcal{L}(\mathbb{C}^d)$  (i.e.  $UU^\dagger = U^\dagger U = I$ ). In particular, this means pure-state quantum computation is fully reversible, since all gates have inverses.

You have already seen two of the three single-qubit Pauli matrices below, which are unitary. The fourth gate,  $H$ , is the Hadamard.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

**Exercise 23.** What classical gate does Pauli  $X$  simulate? (Hint: Look at the action of  $X$  on  $|0\rangle$  and  $|1\rangle$ .)

**Exercise 24.** What is the action of Pauli  $Z$  on the standard basis? Give the spectral decomposition of  $Z$ .

Recall the  $Z$  gate allows us to inject a *relative phase* into a quantum state. For example,

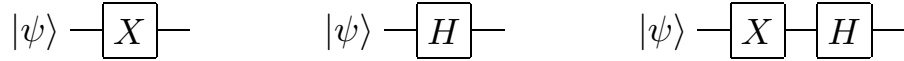
$$Z|+\rangle = Z \left( \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right) = \frac{1}{\sqrt{2}}Z|0\rangle + \frac{1}{\sqrt{2}}Z|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle.$$

By relative phase, we mean that only the amplitude on  $|1\rangle$  was multiplied by phase  $e^{i\pi} = -1$ . If *all* the amplitudes in the state were instead multiplied by  $e^{i\pi}$ , we could simply factor out the  $e^{i\pi}$  from the entire state — in this case,  $e^{i\pi}$  is a *global* phase, which cannot be detected via experiment, and hence is ignored.

The Hadamard, on the other hand, allows us to create or destroy certain superpositions. Namely,  $H|0\rangle = |+\rangle$  and  $H|1\rangle = |-\rangle$ , and  $H|+\rangle = |0\rangle$  and  $H|-\rangle = |1\rangle$ . In other words,  $H$  is self-inverse.

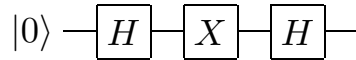
**Exercise 25.** Verify that  $X, Y, Z, H$  are all self-inverse, e.g. the inverse of  $X$  is just  $X$ . What does this mean about the eigenvalues of  $X$ ? (Hint: Use the fact that the eigenvalues of any unitary must lie on the unit circle.)

In this course, we work with the *quantum circuit model*, which allows us to graphically depict gates:



These correspond to evolutions  $X|\psi\rangle$ ,  $H|\psi\rangle$ , and  $HX|\psi\rangle$ , respectively. Each wire in such a diagram denotes a quantum system, and a box labelled by gate  $U$  depicts the action of unitary  $U$ . We think of time going from left to right; for the last circuit above, note that the  $X$  appears on the “left” in the circuit diagram but on the “right” in the expression  $HX|\psi\rangle$ ; this is because  $X$  should be applied first to  $|\psi\rangle$ , then  $H$ .

**Exercise 26.** Which Pauli matrix does the following circuit simulate? (Hint: Use the spectral decomposition of  $X$ .)



### 2.1.3 Composite quantum systems

Thus far we have described single qudit systems. The mathematical formalism for describing the joint state for *multiple* qudits is the *tensor product*,  $\otimes : \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \mapsto \mathbb{C}^{d_1 \times d_2}$ . For input vectors  $|\psi\rangle \in \mathbb{C}^{d_1}$ ,  $|\phi\rangle \in \mathbb{C}^{d_2}$ , the  $(i, j)$ -th entry of their tensor product is  $(|\psi\rangle \otimes |\phi\rangle)(i, j) := \psi_i \phi_j$ , where recall  $\psi_i$  and  $\phi_j$  are the  $i$ th and  $j$ th entries of  $|\psi\rangle$  and  $|\phi\rangle$ , respectively. For example,

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

It is crucial to note that the tensor product *multiplies* the dimensions of its input spaces. This is why classical simulations of quantum mechanics appear to require an exponential overhead.

**Exercise 27.** What is  $|+\rangle \otimes |0\rangle$  (expressed in the standard basis)?

**Exercise 28.** What dimension do  $n$ -qubit states live in, i.e. what is the dimension of space  $(\mathbb{C}^2)^{\otimes n}$ ?

