Complex Linear Algebra

R. J. Renka

Department of Computer Science & Engineering
University of North Texas

11/28/2017
The first postulate of quantum mechanics states that any isolated physical system is completely described by a unit vector in a complex Hilbert space. The state space for a particle moving on a line would be $L^2(\mathbb{R},\mathbb{C})$, but for quantum computing we operate in the finite dimensional space $\mathbb{C}^n, n \geq 2$. We will use Dirac’s bracket notation.

- $z^*$ is the complex conjugate of $z: (x + iy)^* = (x - iy)$.
- $|\psi\rangle$ is a ket (vector in $\mathbb{C}^n$), where $\psi$ is a label. Note that $|0\rangle$ is NOT the zero vector, which is denoted 0.
- $\langle \psi |$ is a bra (dual to or conjugate transpose of $|\psi\rangle$).
- $\langle \phi | \psi \rangle$ is an inner product.
- $|\phi\rangle \otimes |\psi\rangle = |\phi\rangle |\psi\rangle$ is a tensor product.
- $A^*$ is the complex conjugate of matrix $A$.
- $A^T$ is the transpose of matrix $A$.
- $A^\dagger = (A^*)^T = (A^T)^*$ is the adjoint of $A$.
- $\langle \phi | A |\psi \rangle$ is an inner product of $|\phi\rangle$ with $A|\psi\rangle$ or $A^\dagger |\phi\rangle$ with $|\psi\rangle$. 

R. J. Renka  
Complex Linear Algebra
A set of nonzero vectors $|v_1\rangle \ldots |v_k\rangle$ in $\mathbb{C}^n$ with $k \leq n$ is **linearly independent** if $\sum_{i=1}^{k} \alpha_i |v_i\rangle = 0 \Rightarrow \alpha_i = 0$ for all $i$.

A **spanning set** for $\mathbb{C}^n$ is a set of vectors $|v_1\rangle \ldots |v_k\rangle$ with $k \geq n$ such that any vector $|v\rangle$ in $\mathbb{C}^n$ can be written as a linear combination of vectors in the set: $|v\rangle = \sum_{i=1}^{k} \alpha_i |v_i\rangle$.

A **basis** for a linear space is a set of linearly independent vectors that span the space. The number of elements in the basis is the **dimension** of the space.

**Exercise 1:** Show that $(1,-1), (1,2),$ and $(2,1)$ are linearly dependent.
The **standard basis** (**computational basis**) states for $\mathbb{C}^2$ are

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$ 

Any vector $|v\rangle = (\alpha_1, \alpha_2)$ in $\mathbb{C}^2$ can be written as $|v\rangle = \alpha_1|0\rangle + \alpha_2|1\rangle$. Another basis for $\mathbb{C}^2$ is

$$|+\rangle \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad \text{and} \quad |-\rangle \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

since

$$|v\rangle = \frac{\alpha_1 + \alpha_2}{\sqrt{2}}|+\rangle + \frac{\alpha_1 - \alpha_2}{\sqrt{2}}|-\rangle.$$
A linear transformation (**linear operator**) from a linear space $V$ to a linear space $W$ is a function $A : V \rightarrow W$ such that $A$ is linear:

$$A(\alpha|v\rangle) = \alpha A|v\rangle \text{ and } A(|u\rangle + |v\rangle) = A|u\rangle + A|v\rangle$$

for all elements $|u\rangle, |v\rangle$ in $V$ and scalars $\alpha$ in $\mathbb{C}$. Note that we usually omit the parentheses around the argument in the expression for the function value $A(|v\rangle)$.

The **identity operator** on $V$ (from $V$ to $V$) is denoted $I_V$ or $I$ when there is no ambiguity, and the zero operator is $0$. For linear operators $A : V \rightarrow W$ and $B : W \rightarrow X$ the composition $BA : V \rightarrow X$ is defined by $BA|v\rangle = B(A|v\rangle)$. 
There is a 1-1 correspondence between linear operators $A$ from $\mathbb{C}^n$ to $\mathbb{C}^m$ and the set of $m$ by $n$ complex matrices. The matrix transforms a vector $|v\rangle$ by computing a matrix-vector product with $|v\rangle$ treated as a column-vector ($n$ by 1 matrix).

