Complex Numbers

Lecture 1

Number systems

- Positive numbers, $P = \{1,2,3,\ldots\}$
- Natural numbers, $N = \{0,1,2,3,\ldots\}$
- Integers (or whole numbers), $Z = \{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$
- Rational numbers, $Q = \left\{ \frac{m}{n} \middle| m \in Z, n \in P \right\}$
- Real numbers, $R = Q \cup \left\{ \ldots, \sqrt{2}, \ldots, e, \ldots, \pi, \ldots, \frac{e}{\pi}, \ldots \right\}$
- New system: complex numbers

Imaginary numbers

$$x^2 + 1 = 0;\ x?$$
$$\Downarrow$$
$$x^2 = -1$$
$$\downarrow \textit{postulate}$$
$$i^2 = -1 \quad \text{or} \quad i = \sqrt{-1}$$

$$\text{Imaginary numbers}: a \times i, a \in R$$

Complex numbers

$$c = a + b \times i = a + bi, \text{ where } a, b \in R$$

real part

imaginary part

$$\text{set of complex numbers}: C$$

Algebra of complex numbers

Definition : $c \mapsto (a,b)$ ordered pair of reals

real numbers : $a \mapsto (a,0)$

imaginary numbers : $b \mapsto (0,b)$, e.g. $i \mapsto (0,1)$

Addition : $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

Multiplication : $(a_1, b_1) \times (a_2, b_2) = (a_1, b_1)(a_2, b_2) =$
$= (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1)$

Algebra (cont'd)

- Addition and multiplication are **commutative:**
  $c_1 + c_2 = c_2 + c_1$ and $c_1 \times c_2 = c_2 \times c_1$
- They are also **associative**:
  $(c_1 + c_2) + c_3 = c_1 + (c_2 + c_3)$ and $(c_1 \times c_2) \times c_3 = c_1 \times (c_2 \times c_3)$
- Multiplication **distributes** over addition:
  $c_1 \times (c_2 + c_3) = (c_1 \times c_2) + (c_1 \times c_3)$

Algebra (cont'd)

$$\text{Subtraction}: c_1 - c_2 = (a_1, b_1) - (a_2, b_2) = (a_1 - a_2, b_1 - b_2)$$

$$\text{Division}: (x, y) = \frac{(a_1, b_1)}{(a_2, b_2)}$$

$$\Rightarrow (a_1, b_1) = (x, y) \times (a_2, b_2) = (a_2 x - b_2 y, a_2 y + b_2 x)$$

So (1) $a_1 = a_2 x - b_2 y \quad \times a_2 \Rightarrow$ (1') $a_1 a_2 = a_2^{\,2} x - b_2 a_2 y$

(2) $b_1 = a_2 y + b_2 x \quad \times b_2 \Rightarrow$ (2') $b_1 b_2 = a_2 b_2 y + b_2^{\,2} x$

(1')+(2') $a_1 a_2 + b_1 b_2 = (a_2^{\,2} + b_2^{\,2})x \quad \Rightarrow x = \dfrac{a_1 a_2 + b_1 b_2}{a_2^{\,2} + b_2^{\,2}}$

In the way: (1)$\times b_2$ + (2)$\times -a_2 \quad \Rightarrow y = \dfrac{a_2 b_1 - a_1 b_2}{a_2^{\,2} + b_2^{\,2}}$

Algebra (cont'd)

- Absolute value for real numbers:

$$|a| = +\sqrt{a^2}$$

- Generalization for complex numbers:

$$|c| = |a + bi| = +\sqrt{a^2 + b^2}$$

modulus of a complex number

Algebra (cont'd)

$$|c_1||c_2| = |c_1 c_2|$$

$$|c_1 + c_2| \le |c_1| + |c_2|$$

$$c + (0,0) = (0,0) + c = c \quad \Rightarrow \quad (0,0) \text{ is additive identity}$$

$$c \times (1,0) = (1,0) \times c = c \quad \Rightarrow \quad (1,0) \text{ is multiplicative identity}$$

Algebra (cont'd)

- Summarizing, defined a set of numbers *C* with 4 operations and following properties:
  1) Addition is commutative and associative
  2) Multiplication is commutative and associative
  3) Addition has identity: (0,0)
  4) Multiplication has identity: (1,0)
  5) Multiplication distributes with respect to addition
  6) Subtraction (i.e., inverse of addition) is defined everywhere
  7) Division (i.e., inverse of multiplication) is defined everywhere except when the divisor is zero.
- → *C* is a
  - **field**
  - **algebraically complete:** contains all solutions for any of its polynominal equations (*R* is not)

Algebra (cont'd)

- Unary operation 'changing sign':
  1) change the sign of the real part
  2) change the sign of the imaginary part
  3) change both
- 3) is obtained by multiplication with (-1,0)
- What about 2) and 1)?

Algebra (cont'd)

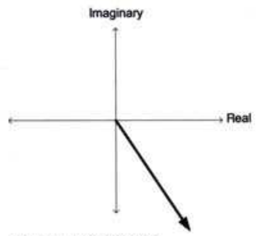
- **Conjugation**

  The conjugate of $c = a + bi$ is $\bar{c} = a - bi$.
- Properties:

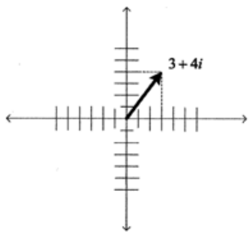
$$\left.\begin{array}{l} \text{Conjugation respects addition}: \overline{c_1} + \overline{c_2} = \overline{c_1 + c_2} \\ \text{Conjugation respects multiplication}: \overline{c_1} \times \overline{c_2} = \overline{c_1 \times c_2} \\ \text{Conjugation } c \mapsto \bar{c} \text{ is bijective} \end{array}\right\} \text{field isomorphism}$$

- Changing the sign of the real part has no particular name.

Geometry of complex numbers



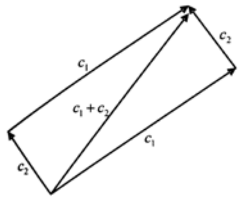
Complex or Argand plane



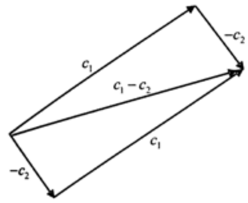
Vector $3 + 4i$

Modulus is the length of the vector

Geometry (cont'd)



Addition: **Parallelogram rule**

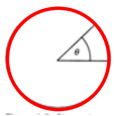


Subtraction

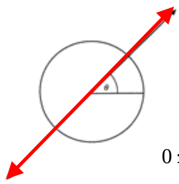
Geometry (cont'd)

- Cartesian representation (a,b)
- Polar representation (ρ,θ), where ρ represents the modulus/magnitude, and θ is called the angle/phase

$\rho \geq 0$



Points with same ρ



$0 \leq \theta < 2\pi$

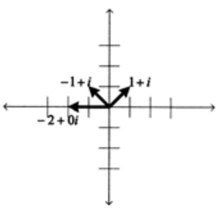
Points with same θ

Geometry (cont'd)

$$\text{From Cartesian} \rightarrow \text{polar} \quad \begin{cases} \rho = \sqrt{(a^2+b^2)} \\ \theta = \tan^{-1}\left(\frac{b}{a}\right) \end{cases}$$

$$\text{From polar} \rightarrow \text{Cartesian} \quad \begin{cases} a = \rho\cos(\theta) \\ b = \rho\sin(\theta) \end{cases}$$

Geometry (cont'd)



$$\text{Multiplication}: (\rho_1,\theta_1)\times(\rho_2,\theta_2) = (\rho_1\rho_2, \theta_1+\theta_2)$$

Errata chapter 1

1. Page. xv. Section ACKNOLWEDGMENTS should be ACKNOWLEDGEMENTS. Alex Sverdlov, 10/26/2008.

2. Page 325: Equation (B.3) should be

$$\begin{aligned} |c_1||c_2| &= \sqrt{a_1^2+b_1^2}\sqrt{a_2^2+b_2^2} = \sqrt{(a_1^2+b_1^2)(a_2^2+b_2^2)} \\ &= \sqrt{a_1^2a_2^2+b_1^2a_2^2+b_1^2b_2^2+a_1^2b_2^2} = \sqrt{(\mathbf{a_1a_2-b_1b_2})^2+(a_1b_2+a_2b_1)^2} \\ &= |(\mathbf{a_1a_2-b_1b_2}, a_1b_2+a_2b_1)| = |c_1c_2|. \end{aligned}$$

Reading

- This lecture: chapter 1, p 7-20
- Next lecture (next week?):
  chapter 2   Complex Vector Spaces

Complex Vector Spaces

Lecture 2

C^n as an example

$\mathbb{C}$

- $C^4 = C \times C \times C \times C$, the vectors of length 4
- E.g. $V = \begin{bmatrix} 6-4i \\ 7+3i \\ 4.2-8.1i \\ -3i \end{bmatrix}$, where $V[1] = 7+3i$ (start with 0 as index)
- Addition $(V + W)[j] = V[j] + W[j]$
  - Commutative $V + W = W + V$
  - Associative $(V + W) + X = V + (W + X)$
  - Zero vector $V + \mathbf{0} = \mathbf{0} + V = V$
  - (Additive) inverse or negative $W + (-W) = (-W) + W = \mathbf{0}$

  Set with these properties is called an Abelian group.

Complex vector space

- Complex number c (a scalar)
- Multiplication of a scalar and a vector $(c \cdot V)[j] = c \times V[j]$, where x is the complex multiply
- Properties
  - $1 \cdot V = V$
  - $c_1 \cdot (c_2 \cdot V) = (c_1 \times c_2) \cdot V$
  - $c \cdot (V + W) = c \cdot V + c \cdot W$
  - $(c_1 + c_2) \cdot V = c_1 \cdot V + c_2 \cdot V$

  An Abelian group with these properties is called a complex vector space.

Formal definition

A complex vector space is a nonempty set **V**, whose elements we call vectors, with three operations
- Addition: $+ : \mathbf{V} \times \mathbf{V} \to \mathbf{V}$
- Negation: $- : \mathbf{V} \to \mathbf{V}$
- Scalar multiplication: $\cdot : \mathbf{C} \times \mathbf{V} \to \mathbf{V}$

and a distinguished element called the zero vector **0**.

They must satisfy the following properties:
i. Commutativity of addition: $V + W = W + V$
ii. Associativity of addition: $(V + W) + X = V + (W + X)$
iii. Zero is an additive identity: $V + \mathbf{0} = V = \mathbf{0} + V$
iv. Every vector has an inverse: $V + (-V) = \mathbf{0} = (-V) + V$
v. Scalar multiplication has a unit: $1 \cdot V = V$
vi. Scalar multiplication respects complex multiplication: $c_1 \cdot (c_2 \cdot V) = (c_1 \times c_2) \cdot V$
vii. Scalar multiplication distributes over addition: $c \cdot (V + W) = c \cdot V + c \cdot W$
viii. Scalar multiplication distributes over complex addition: $(c_1 + c_2) \cdot V = c_1 \cdot V + c_2 \cdot V$

Properties i, ii, iii, and iv: Abelian group;
all properties: complex vector space.

Real vector space

A real vector space is a nonempty set V, analogue to a complex vector space, but there is a scalar multiplication that uses R and not C, i.e.,

$\cdot : R \times V \to V.$

This set and these operations must satisfy the analogous properties of a complex vector space.

C^n

- C^n, the set of vectors of length n with complex entries, will be complex vector space that serves as primary example for the class.
- It is also a real vector space, because every complex vector space is also a real vector space.
- R^n, the set of vectors of length n with real entries, is a real vector space.

$C^{m \times n}$

- $C^{m \times n}$, the set of all m-by-n matrices with complex entries, is a complex vector space.
- $A \in C^{m \times n}$ $A = \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,n-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{0,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m-1,0} & c_{m-1,1} & \cdots & c_{m-1,n-1} \end{bmatrix}$
- Addition: $(A + B)[j,k] = A[j,k] + B[j,k]$
- Inverse: $(-A)[j,k] = -(A[j,k])$
- Scalar multiplication: $(c \cdot A)[j,k] = c \times A[j,k]$

Operations on matrices

- The transpose of A, denoted A^T, is defined as

  $A^T[j,k] = A[k,j]$

- The conjugate of A, denoted $\overline{A}$, is defined as

  $\overline{A}[j,k] = \overline{A[j,k]}$

- Combined gives this the adjoint or dagger operation $A^\dagger$, defined as

  $A^\dagger = (\overline{A})^T = \overline{(A^T)}$ or $A^\dagger[j,k] = \overline{A[k,j]}$

Properties

- Transpose is idempotent: $(A^T)^T = A$
- Transpose respects addtion: $(A + B)^T = A^T + B^T$
- Transpose respects scalar multiplication: $(c \cdot A)^T = c \cdot A^T$

- Conjugate is idempotent: $\overline{\overline{A}} = A$
- Conjugate respects addtion: $\overline{A + B} = \overline{A} + \overline{B}$
- Conjugate respects scalar multiplication: $\overline{c \cdot A} = \overline{c} \cdot \overline{A}$

- Adjoint is idempotent: $(A^\dagger)^\dagger = A$
- Adjoint respects addtion: $(A + B)^\dagger = A^\dagger + B^\dagger$
- Adjoint respects scalar multiplication: $(c \cdot A)^\dagger = \overline{c} \cdot A^\dagger$

Matrix multiplication

- Matrix multiplication is a binary operation

  $$* : C^{m \times n} \times C^{n \times p} \rightarrow C^{m \times p}$$

- Formally

  $$(A * B)[j,k] = \sum_{h=0}^{n-1} (A[j,h] \times B[h,k])$$

- When it is clear * will be omitted.

Properties of matrix multiplication

- Associative: $(A * B) * C = A * (B * C)$
- I_n as unit: $I_n * A = A = A * I_n$ with I_n identity matrix
- Distributes over addition:
  $A * (B + C) = (A * B) + (A * C)$
  $(B + C) * A = (B * A) + (C * A)$
- Respects scalar multiplication:
  $c \cdot (A * B) = (c \cdot A) * B = A * (c \cdot B)$
- Relates to the transpose: $(A * B)^T = B^T * A^T$
- Respects the conjugate: $\overline{A * B} = \overline{A} * \overline{B}$
- Relates to the adjoint: $(A * B)^\dagger = B^\dagger * A^\dagger$
- Note: commutativity is not a basic property!
- A complex vector space V with a multiplication * that satisfies the first four properties is called a complex algebra.

Complex subspace

- Given two complex vector spaces V and V', we say that V is a complex subspace of V' if V is a subset of V and the operations of V are restrictions of operations of V'.

Linear map/operator/isomorphism

- Let V and V' be two complex vector spaces. A linear map from V to V' is a function f : V → V' such that
  - *f* respects addition: $f(V_1+V_2) = f(V_1) + f(V_2)$
  - *f* respects the scalar multiplication: $f(c\cdot V) = c\cdot f(V)$

- A linear map from a complex vector space to itself is called an operator. If $F(V) = A^*V$ is an operator, we say that F is represented by A.

- Two complex vector spaces V and V' are isomorphic if there is a one-to-one linear map f : V → V'. Such a map is called an isomorphism. When two vector spaces are isomorphic, it means that the names of the elements of the vector spaces are renamed but the structure of the two spaces are the same. Two such vector spaces are "essentially the same".

Basis

- Linear combination:
  $V = c_0 \cdot V_0 + c_1 \cdot V_1 + \cdots + c_{n-1} \cdot V_{n-1}$.

- Linearly independent if
  $\mathbf{0} = c_0 \cdot V_0 + c_1 \cdot V_1 + \cdots + c_{n-1} \cdot V_{n-1}$
  implies that $c_0 = c_1 = \cdots = c_{n-1} = 0$.

  Is equivalent that for any nonzero V there are unique coefficients $c_0, c_1, \cdots, c_{n-1}$ such that
  $V = c_0 \cdot V_0 + c_1 \cdot V_1 + \cdots + c_{n-1} \cdot V_{n-1}$.

- A set B = $\{V_0, V_1, \ldots, V_{n-1}\}$ of vectors is called a basis of a (complex) vector space V if both
  i. Every V can be written as a linear combination of vectors from B
  ii. B is linearly independent.

Canonical or standard basis

- R^3: $\left\{ \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix} \right\}$

- C^n (and R^n): $E_0 = \begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}, \; E_1 = \begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix}, \ldots, \; E_{n-2} = \begin{bmatrix}0\\\vdots\\1\\0\end{bmatrix}, \; E_{n-1} = \begin{bmatrix}0\\\vdots\\0\\1\end{bmatrix}.$

- See book for matrices and others.

Dimension

- Bases for R^3, e.g.:

$$\left\{ \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix} \right\} \qquad \left\{ \begin{bmatrix}1\\1\\1\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix} \right\} \qquad \left\{ \begin{bmatrix}1\\0\\-1\end{bmatrix}, \begin{bmatrix}2\\1\\2\end{bmatrix}, \begin{bmatrix}3\\-2\\0\end{bmatrix} \right\}$$

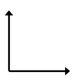
- For every vector space, every basis has the same number of vectors. This is called the dimension of the vector space.

Transition matrix

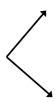
- A change of basis matrix or a transition matrix from basis B to basis D is a matrix $M_{D \leftarrow B}$ such that for any vector V we have

$$V_D = M_{D\leftarrow B} * V_B$$

- Important example: Hadamard matrix



$$\Leftarrow \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} = \begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{bmatrix} \quad \Rightarrow$$



Inner product

Inner product (or dot product or scalar product) on a complex vector space V is a function

$$\langle -,- \rangle : \mathbf{V} \times \mathbf{V} \to \mathbf{C}$$

satisfying the following conditions

i. Nondegenerate $\langle \mathbf{V},\mathbf{V}\rangle \geq 0,$
$\langle \mathbf{V},\mathbf{V}\rangle = \mathbf{0}$ if and only if $\mathbf{V} = \mathbf{0}$

ii. Respects addition $\langle \mathbf{V}_1 + \mathbf{V}_2, \mathbf{V}_3\rangle = \langle \mathbf{V}_1, \mathbf{V}_3\rangle + \langle \mathbf{V}_2, \mathbf{V}_3\rangle,$
$\langle \mathbf{V}_1, \mathbf{V}_2 + \mathbf{V}_3\rangle = \langle \mathbf{V}_1, \mathbf{V}_2\rangle + \langle \mathbf{V}_1, \mathbf{V}_3\rangle.$

iii. Respects scalar multiplication $\langle c \cdot \mathbf{V}_1, \mathbf{V}_2\rangle = \bar{c} \times \langle \mathbf{V}_1, \mathbf{V}_2\rangle,$
$\langle \mathbf{V}_1, c\cdot \mathbf{V}_2\rangle = c \times \langle \mathbf{V}_1, \mathbf{V}_2\rangle.$

iv. Skew symmetric
$\langle \mathbf{V}_1, \mathbf{V}_2\rangle = \overline{\langle \mathbf{V}_2, \mathbf{V}_1\rangle}$

Examples

$\mathbf{R}^n : \langle \mathbf{V}_1, \mathbf{V}_2 \rangle = \mathbf{V}_1^T * \mathbf{V}_2$

$\mathbf{C}^n : \langle \mathbf{V}_1, \mathbf{V}_2 \rangle = \mathbf{V}_1^\dagger * \mathbf{V}_2$

$\mathbf{C}^{n \times n} : \langle \mathbf{A}, \mathbf{B} \rangle = \text{Trace}(\mathbf{A}^\dagger * \mathbf{B})$, where $\text{Trace}(\mathbf{C}) = \sum_{i=0}^{n-1} \mathbf{C}[i,i]$

See book for other examples

Norm or length

Norm or length is a function $|\ |: \mathbf{V} \to \mathbf{R}$
defined as $|\mathbf{V}| = \sqrt{\langle \mathbf{V}, \mathbf{V} \rangle}$

i. Norm is nondegenerate: $|\mathbf{V}| > 0$ if $\mathbf{V} \neq \mathbf{0}$ and $|\mathbf{0}| = 0$
ii. Norm satisfies the triangle inequality: $|\mathbf{V} + \mathbf{W}| \leq |\mathbf{V}| + |\mathbf{W}|$
iii. Norm respects scalar multiplication: $|c \cdot \mathbf{V}| = |c| \times |\mathbf{V}|$

Distance function

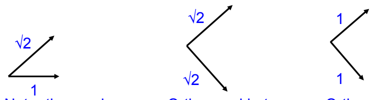
Distance function is a function $d(\ ,\ ): \mathbf{V} \times \mathbf{V} \to \mathbf{R}$
where $d(\mathbf{V}_1, \mathbf{V}_2) = |\mathbf{V}_1 - \mathbf{V}_2| = \sqrt{\langle \mathbf{V}_1 - \mathbf{V}_2, \mathbf{V}_1 - \mathbf{V}_2 \rangle}$

i. Distance is nondegenerate:
$d(\mathbf{V}, \mathbf{W}) > 0$ if $\mathbf{V} \neq \mathbf{W}$ and $d(\mathbf{V}, \mathbf{V}) = 0$
ii. Distance satisfies the triangle inequality:
$d(\mathbf{U}, \mathbf{V}) \leq d(\mathbf{U}, \mathbf{W}) + d(\mathbf{W}, \mathbf{V})$
iii. Distance is symmetric:
$d(\mathbf{V}, \mathbf{W}) = d(\mathbf{W}, \mathbf{V})$

Orthogonal and orthonormal basis

- Orthogonal basis B = $\{V_0, V_1, \ldots, V_{n-1}\}$:
  vectors pairwise orthogonal, $j \neq k$ implies $\langle V_j, V_k \rangle = 0$

- Orthonormal basis B:
  orthogonal and every basis vector is of norm 1



Not orthogonal — Orthogonal but not orthonormal — Orthonormal

Hilbert space

- A Hilbert space is a complex inner product space that is complete (for definition see book).

