Chapter III

Quantum Computation

A Mathematical preliminaries

"[I]nformation is physical, and surprising physical theories such as quantum mechanics may predict surprising information processing abilities." (Nielsen & Chuang, 2010, p. 98)

A.1 Complex numbers

If you go to the course webpage, and look under Quantum Computation in the Topics section, you will see a link to "complex number review [FFC-ch4]." Depending on how familiar you are with complex numbers, read or skim it through section 4.4.2.1 (pp. 41–53). This should tell you all you need to know (and a little more).

A.2 Linear algebra review

A.2.a Dirac bracket notation

¶1. Much of the math of quantum computation is just elementary linear algebra, but the notation is different (and of course there is a physical interpretation). The Dirac notation will seem peculiar if you are not used to it, but it is elegant and powerful, as are all good notations. Think of it like a new programming language.

¶2. Vectors are written using *Dirac's bracket notation*. $|\psi\rangle$ represents an $n \times 1$ complex column vector, $|\psi\rangle = (v_1, \ldots, v_n)^{\mathrm{T}}$.
We pronounce $|\psi\rangle$ "ket psi" or "psi ket."

¶3. Normally the vectors are finite-dimensional, but they can be infinite-dimensional if the vectors have a finite magnitude (their components are square-summable): $\sum_k |v_k|^2 < \infty$.

¶4. The Dirac notation has the advantage that we can use arbitrary names for vectors, for example, $|\text{excited}\rangle$, $|\text{zero}\rangle$, $|\text{one}\rangle$, $|\uparrow\rangle$, $|\nearrow\rangle$, $|1\rangle$, $|101\rangle$, $|5\rangle$, $|f(\mathbf{x})\rangle$, $|1 \otimes g(1)\rangle$.

It looks kind of like an arrow. Cf. $|v\rangle$ and $\vec{v}$.

A.2.b Dual vector

¶1. $\langle\phi|$ represents a $1 \times n$ complex row vector, $\langle\phi| = (u_1, \ldots, u_n)$.
We pronounce $\langle\psi|$ "bra psi" or "psi bra."

¶2. If $|\psi\rangle = (v_1, \ldots, v_n)^{\mathrm{T}}$, then $\langle\psi| = (\overline{v_1}, \ldots, \overline{v_n})$, where $\overline{v_k}$ is the complex conjugate of v_k.

A.2.c Adjoint

¶1. The *adjoint* (*conjugate transpose, Hermitian transpose*) $M^\dagger$ of a matrix M is defined

$$(M^\dagger)_{jk} = \overline{M_{kj}}.$$

We pronounce it "M dagger."

¶2. Note $\langle\psi| = |\psi\rangle^\dagger$.

A.2.d Inner product

¶1. Suppose $|\phi\rangle = (u_1, \ldots, u_n)^{\mathrm{T}}$ and $|\psi\rangle = (v_1, \ldots, v_n)^{\mathrm{T}}$. Then the *complex inner product* is defined $\sum_k \overline{u_k} v_k$.
Thus the inner product of two vectors is the conjugate transpose of the first times the second.

¶2. This is the convention in physics, which we will follow; mathematicians usually put the complex conjugate on the second argument.

¶3. The inner product can be written as a matrix product: $\langle\phi|\ |\psi\rangle = (\overline{u_1}, \ldots, \overline{u_n})\ (v_1, \ldots, v_n)^{\mathrm{T}}$.

¶4. Since this is multiplying a $1 \times n$ matrix by an $n \times 1$ matrix, the result is a 1×1 matrix, or scalar.

¶5. This product is abbreviated $\langle\phi \mid \psi\rangle = \langle\phi|\ |\psi\rangle$.

¶6. **Bra-ket:** $\langle\phi \mid \psi\rangle$ can be pronounced "ϕ-bra ket-ψ" or "ϕ bra-ket ψ." It's the product of a bra and a ket.

¶7. **Sesquilinearity:** The complex inner product satisfies:

positive definite:

$$\begin{aligned} \langle\psi \mid \psi\rangle &> 0, \quad \text{if } |\psi\rangle \neq \mathbf{0}, \\ \langle\psi \mid \psi\rangle &= 0, \quad \text{if } |\psi\rangle = \mathbf{0}. \end{aligned}$$

conjugate symmetry:

$$\langle\phi \mid \psi\rangle = \overline{\langle\psi \mid \phi\rangle}.$$

linearity in second argument:

$$\begin{aligned} \langle\phi \mid c\psi\rangle &= c\langle\phi \mid \psi\rangle, \quad \text{for } c \in \mathbb{C}, \\ \langle\phi \mid \psi + \chi\rangle &= \langle\phi \mid \psi\rangle + \langle\phi \mid \chi\rangle. \end{aligned}$$

¶8. **Antilinearity in first argument:** Note $\langle c\phi \mid \psi\rangle = \overline{c}\langle\phi \mid \psi\rangle$.