The tensor product has the following properties for any  $|a\rangle, |b\rangle \in \mathbb{C}^{d_1}$  and  $|c\rangle, |d\rangle \in \mathbb{C}^{d_2}$ :

$$(|a\rangle + |b\rangle) \otimes |c\rangle = |a\rangle \otimes |c\rangle + |b\rangle \otimes |c\rangle \tag{14}$$

$$|a\rangle \otimes (|c\rangle + |d\rangle) = |a\rangle \otimes |c\rangle + |a\rangle \otimes |d\rangle \tag{15}$$

$$c(|a\rangle \otimes |c\rangle) = (c|a\rangle) \otimes |c\rangle = |a\rangle \otimes (c|c\rangle) \tag{16}$$

$$(|a\rangle \otimes |c\rangle)^\dagger = |a\rangle^\dagger \otimes |c\rangle^\dagger = \langle a| \otimes \langle c| \tag{17}$$

$$(\langle a| \otimes \langle c|)(|b\rangle \otimes |d\rangle) = \langle a|b\rangle \langle c|d\rangle. \tag{18}$$

For brevity, we shall often drop the notation  $\otimes$  and simply write  $|\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle$ .

**Exercise 29.** Using the properties above, prove that for orthonormal bases  $B_1 = \{|\psi_0\rangle, |\psi_1\rangle\}$  and  $B_2 = \{|\phi_0\rangle, |\phi_1\rangle\}$  for  $\mathbb{C}^2$ , the set  $\{|\psi_0\rangle \otimes |\phi_0\rangle, |\psi_0\rangle \otimes |\phi_1\rangle, |\psi_1\rangle \otimes |\phi_0\rangle, |\psi_1\rangle \otimes |\phi_1\rangle\}$  is an orthonormal basis for  $\mathbb{C}^4$ .

**Quantum entanglement.** Recall that while any pair of states  $|\psi\rangle, |\phi\rangle \in \mathbb{C}^d$  can be stitched together via the tensor product to obtain a  $d^2$ -dimensional state  $|\psi\rangle \otimes |\phi\rangle \in \mathbb{C}^{d^2}$ , the converse is not always true: Given any  $d^2$ -dimensional state  $|\eta\rangle \in \mathbb{C}^{d^2}$ , it is not always true that there exist  $|\psi\rangle, |\phi\rangle \in \mathbb{C}^d$  satisfying  $|\eta\rangle = |\psi\rangle \otimes |\phi\rangle$ . Such  $|\eta\rangle$  are called *entangled*.

For pure bipartite (i.e. two-party) states, entanglement is easy to characterize fully via the *Schmidt decomposition*, which says that any bipartite state  $|\eta\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$  can be written

$$|\eta\rangle = \sum_{i=0}^{\min(d_1, d_2)-1} s_i |a_i\rangle |b_i\rangle,$$

for non-negative *Schmidt coefficients*  $s_i$  and orthonormal bases  $\{|a_i\rangle\}_{i=0}^{d_1}$  and  $\{|b_i\rangle\}_{i=0}^{d_2}$  for  $\mathbb{C}^{d_1}$  and  $\mathbb{C}^{d_2}$ , respectively. The *Schmidt rank* of  $|\eta\rangle$  is its number of non-zero Schmidt coefficients. The canonical entangled two-qubit states are the Bell states

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle, \end{aligned}$$

where we simplified notation by letting (e.g.)  $|0\rangle|0\rangle = |00\rangle$ .

**Exercise 30.** Prove the Bell states are an orthonormal basis for  $\mathbb{C}^4$ .

It is worth mentioning that while the Schmidt rank of a bipartite pure state  $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$  yields an efficient<sup>1</sup> test for entanglement in pure states, it is highly unlikely for there to be an efficient test for entanglement in mixed states. This is because determining whether a *mixed* state  $\rho \in \mathcal{L}(\mathbb{C}^d \otimes \mathbb{C}^d)$  is separable is (strongly) NP-hard. (Mixed states are reviewed in Section 2.2.)

**Two-qubit quantum gates.** Two qubit gates are either a tensor product of one-qubit gates, such as  $X \otimes Z$  or  $H \otimes I$ , or a genuinely two-qubit gate. For the former, recall the tensor product acts on matrices as

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \quad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}, \quad A \otimes B = \begin{pmatrix} a_1 \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} & a_2 \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \\ a_3 \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} & a_4 \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \end{pmatrix}.$$

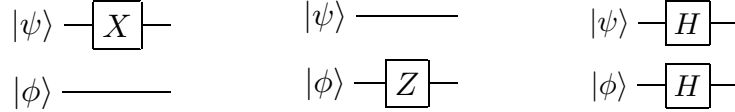
The tensor product for matrices shares the properties of the tensor product for vectors, with the addition of two rules:  $(A \otimes B)(C \otimes D) = AC \otimes BD$  and  $\text{Tr}(A \otimes B) = \text{Tr}(A)\text{Tr}(B)$ .

