Introduction to Quantum Computing

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Dirac's Bra/Ket Notation for Linear Transformations

Bra/ket Notation and Linear Transformations

- Dirac's bra/ket notation provides a convenient way of specifying linear transformations on quantum states.
- Recall that the conjugate transpose of the vector denoted by ket $|\psi\rangle$ is denoted by bra $\langle\psi|$.
- Moreover, the inner product of vectors $|\psi\rangle$ and $|\phi\rangle$ is given by

$$\langle\psi|\phi\rangle.$$

- The outer product of the vectors $|x\rangle$ and $|y\rangle$ is written

$$|x\rangle\langle y|.$$

- Matrix multiplication is associative, and scalars commute with everything.
- So relations such as the following hold:

$$\begin{aligned}(|a\rangle\langle b|)|c\rangle &= |a\rangle(\langle b||c\rangle) \\ &= (\langle b|c\rangle)|a\rangle.\end{aligned}$$

Two-Dimensional Transformations

- Let V be a vector space associated with a single-qubit system.
- The matrix for the operator $|0\rangle\langle 0\rangle$, with respect to the standard basis in the standard order $\{|0\rangle, |1\rangle\}$, is

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

Two-Dimensional Transformations (Cont'd)

- Similarly, we have

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

- So the notation $|0\rangle\langle 1|$ represents the linear transformation that maps $|1\rangle$ to $|0\rangle$ and $|0\rangle$ to the null vector.
- This relationship is suggested by the notation:

$$(|0\rangle\langle 1|)|1\rangle = |0\rangle(\langle 1|1\rangle) = |0\rangle(1) = |0\rangle;$$
$$(|0\rangle\langle 1|)|0\rangle = |0\rangle(\langle 1|0\rangle) = |0\rangle(0) = 0.$$

Two-Dimensional Transformations (Cont'd)

- Similarly
$$|1\rangle\langle 0| = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$
- Thus, all two-dimensional linear transformations on V can be written in Dirac's notation:
$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ &= a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|. \end{aligned}$$

Example

- The linear transformation that exchanges $|0\rangle$ and $|1\rangle$ is given by
$$X = |0\rangle\langle 1| + |1\rangle\langle 0|.$$
- We will also use the notation
$$X: \quad \begin{array}{l} |0\rangle \mapsto |1\rangle, \\ |1\rangle \mapsto |0\rangle. \end{array}$$
- This specifies a linear transformation in terms of its effect on the basis vectors.
- The transformation $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ can also be represented by the matrix
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
with respect to the standard basis.

Example

- Consider the transformation that exchanges the basis vectors $|00\rangle$ and $|10\rangle$ and leaves the others alone.
- It is written

$$|10\rangle\langle 00| + |00\rangle\langle 10| + |11\rangle\langle 11| + |01\rangle\langle 01|.$$

- With respect to the standard basis, it has matrix representation

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

n-Qbit Operators

- An operator on an n-qubit system that maps the basis vector $|j\rangle$ to $|i\rangle$ and all other standard basis elements to 0 can be written
$$O = |i\rangle\langle j|$$
in the standard basis.
- The matrix for O has a single non-zero entry 1 in the ij-th place.
- A general operator O with entries a_{ij} in the standard basis can be written
$$O = \sum_i \sum_j a_{ij}|i\rangle\langle j|.$$
- Similarly, the ij-th entry of the matrix for O in the standard basis is given by
$$\langle i|O|j\rangle.$$

Example

- We give an example of working with this notation.
- We write out the result of applying operator O to a vector

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

- We have

$$\begin{aligned} O|\psi\rangle &= (\textstyle\sum_i \sum_j a_{ij}|i\rangle\langle j|)(\sum_k b_k|k\rangle) \\ &= \textstyle\sum_i \sum_j \sum_k a_{ij} b_k |i\rangle\langle j||k\rangle \\ &= \textstyle\sum_i \sum_j a_{ij} b_j |i\rangle. \end{aligned}$$

Bra/ket Notation for Arbitrary Bases

- Let $\{|\beta_i\rangle\}$ be a basis for an N-dimensional vector space V.
- Then, with respect to this basis, an operator $O : V \to V$ can be written as
$$\sum_{i=1}^{N}\sum_{j=1}^{N} b_{ij}|\beta_i\rangle\langle\beta_j|.$$
- In particular, the matrix for O with respect to $\{|\beta_i\rangle\}$ has entries
$$O_{ij} = b_{ij}.$$

Matrix versus Bra/ket Notation

- Initially the vector/matrix notation may be easier for the reader to comprehend because it is more familiar.
- Sometimes this notation is convenient for performing calculations.
- But it requires choosing a basis and an ordering of that basis.
- The bra/ket notation is independent of the basis and the order of the basis elements.
- It is also more compact, and suggests correct relationships, as for the outer product, so that once it becomes familiar, it is easier to read.

Subsection 2

Projection Operators for Measurement

Orthogonal Complement

- For any subspace S of V, the subspace $S^{\perp}$ consists of all vectors that are perpendicular to all vectors in S.
- The subspaces S and $S^{\perp}$ satisfy

$$V = S \oplus S^{\perp}.$$

- Thus, any vector $|v\rangle \in V$ can be written uniquely as the sum

$$|v\rangle = \vec{s}_1 + \vec{s}_2$$

  of a vector $\vec{s}_1 \in S$ and a vector $\vec{s}_2 \in S^{\perp}$.
- We use the notation $\vec{s}_i$ because $\vec{s}_1$ and $\vec{s}_2$ are generally not unit vectors.

Projection Operators

- Let V be a vector space.
- Let S be a subspace of V.
- The **projection operator**

$$P_S : V \to S$$

is the linear operator that sends

$$|v\rangle \mapsto \vec{s}_1,$$

where $|v\rangle = \vec{s}_1 + \vec{s}_2$ with $\vec{s}_1 \in S$ and $\vec{s}_2 \in S^\perp$.
- The operator $|\psi\rangle\langle\psi|$ is the projection operator onto the subspace spanned by $|\psi\rangle$.
- Projection operators are sometimes called **projectors** for short.

Projection Operators and Measurements

- Let V be a vector space.
- Let $V = S_1 \oplus \cdots \oplus S_k$ be a direct sum decomposition of V into orthogonal subspaces S_i.
- There are k related projection operators

$$P_i : V \to S_i,$$

with

$$P_i|v\rangle = \vec{s}_i,$$

where $|v\rangle = \vec{s}_1 + \cdots + \vec{s}_k$ with $\vec{s}_i \in S_i$.
- In this terminology, a measuring device with associated decomposition $V = S_1 \oplus \cdots \oplus S_k$ acting on a state $|\psi\rangle$ results in the state

$$|\phi\rangle = \frac{P_i|\psi\rangle}{|P_i|\psi\rangle|}$$

with probability $|P_i|\psi\rangle|^2$.