A.2.e Inner product norm

¶1. The *norm* or *magnitude* of a vector is defined $\||\psi\rangle\| = \sqrt{\langle\psi \mid \psi\rangle}$.

¶2. **Normalization:** A vector is normalized if $\||\psi\rangle\| = 1$.

¶3. Note that normalized vectors fall on the surface of an n-dimensional hypersphere.

A.2.f Bases

¶1. **Orthogonality:** Vectors $|\phi\rangle$ and $|\psi\rangle$ are *orthogonal* if $\langle \phi \mid \psi \rangle = 0$.

¶2. **Orthogonal set:** A set of vectors is *orthogonal* if each vector is orthogonal to all the others.

¶3. **Orthonormality:** An *orthonormal* set of vectors is an orthogonal set of normalized vectors.

¶4. **Spanning:** A set of vectors $|\phi_1\rangle, |\phi_2\rangle, \ldots$ *spans* a vector space if for every vector $|\psi\rangle$ in the space there are complex coefficients $c_1, c_2, \ldots$ such that $|\psi\rangle = \sum_k c_k |\phi_k\rangle$.

¶5. **Basis:** A *basis* for a vector space is a linearly independent set of vectors that spans the space.

¶6. Equivalently, a basis is a minimal generating set for the space; that is all of the vectors in the space can be generated by linear combinations of the basis vectors.

¶7. **Orthonormal basis:** An *(orthonormal) basis* for a vector space is an (orthonormal) set of vectors that spans the space.
In general, when I say "basis" I mean "ON basis."

¶8. **Unique representation:** Any vector in the space has a unique representation as a linear combination of the basis vectors.

¶9. **Hilbert space:** A *Hilbert space* is a complete inner-product space.
Complete means that all Cauchy sequences of vectors (or functions) have a limit in the space. (In a Cauchy sequence, $\|x_m - x_n\| \to 0$ as $m, n \to \infty$.)
Hilbert spaces may be finite- or infinite-dimensional.

¶10. **Generalized Fourier series:** If $|1\rangle$, $|2\rangle, \ldots$ is an ON basis for $\mathcal{H}$, then any $|\psi\rangle$ can be expanded in a *generalized Fourier series*:

$$|\psi\rangle = \sum_k c_k |k\rangle.$$

The *generalized Fourier coefficients* c_k can be determined as follows:

$$\langle k \mid \psi \rangle = \langle k| \sum_j c_j |j\rangle = \sum_j c_j \langle k \mid j \rangle = c_k.$$

Therefore, $c_k = \langle k \mid \psi \rangle$. Hence,

$$|\psi\rangle = \sum_k c_k |k\rangle = \sum_k \langle k \mid \psi \rangle \, |k\rangle = \sum_k |k\rangle\langle k \mid \psi \rangle.$$

This is just the vector's representation in a particular basis. (Note that this equation implies $I = \sum_k |k\rangle\langle k|$.)

A.2.g Linear operators

¶1. A *linear operator* $L : \mathcal{H} \to \hat{\mathcal{H}}$ satisfies $L(c|\phi\rangle + d|\psi\rangle) = cL(|\phi\rangle) + dL(|\psi\rangle)$ for all $|\phi\rangle, |\psi\rangle \in \mathcal{H}$ and $c, d \in \mathbb{C}$.

A.2.h Matrix representation

¶1. A linear operator $L : \mathcal{H} \to \hat{\mathcal{H}}$ can be represented by a (possibly infinite-dimensional) matrix relative to bases for $\mathcal{H}$ and $\hat{\mathcal{H}}$.

¶2. Suppose $|1\rangle$, $|2\rangle$, ... is a basis for $\mathcal{H}$ and $|\hat{1}\rangle$, $|\hat{2}\rangle$, ... is a basis for $\hat{\mathcal{H}}$.

¶3. Consider $|\phi\rangle = L|\psi\rangle$ and represent them in these bases by their Fourier coefficients: $b_j = \langle \hat{\jmath} \mid \phi \rangle$ and $c_k = \langle k \mid \psi \rangle$.

¶4. Hence $|\phi\rangle$ is represented by the vector $\mathbf{b} = (b_1, b_2, \ldots)^{\mathrm{T}}$ and $|\psi\rangle$ by the vector $\mathbf{c} = (c_1, c_2, \ldots)^{\mathrm{T}}$.