- Every finite-dimensional complex vector space with an inner product is automatically a Hilbert space.

Errata chapter 2

All errata:
http://www.cambridge.org/resources/0521879965/7337_Errata.pdf

This link will be available soon on the QC-webpage.

Reading

- This lecture: Ch 2.1-2.4, p 29-60.
- Next lecture: Ch 2.5-2.7 & (start of) Ch 3.

Math background

The Leap from Classical to Quantum

Lecture 3

Eigenvalues and eigenvectors

- For a matrix A in $C^{m \times n}$, if there is a number c in C and a vector $V \neq 0$ within C^n such that $AV = c \cdot V$, then c is called an eigenvalue of A and V an eigenvector of A associated with c.
- Some matrices have many eigenvalues and eigenvectors and some matrices have none.

Eigenspace

- If A has eigenvalue c_0 with eigenvector V_0, then for any $c \in C$ we have

$$A(cV_0) = cAV_0 = cc_0V_0 = c_0(cV_0)$$

  which shows that cV_0 is also an eigenvector of A with eigenvalue c_0.

- If cV_0 and $c'V_0$ are two such eigenvectors, then because of

$$\begin{aligned} A(cV_0 + c'V_0) &= AcV_0 + A\,c'V_0 = cAV_0 + c'AV_0 \\ &= c(c_0V_0) + c'(c_0V_0) = (c + c')(c_0V_0) = c_0(c+c')\,V_0 \end{aligned}$$

  we see that the addition of two such eigenvectors is also an eigenvector.

- Therefore, every eigenvector determines a complex subvector space of the vector space. It is known as the eigenspace associated with the given eigenvector.

Hermitian matrices

- An n x n matrix A is called hermitian if $A^\dagger = A$. In other words $A[j,k] = \overline{A[k,j]}$.
- If A is a hermitian matrix then the operator that it represents is called self-adjoint.
- If A is a hermitian n x n matrix, we have $\langle AV,V' \rangle = \langle V,AV' \rangle$.
- If A is hermitian, then all eigenvalues are real.
- For a given hermitian matrix, distinct eigenvectors that have distinct eigenvalues are orthogonal.
- A diagonal matrix is a square matrix whose only nonzero entries are on the diagonal. All entries off the diagonal are zero.
- Every self-adjoint operator A on a finite-dimensional complex vector space **V** can be represented by a diagonal matrix whose diagonal entries are the eigenvalues of A, and whose eigenvectors form an orthonormal basis for **V** (we call this basis an eigenbasis).
- With every physical observable of a quantum system there is a corresponding hermitian matrix. Measurements of the observable always leads to a state that is represented by one of the eigenvectors of the associated hermitian matrix.

Unitary matrices

- An n x n matrix U is called unitary if $U * U^\dagger = I_n$.
- Unitary matrices preserve inner products $\langle UV,UV' \rangle = \langle V,V' \rangle$.
- Unitary matrices preserve distances $d(UV_1,UV_2) = d(V_1,V_2)$. An operator that preserves distances is called an isometry.
- If U is unitary and $UV = V'$, then we can easily form $U^\dagger$ and by multiplying both sides we get $U^\dagger UV = U^\dagger V'$ or $V = U^\dagger V'$. In other words $U^\dagger$ can "undo" the action that U performs. In the quantum world all actions (that are not measurements) are "undoable" or "reversible".

Tensor product

- Most difficult, most essential subject!
- Tensor product of vectors

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_0 \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} \\ a_1 \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} \\ a_2 \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} \\ a_3 \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_0b_0 \\ a_0b_1 \\ a_0b_2 \\ a_1b_0 \\ a_1b_1 \\ a_1b_2 \\ a_2b_0 \\ a_2b_1 \\ a_2b_2 \\ a_3b_0 \\ a_3b_1 \\ a_3b_2 \end{bmatrix}$$

In general $\mathbf{C}^m \times \mathbf{C}^n$ is much smaller than $\mathbf{C}^m \otimes \mathbf{C}^n$.

Separable versus Entangled

$$\begin{bmatrix}8\\12\\6\\12\\18\\9\end{bmatrix} \in \mathbf{C}^6 = \mathbf{C}^2 \otimes \mathbf{C}^3 = \begin{bmatrix}2\\3\end{bmatrix} \otimes \begin{bmatrix}4\\6\\3\end{bmatrix}$$

separable

$$\begin{bmatrix}8\\0\\0\\0\\0\\18\end{bmatrix} \in \mathbf{C}^6 = \mathbf{C}^2 \otimes \mathbf{C}^3 = \begin{bmatrix}x\\y\end{bmatrix} \otimes \begin{bmatrix}a\\b\\c\end{bmatrix} = \begin{bmatrix}xa\\xb\\xc\\ya\\yb\\yc\end{bmatrix}$$

$$\begin{bmatrix}8\\0\\0\\0\\0\\18\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}8\\0\\0\end{bmatrix} + \begin{bmatrix}0\\6\end{bmatrix} \otimes \begin{bmatrix}0\\0\\3\end{bmatrix}$$

no solution!

entangled: sum of tensors

Tensor product of two matrices

$$A \otimes B = \begin{bmatrix}a_{0,0} & a_{0,1}\\ a_{1,0} & a_{1,1}\end{bmatrix} \otimes \begin{bmatrix}b_{0,0} & b_{0,1} & b_{0,2}\\ b_{1,0} & b_{1,1} & b_{1,2}\\ b_{2,0} & b_{2,1} & b_{2,2}\end{bmatrix}$$

$$= \begin{bmatrix} a_{0,0}\cdot\begin{bmatrix}b_{0,0} & b_{0,1} & b_{0,2}\\ b_{1,0} & b_{1,1} & b_{1,2}\\ b_{2,0} & b_{2,1} & b_{2,2}\end{bmatrix} & a_{0,1}\cdot\begin{bmatrix}b_{0,0} & b_{0,1} & b_{0,2}\\ b_{1,0} & b_{1,1} & b_{1,2}\\ b_{2,0} & b_{2,1} & b_{2,2}\end{bmatrix} \\ a_{1,0}\cdot\begin{bmatrix}b_{0,0} & b_{0,1} & b_{0,2}\\ b_{1,0} & b_{1,1} & b_{1,2}\\ b_{2,0} & b_{2,1} & b_{2,2}\end{bmatrix} & a_{1,1}\cdot\begin{bmatrix}b_{0,0} & b_{0,1} & b_{0,2}\\ b_{1,0} & b_{1,1} & b_{1,2}\\ b_{2,0} & b_{2,1} & b_{2,2}\end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix}
a_{0,0}\times b_{0,0} & a_{0,0}\times b_{0,1} & a_{0,0}\times b_{0,2} & a_{0,1}\times b_{0,0} & a_{0,1}\times b_{0,1} & a_{0,1}\times b_{0,2}\\
a_{0,0}\times b_{1,0} & a_{0,0}\times b_{1,1} & a_{0,0}\times b_{1,2} & a_{0,1}\times b_{1,0} & a_{0,1}\times b_{1,1} & a_{0,1}\times b_{1,2}\\
a_{0,0}\times b_{2,0} & a_{0,0}\times b_{2,1} & a_{0,0}\times b_{2,2} & a_{0,1}\times b_{2,0} & a_{0,1}\times b_{2,1} & a_{0,1}\times b_{2,2}\\
a_{1,0}\times b_{0,0} & a_{1,0}\times b_{0,1} & a_{1,0}\times b_{0,2} & a_{1,1}\times b_{0,0} & a_{1,1}\times b_{0,1} & a_{1,1}\times b_{0,2}\\
a_{1,0}\times b_{1,0} & a_{1,0}\times b_{1,1} & a_{1,0}\times b_{1,2} & a_{1,1}\times b_{1,0} & a_{1,1}\times b_{1,1} & a_{1,1}\times b_{1,2}\\
a_{1,0}\times b_{2,0} & a_{1,0}\times b_{2,1} & a_{1,0}\times b_{2,2} & a_{1,1}\times b_{2,0} & a_{1,1}\times b_{2,1} & a_{1,1}\times b_{2,2}
\end{bmatrix}$$

The Leap from Classical to Quantum

Classical Deterministic Systems

- 6 vertices in a graph
- 27 marbles

0 • $\boxed{6}$ 1 • $\boxed{2}$ 2 • $\boxed{1}$

3 • $\boxed{5}$ 4 • $\boxed{3}$ 5 • $\boxed{10}$

- $X = [6,2,1,5,3,10]^T$

Classical Deterministic Systems

- 6 vertices in a graph
- 27 marbles

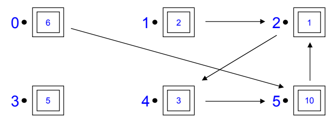
0 • $\boxed{5}$ 1 • $\boxed{5}$ 2 • $\boxed{0}$

3 • $\boxed{2}$ 4 • $\boxed{0}$ 5 • $\boxed{15}$

- $X = [5,5,0,2,0,15]^T$

Dynamics

- arrow from vertex i to vertex j: in one time click all marbles on vertex i will shift to vertex j



- Boolean adjacency matrix M

$$M = \begin{bmatrix}0&0&0&0&0&0\\0&0&0&0&0&0\\0&1&0&0&0&1\\0&0&0&1&0&0\\0&0&1&0&0&0\\1&0&0&0&1&0\end{bmatrix}$$

$M[i,j]=1$

↕

arrow from j to i
(see later)

$$MX = \begin{bmatrix}0&0&0&0&0&0\\0&0&0&0&0&0\\0&1&0&0&0&1\\0&0&0&1&0&0\\0&0&1&0&0&0\\1&0&0&0&1&0\end{bmatrix}\begin{bmatrix}6\\2\\1\\5\\3\\10\end{bmatrix} = \begin{bmatrix}0\\0\\12\\5\\1\\9\end{bmatrix} = Y$$

Dynamics (cont'd)

- In general:
  $M^k[i,j]$ = 1 if and only if there is a path of length k from vertex j to vertex i.

- In Quantum Computing we start with an initial state (vector of numbers), the "input" of the system. Operations correspond with multiplying the vector with matrices. The "output" is the state of the system when all operations are carried out.

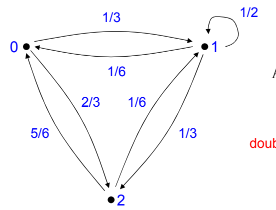
- Summing up:
  - The states of a system correspond to column vectors (state vectors).
  - The dynamics of a system correspond to matrices.
  - To progress from one state to another in one time step, one must multiply the state vector by a matrix.
  - Multiple step dynamics are obtained via matrix multiplications.

Probabilistic systems

- Quantum mechanics:
  - Inherent indeterminacy in knowledge of a state
  - States change with probabilistic laws
  - States transfer with a certain likelihood.

- Instead of many marbles, just look at one:
  - $X = [1/5, 3/10, 1/2]^T$ corresponds with
    - 1/5 chance that marble is on vertex 0
    - 3/10 chance that marble is on vertex 1
    - 1/2 chance that marble is on vertex 2
    - sum must be 1.

Modified dynamics



$$\text{Adjacency matrix } M = \begin{bmatrix} 0 & \frac{1}{6} & \frac{5}{6} \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{6} \\ \frac{2}{3} & \frac{1}{3} & 0 \end{bmatrix}$$

doubly stochastic: ∑rows =1 and ∑columns=1

$$MX = \begin{bmatrix} 0 & \frac{1}{6} & \frac{5}{6} \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{6} \\ \frac{2}{3} & \frac{1}{3} & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{6} \\ \frac{1}{6} \\ \frac{2}{3} \end{bmatrix} = \begin{bmatrix} \frac{21}{36} \\ \frac{9}{36} \\ \frac{6}{36} \end{bmatrix} = Y$$

X is probability at time t

Y is probability at time $t+1$

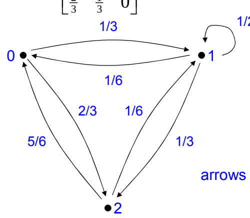
Symmetry

- Multiplication also on the left of a matrix with a row vector (=state vector):

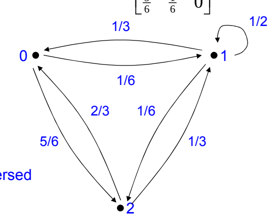
$$WM = \begin{bmatrix} \frac{1}{3} & 0 & \frac{2}{3} \end{bmatrix} \begin{bmatrix} 0 & \frac{1}{6} & \frac{5}{6} \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{6} \\ \frac{2}{3} & \frac{1}{3} & 0 \end{bmatrix} = \begin{bmatrix} \frac{4}{9} & \frac{5}{18} & \frac{5}{18} \end{bmatrix} = Z$$

$$\text{Note}: \sum \text{entries } Z = 1$$

$$M = \begin{bmatrix} 0 & \frac{1}{6} & \frac{5}{6} \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{6} \\ \frac{2}{3} & \frac{1}{3} & 0 \end{bmatrix} \qquad \text{Transpose } M^T = \begin{bmatrix} 0 & \frac{1}{3} & \frac{2}{3} \\ \frac{1}{6} & \frac{1}{2} & \frac{1}{3} \\ \frac{5}{6} & \frac{1}{6} & 0 \end{bmatrix}$$



arrows reversed



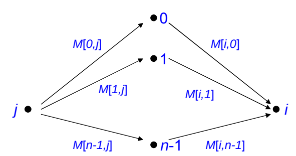
$$M^T W^T = \begin{bmatrix} 0 & \frac{1}{3} & \frac{2}{3} \\ \frac{1}{6} & \frac{1}{2} & \frac{1}{3} \\ \frac{5}{6} & \frac{1}{6} & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{3} \\ 0 \\ \frac{2}{3} \end{bmatrix} = \begin{bmatrix} \frac{4}{9} \\ \frac{5}{18} \\ \frac{5}{18} \end{bmatrix} = Z^T \qquad M^T W^T = (WM)^T = Z^T$$

multiply on the right of M takes states from time t to time $t+1$

multiply on the left of M takes states from time t to time $t-1$

time symmetry

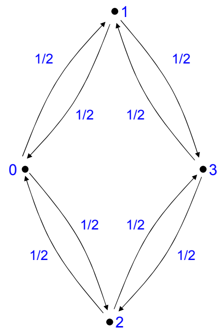
$$MM = M^2 = \begin{bmatrix} 0 & \frac{1}{6} & \frac{5}{6} \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{6} \\ \frac{2}{3} & \frac{1}{3} & 0 \end{bmatrix} \begin{bmatrix} 0 & \frac{1}{6} & \frac{5}{6} \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{6} \\ \frac{2}{3} & \frac{1}{3} & 0 \end{bmatrix} = \begin{bmatrix} \frac{11}{18} & \frac{13}{36} & \frac{1}{36} \\ \frac{5}{18} & \frac{13}{36} & \frac{13}{36} \\ \frac{1}{9} & \frac{5}{18} & \frac{11}{18} \end{bmatrix}$$



$M^2[i,j]$ = the probability of going from vertex j to vertex i in 2 time clicks.

In general for each positive integer k, we have $M^k[i,j]$ = the probability of going from vertex j to vertex i in k time clicks.

The stochastic billiard ball



$$A = \begin{bmatrix} 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}$$

start single marble in vertex 0: $[1,0,0,0]^T$

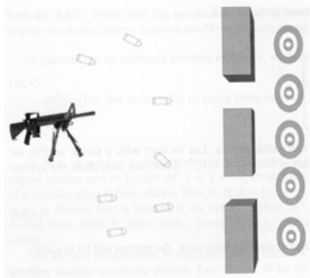
after one time click: $[0,1/2,1/2,0]^T$

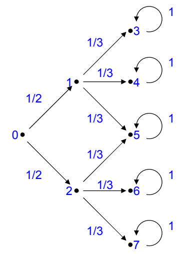
after another time click: $[1/2,0,0,1/2]^T$

marble acts like a billiard ball that bounces back and forth between vertices 1,2 and 0,3

quantum version will follow

Probabilistic double-slit experiment (I)





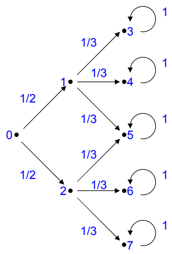
bullet always through one of the two slits

50% chance through top slit, 50% chance through bottom slit

three targets after each slit that can be hit with equal probability

one time click to a slit, one to a target

Probabilistic double-slit experiment (II)



$$B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Probabilistic double-slit experiment (III)

$$B * B = B^2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{6} & \frac{1}{3} & 0 & 1 & 0 & 0 & 0 & 0 \\ \frac{1}{6} & \frac{1}{3} & 0 & 0 & 1 & 0 & 0 & 0 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 1 & 0 & 0 \\ \frac{1}{6} & 0 & \frac{1}{3} & 0 & 0 & 0 & 1 & 0 \\ \frac{1}{6} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Sure that we start with bullet in position 0:
$X = [1,0,0,0,0,0,0,0]^T$

After two time clicks:
$B^2X = [0,0,0,1/6,1/6,1/3,1/6,1/6]^T$

$B^2[5,0] = 1/6 + 1/6 = 1/3$, what we expect.

In QM strange things……

B^2 probabilities of bullet's position after two time ticks

Summarizing

- The vectors that represent states of a probabilistic physical system express a type of indeterminacy about the exact physical state of the system.
- The matrices that represent the dynamics express a type of indeterminacy about the way the physical system will change over time. Their entries enable us to compute the likelihood of transitioning from one state to the next.
- The way in which the indeterminacy progresses is simulated by matrix multiplication, just as in the deterministic scenario.

Quantum Systems

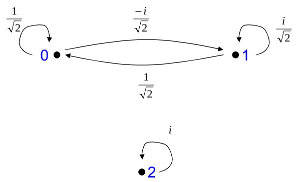
- QM: weight is not a real number p between 0 and 1, rather a complex number c such that $|c|^2$ is a real number between 0 and 1.
- Real number probabilities can only increase when added; complex numbers can cancel each other and lower their probability. This is called interference.

States and Graphs

- States: not sum of entries, but the sum of the modulus squared should be 1.

$$X = \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{2i}{\sqrt{15}} & \sqrt{\frac{2}{5}} \end{bmatrix}^T$$

- Graphs: not with real number weights, but with complex number weights. Adjacency matrix not double stochastic, but unitary.



$$U = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{-i}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0 \\ 0 & 0 & i \end{bmatrix}$$

$$|U[i,j]|^2 = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$UX = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{-i}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0 \\ 0 & 0 & i \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{3}} \\ \frac{2i}{\sqrt{15}} \\ \sqrt{\frac{2}{5}} \end{bmatrix} = \begin{bmatrix} \frac{5+2i}{\sqrt{30}} \\ \frac{-2-\sqrt{5}i}{\sqrt{30}} \\ \sqrt{\frac{2}{5}}i \end{bmatrix} = Y$$

note: sum of the modulus squares of Y is 1

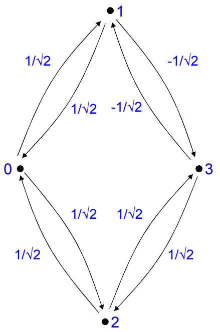
If U is the matrix that takes a state from time t to time $t+1$,

then $U^\dagger$ is the matrix that takes a state from time t to time $t-1$.

$V \rightarrow UV \rightarrow U^\dagger UV = I_3V = V$

"undo" the operation

The quantum billiard ball



$$A = \begin{bmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{bmatrix}$$

start single marble in vertex 0: $[1,0,0,0]^T$

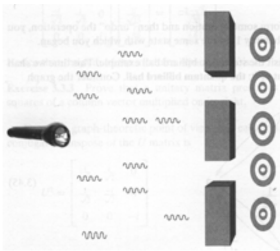
after one time click: $[0,\sqrt{1/2},\sqrt{1/2},0]^T$: 50-50%

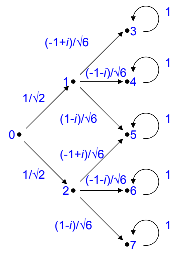
after another time click: $[1,0,0,0]^T$

other paths cancel each other out (interference)

$A^*A = A^2 = I_4$

Double-slit experiment (I)





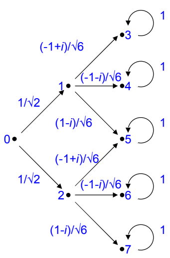
photons follow laws of quantum physics

each slit has a 50% chance of the photon's passing through it

three measuring devices after each slit

one time click from laser to wall, one from wall to measuring devices

Double-slit experiment (II)



$$P = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{-1+i}{\sqrt{6}} & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & \frac{-1-i}{\sqrt{6}} & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & \frac{1-i}{\sqrt{6}} & \frac{-1+i}{\sqrt{6}} & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{-1-i}{\sqrt{6}} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & \frac{1-i}{\sqrt{6}} & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

not unitary: many other paths

Double-slit experiment (III)

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{-1+i}{\sqrt{6}} & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & \frac{-1-i}{\sqrt{6}} & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & \frac{1-i}{\sqrt{6}} & \frac{-1+i}{\sqrt{6}} & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{-1-i}{\sqrt{6}} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & \frac{1-i}{\sqrt{6}} & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$|P[i,j]|^2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

exactly the same as with bullets: nothing strange happens after one time click.