Example

- The projector $|0\rangle\langle 0|$ acts on a single-qubit state $|\psi\rangle$.

  It obtains the component of $|\psi\rangle$ in the subspace generated by $|0\rangle$.

  Let

  $$|\psi\rangle = a|0\rangle + b|1\rangle.$$

  Then

  $$\begin{aligned}(|0\rangle\langle 0|)|\psi\rangle &= (|0\rangle\langle 0|)(a|0\rangle + b|1\rangle) \\ &= a\langle 0|0\rangle|0\rangle + b\langle 0|1\rangle|0\rangle \\ &= a|0\rangle.\end{aligned}$$

Example

- The projector $|1\rangle|0\rangle\langle 1|\langle 0|$ acts on two-qubit states.

  Let

  $$|\phi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle.$$

  Then we have

  $$\begin{aligned}(|1\rangle|0\rangle\langle 1|\langle 0|)|\phi\rangle &= (|1\rangle|0\rangle\langle 1|\langle 0|)(a_{00}|00\rangle + a_{01}|01\rangle \\ &\qquad + a_{10}|10\rangle + a_{11}|11\rangle) \\ &= a_{00}|1\rangle|0\rangle\langle 10||00\rangle + a_{01}|1\rangle|0\rangle\langle 10||01\rangle \\ &\qquad + a_{10}|1\rangle|0\rangle\langle 10||10\rangle + a_{11}|1\rangle|0\rangle\langle 10||11\rangle \\ &= a_{10}|1\rangle|0\rangle.\end{aligned}$$

General Projection Operators

- Let V be an n-dimensional vector space.
- Let S be an s-dimensional subspace, with basis $\{|\alpha_0\rangle, \ldots, |\alpha_{s-1}\rangle\}$.
- Let P_S be the projection operator onto S.
- Then

$$P_S = \sum_{i=1}^{s-1} |\alpha_i\rangle\langle\alpha_i| = |\alpha_0\rangle\langle\alpha_0| + \cdots + |\alpha_{s-1}\rangle\langle\alpha_{s-1}|.$$

Example: Let a two-qubit system have associated vector space V.

Let

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

represent a state of the two-qubit system.

Let S be the subspace spanned by $|00\rangle$, $|01\rangle$.

General Projection Operators (cont'd)

- The operator

$$P_S = |00\rangle\langle 00| + |01\rangle\langle 01|$$

is the projection operator.

It sends $|\psi\rangle$ to

$$\begin{aligned} P_S|\psi\rangle &= (|00\rangle\langle 00| + |01\rangle\langle 01|)(a_{00}|00\rangle + a_{01}|01\rangle \\ &\qquad + a_{10}|10\rangle + a_{11}|11\rangle) \\ &= a_{00}|00\rangle\langle 00||00\rangle + a_{00}|01\rangle\langle 01||00\rangle \\ &\quad + a_{01}|00\rangle\langle 00||01\rangle + a_{01}|01\rangle\langle 01||01\rangle \\ &\quad + a_{10}|00\rangle\langle 00||10\rangle + a_{10}|01\rangle\langle 01||10\rangle \\ &\quad + a_{11}|00\rangle\langle 00||11\rangle + a_{11}|01\rangle\langle 01||11\rangle \\ &= a_{00}|00\rangle + a_{01}|01\rangle. \end{aligned}$$

Adjoint or Conjugate Transpose

- Let V and W be two vector spaces with inner product.
- The **adjoint operator** or **conjugate transpose** $O^\dagger : V \to W$ of an operator $O : W \to V$ is defined to be the operator that satisfies the following inner product relation.

  For any $\vec{v} \in V$ and $\vec{w} \in W$, the inner product between $O^\dagger \vec{v}$ and $\vec{w}$ in W is the same as the inner product between $\vec{v}$ and $O\vec{w}$ in V:

$$O^\dagger \vec{v} \cdot \vec{w} = \vec{v} \cdot O\vec{w}.$$

- The matrix for the adjoint operator $O^\dagger$ of O is obtained by taking the complex conjugate of all entries and then the transpose of the matrix for O, where we are assuming consistent use of bases for V and W.

Adjoint and Bra/ket Notation

- Recall that $\langle x|$ is the conjugate transpose of $|x\rangle$.
- The reader can check that
$$(A|x\rangle)^\dagger = \langle x|A^\dagger.$$
- In bra/ket notation, the relation between the inner product of $O^\dagger|x\rangle$ and $|w\rangle$ and the inner product of $|x\rangle$ and $O|w\rangle$ is reflected in the notation:
$$(\langle x|O)|w\rangle = \langle x|(O|w\rangle) = \langle x|O|w\rangle.$$

Adjoint and Projections

- By definition, a projection operator is idempotent, i.e., applying it many times in succession has the same effect as just applying it once,
$$PP = P.$$
- Furthermore, any projection operator is its own adjoint,
$$P = P^\dagger.$$
- Thus, for any projection operator P and all $|v\rangle \in V$,
$$|P|v\rangle|^2 = (\langle v|P^\dagger)(P|v\rangle) = \langle v|P|v\rangle.$$

Single-Qubit Measurement in the Standard Basis

- Let V be the vector space associated with a single-qubit system.
- The direct sum decomposition for V associated with measurement in the standard basis is
$$V = S \oplus S',$$
where:
  - S is the subspace generated by $|0\rangle$;
  - S' is the subspace generated by $|1\rangle$.
- The related projection operators are:
  - $P : V \to S$, with $P = |0\rangle\langle 0|$;
  - $P' : V \to S'$, with $P' = |1\rangle\langle 1|$.
- Consider the state
$$|\psi\rangle = a|0\rangle + b|1\rangle.$$
- Measurement of ψ results in the state $\frac{P|\psi\rangle}{|P|\psi\rangle|}$ with probability $|P|\psi\rangle|^2$.