Conversely, suppose $A : V \rightarrow W$ is linear, and $|v_1\rangle, \ldots, |v_n\rangle$ and $|w_1\rangle, \ldots, |w_m\rangle$ are bases for $V$ and $W$, respectively. Then for each $j$ in the range 1 to $n$ there are complex numbers $A_{1j}, \ldots, A_{mj}$ such that

$$A|v_j\rangle = \sum_{i=1}^{m} A_{ij} |w_i\rangle.$$ 

This defines the matrix representation of the operator. If the standard basis is used for both spaces, the matrix columns are obtained by applying the operator to the basis vectors.
We deviate from the standard quantum mechanical notation here and denote $\langle u|v \rangle$ by $(|u\rangle, |v\rangle)$. An inner product associated with a complex linear space $V$ is a function $(\cdot, \cdot)$ from $V \times V$ to $\mathbb{C}$ with the following three properties.

1. $(|u\rangle, \sum_i \alpha_i |v_i\rangle) = \sum_i \alpha_i (|u\rangle, |v_i\rangle)$ — linear in the second argument. (This is the physics convention, not the math convention).

2. $(|u\rangle, |v\rangle) = (|v\rangle, |u\rangle)^*$ — sesquilinear.

3. $(|v\rangle, |v\rangle) \geq 0$ with equality if and only if $|v\rangle = 0$ — positive definite.

**Exercise 2:** Show that an inner product is conjugate-linear in the first argument:

$$\left( \sum_i \alpha_i |u_i\rangle, |v\rangle \right) = \sum_i \alpha_i^* (|u_i\rangle, |v\rangle).$$
Exercise 3: Show that the following is an inner product on $\mathbb{C}^n$:

$$\langle |u\rangle, |v\rangle \rangle = \langle u|v \rangle = |u\rangle^\dagger |v\rangle = \sum_{i=1}^{n} u_i^* v_i.$$ 

In the above expression $|u\rangle^\dagger$ is the row vector obtained by applying the conjugate transpose operation to $|u\rangle$ as a column vector associated with the $n$-tuple of complex numbers $(u_1, u_2, \ldots, u_n)$, and the inner product is computed by matrix multiplication. An alternative view is that the bra $\langle u|$ is the element of the dual space (space of bounded linear functionals on the Hilbert space defined by $\mathbb{C}^n$ with the above inner product) whose value at $|v\rangle$ is $\langle u|v \rangle$. 
An **inner product space** is a linear space equipped with an inner product and hence with a norm defined by

\[ \|v\| \equiv \sqrt{\langle v|v \rangle}. \]

A **unit vector** is a vector with norm 1. Any nonzero vector can be **normalized** by dividing it by its norm.

A **Hilbert space** is a complete inner product space — one in which Cauchy sequences of elements in the space converge to an element of the space. All finite dimensional inner product spaces are Hilbert spaces.

Vectors $|u\rangle$ and $|v\rangle$ are **orthogonal** if their inner product is zero. A set of vectors $\{|v_i\rangle\}$ is **orthonormal** if $\langle v_i|v_j \rangle = \delta_{ij}$. 
Suppose $|v_1⟩, \ldots, |v_n⟩$ is a basis for an inner product space $V$. An orthonormal basis for $V$ can be constructed by the Gram-Schmidt procedure. Define $|u_1⟩ \equiv |v_1⟩/\| |v_1⟩ \|$ and

$$|u_k⟩ \equiv \frac{|v_k⟩ - \sum_{i=1}^{k-1} \langle u_i | v_k⟩ |u_i⟩}{\| |v_k⟩ - \sum_{i=1}^{k} \langle u_i | v_k⟩ |u_i⟩ \|}$$

for $2 \leq k \leq n$.

