Notes on Quantum Information Theory

Robert B. Griffiths

Version of 12 Jan. 2004

Sections 1, 2, 3, 4

1 Introduction

★ This is a rough outline to accompany lectures. It is not intended to be self-contained. There is a hierarchy of bullets: ■, ★, •, ○, –. If they don't make sense to you, ignore them.

★ References:
CQT = R. B. Griffiths, *Consistent Quantum Theory* (Cambridge 2002)
QCQI = M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge, 2000)

★ Why the interest in quantum information?

• FACTORING. Peter Shor, 1994.

• CIPHERING. Quantum cryptography: Charles Bennett and others.

• UNDERSTANDING. Founding fathers of quantum mechanics (QM) left a lot of questions unsettled. Will quantum information help solve them?

★ This is a rough outline to accompany lectures. It is not intended to be self-contained. There is a hierarchy of bullets: ■, ★, •, ○, –. If they don't make sense to you, ignore them.

2 Qubits and Hilbert Space

■ *Information* is an abstract concept. But in the real world information requires a *physical representation*:

★ Bit is basic unit of classical information. Quantum counterpart is a *qubit* or 2-dimensional complex Hilbert space.

■ Hilbert space $\mathcal{H}$: Complex vector space with inner product
– See CQT Ch. 3, QCQI Sec. 2.1.

• Vectors: $|\psi\rangle$, $|0\rangle$, $|1\rangle$ are called "kets."

• Scalars: Complex numbers such as $c = 1.2 + 3i$; complex conjugate: $c^* = 1.2 - 3i$

• Addition of kets, multiplication of kets by scalars: e.g., $|\psi\rangle = 2|0\rangle + (1+i)|1\rangle$

• Dual space vector $\langle\psi| = \big(|\psi\rangle\big)^\dagger$ is referred to as a "bra." The dagger † operation is antilinear, e.g. $\big(2|0\rangle + (1+i)|1\rangle\big)^\dagger = 2\langle 0| + (1-i)\langle 1|$, where note that i becomes $-i$. For more on †, see (2.13) and following.

• Inner product of $|\phi\rangle$ with $|\psi\rangle$ is written $\langle\phi|\psi\rangle$, a "*bra* c *ket*"; it is a complex number.

$$\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^* \tag{2.1}$$

where * denotes complex conjugate.

• $|\phi\rangle$ is *orthogonal* to $|\psi\rangle$, and vice versa, if $\langle\phi|\psi\rangle = 0$ (equivalent to$\langle\psi|\phi\rangle = 0$, see (2.1)).

• Norm: $\|\psi\|^2 = \langle\psi|\psi\rangle \geq 0$. Normalized vector: $\|\psi\| = 1$.

• Orthonormal basis $|j\rangle$, $j = 1, 2, \ldots d$ for a d-dimensional Hilbert space:

$$\langle j|k\rangle = \delta_{jk} = \begin{cases} 1 & \text{if } j = k, \\ 0 & \text{if } j \neq k. \end{cases} \tag{2.2}$$

◦ Can expand any ket in such a basis:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle + \cdots; \quad c_j = \langle j|\psi\rangle. \tag{2.3}$$

★ Bloch sphere or spin-1/2 representation of qubit

– See CQT, pp. 50,51

• Every

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.4}$$

is associated with a direction in space w and a ket $|w^+\rangle$ determined by β/α. Note: $|w^-\rangle$ corresponds to direction $-w$.

$$|z^+\rangle = |0\rangle, \quad |z^-\rangle = |1\rangle, \tag{2.5}$$

★ Physical interpretation of kets.

• $|\psi\rangle$ and $c|\psi\rangle$ for $c \neq 0$ mean exactly the same thing, the physical state is associated with the *ray* $\{c|\psi\rangle\}$, $|\psi\rangle$ fixed, c any complex number.

• $|\phi\rangle$ and $|\psi\rangle$ refer to *distinct* or *distinguishable* physical states it they are *orthogonal*, $\langle\phi|\psi\rangle = 0$.

• $\langle\psi|\phi\rangle \neq 0$, but $|\psi\rangle$ is not a multiple of $|\phi\rangle$. Two such states are said to be *nonorthogonal*, or *incompatible*, or *noncomparable*.

◦ No measurement can (reliably) distinguish them

◦ One cannot ascribe both properties to the same system at the same time

◦ Main conceptual difficulties of quantum mechanics (and main power of quantum computation, cryptography) are associated with the possibility of incompatible states.