Single-Qubit Measurement in the Standard Basis (Cont'd)

- We have
$$P|\psi\rangle = (|0\rangle\langle 0|)|\psi\rangle = |0\rangle\langle 0|\psi\rangle = a|0\rangle.$$
- Hence
$$\begin{aligned} |P|\psi\rangle|^2 &= \langle\psi|P|\psi\rangle \\ &= \langle\psi|(|0\rangle\langle 0|)|\psi\rangle \\ &= \langle\psi|0\rangle\langle 0|\psi\rangle \\ &= \overline{a}a \\ &= |a|^2. \end{aligned}$$
- So the result of the measurement is $\frac{a|0\rangle}{|a|}$ with probability $|a|^2$.
- Since an overall phase factor is physically meaningless, the state represented by $|0\rangle$ has been obtained with probability $|a|^2$.
- A similar calculation shows that the state represented by $|1\rangle$ is obtained with probability $|b|^2$.

Two-Qubit Measurement in the Standard Basis

- Let V be the vector space associated with a two-qubit system.
- Consider an arbitrary two-qubit state

$$|\phi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle.$$

- Let a measurement have decomposition

$$V = S_{00} \oplus S_{01} \oplus S_{10} \oplus S_{11},$$

  where S_{ij} is the one-dimensional complex subspace spanned by $|ij\rangle$.
- The related projection operators $P_{ij} : V \to S_{ij}$ are:
  - $P_{00} = |00\rangle\langle 00|$;
  - $P_{01} = |01\rangle\langle 01|$;
  - $P_{10} = |10\rangle\langle 10|$;
  - $P_{11} = |11\rangle\langle 11|$.

Two-Qubit Measurement in the Standard Basis (Cont'd)

- The state after measurement will be $\frac{P_{ij}|\psi\rangle}{|P_{ij}|\psi\rangle|}$ with probability $|P_{ij}|\psi\rangle|^2$.
- Recall that:
  - Two unit vectors $|v\rangle$ and $|w\rangle$ represent the same quantum state if
    $$|v\rangle = e^{\boldsymbol{i}\theta}|w\rangle, \quad \text{for some } \theta;$$
  - $|v\rangle \sim |w\rangle$ indicates that $|v\rangle$ and $|w\rangle$ represent the same quantum state.
- In a way similar to the single qubit case, we can determine that the state after measurement is:
  - $\frac{P_{00}|\psi\rangle}{|P_{00}|\psi\rangle|} = \frac{a_{00}|00\rangle}{|a_{00}|} \sim |00\rangle$, with probability $\langle\psi|P_{00}|\psi\rangle = |a_{00}|^2$;
  - $|01\rangle$ with probability $|a_{01}|^2$;
  - $|10\rangle$ with probability $|a_{10}|^2$;
  - $|11\rangle$, with probability $|a_{11}|^2$.

Measuring a Two-Qubit State for Bit Equality

- Let V be the vector space associated with a two-qubit system.
- Consider a measurement with associated direct sum decomposition

$$V = S_1 \oplus S_2,$$

  where:
  - S_1 is the subspace generated by $\{|00\rangle, |11\rangle\}$, the subspace in which the two bits are equal;
  - S_2 is the subspace generated by $\{|10\rangle, |01\rangle\}$, the subspace in which the two bits are not equal.
- Let P_1 and P_2 be the projection operators onto S_1 and S_2 respectively.
- Suppose a system is in state

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle.$$

- After measurement, the state becomes $\frac{P_i|\psi\rangle}{|P_i|\psi\rangle|}$, with probability $|P_i|\psi\rangle|^2 = \langle\psi|P_i|\psi\rangle$.

Measuring a Two-Qubit State for Bit Equality (Cont'd)

- Let
$$\begin{aligned} c_1 &= \langle\psi|P_1|\psi\rangle = \sqrt{|a_{00}|^2 + |a_{11}|^2}; \\ c_2 &= \langle\psi|P_2|\psi\rangle = \sqrt{|a_{01}|^2 + |a_{10}|^2}. \end{aligned}$$
- After measurement the state will be:
  - $|u\rangle = \frac{1}{c_1}(a_{00}|00\rangle + a_{11}|11\rangle)$, with probability $|c_1|^2 = |a_{00}|^2 + |a_{11}|^2$;
  - $|v\rangle = \frac{1}{c_2}(a_{01}|01\rangle + a_{10}|10\rangle)$, with probability $|c_2|^2 = |a_{01}|^2 + |a_{10}|^2$.
- Thus, we know that:
  - If the first outcome happens, the two bit values are equal, but we do not know whether they are 0 or 1;
  - If the second case happens, the two bit values are not equal, but we do not know which one is 0 and which one is 1.
- Thus, the measurement does not determine the value of the two bits, only whether the two bits are equal.

Comments on the Example

- As in the case of single-qubit states, most states are a superposition with respect to a measurement's subspace decomposition.
- In the previous example, the initial state is a superposition containing components with both equal and unequal bit values.
- This is transformed by measurement either to a state (generally still a superposition of standard basis elements), in which in all components the bit values are equal, or to a state in which the bit values are not equal in all of the components.

Two-Qubit State With Respect to the Bell Basis

- Recall the four Bell states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

- Consider the direct sum decomposition of V into the subspaces generated by the Bell states

$$V = S_{\Phi^+} \oplus S_{\Phi^-} \oplus S_{\Psi^+} \oplus S_{\Psi^-}.$$

- Suppose we measue the state $|00\rangle$ with respect to this decomposition.
- Since $|00\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle)$, this yields:
  - $|\Phi^+\rangle$, with probability $\frac{1}{2}$;
  - $|\Phi^-\rangle$, with probability $\frac{1}{2}$.
- We can also determine the outcomes and their probabilities for the three other standard basis elements, and a general two-qubit state.

Subsection 3

Hermitian Operator Formalism for Measurement

Eigenvalues, Eigenvectors and Eigenspaces

- Let $O : V \to V$ be a linear operator.
- Recall that, if
$$O\vec{v} = \lambda\vec{v},$$
for some non-zero vector $\vec{v} \in V$, then λ is an **eigenvalue** and $\vec{v}$ is a λ-**eigenvector** of O.
- If both $\vec{v}$ and $\vec{w}$ are λ-eigenvectors of O, then $\vec{v} + \vec{w}$ is also a λ-eigenvector.
- So the set of all λ-eigenvectors forms a subspace of V.
- It is called the λ-**eigenspace** of O.
- For an operator with a diagonal matrix representation, the eigenvalues are simply the values along the diagonal.

Hermitian Operators

- An operator $O : V \to V$ is **Hermitian** if it is equal to its adjoint,

$$O^\dagger = O.$$

- The eigenspaces of Hermitian operators have special properties.
- Suppose λ is an eigenvalue of an Hermitian operator O.
- Let $|x\rangle$ be a λ-eigenvector.
- We have

$$\lambda\langle x|x\rangle = \langle x|\lambda|x\rangle = \langle x|(O|x\rangle) = (\langle x|O^\dagger)|x\rangle = \overline{\lambda}\langle x|x\rangle.$$

- Hence, $\lambda = \overline{\lambda}$.
- So all eigenvalues of a Hermitian operator are real.