**Exercise 4:** Prove that $|u_1⟩, \ldots, |u_n⟩$ is an orthonormal basis for $V$.

**Exercise 5:** Suppose $|v⟩ = \sum_{i=1}^{n} v_i |i⟩$ and $|w⟩ = \sum_{i=1}^{n} w_i |i⟩$ for some orthonormal basis $|1⟩, \ldots, |n⟩$. Show that

$$\langle v | w⟩ = \sum_{i=1}^{n} v_i^* w_i.$$
Completeness

A collection of vectors $\{ |v_i\rangle \}$ in a Hilbert space $V$ is complete if $\langle v_i | v \rangle = 0$ for all $i$ implies that $|v\rangle = 0$ or, equivalently, the span of the vectors is dense in $V$. An orthonormal basis for $V$ is a complete orthonormal system.

**Theorem:** Let $\{ |v_i\rangle \}_{i=1}^{\infty}$ be an orthonormal system in a Hilbert space $V$. Then the following are equivalent.

1. $\{ |v_i\rangle \}_{i=1}^{\infty}$ is complete.
2. For all $|v\rangle \in V$, $|v\rangle = \sum_{i=1}^{\infty} \langle v_i | v \rangle |v_i\rangle$, where the sum converges unconditionally (independent of order).
3. $\|v\|^2 = \sum_{i=1}^{\infty} |\langle v_i | v \rangle|^2 = \sum_{i=1}^{\infty} \langle v | v_i \rangle \langle v_i | v \rangle$.
4. For all $|u\rangle, |v\rangle \in V$, $\langle u | v \rangle = \sum_{i=1}^{\infty} \langle v_i | u \rangle^* \langle v_i | v \rangle$. 
Examples of Hilbert spaces with complete orthonormal bases include the following.

1. Any collection of \( n \) linearly independent vectors in an \( n \)-dimensional Hilbert space can be converted by Gram-Schmidt into an orthonormal basis.

2. \( L^2[0, 1] \) is the completion in the \( L^2 \) norm of \( C[0, 1] \). The **Fourier series** of a function in this space is the expansion of the function in the orthonormal basis \( \{ \exp(2\pi ikx) \}_{k=-\infty}^{\infty} \). Another orthonormal basis for \( L^2[0, 1] \) is the set of Legendre polynomials which are obtained by applying Gram-Schmidt to the sequence of monomials \( \{1, x, x^2, \ldots\} \).

3. \( L^2(\mathbb{R}) \) is the completion in the \( L^2 \) norm of the compactly supported functions \( C_c(\mathbb{R}) \) or \( C_c^\infty(\mathbb{R}) \).
Outer product and completeness relation

Given vectors $|v\rangle \in V$ and $|w\rangle \in W$ for inner product spaces $V$ and $W$, we define the outer product operator $|w\rangle\langle v| : V \rightarrow W$ by

$$(|w\rangle\langle v|)(|v'\rangle) \equiv |w\rangle\langle v|v'\rangle = \langle v|v'\rangle|w\rangle$$

for all $|v'\rangle \in V$. Let $\{|v_i\rangle\}$ be an orthonormal basis for $V$, and let $|v\rangle = \sum_i v_i|v_i\rangle$ for $v_i \equiv \langle v_i|v\rangle$. Then

$$\left(\sum_i |v_i\rangle\langle v_i|\right)|v\rangle = \sum_i |v_i\rangle\langle v_i|v\rangle = \sum_i v_i|v_i\rangle = |v\rangle.$$

Since $|v\rangle$ is arbitrary, we have the completeness relation:

$$\sum_i |v_i\rangle\langle v_i| = I.$$
Suppose $A : V \to W$ is a linear operator, $\{|v_i\rangle\}$ is an orthonormal basis for $V$, and $\{|w_i\rangle\}$ is an orthonormal basis for $W$. Then

$$A = I_W A I_V = \sum_{ij} |w_i\rangle \langle w_i| A |v_j\rangle \langle v_j| = \sum_{ij} \langle w_i| A |v_j\rangle |w_i\rangle \langle v_j|. $$

Thus the matrix entries of $A$ with respect to the bases are $A_{ij} = \langle w_i| A |v_j\rangle$.

**Exercise 6**: Suppose $|v_1\rangle, \ldots, |v_n\rangle$ is an orthonormal basis for inner product space $V$. What is the outer product representation for the operator $|v_k\rangle \langle v_l|$ with respect to the $|v_i\rangle$ basis?
The Cauchy-Schwarz theorem relates algebra to geometry in an inner product space.