¶5. Apply the linearity of L:

$$\begin{aligned} b_j &= \langle \hat{\jmath} \mid \phi \rangle \\ &= \langle \hat{\jmath} \mid L \mid \psi \rangle \\ &= \langle \hat{\jmath} | L \left(\sum_k c_k |k\rangle \right) \\ &= \langle \hat{\jmath} | \left(\sum_k c_k L |k\rangle \right) \\ &= \sum_k \langle \hat{\jmath} \mid L \mid k \rangle c_k. \end{aligned}$$

¶6. Define the matrix $M_{jk} \stackrel{\text{def}}{=} \langle \hat{\jmath} \mid L \mid k \rangle$ and we see $\mathbf{b} = \mathbf{Mc}$. For this reason, an expression of the form $\langle \hat{\jmath} \mid L \mid k \rangle$ is sometimes called a *matrix element*.

¶7. Note that the matrix depends on the basis we choose.

A.2.i Outer product or dyad

¶1. We can form the product of a ket and a bra, which is called a *dyad* or *outer product.*

¶2. **Finite dimensional:** If $|\phi\rangle$ is an $m \times 1$ column vector, and $|\psi\rangle$ is an $n \times 1$ column vector (so that $\langle\psi|$ is a $1 \times n$ row vector), then the outer product $|\phi\rangle\langle\psi|$ is an $m \times n$ matrix.
Usually $m = n$.

¶3. **Infinite dimensional:** More generally, if $|\phi\rangle \in \mathcal{H}'$ and $|\psi\rangle \in \mathcal{H}$, then $|\phi\rangle\langle\psi|$ is the linear operator $L : \mathcal{H} \to \mathcal{H}'$ defined, for any $|\chi\rangle \in \mathcal{H}$:

$$L|\chi\rangle = (|\phi\rangle\langle\psi|)|\chi\rangle = |\phi\rangle \ \langle\psi \mid \chi\rangle.$$

¶4. That is, $|\phi\rangle\langle\psi|$ is the operator that returns $|\phi\rangle$ scaled by the inner product of $|\psi\rangle$ and its argument. To the extent that the inner product measures the similarity of $|\psi\rangle$ and $|\chi\rangle$, the result $|\phi\rangle$ is weighted by this similarity.

¶5. **Ket-bra:** The product $|\phi\rangle\langle\psi|$ can be pronounced "ϕ-ket bra-ψ" or "ϕ ket-bra ψ," and abbreviated $|\phi\rangle\!\langle\psi|$.
It's the product of a ket and a bra.

¶6. **Projector:** $|\phi\rangle\langle\phi|$ is a *projector* onto $|\phi\rangle$.

¶7. More generally, if $|\eta_1\rangle, \ldots, |\eta_m\rangle$ are ON, then $\sum_{k=1}^{m} |\eta_k\rangle\langle\eta_k|$ projects into the m-dimensional subspace spanned by these vectors.

A.2.j Outer product representation

¶1. Any linear operator can be represented as a weighted sum of outer products.

¶2. Suppose $L : \mathcal{H} \to \hat{\mathcal{H}}$, $|\hat{\jmath}\rangle$ is a basis for $\hat{\mathcal{H}}$, and $|k\rangle$ is a basis for $\mathcal{H}$.

¶3. Suppose $|\phi\rangle = L|\psi\rangle$.

¶4. We know from Sec. A.2.h that

$$\langle \hat{\jmath} \mid \phi \rangle = \sum_k M_{jk} c_k, \text{ where } M_{jk} = \langle \hat{\jmath} \mid L \mid k \rangle, \text{ and } c_k = \langle k \mid \psi \rangle.$$

¶5. Hence,

$$\begin{aligned} |\phi\rangle &= \sum_j |\hat{\jmath}\rangle \, \langle \hat{\jmath} \mid \phi \rangle \\ &= \sum_j |\hat{\jmath}\rangle \, \left(\sum_k M_{jk} \langle k \mid \psi \rangle \right) \\ &= \left(\sum_j |\hat{\jmath}\rangle \sum_k M_{jk} \langle k| \right) |\psi\rangle \\ &= \left(\sum_{jk} M_{jk} |\hat{\jmath}\rangle \langle k| \right) |\psi\rangle. \end{aligned}$$

¶6. Hence, we have a sum-of-outer-products representation of the operator:

$$L = \sum_{jk} M_{jk} |\hat{\jmath}\rangle\langle k|, \text{ where } M_{jk} = \langle \hat{\jmath} \mid L \mid k \rangle.$$

A.2.k Tensor product

¶1. **Tensor product of vectors:** Suppose that $|\eta_j\rangle$ is an ON basis for $\mathcal{H}$ and $|\eta'_k\rangle$ is an ON basis for $\mathcal{H}'$. For every pair of basis vectors, define the *tensor product* $|\eta_j\rangle \otimes |\eta'_k\rangle$ as a sort of couple or pair of the two basis vectors.