Hermitian Operators and Orthogonal Decompositions

- We show that the eigenspaces $S_{\lambda_1}, S_{\lambda_2}, \ldots, S_{\lambda_k}$ of a Hermitian operator are orthogonal and satisfy

$$S_{\lambda_1} \oplus S_{\lambda_2} \oplus \cdots \oplus S_{\lambda_k} = V.$$

Claim: For any operator, two distinct eigenvalues have disjoint eigenspaces.

Assume $|x\rangle$ is a unit vector.

Suppose $O|x\rangle = \lambda|x\rangle$ and $O|x\rangle = \mu|x\rangle$.

Thus, $(\lambda - \mu)|x\rangle = 0$.

This implies that $\lambda = \mu$.

Hermitian Operators and Decompositions (Cont'd)

Claim: For any Hermitian operator, the eigenvectors for distinct eigenvalues must be orthogonal.

Let $\lambda \neq \mu$ be two eigenvalues.

Let $|v\rangle$ be a λ-eigenvector and $|w\rangle$ is a μ-eigenvector.

Then

$$\lambda\langle v|w\rangle = (\langle v|O^\dagger)|w\rangle = \langle v|(O|w\rangle) = \mu\langle v|w\rangle.$$

By hypothesis, λ and μ are distinct eigenvalues.

So $\langle v|w\rangle = 0$.

Thus, S_{λ_i} and S_{λ_j} are orthogonal for $\lambda_i \neq \lambda_j$.

Hermitian Operators and Decompositions (Cont'd)

Claim: The direct sum of all of the eigenspaces for a Hermitian operator $O : V \to V$ is the whole space V.

A **unitary operator** U satisfies $U^\dagger U = I$.

The columns of a unitary matrix U form an orthonormal set.

If O is Hermitian, then so is UOU^{-1} for any unitary operator U.

Any operator has at least one eigenvalue λ and λ-eigenvector v_λ.

This implies that, for any matrix $A : V \to V$, there is a unitary operator U, such that the matrix for UAU^{-1} is upper triangular.

(That is, all entries below the diagonal are zero).

It follows that, for any Hermitian operator $O : V \to V$, with eigenvalues $\lambda_1, \ldots, \lambda_k$, the direct sum of the λ_i-eigenspaces S_i gives the whole space,

$$V = S_{\lambda_1} \oplus S_{\lambda_2} \oplus \cdots \oplus S_{\lambda_k}.$$

The Eigenspace Decomposition

- Let V be an N-dimensional vector space.
- $O : V \to V$ be an Hermitian operator.
- Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the $k \leq N$ distinct eigenvalues of O.
- We have just shown that

$$V = S_{\lambda_1} \oplus \cdots \oplus S_{\lambda_k},$$

  where S_{λ_i} is the eigenspace of O with eigenvalue λ_i.
- This direct sum decomposition of V is called the **eigenspace decomposition** of V for the Hermitian operator O.
- Thus, any Hermitian operator $O : V \to V$ uniquely determines a subspace decomposition for V.

Arbitrary Decompositions as Eigenspace Decompositions

- Any decomposition of a vector space V into the direct sum of subspaces $S_1, \ldots, S_k$ can be realized as the eigenspace decomposition of a Hermitian operator $O : V \to V$.
- Let P_i be the projectors onto the subspaces S_i.
- Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be any set of distinct real values.
- Then

$$O = \sum_{i=1}^{k} \lambda_i P_i$$

  is a Hermitian operator with the desired direct sum decomposition.
- When describing a measurement, instead of directly specifying the associated subspace decomposition, we can specify a Hermitian operator whose eigenspace decomposition is that decomposition.

Remarks

- It is important to recognize that quantum measurement is not modeled by the action of a Hermitian operator on a state.
- The projectors P_j associated with a Hermitian operator O act on a state.
- The Hermitian operator O itself does not act on a state.
- Which projector acts on the state depends on the probabilities

$$p_j = \langle\psi|P_j|\psi\rangle.$$

Example

- Consider a state
$$|\psi\rangle = a|0\rangle + b|1\rangle.$$
- Suppose we measure it according to the Hermitian operator
$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|.$$
- We do have
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ -b \end{pmatrix}.$$
- However, this does not result in the state $a|0\rangle - b|1\rangle$.

Multiplication by a Hermitian Operator

- Direct multiplication by a Hermitian operator generally does not even result in a well-defined state.

  Example:

$$\begin{aligned}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}|0\rangle &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \end{pmatrix}.\end{aligned}$$

Observables

- As we already saw, given a single instance of an unknown single-qubit state $a|0\rangle + b|1\rangle$, there is no way to determine experimentally what state it is in.
- That is, we cannot directly observe the quantum state.
- It is only the results of measurements that we can directly observe.
- For this reason, the Hermitian operators we use to specify measurements are called **observables**.

The Measurement Postulate

- The *measurement postulate* of quantum mechanics states that:
  - Any quantum measurement can be specified by a Hermitian operator O, called an observable.
  - The possible outcomes of measuring a state $|\psi\rangle$ with an observable O are labeled by the eigenvalues of O.
    Measurement of state $|\psi\rangle$ results in the outcome labeled by the eigenvalue λ_i of O with probability $|P_i|\psi\rangle|^2$, where P_i is the projector onto the λ_i-eigenspace.
  - (Projection) The state after measurement is the normalized projection

$$\frac{P_i|\psi\rangle}{|P_i|\psi\rangle|}$$

    of $|\psi\rangle$ onto the λ_i-eigenspace S_i.
    Thus, the state after measurement is a unit length eigenvector of O with eigenvalue λ_i.

Measuring a Single Qubit in the Standard Basis

- We build up a Hermitian operator that specifies the measurement of a single qubit system in the standard basis.

  The subspace decomposition corresponding to this measurement is

$$V = S \oplus S',$$

  where:
  - S is the subspace generated by $|0\rangle$;
  - S' is the subspace generated by $|1\rangle$.

  The projectors associated with S and S' are $P = |0\rangle\langle 0|$ and $P' = |1\rangle\langle 1|$, respectively.

  Let λ and λ' be any two distinct real values, say $\lambda = 2$ and $\lambda' = -3$.