**Theorem:** For any two vectors $|v\rangle$ and $|w\rangle$ in $V$, 

$$|\langle v|w\rangle|^2 \leq \langle v|v\rangle \langle w|w\rangle$$

with equality if and only if $|v\rangle = z|w\rangle$ for some scalar $z$.

**proof:** The theorem is true for $w = 0$. Otherwise, use the Gram-Schmidt procedure to construct an orthonormal basis $\{|v_i\rangle\}$ such that the first member is $|w\rangle/\sqrt{\langle w|w\rangle}$. Then 

$$\langle v|v\rangle \langle w|w\rangle = \sum_i \langle v|v_i\rangle \langle v_i|v\rangle \langle w|w\rangle$$

$$\geq \frac{\langle v|w\rangle \langle w|v\rangle}{\langle w|w\rangle} \langle w|w\rangle$$

$$= \langle v|w\rangle \langle w|v\rangle = |\langle v|w\rangle|^2.$$ 

Equality in the case of linear dependence is easily verified. \qed
An eigenvalue of a linear operator $A : V \to V$ is a complex number $\lambda$ such that $A|\nu\rangle = \lambda|\nu\rangle$ for some nonzero vector $|\nu\rangle$, referred to as an eigenvector. The set of such eigenvectors, along with the zero vector, is the eigenspace of $\lambda$ — a subspace of $V$. The geometric multiplicity of $\lambda$ is the dimension of its eigenspace. If this dimension is greater than one, $\lambda$ is said to be degenerate. For $n > 1$ the order-$n$ identity matrix has degenerate eigenvalue 1.

Since the operator $\lambda I - A$ has a nonzero vector in its null space, it is not invertible. In the case that $V$ has dimension $n$, $\lambda$ is an eigenvalue of $A$ if and only the matrix $\lambda I - A$ has determinant equal to zero. In this case the eigenvalues can be computed as zeros of the characteristic polynomial $c(\lambda) \equiv \det(\lambda I - A)$. This is a polynomial of degree $n > 0$ and has at least one complex zero by the fundamental theorem of algebra.
In the infinite-dimensional case, the operator $\lambda I - A$ may not have an inverse even if $\lambda$ is not an eigenvalue. The set of eigenvalues of $A$ can be generalized to the **spectrum** of $A$: the set of all scalars $\lambda$ for which the operator $\lambda I - A$ has no bounded inverse.

The **diagonal representation** or **orthonormal decomposition** of an operator $A$ on a Hilbert space $V$ is

$$A = \sum_i \lambda_i |v_i\rangle \langle v_i|,$$

where $\{|v_i\rangle\}_i$ is an orthonormal set of eigenvectors for $A$ with corresponding eigenvalues $\lambda_i$. The operator is **diagonalizable** (by a unitary matrix) if it has such a representation: $U^\dagger AU = \Lambda$.

**Exercise 7**: Prove that the following matrix is not diagonalizable.

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$
Suppose $A$ is a bounded linear transformation from Hilbert space $V$ to Hilbert space $W$. Then for each $|w\rangle \in W$ define $\phi_w : V \to \mathbb{C}$ by

$$\phi_w(|v\rangle) \equiv (A|v\rangle, |w\rangle)_W$$

It is easily shown that $\phi_w$ is a bounded linear functional on $V$ and, by the Riesz Representation Theorem, is uniquely represented by an element $|v'\rangle \in V$ such that $\phi_w(|v\rangle) = (|v\rangle, |v'\rangle)_V$. We define the **adjoint** operator $A^\dagger : W \to V$ by $A^\dagger|w\rangle = |v'\rangle$. Thus $A^\dagger$ is the unique operator that satisfies

$$(A|v\rangle, |w\rangle)_W = (|v\rangle, A^\dagger|w\rangle)_V$$

for all $|v\rangle \in V$ and $|w\rangle \in W$. It can be shown that $A^\dagger$ is linear and bounded with the same operator norm as $A$, and that $(A^\dagger)^\dagger = A$. 
If $A : V \rightarrow W$ and $B : W \rightarrow X$ are bounded linear operators, then the adjoint of $BA : V \rightarrow X$ is $(BA)^\dagger = A^\dagger B^\dagger : X \rightarrow V$.