(I.e., there is a one-to-one correspondence between the $|\eta_j\rangle \otimes |\eta'_k\rangle$ and the pairs in $\{|\eta_0\rangle, |\eta_1\rangle, \ldots\} \times \{|\eta'_0\rangle, |\eta'_1\rangle, \ldots\}$.

¶2. **Tensor product space:** Define the *tensor product space* $\mathcal{H} \otimes \mathcal{H}'$ as the space spanned by all linear combinations of the basis vectors $|\eta_j\rangle \otimes |\eta'_k\rangle$.

Therefore each element of $\mathcal{H} \otimes \mathcal{H}'$ is represented by a unique sum $\sum_{jk} c_{jk} |\eta_j\rangle \otimes |\eta'_k\rangle$.

¶3. The tensor product is essential to much of the power of quantum computation.

¶4. **Kronecker product of vectors:** If $|\phi\rangle = (u_1, \ldots, u_m)^{\mathrm{T}}$ and $|\psi\rangle = (v_1, \ldots, v_n)^{\mathrm{T}}$, then their tensor product can be defined by the *Kronecker product*):

$$\begin{aligned} |\phi\rangle \otimes |\psi\rangle &= \begin{pmatrix} u_1|\psi\rangle \\ \vdots \\ u_m|\psi\rangle \end{pmatrix} \\ &= \left(u_1|\psi\rangle^{\mathrm{T}}, \ldots, u_m|\psi\rangle^{\mathrm{T}}\right)^{\mathrm{T}} \\ &= (u_1v_1, \ldots, u_1v_n, \ldots, u_mv_1 \ldots, u_mv_n)^{\mathrm{T}}. \end{aligned}$$

Note that this is an $mn \times 1$ column vector and that

$$(|\phi\rangle \otimes |\psi\rangle)_{(j-1)n+k} = u_j v_k.$$

¶5. The following abbreviations are frequent: $|\phi\psi\rangle = |\phi, \psi\rangle = |\phi\rangle|\psi\rangle = |\phi\rangle \otimes |\psi\rangle$. Note that $|\phi\rangle|\psi\rangle$ can only be a tensor product because it would not be a legal matrix product.

¶6. Some properties of the tensor product:

$$\begin{aligned} (c|\phi\rangle) \otimes |\psi\rangle &= c(|\phi\rangle \otimes |\psi\rangle) = |\phi\rangle \otimes (c|\psi\rangle), \\ (|\phi\rangle + |\psi\rangle) \otimes |\chi\rangle &= (|\phi\rangle|\chi\rangle) + (|\psi\rangle|\chi\rangle), \\ |\phi\rangle \otimes (|\psi\rangle + |\chi\rangle) &= (|\phi\rangle \otimes |\psi\rangle) + (|\phi\rangle \otimes |\chi\rangle). \end{aligned}$$

¶7. **Inner products of tensor products:**

$$\langle \phi_1\phi_2 \mid \psi_1\psi_2\rangle = \langle \phi_1 \otimes \phi_2 \mid \psi_1 \otimes \psi_2\rangle = \langle \phi_1 \mid \psi_1\rangle \, \langle \phi_2 \mid \psi_2\rangle.$$

¶8. **Tensor product of operators:** The tensor product of linear operators is defined

$$(L \otimes M)\,(|\phi\rangle \otimes |\psi\rangle) = L|\phi\rangle \otimes M|\psi\rangle.$$

¶9. Using the fact that $|\psi\rangle = \sum_{jk} c_{jk}|\eta_j\rangle \otimes |\eta'_k\rangle$ you can compute $(L \otimes M)|\psi\rangle$ for an arbitrary $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}'$ (exercise).

¶10. **Kronecker product of matrices:** If $\mathbf{M}$ is a $k \times m$ matrix and $\mathbf{N}$ is a $l \times n$ matrix, then their Kronecker product is a $kl \times mn$ matrix:

$$\mathbf{M} \otimes \mathbf{N} = \begin{pmatrix} M_{11}\mathbf{N} & M_{12}\mathbf{N} & \cdots & M_{1m}\mathbf{N} \\ M_{21}\mathbf{N} & M_{22}\mathbf{N} & \cdots & M_{2m}\mathbf{N} \\ \vdots & \vdots & \ddots & \vdots \\ M_{k1}\mathbf{N} & M_{k2}\mathbf{N} & \cdots & M_{km}\mathbf{N} \end{pmatrix}.$$

¶11. For vectors, operators, and spaces, we pronounce $M \otimes N$ as "M tensor N."