  Consider the operator

$$O = 2|0\rangle\langle 0| - 3|1\rangle\langle 1| = \begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix}.$$

Measuring a Single Qubit in the Standard Basis (Cont'd)

- O is a Hermitian operator specifying the measurement of a single-qubit state in the standard basis.

  Any other distinct values for λ and λ' could have been used.

  To specify single-qubit measurements in the standard basis, we will generally use either of

$$\begin{aligned} |1\rangle\langle 1| &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \\ Z = |0\rangle\langle 0| - |1\rangle\langle 1| &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned}$$

Measuring a Single Qubit in the Hadamard Basis

- We construct a Hermitian operator corresponding to measurement of a single qubit in the Hadamard basis $\{|+\rangle, |-\rangle\}$.
  The subspaces under consideration are:
  - S_+, generated by $|+\rangle$;
  - S_-, generated by $|-\rangle$.

  They have associated projectors

$$\begin{aligned} P_+ &= |+\rangle\langle+| = \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|); \\ P_- &= |-\rangle\langle-| = \frac{1}{2}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|). \end{aligned}$$

  We are free to choose distinct λ_+ and λ_- any way we like.
  Say we take $\lambda_+ = 1$ and $\lambda_- = -1$.
  Then

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

  is a Hermitian operator for single-qubit measurement in the Hadamard basis.

Example

- Consider the Hermitian operator

$$A = |01\rangle\langle 01| + 2|10\rangle\langle 10| + 3|11\rangle\langle 11|.$$

Take the standard basis in the standard order $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.
Then A has matrix representation

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

The eigenspace decomposition for A consists of four subspaces.
Each subspace is generated by one of the vectors $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.
The operator A is one of many Hermitian operators that specify measurement with respect to the full standard basis decomposition described in a previous example.

Example

- Consider the Hermitian operator

$$B = |00\rangle\langle 00| + |01\rangle\langle 01| + \pi(|10\rangle\langle 10| + |11\rangle\langle 11|) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \pi & 0 \\ 0 & 0 & 0 & \pi \end{pmatrix}.$$

It specifies measurement of a two-qubit system with respect to the subspace decomposition

$$V = S_0 \oplus S_1,$$

where:

- S_0 is generated by $\{|00\rangle, |01\rangle\}$;
- S_1 is generated by $\{|10\rangle, |11\rangle\}$.

So B specifies measurement of the first qubit in the standard basis, as described in a previous example.

Example

- Consider the Hermitian operator

$$C = 2(|00\rangle\langle 00| + |11\rangle\langle 11|) + 3(|01\rangle\langle 01| + |10\rangle\langle 10|) = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

It specifies measurement with respect to the subspace decomposition

$$V = S_2 \oplus S_3,$$

where:

- S_2 is generated by $\{|00\rangle, |11\rangle\}$;
- S_3 is generated by $\{|01\rangle, |10\rangle\}$.

So C specifies the measurement for bit equality, also described in a previous example.

Orthonormal Eigenbases

- Given the subspace decomposition for a Hermitian operator O, it is possible to find an orthonormal eigenbasis of V for O.
- If O has n distinct eigenvalues, as in the general case, the eigenbasis is unique up to length one complex factors.
- If O has fewer than n eigenvalues, some of the eigenvalues are associated with an eigenspace of more than one dimension.
- In this case, a random orthonormal basis can be chosen for each eigenspace S_i.
- The matrix for the Hermitian operator O with respect to any of these eigenbases is diagonal.

Hermitian Operators and Projectors

- Any Hermitian operator O with eigenvalues λ_j can be written as

$$O = \sum_j \lambda_j P_j,$$

  where P_j are the projectors for the λ_j-eigenspaces of O.
- Every projector is Hermitian with eigenvalues 1 and 0 where the 1-eigenspace is the image of the operator.
- Let S be an m-dimensional subspace of V.
- Suppose S is spanned by the basis $\{|i_1\rangle, \ldots, |i_m\rangle\}$.
- The associated projector

$$P_S = \sum_{j=1}^{m} |i_j\rangle\langle i_j|$$

  maps vectors in V into S.

Projectors, Direct Sums and Traces

- Let S and T be orthogonal subspaces of V.
- Let P_S and P_T be projectors for S and T, respectively.
- The projector for the direct sum $S \oplus T$ is

$$P_S + P_T.$$

- Let P be a projector onto a subspace S.
- Then $\text{tr}(P)$, the sum of the diagonal elements of any matrix representing P, is the dimension of S.
- This argument applies to any basis, since the trace is basis independent.

Tensor Product

- Let V and W be vector spaces.
- Let A be a linear operator on V.
- Let B be a linear operator on W.
- The **tensor product**

$$A \otimes B$$

  acts on elements $v \otimes w$ of the tensor product space $V \otimes W$ by

$$(A \otimes B)(v \otimes w) = Av \otimes Bw.$$

- It follows from this definition that

$$(A \otimes B)(C \otimes D) = AC \otimes BD.$$

Tensor Product, Eigenvalues and Eigenspaces

- Let V_0 and V_1 be vector spaces.
- Let O_0 be a Hermitian operator on V_0.
- Let O_1 be a Hermitian operator on V_1.
- Then $O_0 \otimes O_1$ is a Hermitian operator on the space $V_0 \otimes V_1$.
- Suppose O_i has eigenvalues λ_{ij} with associated eigenspaces S_{ij}.
- Then $O_0 \otimes O_1$ has eigenvalues $\lambda'_{jk} = \lambda_{0j}\lambda_{1k}$.
- If an eigenvalue $\lambda'_{jk} = \lambda_{0j}\lambda_{1k}$ is unique, then its associated eigenspace S'_{jk} is the tensor product of S_{0j} and S_{1k}.
- In general, the eigenvalues λ'_{jk} need not be distinct.
- Suppose an eigenvalue λ' of $O_0 \otimes O_1$ that is the product of eigenvalues of O_0 and O_1 in multiple ways, $\lambda' = \lambda'_{j_1 k_1} = \cdots = \lambda'_{j_m k_m}$.
- Then λ' has eigenspace

$$S = (S_{0j_1} \otimes S_{1k_1}) \oplus \cdots \oplus (S_{0j_m} \otimes S_{1k_m}).$$

Hermitian Operators on Tensor Products

- Most Hermitian operators O on $V_0 \otimes V_1$ cannot be written as a tensor product of two Hermitian operators O_0 and O_1 acting on V_0 and V_1, respectively.
- Such a decomposition is possible only if each subspace in the subspace decomposition described by O can be written as

  $$S = S_0 \otimes S_1,$$

  for S_0 and S_1 in the subspace decompositions associated to O_0 and O_1, respectively.
- For most Hermitian operators this condition does not hold.
- However, it does hold for all observables we have described so far.