If $V = \mathbb{C}^n$ and $W = \mathbb{C}^m$, then $A : V \rightarrow W$ is represented by an $m$ by $n$ matrix, and its adjoint $A^\dagger$ is the conjugate transpose of $A$. This includes the case $n = 1$ with $A$ and $A^\dagger$ represented by a column vector and a row vector, respectively so that the adjoint is the dual. Thus, $(A|v\rangle)^\dagger = \langle v|A^\dagger$ and $(|u\rangle\langle v|)^\dagger = |v\rangle\langle u|$.

**Exercise 8**: Show that the adjoint is anti-linear:

$\left( \sum_i \alpha_i A_i \right)^\dagger = \sum_i \alpha_i^* A_i^\dagger$. 

R. J. Renka

Complex Linear Algebra
If $A : V \to V$ and $A^\dagger = A$ then $A$ is said to be self-adjoint or Hermitian.

Suppose $V$ has dimension $n$ and $W$ is a $k$-dimensional subspace of $V$ for $k < n$. Using the Gram-Schmidt procedure, we can construct an orthonormal basis $|v_1\rangle, \ldots, |v_n\rangle$ for $V$ such that $|v_1\rangle, \ldots, |v_k\rangle$ is an orthonormal basis for $W$. The projector onto $W$ is

$$P \equiv \sum_{i=1}^{k} |v_i\rangle\langle v_i|.$$ 

This definition is independent of the choice of basis vectors. $P$ and its orthogonal complement $Q = I - P$ are Hermitian operators.

Exercise 9: Show that $P$ and $Q$ are idempotent: $P^2 = P$ and $Q^2 = Q$. 

An operator $A : V \to V$ is **normal** if it commutes with its adjoint: $AA^\dagger = A^\dagger A$. Hermitian operators are normal.

**Exercise 10**: Show that a normal matrix is Hermitian if and only if it has real eigenvalues. Use the following theorem.

**Exercise 11**: Show that any diagonalizable operator is normal.

**Theorem**: (Spectral decomposition) A normal matrix $A$ on a vector space $V$ is diagonal with respect to some orthonormal basis for $V$.

**proof**: We use induction on the dimension $n$ of $V$. The case $n = 1$ is trivial. Let $\lambda$ be an eigenvalue of $A$, and denote by $P$ and $Q$ the projectors onto the eigenspace of $\lambda$ and its complement, respectively. Then, since $P + Q = I$,

$$A = (P + Q)A(P + Q) = PAP + QAP + PAQ + QAQ.$$
proof of spectral decomposition continued

Since \( AP|v\rangle = \lambda P|v\rangle \) for all \(|v\rangle \in V\), we have \( PAP = \lambda P \). Also, \( QAP = 0 \) since \( AP = \lambda P \). Furthermore, \( AA^\dagger P|v\rangle = A^\dagger AP|v\rangle = \lambda A^\dagger P|v\rangle \) implies that \( A^\dagger P|v\rangle \) is in the eigenspace of \( \lambda \) (range of \( P \)). Hence \( QA^\dagger P|v\rangle = 0 \) for all \(|v\rangle\), implying that \( QA^\dagger P = 0 \) and \( (QA^\dagger P)^\dagger = PAQ = 0 \). We next show that \( QAQ \) is normal. First, note that \( QA = QA(P + Q) = QAQ \) and \( QA^\dagger = QA^\dagger(P + Q) = QA^\dagger Q \). Then, using normality of \( A \) and the fact that \( Q^2 = Q \), we have \( QAQQA^\dagger Q = QAQA^\dagger Q = QAA^\dagger Q = QA^\dagger AQ = QA^\dagger QAQ = QA^\dagger QQAQ \). Thus, by the inductive hypothesis, \( QAQ \) is diagonal with respect to some orthonormal basis for the range of \( Q \), and since \( PAP = \lambda P \) is diagonal with respect to some orthonormal basis for the range of \( P \), it follows that \( A = PAP + QAQ \) is diagonal with respect to some orthonormal basis for \( V \). \( \square \)
A **unitary** operator is a bounded linear operator $U$ on a Hilbert space $V$ that satisfies $U^\dagger U = UU^\dagger = I$. Since $U$ is normal, the spectral theorem applies. A unitary matrix has orthonormal columns. A unitary operator preserves inner products and hence norms:

$$(U|v\rangle, U|w\rangle) = \langle v|U^\dagger U|w\rangle = \langle v|I|w\rangle = \langle v|w\rangle.$$ 

**Exercise 12**: Show that the spectrum of a unitary operator lies on the unit circle of modulus-1 complex numbers $e^{i\theta}, \theta \in \mathbb{R}$.