■ Operators

★ Operators are linear maps of $\mathcal{H}$ to itself

$$|\omega\rangle = A\big(b|\psi\rangle + c|\phi\rangle\big) = bA|\psi\rangle + cA|\phi\rangle \tag{2.6}$$

• Product of operators defined by:

$$(AB)|\psi\rangle = A\big(B|\psi\rangle\big) = AB|\psi\rangle. \tag{2.7}$$

• In general $AB \neq BA$. When $AB = BA$ one says that A and B *commute*. Otherwise they do not commute. The *commutator*

$$[A, B] := AB - BA \tag{2.8}$$

of two operators is zero if and only if they commute.

★ Dyad, e.g. $|\chi\rangle\langle\omega|$, defined by:

$$\big(|\chi\rangle\langle\omega|\big)|\psi\rangle = |\chi\rangle\langle\omega|\psi\rangle = \big(\langle\omega|\psi\rangle\big)|\chi\rangle. \tag{2.9}$$

• Completeness relation. If $\{|j\rangle\}$ is an orthonormal basis, then

$$I = \sum_j |j\rangle\langle j|, \tag{2.10}$$

• Expansion of arbitrary operator A in orthonormal basis dyads:

$$A = \sum_j \sum_k \langle j|A|k\rangle \cdot |j\rangle\langle k|. \tag{2.11}$$

◦ The $\langle j|A|k\rangle$ are *matrix elements* in Dirac notation; the usual notation would be A_{jk}.
– For more about column, row vectors and matrices: CQT Sec. 3.6.

• According to (2.11), an operator is uniquely determined by its matrix elements in an orthonormal basis. It is also uniquely determined by its action on every member of an orthonormal basis.

• When the operator A refers to a qubit, the standard way of writing the matrix using the *computational* or *standard* basis is (note the order of the elements):

$$\begin{pmatrix} \langle 0|A|0\rangle & \langle 0|A|1\rangle \\ \langle 1|A|0\rangle & \langle 1|A|1\rangle \end{pmatrix} \tag{2.12}$$

★ Adjoints and dagger (†) operation. Examples:

$$\big(|\psi\rangle\big)^\dagger = \langle\psi|, \quad \big(\langle\psi|\big)^\dagger = |\psi\rangle, \tag{2.13}$$

$$\big(b|\psi\rangle + c|\phi\rangle\big)^\dagger = b^*\langle\psi| + c*\langle\phi|, \tag{2.14}$$

$$\big(|\psi\rangle\langle\omega|\big)^\dagger = |\omega\rangle\langle\psi| \tag{2.15}$$

$$\langle j|A^\dagger|k\rangle = \big(\langle k|A|j\rangle\big)^*, \tag{2.16}$$

$$\big(aA + bB\big)^\dagger = a^*A^\dagger + b^*B^\dagger, \tag{2.17}$$

$$(AB)^\dagger = B^\dagger A^\dagger. \tag{2.18}$$

Operator $A^\dagger$ is the *adjoint* of A

■ Classes of operators: Hermitian, projectors, positive, unitary

★ $A = A^\dagger$ defines a Hermitian operator. In quantum theory physical variables (energy, momentum, angular momentum, etc.) are represented by Hermitian operators.

• Quantum physical variable A has well-defined value in state $|\psi\rangle$ if and only if $|\psi\rangle$ is an *eigenstate* of A:

$$A|\psi\rangle = a|\psi\rangle, \tag{2.19}$$

in which case the value of A in $|\psi\rangle$ is its *eigenvalue* a.

◦ $A = A^\dagger$ implies a is a real number.

◦ If $|\psi\rangle$ is not an eigenstate of A, then the value of A in the state $|\psi\rangle$ is *undefined* or *meaningless*: quantum theory does not assign it any meaning.

• Spectral theorem for Hermitian operators: $A = A^\dagger$ implies there is an orthonormal basis $\{|\nu_j\rangle\}$ (which depends on A) such that

$$A = \sum_j a_j |\nu_j\rangle\langle\nu_j|, \tag{2.20}$$

where the $|\nu_j\rangle$ are eigenvectors of A, and the a_j are the corresponding eigenvalues. Equivalently, the matrix of A in this basis is diagonal:

$$\langle\nu_j|A|\nu_k\rangle = a_j\delta_{jk}. \tag{2.21}$$

• Extended spectral theorem. Let $A, B, C, \ldots$ be a collection of Hermitian operators on the same Hilbert space, and suppose that each operator commutes with every other operator in the collection. Then there is an orthonormal basis $\{|\nu_j\rangle\}$, which depends upon the operators in the collection, such that each operator has a representation in the form (2.20), but with different eigenvalues. E.g.,

$$B = \sum_j b_j |\nu_j\rangle\langle\nu_j|, \tag{2.22}$$

and similarly for C, etc.