Example

- Consider the operator

$$\begin{aligned}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} &= (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes (2|0\rangle\langle 0| + 3|1\rangle\langle 1|) \\ &= 2|00\rangle\langle 00| + 3|01\rangle\langle 01| \\ &\qquad - 2|10\rangle\langle 10| - 3|11\rangle\langle 11|.\end{aligned}$$

  This specifies the full measurement in the standard basis.

  However, it uses a different Hermitian operator from the one used in a previous example for the same purpose.

Example

- Consider the operator

$$\begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = |00\rangle\langle 00\rangle + |01\rangle\langle 01| + \pi(|10\rangle\langle 10| + |11\rangle\langle 11|).$$

  It specifies measurement of the first qubit in the standard basis, as described in a previous example.

  The same role is played by

$$Z \otimes I,$$

  where $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.

Example

- Consider the Hermitian operator

$$Z \otimes Z = |00\rangle\langle 00| - |01\rangle\langle 01| - |10\rangle\langle 10| + |11\rangle\langle 11|.$$

It specifies the measurement for bit equality, also described in a previous example.

A Non-Tensor Two-Qubit Measurement

- We now give an example of a two-qubit measurement that cannot be expressed as the tensor product of two single-qubit measurements.
- This shows that not all measurements are tensor products of single qubit measurements.
- Consider a two-qubit state.
- Let M be the observable, with matrix representation

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

- M determines whether both bits are set to one.

A Non-Tensor Two-Qubit Measurement (Cont'd)

- Measurement with the operator M results in a state contained in one of the two subspaces S_0 and S_1, where:
  - S_1 is the subspace spanned by $\{|11\rangle\}$;
  - S_0 is spanned by $\{|00\rangle, |01\rangle, |10\rangle\}$.
- Measuring with M is quite different from measuring both qubits in the standard basis and then performing the classical AND operation.
- E.g., consider the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle).$$

  - It remains unchanged when measured with M.
  - Measuring both qubits of $|\psi\rangle$ would result in either the state $|01\rangle$ or $|10\rangle$.

Measurements on Single Qubits and on Subsystems

- Any Hermitian operator $Q_1 \otimes Q_2$ on a two-qubit system is said to be **composed of single-qubit measurements** if Q_1 and Q_2 are Hermitian operators on the single-qubit systems.
- Furthermore, any Hermitian operator of the form $Q \otimes I$ or $I \otimes Q'$ on a two-qubit system is said to be a **measurement on a single qubit** of the system.
- More generally, a Hermitian operator of the form

$$I \otimes \cdots \otimes I \otimes Q \otimes I \otimes \cdots \otimes I$$

  on an n-qubit system is said to be a **single-qubit measurement** of the system.
- Any Hermitian operator of the form $A \otimes I$ on a system $V \otimes W$, where A is a Hermitian operator acting on V, is said to be a **measurement of subsystem V**.

Distinguishing Two Decompositions

- Suppose we are measuring an n-qubit system.
- There are two totally distinct types of decompositions of the vector space V under consideration:
  - The tensor product decomposition into the n separate qubits;
  - The direct sum decomposition into $k \leq 2^n$ subspaces associated with the measuring device.
- These decompositions could not be more different.
- In particular, a tensor component V_i of $V = V_1 \otimes \cdots \otimes V_n$ is not a subspace of V.
- Similarly, the subspaces associated with measurements do not correspond to the subsystems, such as individual qubits, of the whole system.

Measuring n-Qubit Systems

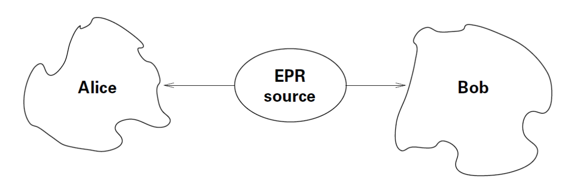
- We mentioned that only one classical bit of information can be extracted from a single qubit.
- We can now both generalize this statement and make it more precise.
- Any observable on an n-qubit system has $\leq 2^n$ distinct eigenvalues.
- So there are at most 2^n possible results of a given measurement.
- Thus, a single measurement of an n-qubit system will reveal at most n bits of classical information.
- In general, the measurement changes the state.
- So any further measurements give information about the new state, not the original one.

Subsection 4

EPR Paradox and Bell's Theorems

Bohm's Experiment

- Imagine a source that:
  - Generates EPR pairs $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$;
  - Sends the first particle to Alice;
  - Sends the second particle to Bob.



- Alice and Bob can be arbitrarily far apart.
- Each person can measure only the particle he or she receives.
- More precisely, for O and O' single-qubit observables:
  - Alice can use only observables of the form $O \otimes I$;
  - Bob can use only observables of the form $I \otimes O'$.

Bohm's Experiment (Cont'd)

- Suppose Alice measures her particle in the standard single-qubit basis and observes the state $|0\rangle$.
- The effect of this measurement is to project the state of the quantum system onto that part of the state compatible with the results of Alice's measurement.
- So the combined state will now be $|00\rangle$.
- Suppose Bob now measures his particle.
- He will always observe $|0\rangle$.
- Thus it appears that Alice's measurement has affected the state of Bob's particle.
- Similarly, if Alice measures $|1\rangle$, so will Bob.

Bohm's Experiment (Cont'd)

- By symmetry, if Bob were to measure his qubit first, Alice would observe the same result as Bob.
- When measuring in the standard basis, Alice and Bob will always observe the same results, regardless of the relative timing.
- The probability that either qubit is measured to be $|0\rangle$ is $\frac{1}{2}$.
- However, the two results are always correlated.

EPR (Einstein, Podolsky, Rosen) Paradox

- Suppose the measurements are **relativistically spacelike separated**:
  - The particles are far enough apart;
  - The measurements happen close in time.
- It may then sound as if an interaction between these particles is happening faster than the speed of light.
- We said earlier that a measurement performed by Alice appears to affect the state of Bob's particle, but this wording is misleading.
- Following special relativity, it is incorrect to think of one measurement happening first and causing the results of the other.
- It is possible to set up the EPR scenario so that:
  - One observer sees Alice measure first, then Bob;
  - Another observer sees Bob measure first, then Alice.
- According to relativity, physics must explain equally well the observations of both observers.