**Exercise 31.** What is  $\text{Tr}((X \otimes X)(X \otimes X))$ ?

Circuit diagrams for tensor products of unitaries are depicted below: We consider the cases of  $X \otimes I$ ,  $I \otimes Z$ , and  $H \otimes H$ , respectively.

<sup>1</sup>“Efficient” here means the test can be computed in time polynomial in the *dimension*,  $d$ , of the system.





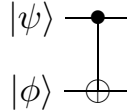
**Exercise 32.** What is the circuit diagram for  $Z \otimes Z$ ? What is  $(X \otimes X)|0\rangle \otimes |1\rangle$ ? How about  $(Z \otimes Z)|1\rangle \otimes |1\rangle$ ?

An important genuinely two-qubit gate is the *controlled-NOT* gate, denoted CNOT. The CNOT treats one qubit as the *control* qubit, and the other as the target *qubit*. It then applies the Pauli  $X$  gate to the target qubit only if the control qubit is set to  $|1\rangle$ . More precisely, the action of the CNOT on a two-qubit basis is given as follows, where qubit 1 is the control and qubit 2 is the target:

$$\text{CNOT } |00\rangle = |00\rangle \quad \text{CNOT } |01\rangle = |01\rangle \quad \text{CNOT } |10\rangle = |11\rangle \quad \text{CNOT } |11\rangle = |10\rangle.$$

**Exercise 33.** What is the matrix representation for CNOT?

The circuit diagram for the CNOT is given by



**Exercise 34.** What is  $\text{CNOT } |\Phi^+\rangle$  for  $|\Phi^+\rangle$  the Bell state? Based on this, give a circuit diagram mapping  $|00\rangle$  to the Bell state  $|\Phi^+\rangle$ .

### 2.1.4 Measurement

Recall that measuring or *observing* a quantum system allows us to extract classical information from the system.

The most basic type of measurement is a *projective measurement*, given by a set of projectors  $B = \{\Pi_i\}_{i=0}^m$  such that  $\sum_{i=0}^m \Pi_i = I$ , where the latter condition is the *completeness* relation. If each  $\Pi_i$  is rank one, i.e.  $\Pi_i = |\psi_i\rangle\langle\psi_i|$ , then we say  $B$  models a *measurement in basis*  $\{|\psi_i\rangle\}$ . Often, we shall measure in the computational basis for  $\mathbb{C}^d$ , which is specified by  $B = \{|i\rangle\langle i|\}_{i=0}^{d-1}$  for standard basis vectors  $|i\rangle \in \mathbb{C}^d$ .

**Exercise 35.** Verify that  $B = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$  is a projective measurement on  $\mathbb{C}^2$ .

Given a projective measurement  $B = \{\Pi_i\}_{i=0}^m \subseteq \mathbb{C}^d$  and quantum state  $|\psi\rangle \in \mathbb{C}^d$ , recall the probability of obtaining outcome  $i \in \{0, \dots, m\}$  when measuring  $|\psi\rangle$  with  $B$  is given by

$$\Pr(\text{outcome } i) = \text{Tr}(\Pi_i |\psi\rangle\langle\psi| \Pi_i) = \text{Tr}(\Pi_i^2 |\psi\rangle\langle\psi|) = \text{Tr}(\Pi_i |\psi\rangle\langle\psi|),$$

where the second equality follows by the cyclic property of the trace and the third since  $\Pi_i$  is a projector. Upon obtaining outcome  $i$ , our state  $|\psi\rangle$  *collapses* to a state  $|\psi'\rangle$  consistent with this outcome, i.e.

$$|\psi'\rangle = \frac{\Pi_i |\psi\rangle}{\|\Pi_i |\psi\rangle\|_2} = \frac{\Pi_i |\psi\rangle}{\sqrt{\langle\psi|\Pi_i|\psi\rangle}} = \frac{\Pi_i |\psi\rangle}{\sqrt{\langle\psi|\Pi_i|\psi\rangle}}.$$

**Exercise 36.** Let  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2$ . Show that if we measure in the computational basis, i.e. using  $B = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ , then the probabilities of obtaining outcomes 0 and 1 are  $|\alpha|^2$  and  $|\beta|^2$ , respectively. What is the postmeasurement state  $|\psi'\rangle$  if outcome 0 is obtained?