◦ In the state $|\nu_j\rangle$ the physical variable A has the value a_j, B has the value b_j, etc.

◦ In classical mechanics *all* physical variables (energy, momentum, etc.) have well-defined values, but in quantum mechanics this is no longer case. There have been various attempts to make quantum theory look more classical by supplementing the quantum Hilbert space with additional "hidden variables." The best known effort in this direction is *Bohmian mechanics*, based upon the ideas of David Bohm. There is no experimental evidence supporting the existence of such variables, and postulating them leads to a more complicated theory with mysterious undetectable nonlocal influences.

★ Projector (orthogonal projection operator) P is Hermitian and idempotent: $P = P^\dagger$ and $P^2 = P$.

• Its eigenvalues are either 0 or 1.

◦ Examples include identity I, zero operator 0: for all $|\psi\rangle$, $I|\psi\rangle = |\psi\rangle$, $0|\psi\rangle = 0$.

◦ More interesting example: For normalized $|\psi\rangle$, the dyad $|\psi\rangle\langle\psi|$ is a projector.

◦ If $|\phi\rangle$ and $|\psi\rangle$ are normalized states which are orthogonal to each other,

$$P = |\phi\rangle\langle\phi| + |\psi\rangle\langle\psi| \tag{2.23}$$

is a projector.

• Geometrical property of projector: it projects a vector in a "perpendicular" manner onto a subspace.

• A projector represents a physical property of a system that can be true or false. E.g., $|\psi\rangle\langle\psi|$ is the property that the system is in the state $|\psi\rangle$.

• The physical properties corresponding to two projectors P and Q are said to be *compatible* if and only if P and Q commute, $PQ = QP$. Otherwise they are *incompatible*.

◦ It does not make sense to ascribe two *incompatible* properties to a single quantum system at the same time. E.g., for a spin-half particle, saying that $S_x = +1/2$ AND $S_z = +1/2$ is meaningless. See the discussion in CQT Sec. 4.6.

★ A *positive* (positive semi-definite) operator R is a Hermitian operator with the property that all of its eigenvalues are positive or 0.

• An alternative (very useful) characterization: R is positive if and only if $\langle\psi|R|\psi\rangle$ is real and nonnegative for every $|\psi\rangle$ in the Hilbert space.

◦ Examples include projectors, density operators (discussed later).

★ A *unitary* operator U is defined by (CQT Sec. 7.2):

$$U^\dagger U = I = UU^\dagger. \tag{2.24}$$

◦ In a finite-dimensional vector space each equality implies the other, so one need only check one of them, say $UU^\dagger = I$, to see if U is unitary.

• Think of U as a matrix. The first equality in (2.24) means that the columns of U, thought of as column vectors, make up an orthonormal basis of $\mathcal{H}$. The second equality is the same statement for the rows.

• A unitary operator preserves inner products: if $|\psi'\rangle = U|\psi\rangle$ and $|\phi'\rangle = U|\phi\rangle$, then $\langle\phi'|\psi'\rangle = \langle\phi|\psi\rangle$. In particular, the norm is preserved, $\|\psi'\| = \|\psi\|$. Thus a unitary operator "preserves lengths," so it is analogous to a rotation.

• A unitary operator maps an orthonormal basis to another orthonormal basis, and in a finite-dimensional space this is a sufficient as well as necessary condition, so it is a convenient way to show that an operator is unitary.

3 Composite systems and tensor products

■ In quantum theory the Hilbert space of a composite system (such as *two* qubits) is the *tensor product* of the Hilbert spaces for the subsystems.

– Composite systems, tensor products are discussed in CQT Ch. 6, QCQI Sec. 2.1.7

★ For two subsystems, $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$ has dimension $d = d_a \cdot d_b$, where d_a, d_b are dimensions of $\mathcal{A}$, $\mathcal{B}$. Let $\{|a_j\rangle\}$ and $\{|b_p\rangle\}$ be orthonormal bases. Any $|\psi\rangle$ in $\mathcal{H}$ can be written in the form

$$|\psi\rangle = \sum_j \sum_p \gamma_{jp} \big(|a_j\rangle \otimes |b_p\rangle \big) \tag{3.1}$$

for a suitable choice of complex coefficients $\{\gamma_{jp}\}$.