Double-slit experiment (IV)

$$P^2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{-1+i}{\sqrt{12}} & \frac{-1+i}{\sqrt{6}} & 0 & 1 & 0 & 0 & 0 & 0 \\ \frac{-1-i}{\sqrt{12}} & \frac{-1-i}{\sqrt{6}} & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & \frac{1-i}{\sqrt{6}} & \frac{-1+i}{\sqrt{6}} & 0 & 0 & 1 & 0 & 0 \\ \frac{-1-i}{\sqrt{12}} & 0 & \frac{-1-i}{\sqrt{6}} & 0 & 0 & 0 & 1 & 0 \\ \frac{1-i}{\sqrt{12}} & 0 & \frac{1-i}{\sqrt{6}} & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\left|P^2[i,j]\right|^2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{6} & \frac{1}{3} & 0 & 1 & 0 & 0 & 0 & 0 \\ \frac{1}{6} & \frac{1}{3} & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 1 & 0 & 0 \\ \frac{1}{6} & 0 & \frac{1}{3} & 0 & 0 & 0 & 1 & 0 \\ \frac{1}{6} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Almost exactly as B^2, but one glaring difference: $B^2[5,0] = 1/3$, but $|P^2[5,0]|^2 = 0$

Explanation

- Interference: waves?
- However, experiment can be done with a *single* photon: interference!
- Superposition: *all* positions simultaneously!
- Measurement: no longer superposition, but collapse to a single classical state.

Review

- States in a quantum system are represented by column vectors of complex numbers whose sum of moduli squared is 1.
- The dynamics of a quantum system is represented by unitary matrices and is therefore reversible. The "undoing" is obtained via the algebraic inverse, i.e., the adjoint of the unitary matrix representing forward evolution.
- The probabilities of quantum mechanics are always given as the modulus square of complex numbers.
- Quantum states can be superposed, i.e., a physical system can be in more than one basic state simultaneously.

Errata

All errata:
http://www.cambridge.org/resources/0521879965/7337_Errata.pdf

This link can be found on the QC-webpage.

Reading

- This lecture: Ch 2.5-2.7 & Ch 3.1-3.3, p 60-97.
- Next lecture: Ch 3.4 & (start) Ch 4.

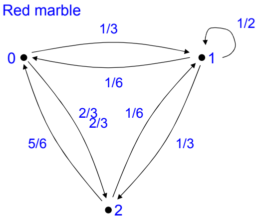
Assembling Systems

Basic Quantum Theory

Lecture 4

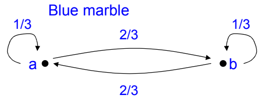
Assembling Systems

Red marble



$$\text{Adjacency matrix } M = \begin{bmatrix} 0 & \frac{1}{6} & \frac{5}{6} \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{6} \\ \frac{2}{3} & \frac{1}{3} & 0 \end{bmatrix}$$

Blue marble



$$\text{Adjacency matrix } N = \begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \end{bmatrix}$$

$$\text{Typical state } X = \begin{array}{c} 0a \\ 0b \\ 1a \\ 1b \\ 2a \\ 2b \end{array} \begin{bmatrix} \frac{1}{18} \\ 0 \\ \frac{2}{18} \\ \frac{1}{3} \\ 0 \\ \frac{1}{2} \end{bmatrix}$$

Dynamics: $i\,j \xrightarrow{M[i',i] \times N[j',j]} i'\,j'$

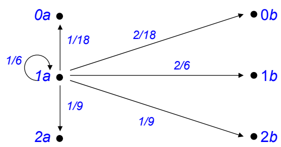
Assembling Systems (cont'd)

$$M \otimes N = \begin{bmatrix} 0\begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \end{bmatrix} & \frac{1}{6}\begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \end{bmatrix} & \frac{5}{6}\begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \end{bmatrix} \\ \frac{1}{3}\begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \end{bmatrix} & \frac{1}{2}\begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \end{bmatrix} & \frac{1}{6}\begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \end{bmatrix} \\ \frac{2}{3}\begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \end{bmatrix} & \frac{1}{3}\begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \end{bmatrix} & 0\begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \frac{1}{18} & \frac{2}{18} & \frac{5}{18} & \frac{10}{18} \\ 0 & 0 & \frac{2}{18} & \frac{1}{18} & \frac{10}{18} & \frac{5}{18} \\ \frac{1}{9} & \frac{2}{9} & \frac{1}{6} & \frac{2}{6} & \frac{1}{18} & \frac{2}{18} \\ \frac{2}{9} & \frac{1}{9} & \frac{2}{6} & \frac{1}{6} & \frac{2}{18} & \frac{1}{18} \\ \frac{2}{9} & \frac{4}{9} & \frac{1}{9} & \frac{2}{9} & 0 & 0 \\ \frac{4}{9} & \frac{2}{9} & \frac{2}{9} & \frac{1}{9} & 0 & 0 \end{bmatrix}$$

Corresponding graph

Cartesian product G_M x G_N

(only third column of tensor product of *M* and *N*)



Assembling Systems (cont'd)

- Quantum theory:
  - States can be combined using the tensor product of the vectors
  - Changes of the system are combined by using the tensor product of matrices
  - Important: there are many more states that cannot be combined from "smaller" ones:
    - No tensor product of smaller states
    - More interesting ones
    - Called entangled states
  - Similar for actions

Assembling Systems (cont'd)

- In general:
  - Cartesian product of an *n*-vertex graph with an *n'*-vertex graph is an (*n x n'*)-vertex graph.
  - If we have an n-vertex graph and we are interested in m different marbles within this system, this results in the graph with n^m vertices

$$G^m = \underbrace{G \times G \times \cdots \times G}_{m \text{ times}}$$

  - with the associated n^m-by-n^m adjacency matrix

$$M_G^{\otimes m} = \underbrace{M_G \otimes M_G \otimes \cdots \otimes M_G}_{m \text{ times}}$$

- Example: bit as a two-vertex graph with a marble on the 0 vertex or a marble on the 1 vertex. For *m* bits with a single marble one needs a 2^m vertex graph or a 2^m-by-2^m matrix, which demonstrates an exponential growth.

Basic Quantum Theory

Why Quantum Mechanics?

- Classical mechanics:
  - Dichotomy: particles (matter) ↔ waves (light)
  - Several experiments prove falseness
- New theory of microscopic world: *both matter and light manifest a particle-like and a wave-like behavior.*
- Double-slit experiment:
  - Also with just one photon: which region is more likely for the single photon to land. The photon is a true chameleon: sometimes it behaves as a particle and sometimes as a wave, depending on how it is observed.
  - Not only for light (photons), but also with electrons, protons, and even atomic nuclei. Clearly indicates: no rigid distinction between waves and particles.

Quantum states

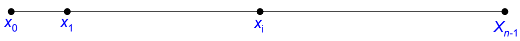
Two examples:

I. A particle confined to a set of discrete positions on a line

II. A single-particles spin system

Classical state

Subatomic particle on a line: can only be detected at one of the equally spaced points $\{x_0, x_1, \dots, x_{n-1}\}$, where $x_1 = x_0 + \delta x$, $x_2 = x_1 + \delta x$.



δx can be made as small as one wishes.

Associate to this current state of the particle an n-dimensional complex column vector $[c_0, c_1, \dots, c_{n-1}]^T$. Particle at point x_i shall be denoted by the Dirac ket notation $|x_i\rangle$.

To each of these n basic states, we assiciate:

$$
\begin{aligned}
|x_0\rangle &\mapsto [1, 0, \dots, 0]^T \\
|x_1\rangle &\mapsto [0, 1, \dots, 0]^T \\
&\vdots \\
|x_{n-1}\rangle &\mapsto [0, 1, \dots, 0]^T
\end{aligned}
$$

Canonical basis of C^n

Classical viewpoint: that's all we need!

Quantum state

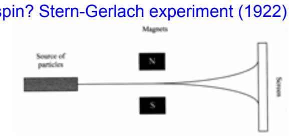
- Experiments demonstrate that the particle can be in a strange fuzzy blending of these states. What does this mean?
- An arbitrary state (c_i's are the complex amplitudes)
  $$|\phi\rangle = c_0\,|x_0\rangle + c_1\,|x_1\rangle + \cdots + c_{n-1}\,|x_{n-1}\rangle$$
- Represented in $\mathbf{C}^n$ as $|\phi\rangle \mapsto [c_0, c_1, \dots, c_{n-1}]^T$
- This state is a superposition of the basis states: it is simultaneously in all $\{x_0, x_1, \dots, x_{n-1}\}$ locations.
- The complex numbers $c_0, c_1, \dots, c_{n-1}$ tells precisely which superposition our particle is in.
- We will detect the particle in point x_i with a probability $p(x_i) = \frac{|c_i|^2}{\||\phi\rangle\|^2} = \frac{|c_i|^2}{\sum_j |c_j|^2}$
- After the observation we will find the system in one of the basis states
  $$|\phi\rangle \rightsquigarrow |x_i\rangle$$

Properties of kets

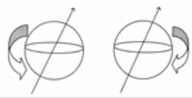
- Kets can be added
  $$|\phi\rangle + |\phi'\rangle = (c_0 + c'_0)\,|x_0\rangle + \cdots + (c_{n-1} + c'_{n-1})\,|x_{n-1}\rangle$$
- Scalar multiply a ket by c
  $$c\,|\phi\rangle = cc_0\,|x_0\rangle + \cdots + cc_{n-1}\,|x_{n-1}\rangle$$
- A ket and all its complex scalar multiples describe the same physical state. So the length of a ket does not matter as far as physics goes.
- A normalized ket $\frac{|\phi\rangle}{\||\phi\rangle\|}$
- Given a normalized ket, we get $p(x_i) = |c_i|^2$

Spin

- What is spin? Stern-Gerlach experiment (1922)



- Split of beam electrons into two streams with opposite spin. Wrt a classical spinning top two striking differences:
  - Electron does not have an internal structure, it is just a charged point.
  - All electrons either at the top or at the bottom. Two states: it spins either clockwise or anticlockwise.
- Two basic spin states: spin **up** and **down**
  $$|\phi\rangle = c_0\,|\uparrow\rangle + c_1\,|\downarrow\rangle$$



Bra-ket

- Physical meaning of inner product: transition amplitudes, how likely will the state of the system change *before* a specific measurement (start state) to another (end state) *after* the measurement.
- How to calculate a transition amplitude? start state $|\phi\rangle = \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix}$ and end state $|\phi'\rangle = \begin{bmatrix} c_0' \\ c_1' \\ \vdots \\ c_{n-1}' \end{bmatrix}$
  - Bra state: $\langle \phi' | = |\phi'\rangle^{\dagger} = [\overline{c_0'}, \overline{c_1'}, \ldots, \overline{c_{n-1}'}]$
  - Transition amplitude: multiply as *matrices*

$$\langle \phi' | \phi \rangle = [\overline{c_0'}, \overline{c_1'}, \ldots, \overline{c_{n-1}'}] \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = \overline{c_0'} \times c_0 + \overline{c_1'} \times c_1 + \cdots + \overline{c_{n-1}'} \times c_{n-1}$$

  - Denoted as: $|\phi\rangle \xrightarrow{\langle \phi' | \phi \rangle} |\phi'\rangle$
  - Nothing else than the inner product: from states to state transitions.

Summary Quantum States

- Association of a vector space to a quantum space. The dimension reflects the amount of basis states of the system.
- States can be superposed, by adding their representing vectors.
- A state is left unchanged if its representing vector is multiplied by a complex scalar.
- The state space has a geometry, given by its inner product. This geometry has a physical meaning: it tells us the likelihood for a given state to transition into another one after being measured. States that are orthogonal to one another are mutually exclusive.

Observables

- To each physical observable there corresponds a hermitian operator.
  - An observable is a linear operator, which means it maps states to states. Apply Ω to the state vector |ψ>, the resulting state is Ω |ψ>.
  - The eigenvalues of a hermitian operator are all real.
- The eigenvalues of a hermitian operator Ω associated with a physical observable are the only possible values the observable can take as a result of measuring it on a given state. Furthermore, the eigenvectors of Ω form a basis for the state space.

Position observable

- Where can the particle be found?
- Acts on the basic states:
  - $P(|x_i\rangle) = x_i |x_i\rangle$ *P* acts as multiplication by position.
- On arbitrary states: $P|\phi\rangle = P(\sum c_i |x_i\rangle) = \sum x_i c_i |x_i\rangle$
- Matrix representation of the operator in the standard basis:

$$P = \begin{bmatrix} x_0 & 0 & \cdots & 0 \\ 0 & x_1 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x_{n-1} \end{bmatrix}$$

Momentum observable

- Classical: momentum = velocity x mass
- Quantum analog: $M(|\phi\rangle) = -i * \hbar * \frac{|\phi(x+\delta x)\rangle - |\phi(x)\rangle}{\delta x}$
  - Is the rate of change of the state vector from one point to the next.
  - The constant ħ (pronounced h bar) is a universal constant, called the reduced Planc constant.
- Many more observables, but position and momentum are in a sense building blocks.

Spin operators

- Given a direction in space, in which way is the particle spinning?
- Is the particle spinning up or down in the *z* direction? Left or right in the *x* direction? In or out in the *y* direction?
- The three corresponding operators:

$$S_z = \frac{\hbar}{2}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad S_y = \frac{\hbar}{2}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad S_x = \frac{\hbar}{2}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- Orthonormal bases:
  - S_z has eigenbasis up and down $\{|\uparrow\rangle, |\downarrow\rangle\}$
  - S_y has eigenbasis in and out $\{|\swarrow\rangle, |\nearrow\rangle\}$
  - S_x has eigenbasis left and right $\{|\leftarrow\rangle, |\rightarrow\rangle\}$

More on operators/observables

- p117-125: FYI, not really important for quantum computation

Sum up on observables

- Observables are represented by hermitian operators. The result of an observation is always an eigenvalue of the hermitian.
- The expression $<\psi|\Omega|\psi>$ represents the expected value of observing Ω on $|\psi>$.
- Observables in general do not commute. This means that the order of observations matters. Moreover, if the commutator of two observables is not zero, there is an intrinsic limit to our capability of measuring their values simultaneously.

Measuring

- The act of carrying out an observation on a given physical system is called measuring.
- Classical:
  - Measuring leaves the system in whatever state it already was, at least in principle.
  - The result of a measurement on a well-defined state is predictable.
- Quantum world:
  - Systems do get perturbed and modified as a result of a measurement.
  - Only the probability of observing specific values can be calculated: measurement is inherently a nondeterministic process.

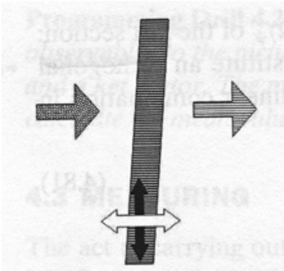
What happens?

- Let Ω be an observable and $|\psi>$ be a state. If the result of measuring Ω is the eigenvalue λ, the state after measurement will always be an eigenvector corresponding to λ.
- The probability of the transition to an eigenvector is equal to $|<e|\psi>|^2$. It is the projection of $|\psi>$ along $|e>$.

Measurement with more than one observable

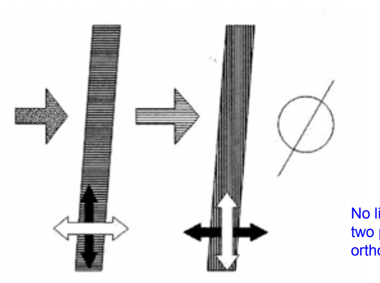
- Beam of light:
  - Vibrates along all possible directions orthogonal to its line of propagation.
  - Vibrates only in a specific direction: polarization.
- Experiment: multiple polarization sheets.

One sheet



Light partially passing through one polarization sheet.

Two sheets

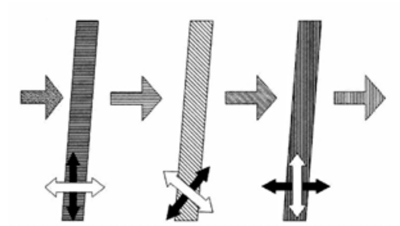


No light passing through two polarization sheets at orthogonal angles.

Three sheets

No effect if third sheets is placed on left or right of the two other sheets: no light!

However, placed in-between: only one-eight of the original light will pass through all three sheets!



Summary on measuring

- The end state of the measurement of an observable is always one of its eigenvectors.
- The probability for an initial state to collapse into an eigenvector of the observable is given by the length squared of the projection.
- When we measure several observables, the order of measurement matters.

Quantum dynamics

- Systems evolving in time.
- The evolution of a quantum system (that is not a measurement) is given by a unitary operator or transformation

$$|\phi(t+1)\rangle = U\,|\phi(t)\rangle$$

- Unitary transformations are closed under composition and inverse:
  - The product of two arbitrary unitary matrices is unitary.
  - The inverse of a unitary transformation is unitary.

Quantum dynamics (cont'd)

- Assume we have a rule $\mathfrak{R}$ that associates with each instance of time $t_0, t_1, t_2, \ldots, t_{n-1}$

  a unitary matrix $\mathfrak{R}[t_0], \mathfrak{R}[t_1], \ldots, \mathfrak{R}[t_{n-1}]$

- Starting with an initial state vector $|\phi\rangle$

$$\begin{gathered}\mathfrak{R}[t_0]|\phi\rangle,\\ \mathfrak{R}[t_1]\mathfrak{R}[t_0]|\phi\rangle,\\ \vdots\\ \mathfrak{R}[t_{n-1}]\mathfrak{R}[t_{n-2}]\cdots\mathfrak{R}[t_0]|\phi\rangle\end{gathered}$$

Quantum dynamics (cont'd)

Orbit of $|\psi>$

$$|\phi\rangle \underset{\mathfrak{R}[t_0]^\dagger}{\overset{\mathfrak{R}[t_0]}{\rightleftarrows}} \mathfrak{R}[t_0]|\phi\rangle \underset{\mathfrak{R}[t_1]^\dagger}{\overset{\mathfrak{R}[t_1]}{\rightleftarrows}} \mathfrak{R}[t_1]\mathfrak{R}[t_0]|\phi\rangle \underset{\mathfrak{R}[t_2]^\dagger}{\overset{\mathfrak{R}[t_2]}{\rightleftarrows}} \mathfrak{R}[t_2]\mathfrak{R}[t_1]\mathfrak{R}[t_0]|\phi\rangle$$

$$\rightleftarrows \cdots \underset{\mathfrak{R}[t_{n-1}]^\dagger}{\overset{\mathfrak{R}[t_{n-1}]}{\rightleftarrows}} \mathfrak{R}[t_{n-1}]\mathfrak{R}[t_{n-2}]\cdots\mathfrak{R}[t_0]|\phi\rangle$$

Symmetric in time

A quantum computation will start with an initial state $|\psi>$, followed by the application of a sequence of unitary operators to that state. When we are done, we will measure the output and get the final state.

Quantum dynamics (cont'd)

- How is the sequence of unitary transformations selected in real-life quantum mechanics?
- How is the dynamics determined?
- How does the system change?
- Answer: the Schrödinger equation (see book)

Quantum dynamics: recap

- Quantum dynamics is given by unitary transformations.
- Unitary transformations are invertible: thus, all closed system dynamics are reversible in time (as long as no measurement is involved).
- The concrete dynamics is given by the Schrödinger equation, which determines the evolution of a quantum system.

Reading

- This lecture: Ch 3.4 & Ch 4.1-4.4, p 97-132.
- Next lecture: Ch 4.5 & start Ch 5.

Assembling Quantum Systems

Architecture

Lecture 5

Assembling Quantum States

Assume we have two independent quantum systems *Q* and *Q'*, represented respectively by the vector spaces ***V*** and ***V'***. The quantum system obtained by merging *Q* and *Q'* will have the tensor product ***V*** and ***V'*** as a state space.

We can assemble as many systems as we like: $V_0 \otimes V_1 \otimes \cdots \otimes V_k$

Two particles moving in a one-dimensional grid: first particle on $\{x_0, x_1, \ldots, x_{n-1}\}$, the second particle on $\{y_0, y_1, \ldots, y_{m-1}\}$.

n x *m* possible basic states:

$|x_0\rangle \otimes |y_0\rangle$, meaning the first particle is at x_0, and the second particle at y_0.

⋮

$|x_{n-1}\rangle \otimes |y_{m-1}\rangle$, meaning the first particle is at x_{n-1} and the second at y_{m-1}.

Assembling (cont'd)

- Generic state vector:

  $|\phi\rangle = c_{0,0}\,|x_0\rangle \otimes |y_0\rangle + \cdots c_{i,j}\,|x_i\rangle \otimes |y_j\rangle + \cdots + c_{n-1,m-1}\,|x_{n-1}\rangle \otimes |y_{m-1}\rangle$

  which is a vector in the (*n* x *m*)-dimensional complex space $\boldsymbol{C}^{nxm}$.

- The quantum amplitude $|c_{i,j}|$ squared is the probability of finding the two particles at positions x_i and y_j.

- Example:

  $|\phi\rangle = i\,|x_0\rangle \otimes |y_0\rangle + (1-i)\,|x_0\rangle \otimes |y_1\rangle + 2\,|x_1\rangle \otimes |y_0\rangle + (-1-i)\,|x_1\rangle \otimes |y_1\rangle$

- What is probability of finding first particle at x_1 and second one at y_1?

  $$p(x_1, y_1) = \frac{|-1-i|^2}{|i|^2 + |1-i|^2 + |2|^2 + |-1-i|^2} = 0.2222$$

Assembling (cont'd)

- Entanglement:
  - The basic states of the assembled system are just the tensor product of basic states of its constituents.
  - *Each* generic state vector can be rewritten as the tensor product of two states, coming from one subsystem and a second one? **NOT TRUE**

- Example: simplest two-particle system, where each particle is allowed only in two points. Consider the state

  $|\phi\rangle = |x_0\rangle \otimes |y_0\rangle + |x_1\rangle \otimes |y_1\rangle$

  In order to clarify what is left out, we might write this as

  $|\phi\rangle = 1\,|x_0\rangle \otimes |y_0\rangle + 0\,|x_0\rangle \otimes |y_1\rangle + 0\,|x_1\rangle \otimes |y_0\rangle + 1\,|x_1\rangle \otimes |y_1\rangle$

- Can we write this as the tensor product of two states coming from two subsystems? 1st particle $c_0\,|x_0\rangle + c_1\,|x_1\rangle$, 2nd particle $c_0'\,|y_0\rangle + c_1'\,|y_1\rangle$

  Tensor product

  $$(c_0\,|x_0\rangle + c_1\,|x_1\rangle) \otimes (c_0'\,|y_0\rangle + c_1'\,|y_1\rangle) = c_0c_0'\,|x_0\rangle \otimes |y_0\rangle + c_0c_1'\,|x_0\rangle \otimes |y_1\rangle + c_1c_0'\,|x_1\rangle \otimes |y_0\rangle + c_1c_1'\,|x_1\rangle \otimes |y_1\rangle$$

- No solution: $|\psi\rangle$ cannot be written as a tensor product.