An operator $A$ is **positive definite** if $\langle v|A|v\rangle > 0$ (and real) for all $|v\rangle \neq 0$. If the inequality is nonstrict we say $A$ is **positive** or **positive semidefinite**.
Exercise 13: Simplify the proof of the spectral decomposition theorem for the case of a Hermitian operator.

Exercise 14: Prove that two eigenvectors of a Hermitian operator with different eigenvalues are necessarily orthogonal.

Exercise 15: Prove that the eigenvalues of a projector $P$ are all either 0 or 1.

Exercise 16: Show that a positive operator is necessarily Hermitian and therefore has a diagonal representation with nonnegative eigenvalues. Hint: show that an arbitrary operator $A$ can be written as $A = B + iC$ where $B$ and $C$ are Hermitian.

Exercise 17: Show that for any operator $A$, $A^\dagger A$ is positive.
The Pauli matrices are as follows.

\[\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \sigma_1 \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\]

\[\sigma_2 \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \sigma_3 \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\]

**Exercise 18:** Show that the Pauli matrices are Hermitian and unitary.

**Exercise 19:** Find the eigenvectors, eigenvalues, and diagonal representations of the Pauli matrices \(X\), \(Y\), and \(Z\) for the orthonormal vectors \(|0\rangle\) and \(|1\rangle\).
Suppose $V$ is a Hilbert space with orthonormal basis $|v_1\rangle, \ldots, |v_m\rangle$ and $W$ is a Hilbert space with orthonormal basis $|w\rangle, \ldots, |w_n\rangle$. Then the tensor product space $V \otimes W$ is the $mn$-dimensional vector space spanned by a basis consisting of all pairwise products of the form $|v_i\rangle \otimes |w_j\rangle$. A tensor product $|v\rangle \otimes |w\rangle$ is often abbreviated as $|v\rangle|w\rangle$, $|v, w\rangle$, or $|vw\rangle$.

The tensor product operator is bilinear. For scalar $z$,

$$z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle),$$

$$]|v_1\rangle + |v_2\rangle\rangle \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle,$$

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$$

for $|v\rangle, |v_1\rangle, |v_2\rangle \in V$ and $|w\rangle, |w_1\rangle, |w_2\rangle \in W$. 
Suppose $A : V \rightarrow V'$ and $B : W \rightarrow W'$ are linear operators. Then we can define a linear operator $A \otimes B : V \otimes W \rightarrow V' \otimes W'$ by

$$(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv A|v\rangle \otimes B|w\rangle.$$ 

Like composition and matrix multiplication operators, the tensor product is bilinear and associative but not commutative. An inner product on $V \otimes W$ can be defined by the inner products on $V$ and $W$:

$$(|v\rangle \otimes |w\rangle, |v'\rangle \otimes |w'\rangle) \equiv \langle v|v'\rangle\langle w|w'\rangle$$

with extension by linearity. With completion under this inner product, $V \otimes W$ is a Hilbert space and inherits the structure associated with adjoints, unitarity, normality, and Hermiticity.
A **Kronecker product** is a generalization of an outer product from vectors to matrices, and gives the matrix representing a tensor product with respect to a basis. Suppose $A$ is an $m$ by $n$ matrix, and $B$ is a $p$ by $q$ matrix. Then $A \otimes B$ is represented by an $mp$ by $nq$ matrix:

$$
A \otimes B \equiv \begin{bmatrix}
    a_{11}B & a_{12}B & \ldots & a_{1n}B \\
    a_{21}B & a_{22}B & \ldots & a_{2n}B \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{m1}B & a_{m2}B & \ldots & a_{mn}B
\end{bmatrix}.
$$

**Notation:** $|\psi\rangle^\otimes k$ is a generalization of $|\psi\rangle^\otimes 2 = |\psi\rangle \otimes |\psi\rangle$.