Randomness and Correlation

- The causal terminology we used cannot be compatible with both observers' observations.
- The actual experimental values are invariant under change of observer.
- The experimental results can be explained equally well by Bob measuring first and then Alice as the other way around.
- This symmetry shows, while there is correlation between the two particles, Alice and Bob cannot use their EPR pair to communicate faster than the speed of light.
- All that can be said is that Alice and Bob will observe *correlated random behavior*.

Randomness and Correlation (Cont'd)

- Even though the results themselves are perfectly compatible with relativity theory, the behavior remains mysterious.
- Suppose Alice and Bob had a large number of EPR pairs that they measure in sequence.
- Then they would see an odd mixture of correlated and probabilistic results.
  - Each of their sequences of measurements appears completely random;
  - But if Alice and Bob compare their results, they see that they witnessed the same random sequence from their two separate particles.
- Their sequence of entangled pairs behaves like a pair of magic coins.
  - They always land the same way up when tossed together;
  - But whether they both land heads or both land tails is completely random.

Local Hidden Variable Theories

- So far, quantum mechanics is not the only theory that can explain these results.
- They could also be explained by a classical theory that postulates that:
  - Particles have an internal **hidden state** that determines the result of the measurement;
  - This hidden state is:
    - Identical in two particles generated at the same time by the EPR source;
    - Varies randomly over time as the pairs are generated.
- Such theories are known as **local hidden variable theories**.

Local Hidden Variable Theories (Cont'd)

- According to local hidden variable theories, the reason we see random, instead of deterministic, results is simply because we, as of yet, have no way of accessing the hidden states.
- The hope of proponents of such theories was that, eventually, physics would advance to a stage in which this hidden state would be known to us.
- The local part comes from the assumption that the hidden variables are internal to each of the particles and do not depend on external influences.
- In particular, the hidden variables do not depend on the state of faraway particles or measuring devices.

Limitations of Local Hidden Variable Theories

- Is it possible to construct a local hidden variable theory that agrees with all of the experimental results we use quantum mechanics to model?
- The answer is "no".
- Bell's work of 1964 made it possible to construct experiments that could distinguish quantum mechanics from all local hidden variable theories.
- Since then such experiments have been done, and all of the results have agreed with those predicted by quantum mechanics.
- Thus, no local hidden variable theory can explain how nature works.
- Bell showed that any local hidden variable theory predicts results that satisfy an inequality, known as **Bell's inequality**.

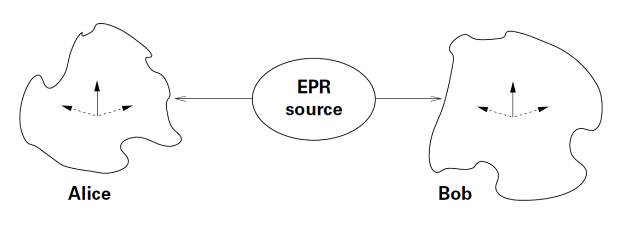
Setup for Bell's Theorem

- Imagine an EPR source that emits pairs of photons whose polarizations are in an entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\rightarrow\rightarrow\rangle),$$

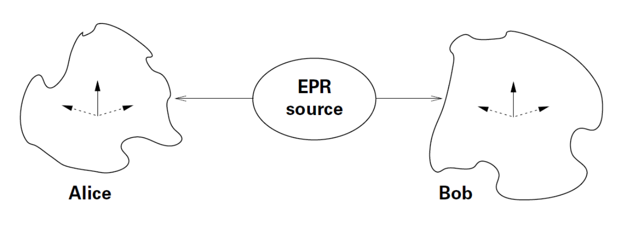
where we are using the notation $|\uparrow\rangle$ and $|\rightarrow\rangle$ for photon polarization.

- We suppose that the two photons travel in opposite directions.
- Each is raveling towards a polaroid (polarization filter).



Setup for Bell's Theorem (Cont'd)

- The polaroids can be set at three different angles.



- In the special case we consider first, the polaroids can be set to:
  - Vertical;
  - $+60^\circ$ off vertical;
  - -60° off vertical.

Quantum-Mechanical Predictions

- Let O_θ be a single-qubit observable with:
  - 1-eigenspace generated by $|v\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$;
  - -1-eigenspace generated by $|v^\perp\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle$.
- Suppose we measure the state $|\psi\rangle$ using $O_{\theta_1} \otimes O_{\theta_2}$.
- Quantum mechanics predicts this results in a state with eigenvalue 1 with probability $\cos^2(\theta_1 - \theta_2)$.
- In other words, we can show that the probability that the state ends up in the subspace generated by $\{|v_1\rangle|v_2\rangle, |v_1^\perp\rangle|v_2^\perp\rangle\}$, and not the -1-eigenspace generated by $\{|v_1\rangle|v_2^\perp\rangle, |v_1^\perp\rangle|v_2\rangle\}$, is $\cos^2(\theta_1 - \theta_2)$.

Polaroids and Observables

- We use the following notation.
  - $M_{\nearrow}$ for the observable corresponding to the -60° setting;
  - $M_{\uparrow}$ for the observable corresponding to the vertical setting;
  - $M_{\nwarrow}$ for the observable corresponding to the $+60^\circ$ setting.
- Each observable has two possible outcomes.
  - Outcome P, in which the photon passes through the polaroid;
  - Outcome A, in which the photon is absorbed by the polaroid.

Polaroids, Observables and Probabilities

- Measurement with observable $O_{\theta_1} \otimes O_{\theta_2}$ results in a state with eigenvalue 1 with probability $\cos^2(\theta_1 - \theta_2)$.
- We can compute the probability that measurement of two photons, by polaroids set at angles θ_1 and θ_2, give the same result, PP or AA.
- Suppose both polaroids are set at the same angle.

  Both photons will pass through or both will be absorbed.

  So both photon measurements give the same results with probability $\cos^2 0 = 1$.
- Suppose the polaroid on the right is set to vertical, and the one on the left is set to $+60^\circ$.

  Then both measurements agree with probability $\cos^2 60 = \frac{1}{4}$.

Polaroids, Observables and Probabilities (Cont'd)

- Assume the two polaroids are not set at the same angle.
- The difference between the angles is either 60 or 120 degrees.
- So in all of these cases the two measurements:
  - Agree $\frac{1}{4}$ of the time;
  - Disagree $\frac{3}{4}$ of the time.
- Suppose the polaroids are set randomly for a series of EPR pairs emanating from the source.
  - With probability $\frac{1}{3}$ the polaroid orientation will be the same and the measurements will agree.
  - With probability $\frac{2}{3}$ the polaroid orientation will differ and the measurements will agree with probability $\frac{1}{4}$.
- Thus, overall, the measurements will agree with probability $\frac{1}{3} + \frac{2}{3} \cdot \frac{1}{4} = \frac{1}{2}$ and disagree half the time.
- These are indeed the probabilities observed experimentally.

