

Chapter III

Quantum Computation

These lecture notes are exclusively for the use of students in Prof. MacLennan's *Unconventional Computation* course. ©2014, B. J. MacLennan, EECS, University of Tennessee, Knoxville. Version of September 9, 2014.

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

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 bracket 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.

First, the notation $|\psi\rangle$ represents an $n \times 1$ complex column vector, $|\psi\rangle = (v_1, \dots, v_n)^T$. We pronounce $|\psi\rangle$ “ket psi” or “psi ket.” Normally the vectors are finite-dimensional, but they can be infinite-dimensional if the vectors have a finite magnitude (their components are square-summable), $\sum_k |v_k|^2 < \infty$.

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 may be easier to remember if you notice that it looks kind of like an arrow; compare $|v\rangle$ and \vec{v} .

The notation $\langle\phi|$ represents a $1 \times n$ complex row vector, $\langle\phi| = (u_1, \dots, u_n)$. We pronounce $\langle\psi|$ “bra psi” or “psi bra.” If $|\psi\rangle = (v_1, \dots, v_n)^T$, then $\langle\psi| = (\bar{v}_1, \dots, \bar{v}_n)$, where \bar{v}_k is the complex conjugate of v_k .

We define the *adjoint* (*conjugate transpose*, *Hermitian transpose*) M^\dagger of a matrix M by

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

We pronounce it “ M dagger.” Note that corresponding bras and kets are adjoints: $\langle\psi| = |\psi\rangle^\dagger$ and $|\psi\rangle = \langle\psi|^\dagger$.

A.2.b INNER PRODUCT

Suppose $|\phi\rangle = (u_1, \dots, u_n)^T$ and $|\psi\rangle = (v_1, \dots, v_n)^T$. Then the *complex inner product* of the vectors is defined $\sum_k \bar{u}_k v_k = \langle\phi| |\psi\rangle$. Thus, the inner product of two vectors is the conjugate transpose of the first times the second. This is the convention in physics, which we will follow; mathematicians usually put the complex conjugate on the second argument. Since the inner product multiplies a $1 \times n$ matrix by an $n \times 1$ matrix, the result is a 1×1 matrix, or scalar. This product is usually abbreviated $\langle\phi | \psi\rangle = \langle\phi| |\psi\rangle$, which can be pronounced “ ϕ -bra ket- ψ ” or “ ϕ bra-ket ψ .” It’s the product of a bra and a ket.

The complex inner product satisfies several important properties:

1. It is *positive definite*:

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

2. It has *conjugate symmetry*: $\langle \phi | \psi \rangle = \overline{\langle \psi | \phi \rangle}$.
3. It is *linear in its second argument*:

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

Note that conjugate symmetry and linearity in the second argument together imply that $\langle c\phi | \psi \rangle = \bar{c}\langle \phi | \psi \rangle$. The complex inner product is called *sesquilinear*, which means “one-and-a-half linear” (in contrast to the inner product of real vectors, which is linear in both arguments, i.e., *bilinear*).

The *norm* or *magnitude* of a vector is defined $\|\psi\rangle\| = \sqrt{\langle \psi | \psi \rangle}$. A vector is *normalized* if $\|\psi\rangle\| = 1$. Note that normalized vectors fall on the surface of an n -dimensional hypersphere.

A.2.c BASES AND GENERALIZED FOURIER SERIES

Vectors $|\phi\rangle$ and $|\psi\rangle$ are *orthogonal* if $\langle \phi | \psi \rangle = 0$. A set of vectors is *orthogonal* if each vector is orthogonal to all the others. An *orthonormal (ON)* set of vectors is an orthogonal set of normalized vectors. A set of vectors $|\phi_1\rangle, |\phi_2\rangle, \dots$ *spans* a vector space if for every vector $|\psi\rangle$ in the space there are complex coefficients c_1, c_2, \dots such that $|\psi\rangle = \sum_k c_k |\phi_k\rangle$. A *basis* for a vector space is a linearly independent set of vectors that spans the space. 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. An (*orthonormal*) *basis* for a vector space is an (orthonormal) set of vectors that spans the space. In general, when I write “basis” I mean “orthonormal basis.” Any vector in the space has a unique representation as a linear combination of the basis vectors.