**Exercise 20:** Let $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Write out $|\psi\rangle^\otimes 2$ and $|\psi\rangle^\otimes 3$ explicitly, both in terms of tensor products like $|0\rangle|1\rangle$, and using the Kronecker product.
Exercise 21: Calculate the matrix representation of the tensor products of the Pauli operators (a) $X$ and $Z$; (b) $I$ and $X$; (c) $X$ and $I$. Is the tensor product commutative?

Exercise 22: Show that the transpose, complex conjugation, and adjoint operations distribute over the tensor product:

$$(A \otimes B)^* = A^* \otimes B^*; (A \otimes B)^T = A^T \otimes B^T; (A \otimes B)^\dagger = A^\dagger \otimes B^\dagger.$$ 

Exercise 23: Show that the tensor product of two unitary operators is unitary.

Exercise 24: Show that the tensor product of two Hermitian operators is Hermitian.

Exercise 25: Show that the tensor product of two positive operators is positive.

Exercise 26: Show that the tensor product of two projectors is a projector.
The Hadamard operator on one qubit can be written as

$$H = \frac{1}{\sqrt{2}} \left[ |0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1| \right].$$

**Exercise 27**: Show that the Hadamard transform on $n$ qubits may be written as

$$H^\otimes n = \frac{1}{\sqrt{2^n}} \sum_{i,j=0}^{2^n-1} (-1)^{i\cdot j} |i\rangle\langle j|,$$

where $i \cdot j = \sum_{k=0}^{n-1} i_k j_k$ is the bitwise inner product of the binary representations of $i$ and $j$. Write an explicit matrix representation for $H^\otimes 2$.

$H^\otimes n$ is unitary, involutory, and symmetric (but not Hermitian).
Any function $f : \mathbb{C} \rightarrow \mathbb{C}$ can be extended to a mapping from normal operators to normal operators by evaluating $f$ at the eigenvalues. For $A = \sum_i \lambda_i |v_i\rangle\langle v_i|$, define

$$f(A) \equiv \sum_i f(\lambda_i) |v_i\rangle\langle v_i|.$$ 

This procedure can be used to define functions such as polynomials, rational functions of invertible operators, the exponential function, the square root of a positive operator, and the logarithm of a positive definite operator. For example,

$$A^2 = \left( \sum_i \lambda_i |v_i\rangle\langle v_i| \right) \left( \sum_j \lambda_j |v_j\rangle\langle v_j| \right) = \sum_{i,j} \lambda_i \lambda_j |v_i\rangle\delta_{ij} \langle v_j|$$

$$= \sum_i \lambda_i^2 |v_i\rangle\langle v_i| = f(A)$$

for $f(x) \equiv x^2$. 
The **trace** of an \( n \) by \( n \) matrix \( A \), denoted \( \text{tr}(A) \) is the sum of the diagonal elements: \( \text{tr}(A) = \sum_{i=1}^{n} a_{ii} \). Properties of the trace include the following.

- **linearity:** \( \text{tr}(\alpha A + \beta B) = \alpha \text{tr}(A) + \beta \text{tr}(B) \).
- **invariance under transpose:** \( \text{tr}(A^T) = \text{tr}(A) \).
- **Kronecker product:** \( \text{tr}(A \otimes B) = \text{tr}(A)\text{tr}(B) \).
- **invariance under cyclic permutations:** \( \text{tr}(AB) = \text{tr}(BA), \text{tr}(ABC) = \text{tr}(BCA) = \text{tr}(CAB) \), etc.
- **similarity invariance:** \( \text{tr}(V^{-1}AV) = \text{tr}(VV^{-1}A) = \text{tr}(A) \).
- **outer product:** \( \text{tr}(A|\psi\rangle\langle\psi|) = \text{tr}(\langle\psi|A|\psi\rangle) = \langle\psi|A|\psi\rangle \).