• Multiplication using $\otimes$ satisfies the usual distributive laws:

$$\big(|a\rangle + |a'\rangle \big) \otimes \big(|b\rangle + |b'\rangle \big) = |a\rangle \otimes |b\rangle + |a\rangle \otimes |b'\rangle + |a'\rangle \otimes |b\rangle + |a'\rangle \otimes |b'\rangle, \tag{3.2}$$

and scalar constants (complex numbers) can always be placed at the left:

$$\big(c|a\rangle \big) \otimes |b\rangle = |a\rangle \otimes \big(c|b\rangle \big) = c\big(|a\rangle \otimes |b\rangle \big) = c|a\rangle \otimes |b\rangle, \tag{3.3}$$

★ Bra vectors are formed from kets using the dagger operation †:

$$\big(|a\rangle \otimes |b\rangle \big)^\dagger = \langle a| \otimes \langle b|; \quad \big(\langle a| \otimes \langle b| \big)^\dagger = |a\rangle \otimes |b\rangle \tag{3.4}$$

◦ Note that the order a to the left of b is not changed by the dagger operation; this is an exception to the "reverse the order" rule.

• Using (3.4) plus the fact that † is *anti*linear, one sees that if $|\psi\rangle$ is given by (3.1), then

$$\langle \psi| = \sum_j \sum_p \gamma_{jp}^* \big(\langle a_j| \otimes \langle b_p| \big) \tag{3.5}$$

★ States in $\mathcal{H}$ of the form $|a\rangle \otimes |b\rangle$ are *product* states; all others are *entangled* states.

• Notation. $|a\rangle \otimes |b\rangle$ is often abbreviated to $|a\rangle|b\rangle$, or even to $|ab\rangle$ when the context makes plain what the symbols mean. Sometimes inserting an $\otimes$ is useful because it makes things clearer.

★ Schmidt decomposition. Any $|\psi\rangle$ in $\mathcal{A} \otimes \mathcal{B}$ can be written as

$$|\psi\rangle = \sum_j \lambda_j |\hat{a}_j\rangle \otimes |\hat{b}_j\rangle, \tag{3.6}$$

where $\{|\hat{a}_j\rangle\}$ and $\{|\hat{b}_p\rangle\}$ are *special bases* which depend upon the $|\psi\rangle$ that one is considering, and these bases can in addition be chosen so that the $\{\lambda_j\}$ are nonnegative real numbers.

★ Physical interpretation: Product state $|a\rangle \otimes |b\rangle$ has the meaning that $\mathcal{A}$ has the property $|a\rangle$ and $\mathcal{B}$ the property $|b\rangle$. For an entangled state one *cannot* assign definite properties to $\mathcal{A}$ and $\mathcal{B}$; they are in some sense correlated.

• Consider the case of two qubits, and assume that

$$|\psi\rangle = \alpha|00\rangle + \beta|11\rangle, \tag{3.7}$$

with $\alpha \neq 0$, $\beta \neq 0$. One can show that the only projectors on $\mathcal{A}$ that commute with $P = |\psi\rangle\langle\psi|$ are I and 0, so in this case it is not possible to say that the composite system possesses property P and that the subsystem $\mathcal{A}$ possesses *any* nontrivial property.

◦ We shall see later (Sec. 4) that if $|\psi\rangle$ is thought of not as representing an actual physical property, but instead as a *pre-probability*, then it does make sense to talk about properties of the separate subsystems $\mathcal{A}$ and $\mathcal{B}$.

★ Identical particles. In quantum mechanics the tensor product space for identical particles is complicated, because of symmetry requirements. We will ignore these because usually we deal with quantum particles in separate locations. In other situations one can get away with treating the particles as if they were nonidentical by introducing fictitious "exchange interactions."

■ Operators on tensor products

★ Product operators $A \otimes B$ act in the following way:

$$\big(A \otimes B\big)\big(|a\rangle \otimes |b\rangle\big) = \big(A|a\rangle\big) \otimes \big(B|b\rangle\big). \tag{3.8}$$

◦ One can use linearity and (3.1) to extend this to the action of $A \otimes B$ on any $|\psi\rangle$ in $\mathcal{A} \otimes \mathcal{B}$.

• Any operator on $A \otimes B$ can be written as a sum of product operators, so (3.8) suffices to define the action of any operator on any state of $\mathcal{A} \otimes \mathcal{B}$.