¶12. For a vector, operator, or space M, we define the *tensor power* $M^{\otimes n}$ to be M tensored with itself n times:

$$M^{\otimes n} = \overbrace{M \otimes M \otimes \cdots \otimes M}^{n}.$$

A.2.l Properies of operators and matrices

¶1. **Normal:** An operator $L : \mathcal{H} \to \mathcal{H}$ is *normal* if $L^\dagger L = LL^\dagger$. The same applies to square matrices. That is, normal operators commute with their adjoints.

¶2. **Spectral decomposition:** For any normal operator on a finite-dimensional Hilbert space, there is an ON basis that diagonalizes the operator, and conversely, any diagonalizable operator is normal.

The ON basis is the eigenvectors $|0\rangle$, $|1\rangle$, ..., and the corresponding eigenvalues λ_k are the diagonal elements (cf. Sec. A.2.j, ¶6, p. 83): $L = \sum_k \lambda_k |k\rangle\langle k|$.

¶3. Therefore, a matrix is normal iff it can be diagonalized by a unitary transform (see ¶8, below).
That is, there is a unitary U such that $L = U \Lambda U^\dagger$, where $\Lambda = \text{diag}(\lambda_1, \ldots \lambda_n)$.
If $|0\rangle, |1\rangle, \ldots$ is the basis, then $U = (|0\rangle, |1\rangle, \ldots)$ and $U^\dagger = \begin{pmatrix} \langle 0| \\ \langle 1| \\ \vdots \end{pmatrix}$.
More generally, this applies to compact normal operators.

¶4. **Hermitian or self-adjoint:** An operator $L : \mathcal{H} \to \mathcal{H}$ is *Hermitian* or *self-adjoint* if $L^\dagger = L$. The same applies to square matrices.
(They are the complex analogues of symmetric matrices.)

¶5. Hermitian operators are normal.

¶6. It is easy to see that L is Hermitian iff $\langle \phi \mid L \mid \psi \rangle = \langle \psi \mid L \mid \phi \rangle$ for all $|\phi\rangle, |\psi\rangle$.
(Since $\langle \psi \mid L \mid \phi \rangle = \langle \phi \mid L^\dagger \mid \psi \rangle = \langle \phi \mid L \mid \psi \rangle$.)

¶7. A normal matrix is Hermitian iff it has real eigenvalues (exercise).
This is important in QM, since measurement results are real.

¶8. **Unitary operators:** An operator U is *unitary* if $U^\dagger U = UU^\dagger = I$. That is, a unitary operator is invertible and its inverse is its adjoint.

¶9. Therefore every unitary operator is normal.

¶10. A normal matrix is unitary iff its spectrum is contained in the unit circle in the complex plane.

¶11. If U is unitary, $U^{-1} = U^\dagger$.

¶12. Unitary operators preserve inner products: $\langle \phi \mid U^\dagger U \mid \psi \rangle = \langle \phi \mid \psi \rangle$. That is, the inner product of $U|\phi\rangle$ and $U|\psi\rangle$ is the same as the inner product of $|\phi\rangle$ and $|\psi\rangle$.
Note $\langle \phi \mid U^\dagger U \mid \psi \rangle = (U|\phi\rangle)^\dagger U|\psi\rangle$, the inner product.

¶13. Unitary operators are *isometric*, i.e., they preserve norms:

$$\|U|\psi\rangle\|^2 = \langle \psi \mid U^\dagger U \mid \psi \rangle = \langle \psi \mid \psi \rangle = \||\psi\rangle\|^2.$$

¶14. Unitary operators are like rotations of a complex vector space (analogous to orthogonal operators, which are rotations of a real vector space).

¶15. Unitary operators are important because the evolution of quantum systems is unitary.

A.2.m Operator functions

¶1. It is often convenient to extend various complex functions (e.g., ln, exp, $\surd$) to normal matrices and operators.

¶2. If $f : \mathbb{C} \to \mathbb{C}$ and $L : \mathcal{H} \to \mathcal{H}$, then we define:

$$f(L) \stackrel{\text{def}}{=} \sum_k f(\lambda_k)|k\rangle\langle k|,$$

where $L = \sum_k \lambda_k |k\rangle\langle k|$ is a spectral decomposition of L (Sec. A.2.l, ¶2).

¶3. Therefore, for a normal linear operator or matrix L we can write $\sqrt{L}$, $\ln L$, e^L, etc.