By similarity invariance, the trace is the sum of eigenvalues. Also, since any matrix representation can be used, the trace can be defined for an arbitrary linear operator on a finite-dimensional space.
The **commutator** and **anti-commutator** between linear operators $A$ and $B$ on a vector space $V$ are defined by

\[
[A, B] \equiv AB - BA \quad \text{and} \quad \{A, B\} \equiv AB + BA,
\]

respectively. For Hermitian operators $A$ and $B$, $AB$ is Hermitian if and only if $[A, B] = 0$. Also, Hermitian operators $A$ and $B$ are **simultaneously diagonalizable** if they share a common set of eigenvectors; i.e., $A = \sum_i a_i |v_i\rangle\langle v_i|$ and $B = \sum_i b_i |v_i\rangle\langle v_i|$ for some orthonormal basis $|v_i\rangle$. The Pauli matrices $X$ and $Y$, for example, do not share eigenvectors (Exercise 19). The following theorem provides an easy means of verifying that fact.

**Theorem:** Suppose $A$ and $B$ are Hermitian operators. Then $[A, B] = 0$ if and only if $A$ and $B$ are simultaneously diagonalizable (measurement of the observables associated with $A$ and $B$ can result in sharp values of both).
Proof of simultaneous diagonalization theorem

**proof:** It is easily shown that, if $A$ and $B$ are simultaneously diagonalizable, then $[A, B] = 0$. For the converse, suppose $U^\dagger AU = \Lambda$ is diagonal, and define $B' = U^\dagger BU$. Then

$$\Lambda B' = (U^\dagger AU)(U^\dagger BU) = U^\dagger ABU = U^\dagger BAU = (U^\dagger BU)(U^\dagger AU) = B'\Lambda.$$ 

Hence $(\Lambda B' - B'\Lambda)_{ij} = (\lambda_i - \lambda_j)b'_{ij} = 0$ for all $i$ and $j$. If the eigenvalues of $A$ are distinct, then $B'$ is diagonal. If some of the eigenvalues of $A$ are degenerate, then by ordering the columns of $U$ so that the degenerate eigenvalues are contiguous, we can write $\Lambda$ and $B'$ in block matrix form with the off-diagonal blocks of $B'$ as zeros. Since the diagonal blocks of $B'$ are Hermitian matrices, they can be diagonalized by a unitary similarity transformation $U'$ such that $U'^\dagger B'U' = D$ is diagonal and $U'^\dagger \Lambda U' = \Lambda$. We then have an invertible matrix $W = UU'$ such that $W^\dagger AW = \Lambda$ and $W^\dagger BW = D$. □
Exercises

**Exercise 28:** Show that the Pauli matrices $X$, $Y$, and $Z$ have trace 0.

**Exercise 29:** Verify the commutation relations

$$[X, Y] = 2iZ, \quad [Y, Z] = 2iX, \quad [Z, X] = 2iY.$$

**Exercise 30:** Verify the anti-commutation relations $\{\sigma_i, \sigma_j\} = 0$ for $i, j \in \{1, 2, 3\}$ with $i \neq j$. Also verify that $\sigma_i^2 = I$.

**Exercise 31:** Verify that

$$AB = \frac{[A, B] + \{A, B\}}{2}.$$

**Exercise 32:** Show that $[A, B]^\dagger = [B^\dagger, A^\dagger]$ and $[A, B] = -[B, A]$.

**Exercise 33:** Show that $i[A, B]$ is Hermitian for $A$ and $B$ Hermitian.
The left and right \textbf{polar decompositions} of an operator or square matrix are defined by the following theorem.

\textbf{Theorem}: Let $A$ be a linear operator on a vector space $V$. Then there exists a unitary operator $U$ and positive operators $J$ and $K$ such that

$$A = UJ = KU,$$

where $J \equiv \sqrt{A^\dagger A}$ and $K = \sqrt{AA^\dagger}$. If $A$ is invertible then $U$ is unique.

\textbf{Corollary}: For a square matrix $A$ there exist unitary matrices $U$ and $V$ such that

$$A = U\Sigma V,$$

where $\Sigma$ is a diagonal matrix with nonnegative entries referred to as \textit{singular values}. 

R. J. Renka  
Complex Linear Algebra