• A dyad constructed from two product states is a product operator. Note how one rearranges the terms to make this explicit:

$$\big(|a\rangle \otimes |b\rangle\big)\big(\langle a'| \otimes \langle b'|\big) = \big(|a\rangle\langle a'|\big) \otimes \big(|b\rangle\langle b'|\big) = |a\rangle\langle a'| \otimes |b\rangle\langle b'| \tag{3.9}$$

★ Adjoint: $\big(A \otimes B\big)^\dagger = A^\dagger \otimes B^\dagger$, and extend to other cases using the fact that † is antilinear. Note that the order of A and B does not change.

★ Note that $A \otimes I$ is often written as A if it is obvious that the operator A refers to subsystem $\mathcal{A}$; similarly $I \otimes B$ is often written as B. This sometimes causes confusion.

★ Products of product operators:

$$(A \otimes B)(A' \otimes B') = AA' \otimes BB'. \tag{3.10}$$

■ Example of two qubits.

★ We write product states $|a\rangle \otimes |b\rangle$ in the abbreviated form $|ab\rangle$. The computational (standard) basis of the two qubit system is formed by the four states

$$|00\rangle, \quad |01\rangle, \quad |10\rangle, \quad |11\rangle. \tag{3.11}$$

• Matrices (and column/row vectors) are written using these basis elements in (binary) numerical order, thus for an operator R:

$$\begin{pmatrix} \langle 00|R|00\rangle & \langle 00|R|01\rangle & \langle 00|R|10\rangle & \langle 00|R|11\rangle \\ \langle 01|R|00\rangle & \langle 01|R|01\rangle & \langle 01|R|10\rangle & \langle 01|R|11\rangle \\ \langle 10|R|00\rangle & \langle 10|R|01\rangle & \langle 10|R|10\rangle & \langle 10|R|11\rangle \\ \langle 11|R|00\rangle & \langle 11|R|01\rangle & \langle 11|R|10\rangle & \langle 11|R|11\rangle \end{pmatrix}. \tag{3.12}$$

◦ In the case of a product operator $R = A \otimes B$ one can think of the 4×4 matrix as consisting of four 2×2 blocks obtained by replicating the B matrix 4 times, and multiplying each by the corresponding matrix element of A.

★ The following entangled *Bell states* frequently arise in discussions of two qubits:

$$\begin{aligned} |B_0\rangle &= \big(|00\rangle + |11\rangle\big)/\sqrt{2}, \\ |B_1\rangle &= \big(|01\rangle + |10\rangle\big)/\sqrt{2}, \\ |B_2\rangle &= \big(|00\rangle - |11\rangle\big)/\sqrt{2}, \\ |B_3\rangle &= \big(|01\rangle - |10\rangle\big)/\sqrt{2}, \end{aligned} \tag{3.13}$$

◦ There is no standard notation for denoting a Bell state and sometimes it is convenient to use a different choice of phases. See p. 25 of QCQI for a slightly different notation.

• The states (3.13) form an orthonormal basis of the 2 qubit space.

• The state $|B_3\rangle$ is the spin singlet state used by Bohm in discussing the Einstein-Podolsky-Rosen paradox, and for this reason is sometimes called an "EPR" state, though that term is also sometimes used for other Bell states.

• Physical interpretation. One can think of $|B_0\rangle$ as "something like" a classical situation in which two bits, a and b are either both 0 with probability 1/2, or both 1 with probability 1/2. But there is no really good classical analogy for an entangled quantum state.

■ Tensor products of three or more spaces. For the most part these are obvious generalizations of the case of two spaces. Exception: There is no (satisfactory) generalization of the Schmidt decomposition (3.6) to three or more spaces.

★ The space $\mathcal{H} = \mathcal{A} \otimes \mathcal{B} \otimes \mathcal{C}$ can be thought of as the tensor product of $\mathcal{A} \otimes \mathcal{B}$ with $\mathcal{C}$, or of $\mathcal{A} \otimes \mathcal{C}$ with $\mathcal{B}$, etc.

• $\mathcal{A} \otimes \mathcal{B} \otimes \mathcal{C}$ has an orthonormal basis $\{|a_j\rangle \otimes |b_p\rangle \otimes |c_s\rangle\}$ if $\{|a_j\rangle\}$, $\{|b_p\rangle\}$, and $\{|c_s\rangle\}$ are orthonormal bases of $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$.

• The dimension d of $\mathcal{A} \otimes \mathcal{B} \otimes \mathcal{C}$ is the product of the dimensions of the factors: $d_a \cdot d_b \cdot d_c$.