Entangled states

Assembling: Entanglement

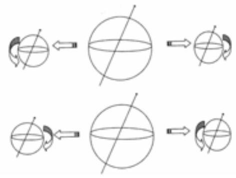
- $|\phi\rangle = |x_0\rangle \otimes |y_0\rangle + |x_1\rangle \otimes |y_1\rangle$ What does it physically mean?
- First particle 50-50 chance of being in x_0 or x_1.
- If in x_0? Term $|x_0\rangle \otimes |y_1\rangle$ has coefficient 0, so no chance that second particle in y_1. We must conclude that it can only be found in y_0.
- Similarly, if first particle in x_1, second one must be in y_1.
- Symmetrical with respect to the two particles: the same if we measure second particle first.
- The individual states of the two particles are intimately related to each other, or entangled.
- Amazing: the x_i's can be *light years* away from the y_i's!
- Sharp contrast: no clue

  Separable states

  $|\phi'\rangle = 1\,|x_0\rangle \otimes |y_0\rangle + 1\,|x_0\rangle \otimes |y_1\rangle + 1\,|x_1\rangle \otimes |y_0\rangle + 1\,|x_1\rangle \otimes |y_1\rangle$

Assembling: spin systems

- Law of conservation of spin: in an isolated system the total amount of spin must stay the same.
- Fix on the *z*-direction and corresponding spin basis: up and down.
- Consider a composite particle, whose total spin is zero.
- This particle might split up into two particles that do have spin:



Assembling: spin systems (cont'd)

- Spin states of the two particles will be entangled.
- Spin of total system zero → sum of the spins of the two particles must cancel each other out:
  - Measure spin of left particle along *z* axis $|\uparrow_L\rangle \rightarrow$ spin of right particle $|\downarrow_R\rangle$
  - Similarly, $|\downarrow_L\rangle \rightarrow |\uparrow_R\rangle$
- Basis left particle $B_L=\{|\uparrow_L\rangle, |\downarrow_L\rangle\}$, basis right particle $B_R=\{|\uparrow_R\rangle, |\downarrow_R\rangle\}$, so basis of total system

$$\{\uparrow_L \otimes \uparrow_R,\ \uparrow_L \otimes \downarrow_R,\ \downarrow_L \otimes \uparrow_R,\ \downarrow_L \otimes \downarrow_R\}$$

- Entangled particles are described by $\dfrac{|\uparrow_L \otimes \downarrow_R\rangle + |\downarrow_L \otimes \uparrow_R\rangle}{\sqrt{2}}$
- Combinations $\uparrow_L \otimes \uparrow_R$ and $\downarrow_L \otimes \downarrow_R$ cannot occur because of the law of conservation of spin.
- Measuring left particle: if it collapses to $|\uparrow_L\rangle$ then instantaneously right particle collapses to $|\downarrow_R\rangle$, even if the particle is millions of light years away.
- Entanglement plays role in: algorithms, cryptography, teleportation, and decoherence.

Assembling systems

Summarizing:

- We can use the tensor product to build complex systems out of simpler ones.
- The new system cannot be analyzed simply in terms of states belonging to its subsystems. An entire set of new states has been created, which cannot be resolved into their constituents.

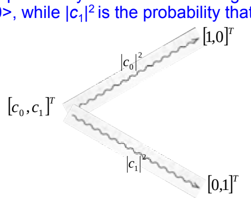
Architecture

Bits and qubits

- A bit is a unit of information describing a two-dimensional classical system.
- A bit is away of describing a system whose set of states is of size 2, usually written as 0 and 1, or F and T, etc.
- By matrices: $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- In a classical world: either in state |0> or in state |1>; in a quantum world this is not sufficient: a quantum system can be in state |0> and in state |1> simultaneously.
- A quantum bit or a qubit is a unit of information describing a two-dimensional quantum system.

Qubits: representation

- Representation of a qubit $\begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$ where $|c_0|^2+|c_1|^2=1$
- $|c_0|^2$ is the probability that after measuring the qubit, it will be found in state |0>, while $|c_1|^2$ is the probability that it will be in state |1>



- Canonical basis of $\mathbb{C}^2$: $\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = c_0 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + c_1 \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = c_0\,|0\rangle + c_1\,|1\rangle$

Qubits: denotations and implementations

Several ways of denoting qubits

$$\tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|1\rangle + |0\rangle}{\sqrt{2}} \qquad \frac{|0\rangle - |1\rangle}{\sqrt{2}} \neq \frac{|1\rangle - |0\rangle}{\sqrt{2}} \qquad \frac{|0\rangle - |1\rangle}{\sqrt{2}} = (-1)\frac{|1\rangle - |0\rangle}{\sqrt{2}}$$

Examples of qubit implementations (see chapter 11)

- An electron in an atom might be in one of two different energy levels (ground state and excited states).
- A photon might be in one of two polarized states.
- A subatomic particle might have one of two spin directions.

There will be enough quantum indeterminacy and quantum superposition effects within all these systems to represent a qubit.

Qubits: more than 1 bit

- Only one bit of storage not very interesting. Consider a byte or eight bits 01101011
- Following the preceding method of describing bits

$$\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}$$

- To combine quantum systems one should use tensor products

$$|0\rangle\otimes|1\rangle\otimes|1\rangle\otimes|0\rangle\otimes|1\rangle\otimes|0\rangle\otimes|0\rangle\otimes|1\rangle$$

- This is an element of

$$\mathbf{C}^2\otimes\mathbf{C}^2\otimes\mathbf{C}^2\otimes\mathbf{C}^2\otimes\mathbf{C}^2\otimes\mathbf{C}^2\otimes\mathbf{C}^2\otimes\mathbf{C}^2$$

- This vector space may be denoted as $(\mathbf{C}^2)^{\otimes 8}$. This is a complex vector space of dimension 2^8=256, isomorphic to $\mathbf{C}^{256}$.

Qubyte

- Another description: a 2^8=256 row vector

$$\begin{array}{c}00000000\\00000001\\\vdots\\01101010\\01101011\\01101100\\\vdots\\11111110\\11111111\end{array}\begin{bmatrix}0\\0\\\vdots\\0\\1\\0\\\vdots\\0\\0\end{bmatrix}\qquad\begin{array}{c}00000000\\00000001\\\vdots\\01101010\\01101011\\01101100\\\vdots\\11111110\\11111111\end{array}\begin{bmatrix}c_0\\c_1\\\vdots\\c_{106}\\c_{107}\\c_{108}\\\vdots\\c_{254}\\c_{255}\end{bmatrix}\qquad\sum_{i=0}^{255}|c_i|^2=1$$

- Classical world: indicate the state of each bit of a byte → eight bits.
- Quantum world: a state of eight qubits is given by writing 256 complex numbers.
- A 64-qubit register: 2^{64} = 18,446,744,073,709,551,616 complex numbers.
- Exponential growth: thought to the notion of quantum computing.

Two-qubit system

- Qubit pair: $|0\rangle\otimes|1\rangle$ or $|0\otimes 1\rangle$
- Tensor product clear: $|0\rangle|1\rangle, |0,1\rangle$ or $|01\rangle$
- Another way: $\begin{array}{c}00\\01\\10\\11\end{array}\begin{bmatrix}0\\1\\0\\0\end{bmatrix}$
- A general state of a two-qubit system:

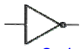
$$|\phi\rangle = c_{0,0}|00\rangle + c_{0,1}|01\rangle + c_{1,0}|10\rangle + c_{1,1}|11\rangle$$

- Tensor product of two states not commutative:

$$|0\otimes 1\rangle = |0\rangle\otimes|1\rangle = |0,1\rangle = |01\rangle \neq |10\rangle = |1,0\rangle = |1\rangle\otimes|0\rangle = |1\otimes 0\rangle$$

- Entangled states: $\dfrac{|11\rangle+|00\rangle}{\sqrt{2}} = \dfrac{1}{\sqrt{2}}|11\rangle + \dfrac{1}{\sqrt{2}}|00\rangle$

Classical gates: NOT

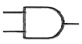
NOT gate 

- Input 1 bit or a 2x1 matrix
- Output 1 bit or a 2x1 matrix
- NOT of $|0\rangle$ equals $|1\rangle$ and NOT of $|1\rangle$ equals $|0\rangle$
- Consider the matrix

$$\mathrm{NOT} = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}\qquad\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}$$

Classical gates: AND

AND gate 

- Input 2 bits, output 1 bit, so a 2^1-by-2^2 matrix
- Consider the matrix

$$\mathrm{AND} = \begin{bmatrix}1 & 1 & 1 & 0\\0 & 0 & 0 & 1\end{bmatrix}$$

$$\begin{bmatrix}1 & 1 & 1 & 0\\0 & 0 & 0 & 1\end{bmatrix}\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}\quad\text{or}\quad \mathrm{AND}|11\rangle=|1\rangle$$

$$\begin{bmatrix}1 & 1 & 1 & 0\\0 & 0 & 0 & 1\end{bmatrix}\begin{bmatrix}0\\1\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}\quad\text{or}\quad \mathrm{AND}|01\rangle=|0\rangle$$

$$\begin{bmatrix}1 & 1 & 1 & 0\\0 & 0 & 0 & 1\end{bmatrix}\begin{bmatrix}3.5\\2\\0\\-4.1\end{bmatrix}=\begin{bmatrix}5.5\\-4.1\end{bmatrix}$$

NONSENS! Only classical states, i.e. columns matrices with a single 1 entry and all other entries 0. Later more…..

Classical gates: OR

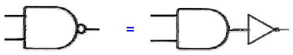
OR gate 

- Consider the matrix

$$\mathrm{OR} = \begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 1 & 1\end{bmatrix}$$

 ?

Classical gates: NAND

NAND gate 

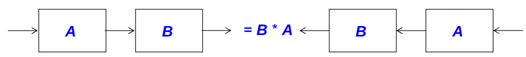
- Special importance because every logical gate can be composed of NAND gates.

$$\text{NAND} = \begin{array}{c} \\ 0 \\ 1 \end{array}\begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

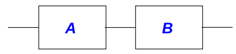
- NAND = AND followed by NOT

$$\text{NOT} * \text{AND} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} * \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} = \text{NAND}$$

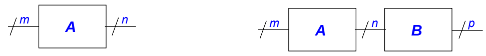
Sequential operations



Convention: computation flows from left to right, so A followed by B shall be denoted as

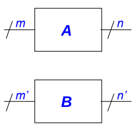


m input bits and *n* output bits



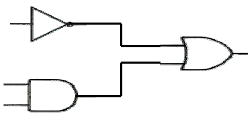
A will be of size 2^n-by-2^m ***B*A*** is a (2^p-by-2^n)*(2^n-by-2^m)= (2^p-by-2^m) matrix

Parallel operations

$\mathbf{A} \otimes \mathbf{B} =$ 

$$\mathbf{A} \otimes \mathbf{B} \text{ is of size } 2^n 2^{n'} = 2^{n+n'} \text{ - by - } 2^m 2^{m'} = 2^{m+m'}$$

Parallel operations: example

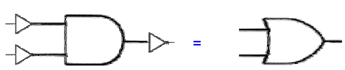


$\text{OR} * (\text{NOT} \otimes \text{AND})$

$$\text{NOT} \otimes \text{AND} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\text{OR} * (\text{NOT} \otimes \text{AND}) = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Example DeMorgan's laws

$\neg(\neg P \wedge \neg Q) = P \vee Q$ 

$$\text{NOT} * \text{AND} * (\text{NOT} \otimes \text{NOT}) = \text{OR}$$

$$\text{NOT} \otimes \text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} * \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Reading

- This lecture: Ch 4.5 & Ch 5.1-5.2, p 132-151.
- Next lecture: Ch 5.3-5.5

Architecture

Reversible Gates

Quantum Gates

Lecture 6

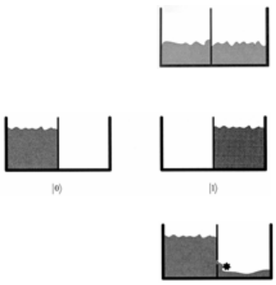
Reversible Gates

- In quantum world all operations that are not measurements:
  - reversible
  - represented by unitary matrices
  - e.g., AND gate are not reversible
    NOT gate and identity gate are reversible
- Today's computers lose energy and generate heat. In 1960s Rolf Landauer showed:
  - Erasing information causes energy loss and heat
  - Writing information not

Landauer's principle

Landauer's principle (I)

Intuition (not completely correct): tub of water

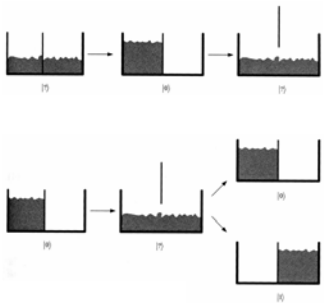


No state

In state |0> and in state |1>

State |0> dissipating and creating energy

Landauer's principle (II)



Reversibility of writing

Irreversibility of erasing

Landauer's principle (III)

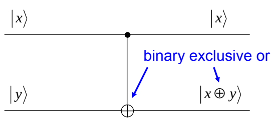
- Intuition with two people, Alice and Bob
- Writing
  - Alice writes letter on empty blackboard
  - Bob walks into the room
  - Bob erases the letter
  - Blackboard in its original state
  - Writing is reversible
- Erasing
  - Blackboard with writing on it
  - Alice erases the board
  - Bob walks into the room
  - Bob cannot write what was on the board
  - Erasing not reversible

Landauer's principle (IV)

- Erasing information is an irreversible, energy-dissipating operation.
- Charles H. Bennett in 1970s: if erasing information is the only operation that uses energy, then a computer that is reversible and does not erase would not use any energy → reversible circuits and programs.

Reversible gates: controlled-NOT gate

- Identity gate
- NOT gate
- Controlled-NOT gate:



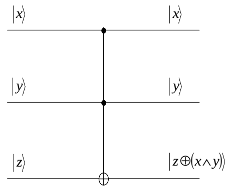
	00	01	10	11
00	1	0	0	0
01	0	1	0	0
10	0	0	0	1
11	0	0	1	0

Top input is control bit:

- if |x›=0 then bottom output of |y› will be the same as the input
- if |x› =1 then the bottom output will be the opposite

Controlled-NOT gate can be reversed by itself

Reversible gates: Toffoli gate



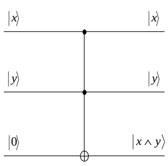
	000	001	010	011	100	101	110	111
000	1	0	0	0	0	0	0	0
001	0	1	0	0	0	0	0	0
010	0	0	1	0	0	0	0	0
011	0	0	0	1	0	0	0	0
100	0	0	0	0	1	0	0	0
101	0	0	0	0	0	1	0	0
110	0	0	0	0	0	0	0	1
111	0	0	0	0	0	0	1	0

Similar to the controlled-NOT gate, but with two controlling bits:

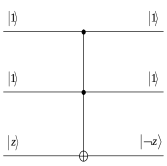
- the bottom bit flips only when *both* of the two top bits are in state |1›.
- can be written as $|z\oplus(x\wedge y)\rangle$

Toffoli gate (cont'd)

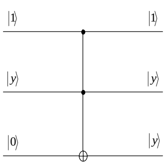
- Toffoli gate is universal: with copies one can make any logical gate.
- You can make a reversible computer using only Toffoli gates.
- In theory this computer will neither use any energy nor give off any heat.



AND gate



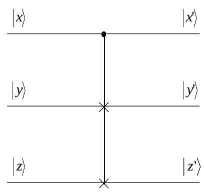
NOT gate



fanout gate

Fredkin gate

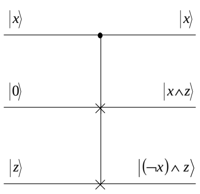
- Fredkin gate is also universal:
  - the top input is the control input
  - |0, *y*, *z* › → |0, *y*, *z* › and |1, *y*, *z* › → |1, *z*, *y*›



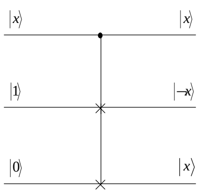
	000	001	010	011	100	101	110	111
000	1	0	0	0	0	0	0	0
001	0	1	0	0	0	0	0	0
010	0	0	1	0	0	0	0	0
011	0	0	0	1	0	0	0	0
100	0	0	0	0	1	0	0	0
101	0	0	0	0	0	0	1	0
110	0	0	0	0	0	1	0	0
111	0	0	0	0	0	0	0	1

Fredkin gate (cont'd)

Universal:



AND gate



NOT gate

Both the Toffoli and the Fredkin gates are universal. Not only are both reversible gates, their matrices are also unitary.

Quantum gates

- A quantum gate is an operator that acts on qubits. Such operators will be represented by unitary matrices.
- Examples: identity operator *I*, the Hadamard gate $H\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\right)$, the NOT gate, the controlled-NOT gate, the Toffoli gate, and the Fredkin gate.
- Pauli matrices:

$$X=\sigma_x=\mathrm{NOT}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \qquad Y=\sigma_y=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \qquad Z=\sigma_z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

- Other important matrices:

$$S=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix} \qquad T=\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$$

- Several relations between these operators (see book)

Square root of NOT gate

- Matrix representation: $\sqrt{\mathrm{NOT}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}$
- Not its own inverse: √NOT ≠ √NOT†
- Reason for name:
  - Put qubits |0> and |1> through √NOT gate twice:

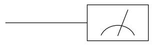
$$\sqrt{\mathrm{NOT}} * \sqrt{\mathrm{NOT}} = \left(\sqrt{\mathrm{NOT}}\right)^2 = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$$

$$|0\rangle = [1,0]^T \mapsto \left[\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right]^T \mapsto [0,1]^T = |1\rangle$$

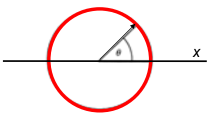
$$|1\rangle = [0,1]^T \mapsto \left[-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right]^T \mapsto [-1,0]^T = -1|0\rangle, \text{ represent same state as } |0\rangle$$

  - Performs same operation as the NOT gate.

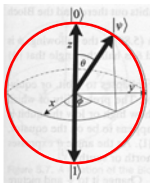
Measurement operation

- Not unitary
- Not reversible
- Usually performed at the end of a computation
- Denoted as 

Geometric representation of qubit states and operations

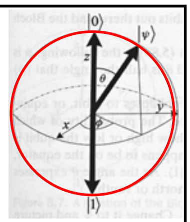


Complex numbers c with $|c|^2 = 1$, only identified by one number, the angle θ between vector and x-axis



Qubits $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$, where $|c_0|^2+|c_1|^2=1$ can be identified by two numbers, the latitude θ and the longitude φ on a three-dimensional sphere of radius1, known as the Bloch sphere.

Bloch sphere



Qubit: $|\psi\rangle = \cos(\theta)|0\rangle + e^{i\varphi}\sin(\theta)|1\rangle$

$$0 \le \phi < 2\pi \text{ and } 0 \le \theta \le \tfrac{\pi}{2}$$

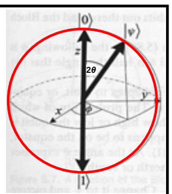
Standard parametrization of the unit sphere:

$$x = \cos\phi\sin\theta$$
$$y = \sin\phi\sin\theta$$
$$z = \cos\theta$$

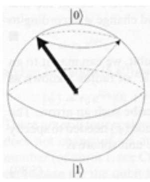
(θ,ϕ) and $(\pi - \theta, \phi + \pi)$ represent the same bit (up to the factor -1)

$$x = \cos\phi\sin 2\theta$$
$$y = \sin\phi\sin 2\theta$$
$$z = \cos\theta$$

Bloch sphere (cont'd)

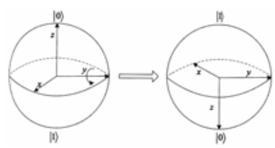


- North pole corresponds to state |0>and south pole to |1>.
- Angle φ is the angle that $|\psi\rangle$ makes from x along the equator (*longitude*) and θ is half the angle that $|\psi\rangle$ makes with the z axis (*latitude*).
- When a qubit is measured in the standard basis, it collapses to the north or south pole of the Bloch sphere. The probability depends on the latitude, so on θ.
- Rotation around the z axis, changing the longitude: does not affect the probability to which classical state it will collapse. It is called a phase change, altering the phase parameter $e^{i\varphi}$.