The circuit symbol denoting a measurement of state  $|\psi\rangle \in \mathbb{C}^2$  in the *computational* basis is:



## 2.2 Mixed state quantum computation

Thus far, we have discussed pure state computation, where we know precisely the quantum state in which our system is throughout the computation. We now review *mixed state* computation, for which we recall the notion of density operators.

Recall that a *density operator*  $\rho$  acting on  $\mathbb{C}^d$  is a  $d \times d$  Hermitian matrix satisfying two properties:  $\rho \succeq 0$  ( $\rho$  is positive-semidefinite) and  $\text{Tr}(\rho) = 1$ . By the former,  $\rho$  has spectral decomposition

$$\rho = \sum_{i=1}^m p_i |\psi_i\rangle\langle\psi_i|,$$

with eigenvalues  $p_i$  and orthonormal basis  $\{|\psi_i\rangle\}$ . One way to interpret  $\rho$  is via the following experiment: With probability  $p_i$ , we prepare pure state  $|\psi_i\rangle$ . This, in particular, means that any pure state  $|\psi\rangle$  has density matrix  $|\psi\rangle\langle\psi|$ . Conversely, any rank one density operator by definition must be of form  $\rho = |\psi\rangle\langle\psi|$  (why?), and hence represents a pure state  $|\psi\rangle$ . The set of density operators acting on  $\mathbb{C}^d$  is denoted  $\mathcal{D}(\mathbb{C}^d)$ .

**Exercise 37.** Prove that the eigenvalues  $\{p_i\}$  of a density operator form a probability distribution.

**Exercise 38.** Write down the density operator  $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$  and state vector  $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ . How do they differ?

**Exercise 39.** What is the density matrix for pure state  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ?

**The maximally mixed state.** A special density matrix in  $\mathcal{L}(\mathbb{C}^d)$  is the *maximally mixed* state  $\rho = I/d$ , which is the state of “maximum uncertainty”. To see why, use the fact that for any orthonormal basis  $\{|\psi_i\rangle\}_{i=1}^d$  for  $\mathbb{C}^d$ ,  $\sum_{i=1}^d |\psi_i\rangle\langle\psi_i| = I$ . In other words, for *any* orthonormal basis  $\{|\psi_i\rangle\}_{i=1}^d$ ,  $\rho$  represents the following experiment: Pick state  $|\psi_i\rangle$  with probability  $1/d$ , and prepare  $|\psi_i\rangle$ . Since this holds for any basis,  $\rho$  gives us absolutely no information about which state  $|\psi\rangle$  we actually have.

**The partial trace operation.** Density operators arise naturally in answering the question: For any entangled state  $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ , how do we describe the marginal state of  $|\psi\rangle$  on (say) qubit 1? There is no way to answer this via pure states, since  $|\psi\rangle$  is not a product state, and hence does not factorize. Instead, we require a density matrix to describe the state of qubit 1, and the correct procedure for obtaining it is the *partial trace* operation, which we now discuss.

For a bipartite density operator  $\rho$  system on parties  $A$  and  $B$ , the partial trace over  $B$  “discards” system  $B$ , and hence has signature  $\text{Tr}_B : \mathcal{L}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}) \mapsto \mathcal{L}(\mathbb{C}^{d_1})$ . To formally define  $\text{Tr}_B$ , recall that we may write the (usual) trace of  $\rho \in \mathcal{L}(\mathbb{C}^d)$  as  $\text{Tr}(\rho) = \sum_i \rho(i, i) = \sum_{i=1}^d \langle i|\rho|i\rangle$ . The *partial trace* over  $B$  applies this formula only to system  $B$ , i.e. for  $\rho \in \mathcal{L}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$ ,

$$\text{Tr}_B(\rho) = \sum_{i=1}^{d_2} (I_A \otimes \langle i|)\rho(I_A \otimes |i\rangle).$$

**Exercise 40.** What should  $\text{Tr}_B(I/4)$  intuitively be? Compute  $\text{Tr}_B(I/4)$  to check your guess.

**Exercise 41.** More generally, prove that  $\text{Tr}_B(\rho_A \otimes \rho_B) = \rho_A \cdot \text{Tr}(\rho_B) = \rho_A$  for density matrices  $\rho_A, \rho_B$ .