4 Unitary dynamics and quantum circuits

★ See CQT Ch. 7, QCQI Secs. 2.2.2, 4.2, 4.3.

★ In general the time development of a quantum system is a stochastic (i.e., random) process governed by probabilities. However, there is also a deterministic unitary dynamics which is of interest in itself, and is also used to calculate the probabilities for the stochastic dynamics.

■ Schrödinger equation

$$i\hbar\frac{d}{dt}|\psi_t\rangle = H|\psi_t\rangle, \tag{4.1}$$

where t is the time, $H = H^\dagger$ the Hamiltonian or energy operator.

★ Time development operators $T(t', t)$. Any solution $|\psi_t\rangle$ to Schrödinger's equation satisfies:

$$|\psi_{t'}\rangle = T(t', t)|\psi_t\rangle \tag{4.2}$$

for any pair of times t' and t.

★ Properties of the time development operator(s) $T(t', t)$:

$$T(t, t) = I \tag{4.3}$$

$$T(t'', t) = T(t'', t')T(t', t) \tag{4.4}$$

$$T(t, t') = T(t', t)^\dagger = T(t', t)^{-1} \tag{4.5}$$

where t, t', t'' are any three times, and $T(t', t)^{-1}$ is the *inverse* of the operator $T(t', t)$. An operator whose adjoint is its inverse is a unitary operator.

★ See the discussion of unitary operators in Sec. 2

■ In studies of quantum information and computation, a unitary time development operator is often thought of, or represented by, a *quantum circuit*.

★ One qubit circuits

• Horizontal line represents time increasing from left to right. One qubit gate U means that starting state $|\psi\rangle$ is mapped to $U|\psi\rangle$.

• The general form of U for one qubit is worked out in QCQI Sec. 4.2.

• Some commonly used 1-qubit gates represented by matrices in the form (2.12):

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{4.6}$$

◦ The first three are the well-known Pauli matrices, also written σ_x, σ_y, and σ_z, while H is the Hadamard transformation.

◦ The X gate is also called a NOT or bit flip since $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$, analogous to the NOT gate in a classical circuit.

★ Two-qubit circuits are drawn with two horizontal lines representing the two qubits, together with various gates which can be one-qubit or two-qubit gates.

• Example: controlled-not = CNOT = controlled-X gate whose action is:

$$|00\rangle \mapsto |00\rangle, \quad |01\rangle \mapsto |01\rangle, \quad |10\rangle \mapsto |11\rangle, \quad |11\rangle \mapsto |10\rangle, \tag{4.7}$$

where $|ab\rangle = |a\rangle \otimes |b\rangle$; the a qubit is the upper line, b qubit the lower line in the circuit. $|\omega\rangle \mapsto |\tau\rangle$ means $|\tau\rangle = T|\omega\rangle$, where T is the unitary corresponding to the gate.

◦ Since the X gate, (4.6), performs the NOT operation, a controlled-not is the same as a controlled-X gate.

◦ A compact way of writing (4.7) is (with $X^0 = I$):

$$T|jk\rangle = |j\rangle \otimes X^j|k\rangle, \tag{4.8}$$

◦ One can also write

$$T = [0] \otimes I + [1] \otimes X; \quad [0] = |0\rangle\langle 0|, \quad [1] = |1\rangle\langle 1| \tag{4.9}$$

• Controlled-U gate, where U is any one-qubit unitary: replace X with U in (4.8) or (4.9).

◦ Warning! In the case where a one-qubit U amounts to multiplying by a complex number $c = e^{i\varphi}$ of unit modulus, it has no physical effect. However, a controlled-U of this form is *not* trivial; take a look at the case $c = -1$.

★ General quantum circuits for any number of qubits are constructed in a similar way.

• Note that time moves from left to right, so the the unitary transformation produced by the complete circuit is obtained by writing the product of the unitaries for individual gates in *reverse* order.

◦ Example: 2-qubit circuit with U applied to a, followed by CNOT, followed by V applied to b yields $(I \otimes V) \cdot \mathrm{CNOT} \cdot (U \otimes I)$.

★ Any unitary transformation on n qubits can be carried out with a circuit employing suitable 1-qubit gates along with CNOT gates. (A large number may be required.)

• A unitary on 2 qubits requires at most 3 CNOT gates

★ In many proposals for a physical realization of a quantum circuit, the 2-qubit gates are more difficult to construct than 1 qubit gates.