Bloch sphere: dynamics

- Every unitary 2-by-2 matrix will 'manipulate' the sphere.
- The X, Y, and Z Pauli matrices "flip" the Bloch sphere 180° about the x, y, and z axes, resp.:
  - X is a NOT gate taking |0> to |1> and vice versa, and even more: it takes everything above the equator to below the equator. Similar for the other Pauli matrices: e.g., Y operation



Bloch sphere: dynamics/rotations

- Phase shift gates: $R(\theta)=\begin{bmatrix}1 & 0\\ 0 & e^{\theta}\end{bmatrix}$
- Following operation on an arbitrary qubit:

$$\cos(\theta')|0\rangle+e^{i\varphi}\sin(\theta')|1\rangle=\begin{bmatrix}\cos(\theta')\\ e^{i\varphi}\sin(\theta')\end{bmatrix}\mapsto\begin{bmatrix}\cos(\theta')\\ e^{\theta}e^{i\varphi}\sin(\theta')\end{bmatrix}$$

Leaves the latitude alone and just changes the longitude. New state will remain unchanged, only the phase will change.

Bloch sphere: dynamics/rotations

- Rotation of θ degrees around x, y, or z axis:

$$R_x(\theta)=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}X=\begin{bmatrix}\cos\frac{\theta}{2} & -i\sin\frac{\theta}{2}\\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix}$$

$$R_y(\theta)=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}Y=\begin{bmatrix}\cos\frac{\theta}{2} & -\sin\frac{\theta}{2}\\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix}$$

$$R_z(\theta)=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}Z=\begin{bmatrix}e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2}\end{bmatrix}$$

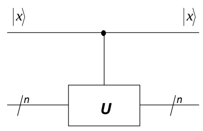
- General rotation around vector $D=(D_x,D_y,D_z)$ with size 1 from the origin:

$$R_D(\theta)=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}(D_xX+D_yY+D_zZ)$$

Bloch sphere: higher dimensions

- Valuable tool for understanding qubits and one-qubit operations.
- For n-qubits there is a higher-dimensional analog of the sphere.
- Research challenge: visualizing what happens when we manipulate several bits at once.
- Entanglement lies beyond the scope of the Bloch sphere.

controlled-U or ^CU



This operation will perform the U operation if the top $|x>$ is a $|1>$ and will perform the identity operation if $|x>$ is $|0>$. Equivalent to an IF-THEN statement.

For the simple case of

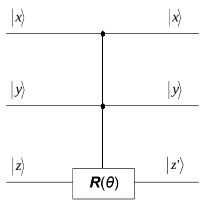
$$U=\begin{bmatrix}a & c\\ b & d\end{bmatrix}\qquad {}^CU=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&a&b\\0&0&c&d\end{bmatrix}$$

Universal quantum gates

- Universal logical gates can simulate every logical circuit:
  - {AND, NOT} gates
  - NAND gate
- Universal reversible gates:
  - Toffoli gate
  - Fredkin gate
- Universal quantum gates:
  - $\{H, {}^C\mathrm{NOT}, R(\cos^{-1}(3/5))\}$

Universal quantum gates (cont'd)

- Deutsch gate $D(\theta)$



If the inputs $|x>$ and $|y>$ are both $|1>$, then the phase shift operation $R(\theta)$ will act on the $|z>$ input. Otherwise, $|z'>$ will be the same as $|z>$.

No-Cloning Theorem

- It is impossible to clone an exact quantum state.
- In other words, it is impossible to make a copy of an arbitrary quantum state without first destroying the original.
- We can “cut” and “paste” a quantum state, we cannot “copy” and “paste”.
- Move is possible, copy is impossible.
- Transporting arbitrary quantum states from one system to another is no problem.
- See book for “proofs”.

No-Cloning Theorem (cont’d)

- What about the fanout gate? The Toffoli and Fredkin quantum gates can mimic the fanout gate.
- Fredkin gate: $(x, 1, 0) \mapsto (x, \neg x, x)$ Cloning?
- Assume x input is superposition $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$, while leaving y = 1 and z = 0.
- This corresponds to the state

$$\begin{bmatrix} 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 \end{bmatrix}^T$$

No-Cloning Theorem (cont’d)

Multiply with Fredkin state:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{bmatrix}$$

Resulting state: $\frac{|0,1,0\rangle + |1,0,1\rangle}{\sqrt{2}}$

So for a classical bit x the Fredkin gate performs the fanout operation, but for a superposition:

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}, 1, 0\right) \mapsto \frac{|0,1,0\rangle + |1,0,1\rangle}{\sqrt{2}}$$

Not a fanout operation, no-cloning theorem safely stands.

Reading

- This lecture: Ch 5.3-5.4.
- Next lecture: Ch 6.1-??.

Algorithms

Lecture 7

Algorithms

- Deutsch's algorithm: $\{0,1\} \to \{0,1\}$
- Deutsch-Jozsa algorithm: $\{0,1\}^n \to \{0,1\}$
- Simon's periodicity algorithm: $\{0,1\}^n \to \{0,1\}^n$
- Grover's search algorithm: unordered array of size n in $\sqrt{n}$ time instead of n time
- Shor's factoring algorithm: factor numbers in polynomial time.

Basic steps in a quantum algorithm

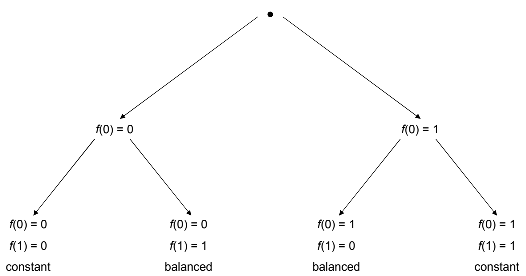
- All quantum algorithms:
  - The system will start with the qubits in a particular classical state.
  - The system is put into a superposition of many states.
  - Acting on this superposition with several unitary operations.
  - A measurement of the qubits

Deutsch's algorithm

- Simplest quantum algorithm
- Concerned with functions from the set {0,1} to the set {0,1}

- A function f: $\{0,1\} \to \{0,1\}$ is balanced if $f(0) \neq f(1)$, i.e. it is one to one; in contrast it is constant if $f(0) = f(1)$.
- Deutsch's algorithm: given a function f: $\{0,1\} \to \{0,1\}$ as a black box, where one can evaluate an input, but cannot "look inside" and "see" how the function is defined, determine if the function is balanced or constant.

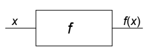
Classical computer

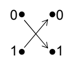


With a classical computer f must be evaluate twice; can we do better on a quantum computer?

A quantum computer can be in a superposition of two basic states at the same time.

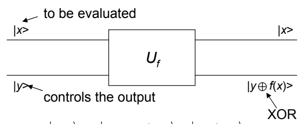
Evaluation of a function

- Classical: 



$\leftrightarrow \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$

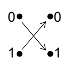
- Quantum system
  - Unitary (reversible)



$$|x,0\rangle \mapsto |x,0 \oplus f(x)\rangle = |x, f(x)\rangle$$

U_f is its own reverse:

$$|x,y\rangle \mapsto |x, y \oplus f(x)\rangle$$
$$\mapsto |x,(y \oplus f(x)) \oplus f(x)\rangle = |x, y \oplus (f(x) \oplus f(x))\rangle = |x, y \oplus 0\rangle = |x,y\rangle$$



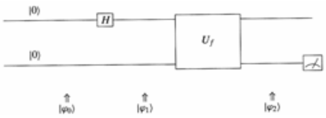
$$\leftrightarrow \quad U_f = \begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

Quantum "trick"

- Rather than evaluating *f* twice, put the top input in superposition: $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$
- This can be achieved by the Hadamard matrix:

$$H|0\rangle=\begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}=\frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

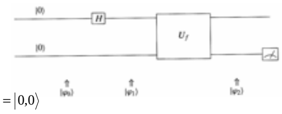
- Following quantum circuit:



- In terms of matrices:

$$U_f(H\otimes I)\big(|0\rangle\otimes|0\rangle\big)=U_f(H\otimes I)\big(|0,0\rangle\big)$$

Quantum "trick" (cont'd)



The system starts in $|\varphi_0\rangle=|0\rangle\otimes|0\rangle=|0,0\rangle$

Apply Hadamard matrix on top input $|\varphi_1\rangle=\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]|0\rangle=\frac{|0,0\rangle+|1,0\rangle}{\sqrt{2}}$

Multiplying with U_f $|\varphi_2\rangle=\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}$

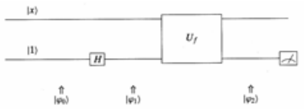
If we measure the top qubit, there will be a 50-50% chance of finding it in state |0> and a 50-50% chance of finding it in state |1>.

Similarly, there is no real information to be gotten by measuring the bottom qubit.

So the obvious algorithm does not work, we need a better trick!

Better "trick"

- Put the bottom qubit in the superposition state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, notice the minus sign!
- Quantum circuit:



- In terms of matrices: $U_f(I\otimes H)\big(|x,1\rangle\big)$
- Start with $|\varphi_0\rangle=|x,1\rangle$
- After the Hadamard matrix $|\varphi_1\rangle=|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]=\frac{|x,0\rangle-|x,1\rangle}{\sqrt{2}}$
- Applying U_f

$$|\varphi_2\rangle=|x\rangle\left[\frac{|0\oplus f(x)\rangle-|1\oplus f(x)\rangle}{\sqrt{2}}\right]=|x\rangle\left[\frac{|f(x)\rangle-|\overline{f(x)}\rangle}{\sqrt{2}}\right]=\begin{cases}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(x)=0\\ |x\rangle\left[\frac{|1\rangle-|0\rangle}{\sqrt{2}}\right] & \text{if } f(x)=1\end{cases}$$

Better "trick" (cont'd)

$$|\varphi_2\rangle=\begin{cases}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(x)=0\\ |x\rangle\left[\frac{|1\rangle-|0\rangle}{\sqrt{2}}\right] & \text{if } f(x)=1\end{cases}$$

with $(a-b)=(-1)(b-a)$

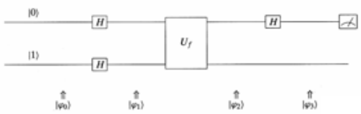
$$|\varphi_2\rangle=(-1)^{f(x)}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Evaluate top or bottom state?

No information: top qubit will be in state |x> and the bottom qubit either in state |0> or in state |1>……

Deutsch's algorithm

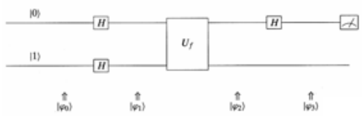
- Combine both "tricks":
  - Both top and bottom qubits in superposition
  - Result of top qubit through Hadamard matrix



- In terms of matrices:

$$(H\otimes I)U_f(H\otimes H)|0,1\rangle \quad \text{or} \quad (H\otimes I)U_f(H\otimes H)\begin{array}{c}00\\01\\10\\11\end{array}\begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

Deutsch's algorithm (cont'd)



- Start with $|\varphi_0\rangle=|0,1\rangle$
- and $|\varphi_1\rangle=\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]=\frac{+|0,0\rangle-|0,1\rangle+|1,0\rangle-|1,1\rangle}{2}=\begin{array}{c}00\\01\\10\\11\end{array}\begin{bmatrix}+\frac{1}{2}\\-\frac{1}{2}\\+\frac{1}{2}\\-\frac{1}{2}\end{bmatrix}$
- We saw that with bottom qubit in superposition and then multiply by U_f $(-1)^{f(x)}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$
- with |x> in a superposition, we have

$$|\varphi_2\rangle=\left[\frac{(-1)^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Deutsch's algorithm (cont'd)

- We have $|\varphi_2\rangle = \left[\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$
- Let have a look at $(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$
  - if *f* is constant $+1(|0\rangle+|1\rangle)$ or $-1(|0\rangle+|1\rangle)$ (constantly 0 or 1, resp.)
  - if *f* is balanced $+1(|0\rangle-|1\rangle)$ or $-1(|0\rangle-|1\rangle)$
- So we have $|\varphi_2\rangle = \begin{cases} (\pm 1)\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right], \text{if } f \text{ is constant} \\ (\pm 1)\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|1\rangle-|0\rangle}{\sqrt{2}}\right], \text{if } f \text{ is balanced} \end{cases}$
- Hadamard matrix is its own reverse $\frac{|0\rangle+|1\rangle}{\sqrt{2}} \mapsto |0\rangle$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}} \mapsto |1\rangle$
- Apply it to top qubit

$$|\varphi_3\rangle = \begin{cases} (\pm 1)|0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right], \text{if } f \text{ is constant} \\ (\pm 1)|1\rangle\left[\frac{|1\rangle-|0\rangle}{\sqrt{2}}\right], \text{if } f \text{ is balanced} \end{cases}$$

- Measure top qubit: if |0> then *f* is constant, otherwise balanced.
  Only one evaluation of *f*.

Deutsch's algorithm (cont'd)

Remarks:

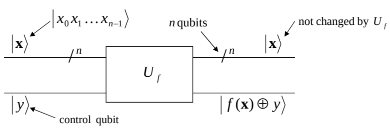
- The ±1 tells us which of the two balanced or constant functions we have, but can not be measured.
- Output of top qubit of U_f not the same as the input: inclusion of Hadamard matrices makes top and bottom qubits entangled.
- Trick? No changing around the information:
  1. Is the function balanced or constant?
  2. What is the value of the function on 0?

Deutsch-Jozsa algorithm

- Generalization:
  - $f: \{0,1\}^n \to \{0,1\}$, which accepts a string of *n* 0's and 1's (natural numbers from 0 to 2^{n-1}) and outputs a zero or one.
  - *f* is called balanced if exactly half of the inputs go to 0 (and the other half go to 1).
  - *f* is called constant if *all* the inputs go to 0 or *all* the inputs go to 1.
- Problem:
  - Given a function of $\{0,1\}^n$ to $\{0,1\}$, which you can evaluate but cannot "see" the way it is defined.
  - The function is either balanced or constant.
  - Determine if the function is balanced or constant.
  - *n*=1: Deutsch algorithm.
- Classically:
  - Evaluate the function on different inputs.
  - Best scenario: first two different inputs have different outputs → balanced function.
  - Worst scenario: $2^n/2+1 = 2^{n-1}+1$ evaluations.

Solution: superposition

- In Deutsch's algorithm we used the superposition of two possible input states. Now we enter a superposition of all 2^n possible input states.



Tensor product of Hadamard matrices

- Single qubit in superposition: single Hadamard matrix; *n* qubits in superposition: tensor product of *n* Hadamard matrices:

$$H, H \otimes H = H^{\otimes 2}, H \otimes H \otimes H = H^{\otimes 3}, \ldots, H^{\otimes n}$$

- Hadamard matrix definition:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ or } H[i,j] = \tfrac{1}{\sqrt{2}}(-1)^{i \wedge j} : \; H = \frac{1}{\sqrt{2}}\begin{bmatrix} (-1)^{0\wedge 0} & (-1)^{0\wedge 1} \\ (-1)^{1\wedge 0} & (-1)^{1\wedge 1} \end{bmatrix}$$

0 and 1 as Boolean values, and $(-1)^0=1$ and $(-1)^1=-1$.

Tensor product of Hadamard matrices (cont'd)

- We can calculate

$$H^{\otimes 2} = H \otimes H = \frac{1}{\sqrt{2}}\begin{bmatrix} (-1)^{0\wedge 0} & (-1)^{0\wedge 1} \\ (-1)^{1\wedge 0} & (-1)^{1\wedge 1} \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix} (-1)^{0\wedge 0} & (-1)^{0\wedge 1} \\ (-1)^{1\wedge 0} & (-1)^{1\wedge 1} \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}} * \frac{1}{\sqrt{2}}\begin{bmatrix} (-1)^{0\wedge 0}*(-1)^{0\wedge 0} & (-1)^{0\wedge 0}*(-1)^{0\wedge 1} & (-1)^{0\wedge 1}*(-1)^{0\wedge 0} & (-1)^{0\wedge 1}*(-1)^{0\wedge 1} \\ (-1)^{0\wedge 0}*(-1)^{1\wedge 0} & (-1)^{0\wedge 0}*(-1)^{1\wedge 1} & (-1)^{0\wedge 1}*(-1)^{1\wedge 0} & (-1)^{0\wedge 1}*(-1)^{1\wedge 1} \\ (-1)^{1\wedge 0}*(-1)^{0\wedge 0} & (-1)^{1\wedge 0}*(-1)^{0\wedge 1} & (-1)^{1\wedge 1}*(-1)^{0\wedge 0} & (-1)^{1\wedge 1}*(-1)^{0\wedge 1} \\ (-1)^{1\wedge 0}*(-1)^{1\wedge 0} & (-1)^{1\wedge 0}*(-1)^{1\wedge 1} & (-1)^{1\wedge 1}*(-1)^{1\wedge 0} & (-1)^{1\wedge 1}*(-1)^{1\wedge 1} \end{bmatrix}$$

- We are not interested in $(-1)^{x+y}$, but in the parity of *x* and *y* (exclusive-or):

$$H^{\otimes 2} = \frac{1}{2}\begin{bmatrix} (-1)^{0\wedge 0\oplus 0\wedge 0} & (-1)^{0\wedge 0\oplus 0\wedge 1} & (-1)^{0\wedge 1\oplus 0\wedge 0} & (-1)^{0\wedge 1\oplus 0\wedge 1} \\ (-1)^{0\wedge 0\oplus 1\wedge 0} & (-1)^{0\wedge 0\oplus 1\wedge 1} & (-1)^{0\wedge 1\oplus 1\wedge 0} & (-1)^{0\wedge 1\oplus 1\wedge 1} \\ (-1)^{1\wedge 0\oplus 0\wedge 0} & (-1)^{1\wedge 0\oplus 0\wedge 1} & (-1)^{1\wedge 1\oplus 0\wedge 0} & (-1)^{1\wedge 1\oplus 0\wedge 1} \\ (-1)^{1\wedge 0\oplus 1\wedge 0} & (-1)^{1\wedge 0\oplus 1\wedge 1} & (-1)^{1\wedge 1\oplus 1\wedge 0} & (-1)^{1\wedge 1\oplus 1\wedge 1} \end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Tensor product of Hadamard matrices (cont'd)

- Proved by induction that the scalar coefficient of $H^{\otimes n}$ is $\frac{1}{\sqrt{2^n}} = 2^{-\frac{n}{2}}$
- Useful operation $\langle\ ,\ \rangle : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$

  Definition : given two binary strings of length n, $\mathbf{x} = x_0x_1x_2\ldots x_{n-1}$ and $\mathbf{y} = y_0y_1y_2\ldots y_{n-1}$, we have

  $$\langle \mathbf{x},\mathbf{y}\rangle = \langle x_0x_1x_2\ldots x_{n-1}, y_0y_1y_2\ldots y_{n-1}\rangle$$
  $$= (x_0 \wedge y_0) \oplus (x_1 \wedge y_1) \oplus \cdots \oplus (x_{n-1} \wedge y_{n-1})$$

  - Basically it gives the parity of the number of times that both bits are 1.
- If **x** and **y** are binary strings of length n, then **x**$\oplus$**y** is the pointwise (bitwise) exclusive-or operation

  $$\mathbf{x} \oplus \mathbf{y} = x_0 \oplus y_0, x_1 \oplus y_1, \ldots, x_{n-1} \oplus y_{n-1}$$

$H^{\otimes 3}$

$$\frac{1}{2\sqrt{2}}\begin{array}{c} \\ \mathbf{000}\\ \mathbf{001}\\ \mathbf{010}\\ \mathbf{011}\\ \mathbf{100}\\ \mathbf{101}\\ \mathbf{110}\\ \mathbf{111}\end{array}\begin{array}{c}\begin{array}{cccccccc}\mathbf{000} & \mathbf{001} & \mathbf{010} & \mathbf{011} & \mathbf{100} & \mathbf{101} & \mathbf{110} & \mathbf{111}\end{array}\\ \left[\begin{array}{cccccccc}
(-1)^{\langle 000,000\rangle} & (-1)^{\langle 000,001\rangle} & (-1)^{\langle 000,010\rangle} & (-1)^{\langle 000,011\rangle} & (-1)^{\langle 000,100\rangle} & (-1)^{\langle 000,101\rangle} & (-1)^{\langle 000,110\rangle} & (-1)^{\langle 000,111\rangle}\\
(-1)^{\langle 001,000\rangle} & (-1)^{\langle 001,001\rangle} & (-1)^{\langle 001,010\rangle} & (-1)^{\langle 001,011\rangle} & (-1)^{\langle 001,100\rangle} & (-1)^{\langle 001,101\rangle} & (-1)^{\langle 001,110\rangle} & (-1)^{\langle 001,111\rangle}\\
(-1)^{\langle 010,000\rangle} & (-1)^{\langle 010,001\rangle} & (-1)^{\langle 010,010\rangle} & (-1)^{\langle 010,011\rangle} & (-1)^{\langle 010,100\rangle} & (-1)^{\langle 010,101\rangle} & (-1)^{\langle 010,110\rangle} & (-1)^{\langle 010,111\rangle}\\
(-1)^{\langle 011,000\rangle} & (-1)^{\langle 011,001\rangle} & (-1)^{\langle 011,010\rangle} & (-1)^{\langle 011,011\rangle} & (-1)^{\langle 011,100\rangle} & (-1)^{\langle 011,101\rangle} & (-1)^{\langle 011,110\rangle} & (-1)^{\langle 011,111\rangle}\\
(-1)^{\langle 100,000\rangle} & (-1)^{\langle 100,001\rangle} & (-1)^{\langle 100,010\rangle} & (-1)^{\langle 100,011\rangle} & (-1)^{\langle 100,100\rangle} & (-1)^{\langle 100,101\rangle} & (-1)^{\langle 100,110\rangle} & (-1)^{\langle 100,111\rangle}\\
(-1)^{\langle 101,000\rangle} & (-1)^{\langle 101,001\rangle} & (-1)^{\langle 101,010\rangle} & (-1)^{\langle 101,011\rangle} & (-1)^{\langle 101,100\rangle} & (-1)^{\langle 101,101\rangle} & (-1)^{\langle 101,110\rangle} & (-1)^{\langle 101,111\rangle}\\
(-1)^{\langle 110,000\rangle} & (-1)^{\langle 110,001\rangle} & (-1)^{\langle 110,010\rangle} & (-1)^{\langle 110,011\rangle} & (-1)^{\langle 110,100\rangle} & (-1)^{\langle 110,101\rangle} & (-1)^{\langle 110,110\rangle} & (-1)^{\langle 110,111\rangle}\\
(-1)^{\langle 111,000\rangle} & (-1)^{\langle 111,001\rangle} & (-1)^{\langle 111,010\rangle} & (-1)^{\langle 111,011\rangle} & (-1)^{\langle 111,100\rangle} & (-1)^{\langle 111,101\rangle} & (-1)^{\langle 111,110\rangle} & (-1)^{\langle 111,111\rangle}
\end{array}\right]\end{array}$$

$$= \frac{1}{2\sqrt{2}}\begin{array}{c} \\ \mathbf{000}\\ \mathbf{001}\\ \mathbf{010}\\ \mathbf{011}\\ \mathbf{100}\\ \mathbf{101}\\ \mathbf{110}\\ \mathbf{111}\end{array}\begin{array}{c}\begin{array}{cccccccc}\mathbf{000} & \mathbf{001} & \mathbf{010} & \mathbf{011} & \mathbf{100} & \mathbf{101} & \mathbf{110} & \mathbf{111}\end{array}\\ \left[\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1\\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1\\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1\\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1\\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1\\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1\\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1
\end{array}\right]\end{array}.$$