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, $\|x_m - x_n\| \rightarrow 0$ as $m, n \rightarrow \infty$.) Hilbert spaces may be finite- or infinite-dimensional. If $|1\rangle, |2\rangle, \dots$ is an ON basis for a Hilbert space \mathcal{H} , then any $|\psi\rangle$ in \mathcal{H} 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:

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

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

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

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

A *linear operator* $L : \mathcal{H} \rightarrow \hat{\mathcal{H}}$ 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 linear operator $L : \mathcal{H} \rightarrow \hat{\mathcal{H}}$ can be represented by a (possibly infinite-dimensional) matrix relative to bases for \mathcal{H} and $\hat{\mathcal{H}}$. To see this, suppose $|1\rangle, |2\rangle, \dots$ is a basis for \mathcal{H} and $|\hat{1}\rangle, |\hat{2}\rangle, \dots$ is a basis for $\hat{\mathcal{H}}$. Consider $|\phi\rangle = L|\psi\rangle$ and represent the vectors in these bases by their Fourier coefficients: $b_j = \langle \hat{j} | \phi \rangle$ and $c_k = \langle k | \psi \rangle$. Hence $|\phi\rangle$ is represented by the vector $\mathbf{b} = (b_1, b_2, \dots)^T$ and $|\psi\rangle$ by the vector $\mathbf{c} = (c_1, c_2, \dots)^T$. Apply the linearity of L :

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

Therefore, define the matrix $M_{jk} \stackrel{\text{def}}{=} \langle \hat{j} | L | k \rangle$ and we see $\mathbf{b} = \mathbf{M}\mathbf{c}$. For this reason, an expression of the form $\langle \hat{j} | L | k \rangle$ is sometimes called a *matrix element*. Note that the matrix depends on the basis we choose.

A.2.d OUTER PRODUCT OR DYAD

We can form the product of a ket and a bra, which is called a *dyad* or *outer product*. Consider first the finite dimensional case. 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. In most cases of interest $m = n$. More generally, we can form outer products of infinite-dimensional vectors in Hilbert spaces. If $|\phi\rangle \in \mathcal{H}'$ and $|\psi\rangle \in \mathcal{H}$, then $|\phi\rangle\langle\psi|$ is the linear operator $L : \mathcal{H} \rightarrow \mathcal{H}'$ defined, for any $|\chi\rangle \in \mathcal{H}$:

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

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. The product $|\phi\rangle\langle\psi|$ can be pronounced “ ϕ -ket bra- ψ ” or “ ϕ ket-bra ψ ,” and abbreviated $|\phi\rangle\langle\psi|$.

The special case $|\phi\rangle\langle\phi|$ is called a *projector* onto $|\phi\rangle$. More generally, if $|\eta_1\rangle, \dots, |\eta_m\rangle$ are orthonormal, then $\sum_{k=1}^m |\eta_k\rangle\langle\eta_k|$ projects into the m -dimensional subspace spanned by these vectors.

Any linear operator can be represented as a weighted sum of outer products. To see this, suppose $L : \mathcal{H} \rightarrow \mathcal{H}'$, $|\hat{j}\rangle$ is a basis for \mathcal{H}' , and $|k\rangle$ is a basis for \mathcal{H} . Suppose $|\phi\rangle = L|\psi\rangle$. We know from Sec. A.2.c that

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

Hence,

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

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

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

A.2.e TENSOR PRODUCTS

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; that is, there is a one-to-one correspondence between the $|\eta_j\rangle \otimes |\eta'_k\rangle$ and the pairs in $\{|\eta_0\rangle, |\eta_1\rangle, \dots\} \times \{|\eta'_0\rangle, |\eta'_1\rangle, \dots\}$. 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 $\sum_{jk} c_{jk} |\eta_j\rangle \otimes |\eta'_k\rangle$. The tensor product is essential to much of the power of quantum computation.