Predictions of Hidden-Variable Theory

- We show that no local hidden variable theory can give these probabilities.
- Suppose there is some hidden state associated with each photon that determines the result of measuring the photon with a polaroid in each of the three possible settings.
- There are only 2^3 binary combinations in which these states can respond to measurement by polaroids in the 3 orientations.
- We label these 8 possibilities $h_0, \ldots, h_7$, as shown in the table on the right.

	$\nearrow$	$\uparrow$	$\nwarrow$
h_0	P	P	P
h_1	P	P	A
h_2	P	A	P
h_3	P	A	A
h_4	A	P	P
h_5	A	P	A
h_6	A	A	P
h_7	A	A	A

Predictions of Hidden-Variable Theory (Cont'd)

- We can think of h_i as the equivalence class of all hidden states, however these might look, that give the indicated measurement results.
- Experimentally, it has been established that both polaroids, when set at the same angle, always give the same result when measuring the photons of an EPR pair $|\psi\rangle$.
- Suppose a local hidden variable theory models experimental results.
- Then it must predict that both photons of the entangled pair are in the same equivalence class of hidden states h_i.
- For example, if the photon on the right responds to the three polaroid positions $\nearrow, \uparrow, \nwarrow$ with PAP, then so must the photon on the left.

Predictions of Hidden-Variable Theory (Cont'd)

- Now consider the 9 possible combinations of orientations of the two polaroids
$$\{(\nearrow,\nearrow),(\nearrow,\uparrow),\ldots,(\nwarrow,\nwarrow)\}.$$
- We calculate the expected agreement of the measurements for photon pairs in each hidden state h_i.
- Consider hidden states h_0 and h_7 ($\{\mathrm{PPP},\mathrm{PPP}\}$ and $\{\mathrm{AAA},\mathrm{AAA}\}$).

  Measurements agree for all possible pairs of orientations.

  So we get 100 percent agreement.
- Consider the hidden state h_1, $\{\mathrm{PPA},\mathrm{PPA}\}$.

  Measurements agree in five of the nine possible orientations and disagree in the others.

  We get $\frac{5}{9}$ agreement and $\frac{4}{9}$ disagreement.

Predictions of Hidden-Variable Theory (Cont'd)

- The other six cases are similar to h_1.
  We get $\frac{5}{9}$ agreement and $\frac{4}{9}$ disagreement.
- No matter with what probability distribution the EPR source emits photons with hidden states, the expected agreement between the two measurements will be at least $\frac{5}{9}$.
- Thus, no local hidden variable theory can give the 50-50 agreement predicted by quantum theory and seen in experiments.

Setup for Bell's Inequality

- A sequence of EPR pairs emanate from a photon source toward two polaroids.
- The polaroids can be set at any triple of three distinct angles a, b and c.
- We record the results of repeated measurements at random settings of the polaroids, chosen among a, b and c.
- We count the number of times that the measurements match for any pair of settings.

Probabilities

- Let P_{xy} denote the sum of the observed probability that either of the following happens:
  - The two photons interact in the same way with both polaroids (either both pass through, or both are absorbed) when the first polaroid is set at angle x and the second at angle y;
  - The two photons interact in the same way with both polaroids when the first polaroid is set at angle y and the second at angle x.
- Whenever the two polaroids are on the same setting, the measurement of the photons will always give the same result.
- So, we have $P_{xx} = 1$, for any setting x.

Bell's Inequality

- We now show that the **Bell's inequality**

$$P_{ab} + P_{ac} + P_{bc} \geq 1$$

  holds for any local hidden variable theory and any sequence of settings for each of the polaroids.
- We show that the inequality holds for the probabilities associated with any one equivalence class of hidden states.
- From this, we deduce that it holds for any distribution of these equivalence classes.
- According to any local hidden variable theory, the result of measuring a photon by a polaroid in each of the three possible settings is determined by a local hidden state h of the photon.
- Again, we think of h as an equivalence class of all hidden states that give the indicated measurement results.

Bell's Inequality (Cont'd)

- We know that both polaroids, when set at the same angle, always give the same result when measuring the photons in an EPR state $|\psi\rangle$.
- This means that both photons of the entangled pair must be in the same equivalence class of hidden states h.
- E.g., if the photon on the right responds to the three polaroid positions a, b, c with PAP, then so must the photon on the left.

Bell's Inequality (Cont'd)

- Let P_{xy}^h be 1 if the result of the two measurements agree on states with hidden variable h, and 0 otherwise.
- Any measurement has only two possible results, P and A.
- So the result of measuring a photon, with a given hidden state h, in each of the three polaroid settings, a, b and c, will be the same for at least one of the settings.
- Moreover, the two photons of state $|\psi\rangle$ are in the same hidden state.
- It follows that, for any h,

$$P_{ab}^h + P_{ac}^h + P_{bc}^h \geq 1.$$

Bell's Inequality (Cont'd)

- Let w_h be the probability with which the source emits photons of kind h.
- Then the sum of the observed probabilities $P_{ab} + P_{ac} + P_{bc}$ is a weighted sum, with weights w_h, of the results for photons of each hidden kind h:

$$P_{ab} + P_{ac} + P_{bc} = \sum_h w_h (P_{ab}^h + P_{ac}^h + P_{bc}^h).$$

- The weighted average of numbers all greater than 1 is greater than 1.
- So, since $P_{ab}^h + P_{ac}^h + P_{bc}^h \geq 1$, for any h, we may conclude that

$$P_{ab} + P_{ac} + P_{bc} \geq 1.$$

- This inequality holds for any local hidden-variable theory and gives us a testable requirement.

Discussion

- Quantum theory predicts that the probability that the two results will be the same is the square of the cosine of the angle between the two polaroid settings.
- Suppose that the angle between settings a and b is θ.
- Suppose that the angle between settings b and c is ϕ.
- Then the inequality becomes

$$\cos^2\theta + \cos^2\phi + \cos^2(\theta+\phi) \geq 1.$$

Discussion (Cont'd)

- Consider the special case of the previous section.
- Quantum theory tells us that for $\theta = \phi = 60^\circ$, each term is $\frac{1}{4}$.
- Since $\frac{3}{4} < 1$, these probabilities violate Bell's inequality.
- Therefore, no local, deterministic theory can give the same predictions as quantum mechanics.
- Experimental results confirm the prediction of quantum theory and nature's violation of Bell like inequalities.