Tensor product of Hadamard matrices (cont'd)

- General formula

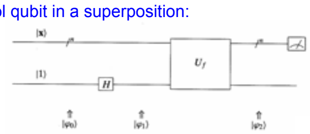
  $$H^{\otimes n}[\mathbf{i},\mathbf{j}] = \frac{1}{\sqrt{2^n}}(-1)^{\langle \mathbf{i},\mathbf{j}\rangle}, \text{ where } \mathbf{i} \text{ and } \mathbf{j} \text{ are the row and column numbers in binary.}$$

- What happens if we multiply a state with this matrix? Notice all elements of the leftmost column of $H^{\otimes n}$ are +1. So if we multiply with the state |**0**> = |00…0> = $[1,0,\ldots,0]^T$ this will be equal to the leftmost column of $H^{\otimes n}$:

$$H^{\otimes n}|\mathbf{0}\rangle = H^{\otimes n}[-,\mathbf{0}] = \frac{1}{\sqrt{2^n}}\begin{array}{c}00000000\\ 00000001\\ 00000010\\ \vdots\\ 11111110\\ 11111111\end{array}\left[\begin{array}{c}1\\1\\1\\ \vdots\\1\\1\end{array}\right] = \frac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\{0,1\}^n}|\mathbf{x}\rangle$$

Deutsch-Jozsa algorithm

- Bottom control qubit in a superposition:



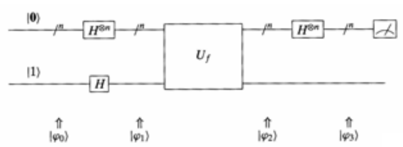
- In terms of matrices $U_f(I \otimes H)|\mathbf{x},1\rangle$
- We start with $|\varphi_0\rangle = |\mathbf{x},1\rangle$
- After the bottom Hadamard matrix $|\varphi_1\rangle = |\mathbf{x}\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] = \frac{|\mathbf{x},0\rangle - |\mathbf{x},1\rangle}{\sqrt{2}}$
- Applying U_f $|\varphi_2\rangle = |\mathbf{x}\rangle\left[\frac{|f(\mathbf{x})\oplus 0\rangle - |f(\mathbf{x})\oplus 1\rangle}{\sqrt{2}}\right] = |\mathbf{x}\rangle\left[\frac{|f(\mathbf{x})\rangle - |\overline{f(\mathbf{x})}\rangle}{\sqrt{2}}\right]$

  $$= \begin{cases} |\mathbf{x}\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(\mathbf{x}) = 0\\ |\mathbf{x}\rangle\left[\frac{|1\rangle-|0\rangle}{\sqrt{2}}\right] & \text{if } f(\mathbf{x}) = 1\end{cases} = (-1)^{f(\mathbf{x})}|\mathbf{x}\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

- Useless!

Deutsch-Jozsa algorithm (cont'd)

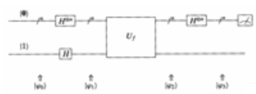
- Put |**x**> into a superposition in which all 2^n possible strings have equal probability



- In terms of matrices $(H^{\otimes n} \otimes I)U_f(H^{\otimes n} \otimes H)|\mathbf{0},1\rangle$

Deutsch-Jozsa algorithm (cont'd)

$(H^{\otimes n} \otimes I)U_f(H^{\otimes n} \otimes H)|\mathbf{0},1\rangle$



We start with $|\varphi_0\rangle = |\mathbf{0},1\rangle$

Then $|\varphi_1\rangle = \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n}|\mathbf{x}\rangle}{\sqrt{2^n}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$

Applying U_f $|\varphi_2\rangle = \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{f(\mathbf{x})}|\mathbf{x}\rangle}{\sqrt{2^n}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$

Make a superposition of a superposition on the top qubits

$$|\varphi_3\rangle = \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{f(\mathbf{x})}\sum_{\mathbf{z}\in\{0,1\}^n}(-1)^{\langle \mathbf{z},\mathbf{x}\rangle}|\mathbf{z}\rangle}{2^n}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Deutsch-Jozsa algorithm (cont'd)

$$|\varphi_3\rangle = \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{f(\mathbf{x})}\sum_{\mathbf{z}\in\{0,1\}^n}(-1)^{\langle\mathbf{z},\mathbf{x}\rangle}|\mathbf{z}\rangle}{2^n}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

$$= \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n}\sum_{\mathbf{z}\in\{0,1\}^n}(-1)^{f(\mathbf{x})}(-1)^{\langle\mathbf{z},\mathbf{x}\rangle}|\mathbf{z}\rangle}{2^n}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

$$= \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n}\sum_{\mathbf{z}\in\{0,1\}^n}(-1)^{f(\mathbf{x})\otimes\langle\mathbf{z},\mathbf{x}\rangle}|\mathbf{z}\rangle}{2^n}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Measure top qubit of φ_3; what is the probability that it will collapse to state |**0**>?

Answer: set **z** = **0** and realize that <**z**,**x**> = <**0**,**x**> = 0 for all x. Then

$$|\varphi_3\rangle = \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{f(\mathbf{x})}|\mathbf{0}\rangle}{2^n}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Deutsch-Jozsa algorithm (cont'd)

$$|\varphi_3\rangle = \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{f(\mathbf{x})}|\mathbf{0}\rangle}{2^n}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Probability of collapsing to |**0**> is totally dependent on *f* (**x**).

If *f* (**x**) is constant 1, the top qubits become

$$\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)|\mathbf{0}\rangle}{2^n} = \frac{-(2^n)|\mathbf{0}\rangle}{2^n} = -1|\mathbf{0}\rangle$$

If *f* (**x**) is constant 0, the top qubits become

$$\frac{\sum_{\mathbf{x}\in\{0,1\}^n}1|\mathbf{0}\rangle}{2^n} = \frac{2^n|\mathbf{0}\rangle}{2^n} = +1|\mathbf{0}\rangle$$

If *f* (**x**) is balanced, then half of the **x**'s will cancel the other half and the top qubits become

$$\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{f(\mathbf{x})}|\mathbf{0}\rangle}{2^n} = \frac{0|\mathbf{0}\rangle}{2^n} = 0|\mathbf{0}\rangle$$

We only get |**0**> if the function is constant. If anything else is measured, then the function is balanced.

Only one function evaluation instead of 2^{n-1}: exponential speedup!

Simon's periodicity algorithm

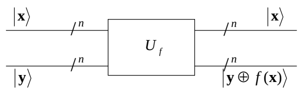
- Finding patterns in functions.
- Given a function $f: \{0,1\}^n \to \{0,1\}^n$ that we can evaluate, but is given as a black box.
- There is a secret (hidden) binary string $\mathbf{c} = c_0c_1c_2\ldots c_{n-1}$, such that for all strings **x**, **y** we have

  $$f(\mathbf{x}) = f(\mathbf{y}) \text{ if and only if } \mathbf{x} = \mathbf{y} \oplus \mathbf{c}$$
- In other words, the values of *f* repeat themselves in some pattern, and the pattern is determined by **c**, the period of *f*.
- Goal of Simon's algorithm is to determine **c**.

Example

- Let *n* = 3. Consider **c** = 101. Then we have the following requirements on *f*:

  $000 \oplus 101 = 101$; hence, $f(000) = f(101)$.
  $001 \oplus 101 = 100$; hence, $f(001) = f(100)$.
  $010 \oplus 101 = 111$; hence, $f(010) = f(111)$.
  $011 \oplus 101 = 110$; hence, $f(011) = f(110)$.
  $100 \oplus 101 = 001$; hence, $f(100) = f(001)$.
  $101 \oplus 101 = 000$; hence, $f(101) = f(000)$.
  $110 \oplus 101 = 011$; hence, $f(110) = f(011)$.
  $111 \oplus 101 = 010$; hence, $f(111) = f(010)$.
- Notice that if **c** = 0^n, then the function is one to one; otherwise it is two to one.



Classically

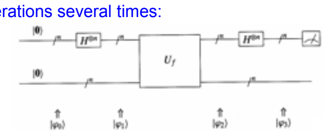
- Evaluate *f* on different binary strings.
- After each evaluation, check if the output has already been found.
- If for two input $\mathbf{x}_1$ and $\mathbf{x}_2$ holds $f(\mathbf{x}_1) = f(\mathbf{x}_2)$ then

  $$\mathbf{x}_1 = \mathbf{x}_2 \oplus \mathbf{c}$$
- and can **c** be obtained by

  $$\mathbf{x}_1 \oplus \mathbf{x}_2 = \mathbf{x}_2 \oplus \mathbf{c} \oplus \mathbf{x}_2 = \mathbf{c}$$
- If the function is two-to-one, we do not have to evaluate more than half the inputs before we get a repeat. If we have to evaluate more, we know **c** = 0^n. So, the worst case is $2^n/2 + 1 = 2^{n-1} + 1$.
- Can we do better?

Quantum version

- Performing the following operations several times:



- We start with $|\varphi_0\rangle = |\mathbf{0},\mathbf{0}\rangle$
- Put the input in a superposition of all possible inputs

  $$|\varphi_1\rangle = \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n}|\mathbf{x},\mathbf{0}\rangle}{\sqrt{2^n}}\right]$$
- Evaluation of *f* on all these possibilities

  $$|\varphi_2\rangle = \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n}|\mathbf{x}, f(\mathbf{x})\rangle}{\sqrt{2^n}}\right]$$
- Apply *n* Hadamard tensor product

  $$|\varphi_3\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^n}\sum_{\mathbf{z}\in\{0,1\}^n}(-1)^{\langle\mathbf{z},\mathbf{x}\rangle}|\mathbf{z}, f(\mathbf{x})\rangle}{2^n}$$

Quantum version (cont'd)

- For each input **x** and for each **z**, we know that the following kets are equal

$$|\mathbf{z}, f(\mathbf{x})\rangle \quad \text{and} \quad |\mathbf{z}, f(\mathbf{x} \oplus \mathbf{c})\rangle$$

- The coefficient for this ket is $\dfrac{(-1)^{\langle \mathbf{z},\mathbf{x}\rangle} + (-1)^{\langle \mathbf{z},\mathbf{x}\oplus\mathbf{c}\rangle}}{2^n}$
- <–,–> is an inner product, so $\dfrac{(-1)^{\langle \mathbf{z},\mathbf{x}\rangle} + (-1)^{\langle \mathbf{z},\mathbf{x}\oplus\mathbf{c}\rangle}}{2^n} = \dfrac{(-1)^{\langle \mathbf{z},\mathbf{x}\rangle} + (-1)^{\langle \mathbf{z},\mathbf{x}\rangle \oplus \langle \mathbf{z},\mathbf{c}\rangle}}{2^n}$

$$= \frac{(-1)^{\langle \mathbf{z},\mathbf{x}\rangle} + (-1)^{\langle \mathbf{z},\mathbf{x}\rangle}(-1)^{\langle \mathbf{z},\mathbf{c}\rangle}}{2^n}$$

- If <**z**,**c**> = 1, the terms will cancel each out and we would get $0/2^n$. In contrast, if <**z**,**c**> = 0, the sum will be $\pm 2/2^n = \pm 1/2^{n-1}$.
- So we will only find those binary strings such that <**z**,**c**> = 0.

Quantum version (cont'd)

- Some concrete examples in the book! Pages 190-195.

Reader Tip. Warning: admittedly, working out all the gory details of an example can be a bit scary. We recommend that the less meticulous reader move on to the next section for now. Return to this example on a calm sunny day, prepare a good cup of your favorite tea or coffee, and go through the details: the effort will pay off. ♡

- In conclusion, for given periodic *f*, we can find the period **c** in *n* function evaluations. This in contrast to the $2^{n-1} + 1$ needed classically.

???

Reading

- This lecture: Ch 6.1-6.3
- Next lecture: Ch 6.4-6.5

Algorithms

Grover's search algorithm

Shor's factoring algorithm

Lecture 8

Grover's search algorithm

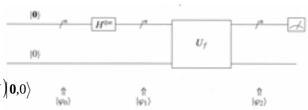
- Search element in an unordered array of size m in $\sqrt{m}$ time instead of $m/2$ time on average.
- In terms of functions, given a function $f : \{0,1\}^n \to \{0,1\}$, where there exists exactly one binary string $\mathbf{x_0}$, such that:

$$f(\mathbf{x}) = \begin{cases} 1, & \text{if } \mathbf{x} = \mathbf{x_0} \\ 0, & \text{if } \mathbf{x} \neq \mathbf{x_0} \end{cases}$$

- Find $\mathbf{x_0}$. Classically, in the worst case, we have to evaluate all 2^n binary strings. Grover's algorithm demands only $\sqrt{2^n} = 2^{n/2}$ evaluations.

First try

- Put |**x**> into a superposition of all possible strings and then evaluate U_f



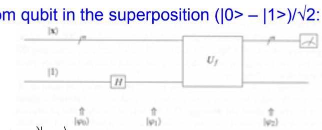
- In terms of matrices $U_f\left(H^{\otimes n} \otimes I\right)|\mathbf{0},0\rangle$
- The states are

$$|\varphi_0\rangle = |\mathbf{0},0\rangle, \quad |\varphi_1\rangle = \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle}{\sqrt{2^n}}\right]|0\rangle, \quad |\varphi_2\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}, f(\mathbf{x})\rangle}{\sqrt{2^n}}$$

- Measuring the top qubits will, with equal probability, give one of the 2^n binary strings. Measuring the bottom qubit will give |0> with probability $2^{n-1}/2^n$, and |1> with probability $1/2^n$. If one is lucky enough to measure |1>, the top qubits will have the correct answer, because of the entanglement. However, probably not so lucky.

First trick: phase inversion

- Change the phase of the desired state.
- Take U_f and place the bottom qubit in the superposition (|0> – |1>)/√2:



- In terms of matrices: $U_f\left(I_n \otimes H\right)|\mathbf{x},1\rangle$
- The states are:

$$|\varphi_0\rangle = |\mathbf{x},1\rangle,$$

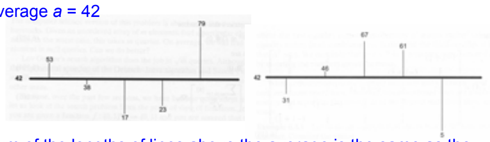
$$|\varphi_1\rangle = |\mathbf{x}\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] = \left[\frac{|\mathbf{x},0\rangle - |\mathbf{x},1\rangle}{\sqrt{2}}\right],$$

$$|\varphi_2\rangle = |\mathbf{x}\rangle\left[\frac{|f(\mathbf{x})\oplus 0\rangle - |f(\mathbf{x})\oplus 1\rangle}{\sqrt{2}}\right] = |\mathbf{x}\rangle\left[\frac{|f(\mathbf{x})\rangle - |\overline{f(\mathbf{x})}\rangle}{\sqrt{2}}\right] = \begin{cases} -1|\mathbf{x}\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } \mathbf{x} = \mathbf{x_0} \\ +1|\mathbf{x}\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } \mathbf{x} \neq \mathbf{x_0} \end{cases}$$

Example: $[½,½,½,½]^T$ and f chooses string "10", then after phase inversion: $[½,½,-½,½]^T$. Measuring |**x**> does not give any information $|½|^2 = |-½|^2 = ¼$.

Second trick: inversion about the mean or inversion about the average

- Boosting the separation of the phases.
- Explain with an example:
  - 53, 38, 17, 23, and 79
  - Average *a* = 42



  - Sum of the lengths of lines above the average is the same as the sum of lines below.
  - Invert each element around the average: $v' = a + (a-v)$; example [53, 38, 17, 23, 79] → [31, 46, 67, 61, 5]
  - In terms of matrices: $V' = (-I + 2A)V$, with $A[i,j] = 1/n$.

Inversion about the mean or average (cont'd)

- In general: n qubits, 2^n possible states, where a state is 2^n vector. Then 2^n-by-2^n matrix

$$A = \begin{bmatrix} \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \vdots & \vdots & \ddots & \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \end{bmatrix}$$

- Multiply any state by a will give state where each amplitude will be the average of all amplitudes.
- The 2^n-by-2^n matrix

$$-I + 2A = \begin{bmatrix} -1+\frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & -1+\frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \vdots & \vdots & \ddots & \\ \frac{2}{2^n} & \frac{2}{2^n} & \cdots & -1+\frac{2}{2^n} \end{bmatrix}$$

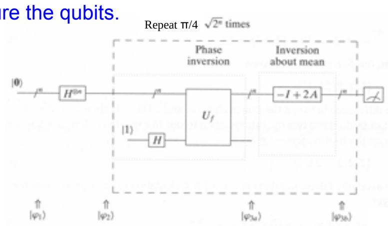
- Multiply a state by $-I+2A$ will invert amplitudes about the mean.

Phase inversion **and** inversion about the mean

- Combination is a powerful operation that separates the amplitude of the desired state from those of all other states.
- Example that demonstrates the combined techniques:
  - Vector $[10,10,10,10]^T$
  - Phase inversion to the fourth element: $[10,10,10,–10,10]^T$
  - Inversion about the mean (=6; -v+2a=2 or 22): $[2,2,2,22,2]^T$
  - Another phase inversion: $[2,2,2,–22,2]^T$
  - Inversion about the mean (=–2.8, -v+2a=–7.6 or 16.4): $[–7.6,–7.6, –7.6,16.4,–7.6]^T$
  - Another time? No, π/4√*n* times, otherwise the numbers will be "overcooked".

Grover's algorithm

1) Start with a state |**0**>
2) Apply $H^{\otimes n}$
3) Repeat π/4√2^n times:
   a) Apply the phase inversion operators: $U_f(I \otimes H)$
   b) Apply the inversion about the mean operation: $-I + 2A$
4) Measure the qubits.



Example Grover's algorithm

- Let *f* be a function that picks out the string "101".
- The states: $|\varphi_1\rangle = [1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0]^T$,

$$|\varphi_2\rangle = \begin{bmatrix} \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} \end{bmatrix}^T,$$

$$|\varphi_{3a}\rangle = \begin{bmatrix} \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & -\frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} \end{bmatrix}^T$$

- The average is: $a = \frac{7 * \frac{1}{\sqrt{8}} - \frac{1}{\sqrt{8}}}{8} = \frac{\frac{6}{\sqrt{8}}}{8} = \frac{3}{4\sqrt{8}}$
- Calculating the inversion about the mean:

$$-v + 2a = -\frac{1}{\sqrt{8}} + \left(2 \times \frac{3}{4\sqrt{8}}\right) = \frac{1}{2\sqrt{8}}$$

and

$$-v + 2a = \frac{1}{\sqrt{8}} + \left(2 \times \frac{3}{4\sqrt{8}}\right) = \frac{5}{2\sqrt{8}}$$

$$|\varphi_{3b}\rangle = \begin{bmatrix} \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{5\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} \end{bmatrix}^T$$

Example Grover's algorithm (cont'd)

- Another phase inversion:

$$|\varphi_{3a}\rangle = \begin{bmatrix} \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} & -\frac{1}{5\sqrt{8}} & \frac{1}{2\sqrt{8}} & \frac{1}{2\sqrt{8}} \end{bmatrix}^T$$

- The average is: $a = \frac{7 * \frac{1}{2\sqrt{8}} - \frac{5}{2\sqrt{8}}}{8} = \frac{1}{8\sqrt{8}}$
- Calculating the inversion about the mean:

$$-v + 2a = -\frac{1}{2\sqrt{8}} + \left(2 \times \frac{1}{8\sqrt{8}}\right) = -\frac{1}{4\sqrt{8}}$$

and

$$-v + 2a = \frac{5}{2\sqrt{8}} + \left(2 \times \frac{1}{8\sqrt{8}}\right) = \frac{11}{4\sqrt{8}}$$

$$|\varphi_{3b}\rangle = \begin{bmatrix} \frac{-1}{4\sqrt{8}} & \frac{-1}{4\sqrt{8}} & \frac{-1}{4\sqrt{8}} & \frac{-1}{4\sqrt{8}} & \frac{-1}{4\sqrt{8}} & \frac{11}{4\sqrt{8}} & \frac{-1}{4\sqrt{8}} & \frac{-1}{4\sqrt{8}} \end{bmatrix}^T$$

- 11/4√8=0.97 and -1/4√8=-0.088, and squaring these numbers gives us the probability of measuring the corresponding states. Most likely we will measure:

$$|\varphi_4\rangle = [0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0]^T$$

OK!