If $|\phi\rangle = (u_1, \dots, u_m)^T$ and $|\psi\rangle = (v_1, \dots, v_n)^T$, then their tensor product can be defined by the *Kronecker product*:

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

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

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

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. These are some useful properties of the tensor product:

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

The inner products of tensor products are given by

$$\langle \phi_1\phi_2 | \psi_1\psi_2 \rangle = \langle \phi_1 \otimes \phi_2 | \psi_1 \otimes \psi_2 \rangle = \langle \phi_1 | \psi_1 \rangle \langle \phi_2 | \psi_2 \rangle.$$

The tensor product of linear operators is defined

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

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). 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:

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

For vectors, operators, and spaces, we pronounce $M \otimes N$ as “ M tensor N .” 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.f PROPERTIES OF OPERATORS AND MATRICES

Several properties of operators and matrices are important in quantum computation. An operator $L : \mathcal{H} \rightarrow \mathcal{H}$ is *normal* if $L^\dagger L = LL^\dagger$. The same applies to square matrices. That is, normal operators commute with their adjoints. 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. This is called a *spectral decomposition* of the operator. The ON basis comprises the eigenvectors $|0\rangle, |1\rangle, \dots$, and the corresponding eigenvalues λ_k are the diagonal elements (cf. Sec. A.2.d, p. 39): $L = \sum_k \lambda_k |k\rangle\langle k|$. Therefore, a matrix is normal if and only if it can be diagonalized by a unitary transform (see A.2.f, below). That is, it is normal if and only if there is a unitary U such that $L = U\Lambda U^\dagger$, where $\Lambda = \text{diag}(\lambda_1, \dots, \lambda_n)$. If $|0\rangle, |1\rangle, \dots$ is the basis, then $U = (|0\rangle, |1\rangle, \dots)$ and

$$U^\dagger = \begin{pmatrix} \langle 0| \\ \langle 1| \\ \vdots \end{pmatrix}.$$

(More generally, this property holds for compact normal operators.)

It is often convenient to extend various complex functions (e.g., \ln , \exp , $\sqrt{}$) to normal matrices and operators. If $f : \mathbb{C} \rightarrow \mathbb{C}$ and $L : \mathcal{H} \rightarrow \mathcal{H}$, 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 . Therefore, for a normal linear operator or matrix L we can write \sqrt{L} , $\ln L$, e^L , etc.

An operator $L : \mathcal{H} \rightarrow \mathcal{H}$ is *Hermitian* or *self-adjoint* if $L^\dagger = L$. The same applies to square matrices. (They are the complex analogues of symmetric matrices.) Hermitian operators are normal. It is easy to see that L is Hermitian if and only if $\langle \phi | L | \psi \rangle = \langle \psi | L | \phi \rangle$ for all $|\phi\rangle, |\psi\rangle$ (since $\langle \psi | L | \phi \rangle = \langle \phi | L^\dagger | \psi \rangle = \langle \phi | L | \psi \rangle$). A normal matrix is Hermitian if and only if it has real eigenvalues (exercise). This is important in quantum mechanics, since measurement results are usually assumed to be real.

An operator U is *unitary* if $U^\dagger U = U U^\dagger = I$. That is, a unitary operator is invertible and its inverse is its adjoint. That is, if U is unitary, then $U^{-1} = U^\dagger$. Obviously every unitary operator is also normal. A normal matrix is unitary if and only if its spectrum is contained in the unit circle in the complex plane. Unitary operators preserve inner products: $\langle \phi | U^\dagger U | \psi \rangle = \langle \phi | \psi \rangle$. 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 that $\langle \phi | U^\dagger U | \psi \rangle = (U|\phi\rangle)^\dagger U|\psi\rangle$, the inner product. Unitary operators are *isometric*, i.e., they preserve norms:

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

Unitary operators are like rotations of a complex vector space (analogous to orthogonal operators, which are rotations of a real vector space). Unitary operators are important in quantum computation because the evolution of quantum systems is unitary.