*Example 1: Separable states.* We have said that a pure state  $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$  is not entangled, or *separable*, if and only if  $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$  for some  $|\psi_1\rangle \in \mathbb{C}^{d_1}$  and  $|\psi_2\rangle \in \mathbb{C}^{d_2}$ . This idea extends to the setting of mixed states as follows: A bipartite density matrix  $\rho \in \mathcal{L}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$  is unentangled or *separable* if

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|,$$

for some (possibly non-orthogonal) sets of vectors  $\{|\psi_i\rangle\} \subseteq \mathbb{C}^{d_1}$  and  $\{|\phi_i\rangle\} \subseteq \mathbb{C}^{d_2}$ , and where the  $\{p_i\}$  form a probability distribution. In other words,  $\rho$  is a probabilistic mixture of pure product states. An example of a separable state is

$$\rho = \frac{1}{2}|0\rangle\langle 0| \otimes |0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \otimes |1\rangle\langle 1|. \quad (19)$$

Since the partial trace is a linear map, and since we know that  $\text{Tr}_B(\rho_1 \otimes \rho_2) = \rho_1 \cdot \text{Tr}(\rho_2) = \rho_1$  for density matrices  $\rho_1, \rho_2$ , computing the partial trace of  $\rho$  for separable states is simple:

$$\text{Tr}_B \left( \sum_i p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i| \right) = \sum_i p_i \text{Tr}_B (|\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|) = \sum_i p_i |\psi_i\rangle\langle\psi_i| \cdot \text{Tr}(|\phi_i\rangle\langle\phi_i|) = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

**Exercise 42.** What is  $\text{Tr}_B(\rho)$  for  $\rho$  from Equation (19)?

*Example 2: Pure entangled states.* We compute the single-qubit state of the Bell state  $|\Phi^+\rangle$  on qubit 1:

$$\begin{aligned} \text{Tr}_B(|\Phi^+\rangle\langle\Phi^+|) &= \frac{1}{2} \text{Tr}_B(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) \\ &= \frac{1}{2}|0\rangle\langle 0| \text{Tr}(|0\rangle\langle 0|) + \frac{1}{2}|0\rangle\langle 1| \text{Tr}(|0\rangle\langle 1|) + \frac{1}{2}|1\rangle\langle 0| \text{Tr}(|1\rangle\langle 0|) + \frac{1}{2}|1\rangle\langle 1| \text{Tr}(|1\rangle\langle 1|) \\ &= \frac{1}{2}I, \end{aligned}$$

where we have used the linearity of the partial trace. Thus, the reduced state on qubit 1 for the Bell state is *maximally mixed*, i.e. it is a completely random state about which we have zero information.

**Exercise 43.** Show that  $\text{Tr}_A(|\Phi^+\rangle\langle\Phi^+|) = I/2$ .

### 2.2.1 Operations and measurements on mixed states

We close this lecture by generalizing our discussion on gates and measurements from the pure state setting to mixed states.

**Composite systems.** If  $\rho_A$  and  $\rho_B$  are density operators, then  $\rho_A \otimes \rho_B$  is a density operator.

**Exercise 44.** Prove the claim above. (Hint: The slightly trickier part is to show that the tensor product preserves positivity — use the spectral decomposition for this.)

**Unitary operations.** For density operator  $\rho \in \mathcal{D}(\mathbb{C}^d)$  and unitary  $U \in \mathcal{U}(\mathbb{C}^d)$ , the action of  $U$  on  $\rho$  is given by  $U\rho U^\dagger$ .

**Exercise 45.** What is the action of any unitary  $U \in \mathcal{U}(\mathbb{C}^d)$  on the maximally mixed state,  $\rho = I/d$ ?

**Measurements.** For projective measurement  $B = \{\Pi_i\}_{i=0}^m \subseteq \mathcal{L}(\mathbb{C}^d)$  applied to density operator  $\rho \in \mathcal{D}(\mathbb{C}^d)$ , the probability of outcome  $i$  and postmeasurement state  $\rho' \in \mathcal{D}(\mathbb{C}^d)$  upon obtaining outcome  $i$  are

$$\Pr(\text{outcome } i) = \text{Tr}(\Pi_i \rho) \quad \text{and} \quad \rho' = \frac{\Pi_i \rho \Pi_i}{\text{Tr}(\Pi_i \rho)}.$$

**Exercise 46.** Show that the following important identity holds: For any bipartite state  $\rho_{AB}$  and matrix  $M_B$  acting on  $B$ , it holds that

$$\text{Tr}(\rho_{AB} I_A \otimes M_B) = \text{Tr}(\text{Tr}_A(\rho_{AB}) M_B).$$

In other words, measuring just system  $B$  of a joint state  $\rho_{AB}$  is equivalent to first discarding system  $A$  of  $\rho_{AB}$ , followed a measurement on the reduced state on system  $B$ . Does this agree with your intuition of how a local measurement should behave?