Generalizations Grover's algorithm

- Search an unordered array of size *m* in *m* time → √*m* time: quadratic speedup.
- What if there is more than one hit? Assume t objects: Grover's algorithm still works, but one must go through the loop π/4√(2^n/*t*) times.
- Many other types of generalizations and assorted changes.

Shor's factoring algorithm

- Factoring integers important: security
- "Hard" on classical computers
- Peter Shor: in polynomial time on quantum computers
- Based on the fact that the factoring problem can be reduced to finding the period of a certain function (see Simon's algorithm)
- In practice *N* will be a large number
- Assume *N* is not a prime number. However, there exists a deterministic, polynomial algorithm that determine if *N* is prime.

Modular exponentiation

- Modular arithmetic: for a positive integer N and any integer a, we write a mod N for the remainder (or residue) of the quotient a/N, e.g. 99 mod 15 = 9.
- $a \equiv a'$ mod N, if and only if (a mod N) = (a' mod N) or equivalent, if N is a divisor of $a-a'$, i.e. $N|(a-a')$.
- Start of the algorithm: choose randomly an interger a that is less than N, but does not have a nontrivial factor in common with N. This can be tested by Euclid's algorithm to calculate GCD(a,N):
  - GCD ≠ 1: found a factor of N and done;
  - GCD = 1: a is called co-prime to N and we can use it.
- We need to find the powers of a mod N, that is, a^0 mod N, a^1 mod N, a^2 mod N, a^3 mod N, …
- In other words, we need to find the values of the function

$$f_{a,N}(x) = a^x \bmod N$$

Examples $f_{a,N}(x) = a^x \bmod N$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	…
$f_{2,15}(x)$	1	2	4	8	1	2	4	8	1	2	4	8	1	…

x	0	1	2	3	4	5	6	7	8	9	10	11	12	…
$f_{4,15}(x)$	1	4	1	4	1	4	1	4	1	4	1	4	1	…

x	0	1	2	3	4	5	6	7	8	9	10	11	12	…
$f_{13,15}(x)$	1	13	4	7	1	13	4	7	1	13	4	7	1	…

In book: N = 371

Not the values, but the period

- Not the values of $f_{a,N}(x) = a^x \bmod N$, but the period of this function, i.e., we need to find the smallest $r > 0$ such that $f_{a,N}(r) = a^r \bmod N = 1$
- Theorem in number theory that for any co-prime $a \leq N$, the function $f_{a,N}$ will output a 1 for some $r < N$. After it hits 1, e.g.,

$$\text{if} \quad f_{a,N}(r) = 1$$
$$\text{then} \quad f_{a,N}(r+1) = f_{a,N}(1)$$
$$\text{and in general} \quad f_{a,N}(r+s) = f_{a,N}(s)$$

Examples

x	0	1	2	3	4	5	6	7	8	9	10	11	12	…
$f_{2,15}(x)$	1	2	4	8	1	2	4	8	1	2	4	8	1	…

period 4

x	0	1	2	3	4	5	6	7	8	9	10	11	12	…
$f_{4,15}(x)$	1	4	1	4	1	4	1	4	1	4	1	4	1	…

period 2

x	0	1	2	3	4	5	6	7	8	9	10	11	12	…
$f_{13,15}(x)$	1	13	4	7	1	13	4	7	1	13	4	7	1	…

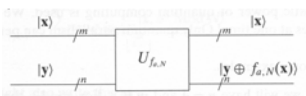
period 4

Quantum part of the algorithm

- For small numbers it is easy to determine the periods of these functions. But what if N is hundred digits long? This will be beyond the ability of any conventional computer: we need to calculate $f_{a,N}$ for ***all*** needed x: superposition.
- First we have to show that there is a quantum circuit that can implement $f_{a,N}$ (later).
- The output of this function will always be less than N, so we need $n = \log_2 N$ output qubits.
- We will need to evaluate $f_{a,N}$ for at least N^2 values of x, so we will need at least $m = \log_2 N^2 = 2 \log_2 N = 2n$ input qubits.

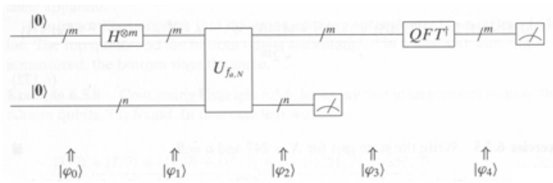
Quantum circuit for $U_{fa,N}$

- Operator $U_{fa,N}$



- where $|\mathbf{x},\mathbf{y}\rangle \mapsto |\mathbf{x},\mathbf{y} \oplus f_{a,N}(\mathbf{x})\rangle = |\mathbf{x},\mathbf{y} \oplus a^x \bmod N\rangle$
- How is it formed? Later…

Quantum circuit



$$(Measure \otimes I)(QFT^{\dagger} \otimes I)(I \otimes Measure)U_{f_{a,N}}(H^{\otimes m} \otimes I)|\mathbf{0}_m,\mathbf{0}_n\rangle$$

States $|\varphi_0\rangle$, $|\varphi_1\rangle$, and $|\varphi_2\rangle$

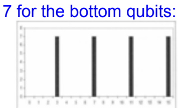
- We start at $|\varphi_0\rangle = |\mathbf{0}_m,\mathbf{0}_n\rangle$
- Then we place the input in an equally weighted superposition of all possible inputs
$$|\varphi_1\rangle = \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^m}|\mathbf{x},\mathbf{0}_n\rangle}{\sqrt{2^m}}\right]$$
- Evaluation of f on all these possibilities gives us
$$|\varphi_2\rangle = \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^m}|\mathbf{x}, f_{a,N}(\mathbf{x})\rangle}{\sqrt{2^m}}\right] = \left[\frac{\sum_{\mathbf{x}\in\{0,1\}^m}|\mathbf{x}, a^{\mathbf{x}} \bmod N\rangle}{\sqrt{2^m}}\right]$$
- These outputs are periodic, e.g., for N = 15, we have n = 4 and m = 8. For a = 13 we have
$$|\varphi_2\rangle = \frac{|0,1\rangle + |1,13\rangle + |2,4\rangle + |3,7\rangle + |4,1\rangle + \cdots |254,4\rangle + |255,7\rangle}{\sqrt{256}}$$

Measure $|\varphi_2\rangle$

- Measuring the bottom qubits gives us $a^{\bar{\mathbf{x}}} \bmod N$ for some $\bar{\mathbf{x}}$
- However, by periodicity we also have
$$a^{\bar{\mathbf{x}}} \equiv a^{\bar{\mathbf{x}}+r} \bmod N \quad \text{and} \quad a^{\bar{\mathbf{x}}} \equiv a^{\bar{\mathbf{x}}+2r} \bmod N,$$
$$\text{and in fact, for any } s \in Z: \quad a^{\bar{\mathbf{x}}} \equiv a^{\bar{\mathbf{x}}+sr} \bmod N$$
- How many of the 2^m superpositions **x** have $a^{\bar{\mathbf{x}}} \bmod N$ as output?
- Answer: $\left\lfloor \frac{2^m}{r} \right\rfloor$

State $|\varphi_3\rangle$

- So
$$|\varphi_3\rangle = \left[\frac{\sum_{a^{\mathbf{x}} \equiv a^{\bar{\mathbf{x}}} \bmod N}|\mathbf{x}, a^{\bar{\mathbf{x}}} \bmod N\rangle}{\sqrt{\left\lfloor \frac{2^m}{r} \right\rfloor}}\right]$$
- We might also write this as
$$|\varphi_3\rangle = \left[\frac{\sum_{j=0}^{2^m/r-1}|t_0 + jr, a^{\bar{\mathbf{x}}} \bmod N\rangle}{\sqrt{\left\lfloor \frac{2^m}{r} \right\rfloor}}\right]$$
- Here t_0 is the first time that the measured value occurs. It is called the offset of the period.
- Example (cont'd), let us say that we measure 7 for the bottom qubits:
$$|\varphi_3\rangle = \frac{|3,7\rangle + |7,7\rangle + |11,7\rangle + |15,7\rangle + \cdots |251,7\rangle + |255,7\rangle}{\sqrt{\left\lfloor \frac{256}{4} \right\rfloor}}$$



Vandermonde matrix

- Evaluating polynomials: $P(x) = a_0 + a_1x^1 + a_2x^2 + a_3x^3 + \cdots + a_{n-1}x^{n-1}$
- This polynomial can be represented by a column vector $[a_0, a_1, a_2, \cdots, a_{n-1}]^T$
- Suppose we want to evaluate this polynomial at numbers $x_0, x_1, x_2, \cdots, x_{n-1}$
- This can be achieved by

$$\begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^j & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^j & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^j & \cdots & x_2^{n-1} \\ \vdots & & & & \vdots & & \vdots \\ 1 & x_k & x_k^2 & \cdots & x_k^j & \cdots & x_k^{n-1} \\ \vdots & & & & \vdots & & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^j & \cdots & x_{n-1}^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_k \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} P(x_0) \\ P(x_1) \\ P(x_2) \\ \vdots \\ P(x_k) \\ \vdots \\ P(x_{n-1}) \end{bmatrix}.$$

Every row is a geometric series, matrix is called the **Vandermonde matrix**, denoted by $V(x_0, x_1, x_2, \cdots, x_{n-1})$

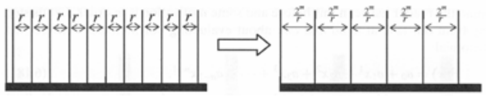
Vandermonde matrix (cont'd)

- Elements changed to "powers of one of the M^{th} roots of unity ω^1_M" (chapter 1)
- $M = 2^m$ is fixed, so ω_M is simply ω. We obtain the M-by-M Vandermonde matrix $\mathbf{V}(\omega^0, \omega^1, \omega^2, \ldots, \omega^{M-1})$
- To evaluate $P(x)$ at the powers of one of the M^{th} roots of unity

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & \cdots & 1 \\ 1 & \omega^1 & \omega^2 & \cdots & \omega^j & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^{2\times 2} & \cdots & \omega^{2j} & \cdots & \omega^{2(M-1)} \\ \vdots & & & & \vdots & & \vdots \\ 1 & \omega^k & \omega^{k2} & \cdots & \omega^{kj} & \cdots & \omega^{k(M-1)} \\ \vdots & & & & \vdots & & \vdots \\ 1 & \omega^{M-1} & \omega^{(M-1)2} & \cdots & \omega^{(M-1)j} & \cdots & \omega^{(M-1)(M-1)} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_k \\ \vdots \\ a_{M-1} \end{bmatrix} = \begin{bmatrix} P(\omega^0) \\ P(\omega^1) \\ P(\omega^2) \\ \vdots \\ P(\omega^k) \\ \vdots \\ P(\omega^{M-1}) \end{bmatrix}.$$

Discrete Fourier transform

- Definition of discrete Fourier transform (DFT)
  $$DFT = \frac{1}{\sqrt{M}}\mathbf{V}(\omega^0, \omega^1, \omega^2, \ldots, \omega^{M-1})$$
- Formally, DFT is defined as $DFT = \frac{1}{\sqrt{M}}\omega^{jk}$
- Two tasks:
  - It modifies the period from r to $2^m/r$
  - It eliminates the offset.



Quantum Fourier transform

- Denoted by *QFT*.
- Same operation, but more suitable for quantum computers.
- This quantum version is very fast and made of “small” unitary operators that are easy to implement.

Measure the top qubits

- Assumption that r evenly divides into 2^m (not in Shor’s actual algorithm: finding period for any r). So we measure the top qubit and we will find some multiple of $2^m/r$. We will measure
  $$x = \frac{\lambda 2^m}{r} \quad \text{for some whole number } \lambda$$
- We know 2^m and after measurement also x, so we get
  $$\frac{x}{2^m} = \frac{\lambda 2^m}{r 2^m} = \frac{\lambda}{r}$$
- Reduce this number to an irreducible fraction and take the denominator to be the period r. If we don’t make the simplifying assumption, given above: perform this process several times.

From the Period to the Factors

- Assumption the period r is an even number; if not, choose another a.
- So $a^r \equiv 1 \bmod N$ and we may subtract 1 from both sides to get $a^r - 1 \equiv 0 \bmod N$, or equivalently $N \mid (a^r - 1)$.
- Or $N \mid (\sqrt{a^r} + 1)(\sqrt{a^r} - 1)$ or $N \mid (a^{r/2} + 1)(a^{r/2} - 1)$, remember r is even.
- So any factor of N is also a factor of either $(a^{r/2} + 1)$ or $(a^{r/2} - 1)$ or both.
- Either way, a factor for N can be found by looking at GCD($(a^{r/2} + 1)$, N) and GCD($(a^{r/2} - 1)$, N), which can be done by the classical Euclidean algorithm.
- One problem: be sure that $a^{r/2} \neq -1 \bmod N$. Solution: start over again.
- Example: period $f_{2,15}$ is 4. So GCD(5,15)=5 and GCD(3,15)=3.

Shor’s algorithm

- Putting all pieces together, see p217 of the book.
- Complexity of this algorithm? $O(n^2 \log n \log\log n)$, where n is the number of bits to represent the number N.
- The best classical algorithms demand
  $$O(e^{cn^{1/3}\log^{2/3} n}) \quad \text{where } c \text{ is some constant}$$
- This is exponential in terms of n.
- Implementation of $U_{fa,N}$: see p217-218.

Final remark

“Even if a real implementation of large-scale quantum computers is years away, the design and study of quantum algorithms is something that is ongoing and is an exciting field of interest.”

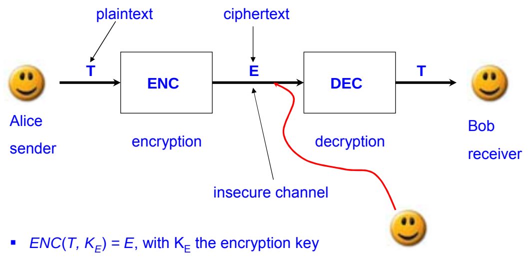
Reading

- This lecture: Ch 6.4-6.5
- Next lecture: Ch 9

Cryptography

Lecture 9

Classical Cryptography



- *ENC*$(T, K_E) = E$, with K_E the encryption key
- *DEC*$(E, K_D) = T$, with K_D the decryption key
- combining: *DEC*(*ENC*$(T,K_E),K_D) = T$

Encryption protocols

- Caesar's protocol:
  - *ENC* = *DEC* = shift(–,–), where shift $(T,n)=T'$, the string obtained from T by shifting each character n steps
  - Original message and encrypted one highly correlated.
- One-Time-Pad protocol of Vernam cipher:
  - Alice generates a random number of bits and uses that as her random key K.
  - Assume Alice and Bob both share K:
    - $K_E = K_D = K$
    - $ENC(T, K) = DEC(T, K) = T \oplus K$
    - $DEC(ENC(T,K),K) = DEC(T \oplus K,K) = (T \oplus K) \oplus K = T \oplus (K \oplus K) = T$

One-Time-Pad protocol example

Original message T	0 1 1 0 1 1
Encryption key K	1 1 1 0 1 0
Encrypted message E	1 0 0 0 0 1
Public channel	↓ ↓ ↓ ↓ ↓ ↓
Received message E	1 0 0 0 0 1
Decryption key K	1 1 1 0 1 0
Decrypted message T	0 1 1 0 1 1

Two issues:

1) Generation of a new key K is required each time a new message is sent. Otherwise, the text can be discovered through statistical analysis. Hence the name "One-Time-Pad".
2) The protocol is secure only insofar as the key K is not intercepted by Eve.

Private key

So far, we assumed that the pair of keys K_E and K_D are kept secret. In fact, only one key was needed. A protocol where the two keys are computable from each other, and thus requiring that *both* keys be kept secret, is said to be private key.

Public-key cryptography

- RSA (Rivest, Shamir, and Adleman, 1978): the knowledge of one key does not enable us to calculate the second one, since the computation will be hard (more than polynomial in the length of the first key).
- Suppose Bob has such a pair of keys K_E and K_D:
  - K_E in public domain.
  - He can safely advertise the protocol, i.e., *ENC*(–,–) and *DEC*(–,–).
  - He guards K_D for himself.
  - Alice uses K_E on her message.
  - If Eve intercepts the encrypted text, she cannot retrieve Bob's decryption key, so the message is safe.
  - Bob has two computable functions:
    - $F_E(–) = ENC(–, K_E)$
    - $F_D(–) = DEC(–, K_D)$

F_E is a trapdoor function: easy to compute, hard to invert without extra information

Pros and cons of public-key cryptography

- Pro:
  - It solves the key distribution problem.
- Cons:
  - The computation of the private key from the public key *appears* to be hard.
  - Public-key protocols tend to be considerable slower than their private-key peers.
- Best of both worlds:
  - Use public-key cryptography to distribute a key K_E of some private-key protocol, rather than the entire text message. Once Alice and Bob safely share K_E they can use the faster private-key scheme.
  - Sending a binary K_E will be the only concern the rest of this class.

Other topics in cryptography

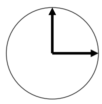
- Secure communication
- Intrusion detection: Alice and Bob would like to determine whether Eve is, in fact, eavesdropping.
- Authentication: we would like to ensure that nobody is impersonating Alice and sending false messages (outside the context of this course).

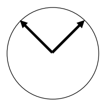
Quantum Key Exchange I: The BB84 Protocol

- 1984: Charles Bennett & Gilles Brassard introduced the first quantum key exchange (QKE) protocol, named BB84.
- Why using the quantum world?
  - Classical: Eve can make copies of arbitrary portions of the encrypted bit stream and store them somewhere.
  - Quantum: With qubits Eve cannot make perfect copies of the qubit stream due to the no-cloning theorem.
  - Classical: Eve can listen without affecting the bitstream, i.e., her eavesdropping does not leave traces.
  - Quantum: Measuring the qubit stream alters it.

BB84 protocol

- Alice wants to send Bob a key via a quantum channel.
- As in the One-Time-Pad protocol this key is a sequence of random (classical) bits.
- Alice will send a qubit each time she generates a new bit of her key.
- But which qubit should she send?
- She will use two different orthogonal bases:





"plus" basis $+ = \{|\rightarrow\rangle, |\uparrow\rangle\} = \{[1,0]^T, [0,1]^T\}$ "times" basis $\times = \{|\nwarrow\rangle, |\nearrow\rangle\} = \left\{\frac{1}{\sqrt{2}}[-1,1]^T, \frac{1}{\sqrt{2}}[1,1]^T\right\}$

State/Basis	+	x
$|0\rangle$	$|\rightarrow\rangle$	$|\nearrow\rangle$
$|1\rangle$	$|\uparrow\rangle$	$|\nwarrow\rangle$

- Basis states given by the table.
- What about superpositions?
  - If Bob measures photon using the + basis, he will only see photons as $|\rightarrow\rangle$ or $|\uparrow\rangle$.
  - What if Alice sends a $|\nearrow\rangle$ and Bob measures it in the + basis? Then it will be in a superposition of states

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$$

So there is a 50-50% chance of Bob's recording a $|0\rangle$ or a $|1\rangle$.

Four possible superpositions

- $|\nwarrow\rangle$ with respect to +, will be $\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\rightarrow\rangle$
- $|\nearrow\rangle$ with respect to +, will be $\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$
- $|\uparrow\rangle$ with respect to x, will be $\frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle$
- $|\rightarrow\rangle$ with respect to x, will be $\frac{1}{\sqrt{2}}|\nearrow\rangle - \frac{1}{\sqrt{2}}|\nwarrow\rangle$

BB84 step 1

- Alice flips a coin *n* times to determine which classical bits to send. She then flips the coin another *n* times to determine in which of the two bases to send those bits. She then sends the bits in their appropriate basis.

- Example for *n* = 12

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	0	1	1	0	1	1	1	0	1	0	1	0
Alice's random basis	+	+	x	+	+	+	x	+	x	x	x	+
Alice sends	→	↑	↖	→	↑	↑	↖	→	↖	↗	↖	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓

BB84 step 2

- As the sequence of qubits reaches Bob, he does not know which basis Alice used to send them, so to determine the basis by which to measure them he also tosses a coin. He then goes on to measure the qubit in those random bases.

- In our example:

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Bob's random bases	x	+	x	x	+	x	+	+	x	x	x	+
Bob observes	↗	↑	↖	↖	↑	↗	↑	→	↖	↗	↖	→
Bob;s bits	0	1	1	1	1	0	1	0	1	0	1	0

For about half of the time, Bob's basis will be the same as Alice's, in which case his result after measuring the qubit will be identical to Alice's original bit. The other half of the time, Bob's basis will differ from Alice's. In that case, the result of Bob's measurement will agree with Alice's original bit about 50% of the time.

- If Eve is eavesdropping, she must reading the information that Alice transmits and sending that information onward to Bob.

- Eve also has to toss a coin each time (Alice's basis unknown)

  – Basis identical: accurate measurement, and she will send accurate information to Bob.

  – Basis different: agreement with Alice's only 50% of the time. However, the qubit has now collapsed to one of the two elements of *Eve's basis*. Bob will receive it in the wrong basis. His chances are 50-50 of getting the same bit as Alice has. Therefore Eve's eavesdropping will negatively affect Bob's chances of agreement with Alice, which can be detected.

BB84 step 3

- Bob and Alice publicly compare which basis they used or chose at each step. Each time they disagree, Alice and Bob scratch out the corresponding bit. At the end they are each left with a subsequence of bits sent and received in same basis. If Eve was not listening to the quantum channel, this subsequence should be exactly identical. On average its length will be *n*/2.

- For our example

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random basis	+	+	x	+	+	+	x	+	x	x	x	+
Public channel	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Bob's random basis	x	+	x	x	+	x	+	+	x	x	x	+
Which agree?		ok	ok		ok			ok	ok	ok	ok	ok
Shared secret keys		1	1		1			0	1	0	1	0

BB84 step 4

- What if Eve was eavesdropping? Bob randomly chooses half of the *n*/2 bits and publicly compares them with Alice.
  – If they disagree by more than a tiny percentage (e.g., due to noise), they know Eve was listening in and then sending in what she received.
  – If the sequence is mostly similar, it means that either Eve has great guessing ability (improbable) or Eve was not listening in. They will use the remaining bits as private key.

- For our example

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Shared secret keys		1	1		1			0	1	0	1	0
Randomly chosen to compare			y						y	y		y
Public channel			⇕						⇕	⇕		⇕
Shared secret keys		1	1		1			0	1	0	1	0
Which agree?			ok						ok	ok		ok
Unrevealed secret keys		1			1			0			1	

BB84: #qubits?

- If we begin with *n* qubits, only *n*/2 qubits will be available after step 3.

- Furthermore, Alice and Bob publicly display half of the resulting qubits in step 4. This leaves *n*/4 of the original qubits.

- However, Alice can make her qubit stream as large as she wants: if she wants an *m* bit key, she simply starts with a 4*m* qubit stream.

Quantum Key Exchange II: The B92 Protocol

- Simplification of the BB84 protocol: the use of two different bases is redundant →
- The B92 protocol, invented by Charles Bennett, published in 1992.
- Main idea: Alice uses only one *nonorthogonal* basis.
- We will work out the protocol with the following example:

$$\{|\rightarrow\rangle, |\nearrow\rangle\} = \left\{[1,0]^T, \frac{1}{\sqrt{2}}[1,1]^T\right\}$$

Alice takes $|\rightarrow\rangle$ to be 0 and $|\nearrow\rangle$ to be 1.

Role of the nonorthogonal basis:

- All observables have an orthogonal basis of eigenvectors.
- Nonorthogonal basis → no observable whose basis of eigenvectors is the one we have chosen.
- No single experiment whose resulting states are precisely the members of our basis.
- In other words, no single experiment can be set up for the specific purpose of discriminating unambiguously between the nonorthogonal states of the basis.

B92 step 1

- Alice flips a coin *n* times and transmits to Bob *n* random bits in the appropriate polarization with a quantum channel.
- An example:

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	0	0	1	0	1	0	1	0	1	1	1	0
Alice's qubits	→	→	↗	→	↗	→	↗	→	↗	↗	↗	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓

B92 step 2

For each of the *n* qubits, Bob measures the received qubits in either the + or x basis. He flips a coin to determine which basis to use. Possible scenarios:

Used basis by Bob	Bob observes	Bob knows Alice must have sent	If Alice had sent	Then Bob should have received
+	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\rightarrow\rangle$	$\|\rightarrow\rangle$
+	$\|\rightarrow\rangle$	???	$\|\rightarrow\rangle$ or $\|\nearrow\rangle$	$\|\rightarrow\rangle$ (100% or 50%)
x	$\|\nwarrow\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$
x	$\|\nearrow\rangle$	???	$\|\nearrow\rangle$ or $\|\rightarrow\rangle$	$\|\nearrow\rangle$ (100% or 50%)

B92 step 2 (cont'd), 3 & 4

For our example:

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	→	→	↗	→	↗	→	↗	→	↗	↗	↗	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓
Bob's random basis	x	+	x	x	+	x	+	+	x	+	x	+
Bob's observations	↖	→	↗	↖	↑	↖	→	→	↗	↑	↗	→
Bob's bits	0	?	?	0	1	0	?	?	?	1	?	?

Step 3. Bob publicly tells Alice which bits were uncertain and they both omit them.

Step 4. To detect whether Eve was listening in, they can sacrifice half of their hidden bits, as in Step 4 of BB84.

Quantum Key Exchange III: The EPR Protocol

- A completely different type of QKE protocol based on entanglement, proposed by Artur K. Ekert in 1991.
- We will discuss a simplified version of the protocol and point to the original version.
- It is possible to place two qubits in the entangled state: $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$
- We have seen that when one of these qubits is measured, they both will collapse to the same value.
- Suppose Alice wants to send Bob a secret key.
  - A sequence of entangled pairs of qubits can be generated and sent.
  - When Alice and Bob wants to communicate, they can measure their respective qubits.
  - It does not matter who measures first, because both qubits will collapse to the same value.
  - Ready: Alice and Bob have a sequence of random bits that no one else has.

EPR protocol steps 1&2

Step 1. Alice and Bob are each assigned one of each of the pairs of a sequence of entangled qubits. When they are ready to communicate, they move to step 2.

Step 2. Alice and Bob separately choose a random sequence of bases to measure their particles. They then measure their qubits in their chosen basis.

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bases	x	x	+	+	x	+	x	+	+	x	+	x
Alice's observations	↗	↖	→	↑	↗	→	↖	→	→	↗	→	↗
Bob's random bases	x	+	+	x	x	+	+	+	+	x	x	+
Bob's observations	↗	→	→	↗	↗	→	↑	→	→	↗	↖	→

EPR protocol step 3

Step 3. Alice and Bob publicly compare what bases were used and keep only those bits that were measured in the same bases.

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bases	x	x	+	+	x	+	x	+	+	x	+	x
Public channel	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Bob's random bases	x	+	+	x	x	+	+	+	+	x	x	+
Which agree?	ok		ok		ok	ok		ok	ok	ok		

If everything worked fine, Alice and Bob share a totally random secret key.

Problems:

1. the entangled pairs could have become disentangled;
2. Eve could have taken hold of one of the pairs, measured them, and sent along disentangled qubits.

Solution: step 4 of BB84, compare half of the bits

Ekert's original protocol

- More sophisticated, measurements with three instead of two different bases.
- Bell's inequality:
  - Requires three different bases.
  - If particles are independent, then the measurements will satisfy the inequality.
  - If the particles are dependent, i.e., entangled, then Bell's inequality fails.
- Ekert proposed to use Bell's inequality to check if Alice and Bob's bit sequences were entangled, when they were measured.
- Details: see book, page 277.

Reading

- This lecture: Ch 9.1-9.4 Cryptography
- Next (last) lecture: Ch 9.5 Teleportation & Ch 11 Hardware

Exam

- Mon Jan 25, 2010, 10-13h

Quantum Teleportation

Hardware

Lecture 10

Quantum Teleportation

- It is the process by which the state of an arbitrary qubit is transferred from one location to another.
- Not science fiction, it has been performed in the laboratory.
- No-cloning theorem: not possible to make a copy of the state of an arbitrary qubit → when the state of the original qubit is teleported to another location, the state of the original will necessarily destroyed. “Move is possible, copy is impossible.”

Some preliminaries

- Switching between a canonical and a noncanonical basis can be helpful (see B92 protocol).
- A single qubit
  - Canonical basis $\{|0\rangle, |1\rangle\}$
  - Noncanonical basis $\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$

- The teleportation algorithm works with two entangled qubits, one held by Alice and one held by Bob.
- Obvious canonical basis for this 4-dimensional space
  $\{|0_A 0_B\rangle, |0_A 1_B\rangle, |1_A 0_B\rangle, |1_A 1_B\rangle\}$
- A noncanonical basis, called the Bell basis, consists of

$$|\Psi^+\rangle = \frac{|0_A 1_B\rangle + |1_A 0_B\rangle}{\sqrt{2}}$$

$$|\Psi^-\rangle = \frac{|0_A 1_B\rangle - |1_A 0_B\rangle}{\sqrt{2}}$$

$$|\Phi^+\rangle = \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$$

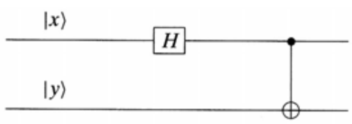
$$|\Phi^-\rangle = \frac{|0_A 0_B\rangle - |1_A 1_B\rangle}{\sqrt{2}}$$

- Every vector in this basis is entangled. See book for prove that it is indeed a basis.

- How are the Bell basis vectors formed?
- In the 2-dimensional case the elements of the noncanonical basis can be formed by the Hadamard matrix:

$$|0\rangle \to \frac{|0\rangle+|1\rangle}{\sqrt{2}} \quad \text{and} \quad |1\rangle \to \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

- In the 4-dimensional case:

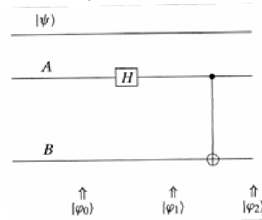


- It can be shown that this quantum circuit with appropriate inputs creates the elements of the Bell basis:

$$|00\rangle \to |\Phi^+\rangle, \quad |01\rangle \to |\Psi^+\rangle, \quad |10\rangle \to |\Phi^-\rangle, \quad |11\rangle \to |\Psi^-\rangle$$

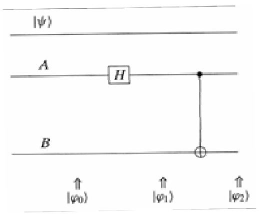
Quantum teleportation protocol

- Alice has qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in an arbitrary state that she would like to teleport to Bob.
- **Step 1.** Two entangled qubits are formed as $|\Phi^+\rangle$. One is given to Alice and one is give to Bob. Three qubits as three lines:



- The top two lines are in Alice’s possession and the bottom line in Bob’s.

Step 1



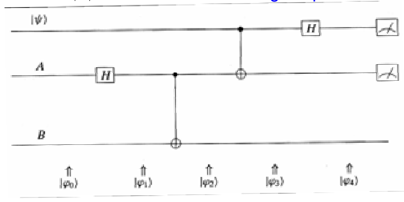
$$|\varphi_0\rangle = |\psi\rangle \otimes |0_A\rangle \otimes |0_B\rangle = |\psi\rangle \otimes |0_A 0_B\rangle,$$

$$|\varphi_1\rangle = |\psi\rangle \otimes \frac{|0_A\rangle + |1_A\rangle}{\sqrt{2}} \otimes |0_B\rangle,$$

$$|\varphi_2\rangle = |\psi\rangle \otimes |\Phi^+\rangle = |\psi\rangle \otimes \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$$
$$= (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$$
$$= \frac{\alpha|0\rangle(|0_A 0_B\rangle + |1_A 1_B\rangle) + \beta|1\rangle(|0_A 0_B\rangle + |1_A 1_B\rangle)}{\sqrt{2}}$$

Step 2

- Alice lets her $|\psi\rangle$ interact with her entangled qubit.



- We have $|\varphi_3\rangle = \dfrac{\alpha|0\rangle(|0_A 0_B\rangle + |1_A 1_B\rangle) + \beta|1\rangle(|1_A 0_B\rangle + |0_A 1_B\rangle)}{\sqrt{2}}$

$$|\varphi_4\rangle = \frac{1}{2}\left(\alpha(|0\rangle + |1\rangle)(|0_A 0_B\rangle + |1_A 1_B\rangle) + \beta(|0\rangle - |1\rangle)(|1_A 0_B\rangle + |0_A 1_B\rangle)\right)$$
$$= \frac{1}{2}\left(\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)\right)$$

Step 2 (cont'd)

- Regrouping these triplets $|xyz\rangle$ in terms of $|xy\rangle$, which is in Alice's possession

$$|\varphi_4\rangle = \frac{1}{2}\left(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\beta|0\rangle + \alpha|1\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(-\beta|0\rangle + \alpha|1\rangle)\right)$$

- So the system of three qubits is now in a superposition of four possible states.

Step 3

- Alice measures her two qubits and determines to which of the four possible states the system collapses.
- At the moment Alice measures her two qubits, all three qubits collapse to one of the four possibilities. So if she measures $|10\rangle$ then the third qubit is in state $\alpha|0\rangle - \beta|1\rangle$.
- Two problems:
  - Alice knows this state but Bob does not.
  - Bob has $\alpha|0\rangle - \beta|1\rangle$, not the desired $\alpha|0\rangle + \beta|1\rangle$
- Both problems are solved in Step 4.

Step 4

- Alice sends copies of her two bits (not qubits) to Bob who uses that information to achieve the desire state $|\psi\rangle$.
- E.g., if Bob receives $|10\rangle$ from Alice, he then knows that his qubits is in a state

$$\alpha|0\rangle - \beta|1\rangle = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix}$$

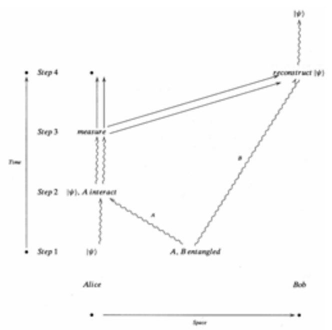
- Hence he should act on his qubit with the following matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ -\beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle$$

- Bob must apply the following matrices

$$\begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} & \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \end{array}$$

- Space-time diagram, where straight arrows correspond to movement of bits and curvy arrows correspond to qubits on the move.



- Notice that $|\psi\rangle$ moves from the lower-left corner in Alice's possession to the upper-right corner in Bob's possession. Mission accomplished!

Remarks

- Alice is no longer in possession of the original state. She has only two classical bits.
- To “teleport” a single quantum particle, Alice has to send two classical bits. Without these Bob cannot know what he has. The classical bits travel via a classical channel (less than the speed of light). So entanglement does not allow you to communicate faster than the speed of light.
- α and β were arbitrary complex numbers. So they could have had an infinite decimal expansion. This potentially infinite amount of information goes from Alice to Bob via only two bits. However, it is passed as a qubit and useless to Bob. As soon as he measures the qubit, it will collapseto a bit.
- Is it teleportation? No particle has been moved at all! However, two particles having exactly the same quantum state are, from a standpoint of physics, indistinguishable and can therefore be treated as the same particle.

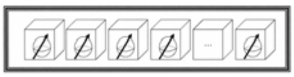
Hardware

- Do we actually know how to build a quantum computer?
- Formidable challenge to engineers and applied physicists
- Considering the amount of resources (academia, private sector, military) it would not be surprising if noticeable progress will be made in the near future.
- Disclaimer: area of research that requires a deep background in quantum physics and quantum engineering. Therefore a rather elementary discussion.

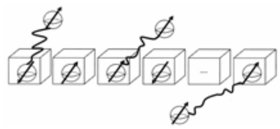
Goals and challenges

- Generic architecture:
  - Number of addressable qubits
  - Capable of initializing them properly
  - Apply a sequence of unitary transformations
  - Finally measuring them.

- Initialization: set machine in a well-defined state
  - Problem: entanglement between subsystems regardless their physical separation
  - Entanglement between machine and environment
    - Pure state



    - Mixed state



  - Problem:
    - No idea about the precise state of the environment’s electrons
    - No details of their interaction with the electrons in the quantum register.

Pure and mixed states

- What’s the difference?
- Consider the following family of spin states: $|\psi_\theta\rangle = \frac{|0\rangle + \exp(i\theta)|1\rangle}{\sqrt{2}}$
- For every choice of the angle θ, there is a distinct pure state.
- Each state is characterized by a specific relative phase (difference between angles of |0> and |1> in the polar representation).
- How can we detect their difference?
  - In standard basis will not work
  - A change of basis will do: the average spin value A along the x-axis depends on θ (see book): $A = \cos(\theta)$
  - Tossing a coin contains no relative phase → mixed state.
- The loss of purity of the state of a quantum system as the result of interaction with the environment is known as decoherence.

Decoherence

- We always implicitly assumed that we knew exactly how the environment affects the quantum system.
- More realistic scenario: a single electron is immersed in a vast environment, e.g., a single external electron.
- Electron has become entangled with another electron

$$|\psi_{\text{global}}\rangle = \frac{|00\rangle + \exp(i\theta)|11\rangle}{\sqrt{2}}$$

- What is the spin of our electron in the x-direction? 0 instead of a dependence on θ! (see book) It turns out that we should measure both electrons to get the dependence on θ.
- In general: we should measure all electrons of the environment. This is impossible, so our pure state is turned into a mixed one.
- Decoherence does not collapse the state vector: all information is still available!

Challenge due to decoherence

- On the one hand, adopting basic quantum systems that are very prone to "hook up" with the environment makes it difficult to manage the state of the machine.
- On the other hand, we do need to interact with the quantum device. Systems that tend to stay aloof makes it difficult to access their states.
- Can we hope to build a reliable quantum computing device if decoherence plays such an important role?
  - Fast gates execution: make decoherence sufficient slow compared to our control.
  - Fault-tolerance:
    - Quantum error-correcting codes
    - Repeat calculations

DiVincenzo's wish list

1. The quantum machine must have a sufficient large number of individually addressable qubits.
2. It must be possible to initialize all the qubits to the zero state.
3. The error rate in doing computations should be reasonable low, i.e., decoherence time must be substantially longer than gate operation time.
4. We should be able to perform elementary logical operations between pairs of qubits.
5. Finally, we should be able to reliably read out the results of measurements.

Implementing a quantum computer

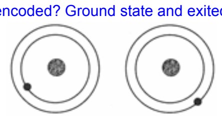
- A qubit is a state vector in a two-dimensional Hilbert space.
- Any physical quantum system whose state space has dimension 2^N can, in principle, be used to store an addressable sequence of N qubits.
- Options
  - Standard: quantum system with a two-dimensional state space.
  - Quantum register can be implemented by a number of copies.
  - Canonical two-dimensional quantum systems are particles with spin, e.g., electrons and single atoms.
  - Another choice is excited states of atoms.

Ion traps

- Oldest, most popular proposal
- Core idea: an ion is an electrically charged atom. Two types:
  - Positive ions or cations (lost one or more electrons)
  - Negative ions or anions (acquired some electrons)
- Ions can be acted upon by means of an electromagnetic field, or even better they can be confined in a specific volume, known as ion trap

- Practice: Ca^+

- How are qubits encoded? Ground state and exited state.



- Initialization:
  - Optical pumping: a laser pumps energy into an atom, that absorbs a photon, and raises from ground state to excited state. It can lose energy by emitting a photon.
  - Initialization of a register to some initial state possible with a high degree of fidelity (almost 100%).
- Manipulation:
  - Single-qubit rotation: by "hitting" the single ion with a laser pulse of a given amplitude, frequency, and duration, one can rotate its state appropriately.
  - Two-qubit gates: the ions in the trap are strung together by what is known as their common vibrational modes. A laser can affect their common mode, achieving the desired entanglement.
- Measurement:
  - Two main long-lived states |0> and |1>, and also a short-lived state |s> in the middle of |0>and |1>.
  - If ion is in ground state, gets pushed to |s>, it will revert to ground state and emits a photon. If it is in the excited state, it will not. Repeat this many times, and detect if photons are emitted to establish where the qubit is.

+ and – of ion trap

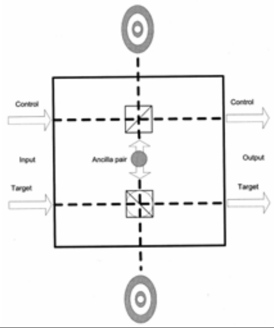
- On the plus side
  - Mode has a long coherence time, order 1-10s.
  - Measurements quite reliable, close to 100%.
  - Qubits can be transported around in the computer.
- On the minus side
  - Ion trap is slow in terms of gate time (order of 10ms)
  - Not apparent how to scale the optical part to thousands of qubits.

Linear optics

- Qubits:
  - Polarized photons
- Initialization:
  - Polarization filter
- Gates:
  - Nontrivial, since photons have a tendency to stay aloof
  - Implement some small universal set of quantum gates, e.g., controlled NOT gate
- Measurement:
  - Polarization filters and single-photon detectors.

Optical controlled-NOT gate

- Linear optics quantum computing (LOQC)
- LOQC-based controlled-NOT gate



+ and – of the optical scheme

- On the plus side:
  - Light *travels*. This means that quantum gates and quantum memory devices can be easily connected via optical fibers.
- On the minus side:
  - It is not easy for photons to become entangled. Also a plus wrt decoherence, but it makes gate creation challenging.

Nuclear Magnetic Resonance (NMR)

- Idea: encode qubits not as single particles or atoms, but as global spin states of many molecules in some fluid.
- These molecules float in a cup which is placed in an NMR machine.
- Contains plenty built-in redundancy → maintain coherence for a relatively long time span (several seconds).
- 1998: first two-qubit NMR computers.

Superconductor Quantum Computers (SQP)

- NMR uses fluids, SQP employs superconductors.
- By means of Josephson junctions – thin layers of nonconducting material sandwiched between two pieces of superconducting metal.
- At very low temperatures, electrons within a superconductor pair up to form a “superfluid” flowing with no resistance and as a single, uniform wave pattern.
- The current flows back and forth through the junction, like a ping-pong ball, in a rhythmic fashion.
- Implementation of qubits:
  - Through the Josephson junction qubit
  - The |0> and |1> states are represented by the two lowest-frequency oscillations of the currents.

Where are we now?

- In 2001 the first execution of Shor’s algorithm was carried out at IBM’s Almaden Research Center and Stanford University: 15 = 5 x 3!
- In 2005 a 12-bit NMR quantum register was benchmarked. Scalability seems to be a major hurdle.
- Recent news: NIST Road Map
  - NIST = US National Institute of Science and Technology
  - Major directions toward quantum hardware
  - http://qist.lanl.gov/qcomp_map.shtml
- Companies whose main business is developing Quantum Computing.

Future of Quantum Ware

- Quantum computing may become a reality in the future, perhaps even in the relatively near future.
- Likely that many areas of information technology will be affected, in particular communication and cryptography.
- If sizeable quantum devices become available: impact of artificial intelligence.
- Science fiction…
- The dreams of today are the reality of tomorrow.

Exam

Date: Mon Jan 11th, 10-13h (not Jan 25th!)

Location: *to be determined*

Book: chapters 1, 2, 3, 4, 5, 6, 9 &11