Richard Jozsa
rj301@

Why quantum computation & information?

What is information?

classical info - bit : Boolean variable, values 0, 1

bit strings - for more alternatives

What is computation?

- updating bit strings by prescribed sequences of steps (the 'program')
- basic elementary Boolean operations / gates

e.g. AND, OR, NOT, SWAP acting on 1 or 2 bits in string

Property: "each step / operation takes a fixed effort to perform, independent of the length of the string"

What is a bit?

not abstract maths but two distinguishable states of a physical system

R. Landauer: "no information without representation"

Computation (info processing) must correspond to a physical evolution of the system representing the information

!! So must obey laws of physics

So All possibilities & limitations of info storage, communication, processing (computation) must rest on laws of physics & cannot rest on abstract thought / maths alone

---

Some benefits of quantum vs classical physics for computing & information

(a) Computing power (computational complexity)

A quantum computer cannot compute anything that's not computable in principle on a classical computer

But: computational 'hardness' ~ amount of resources (time = # steps, space = amount of memory) needed

- if too high then uncomputable in practice

Example Task: given integer N ($n = O(\log N)$ digits, base 2)
find a factor of it

"input size" = n

poly-time algorithm: runs in time (# steps) bounded by a polynomial in n ← $P(n) = O(n^k) = 2^{k \log n}$

poly-time algorithms ~ "feasible in practice"

Algorithms needing exponential (super-poly) time are not feasible in practice ← $O(2^{cn})$ ← $n^{\log n} = 2^{(\log n)^2}$ or $2^{\sqrt{n}}$

e.g. trial division by $x = 1 \to \sqrt{N}$
needs at least $O(\sqrt{N}) = O(2^{n/2})$ time

Best known classical factoring algorithm time $\sim 2^{O(n^{1/3}(\log n)^{2/3})}$
not feasible!

Factoring is in practice - uncomputable classically but computable quantumly

Shor's algorithm runs in $O(n^3)$ time

(b) communication / security benefits

- provably secure communication is possible using quantum effects (impossible in classical physics)
  - BBQ4 quantum key distribution
- novel kinds of communication
  e.g. quantum teleportation
  further benefits no-cloning theorem, ~ quantum entanglement

(c) Technological issues

Moore's law (of classical comp^{n})

miniaturisation of computer computers since 1965

- factor of 4 every $3\frac{1}{2}$ years
- now at atomic level

Build a quantum computer? v. difficult

Principles of QM & Dirac bra-ket notation

Bra & Ket vectors

V: finite dim complex vector space with an (hermitian) inner product.

- vectors written as $|v\rangle$ (rather than e.g. $\underline{v}$) called Ket vectors or just kets
- Often work with 2-dim V_2 with a chosen orthonormal (o.n.) basis $\{|0\rangle, |1\rangle\}$ labelled by bit values

Kets always written as column vectors in components

e.g. $|v\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, $a, b \in \mathbb{C}$

Conjugate transpose $|v\rangle^\dagger$ (denoted $\dagger$) called bra vector, written in mirror image notation

$$\langle v| = |v\rangle^\dagger = a^*\langle 0| + b^*\langle 1| = (a^* \; b^*)$$

row vector in components

More formally: bra vec $\langle v|$ is element of dual vector space V^* of V under canonical isom $V \cong V^*$ given by the inner product i.e. $\langle v|$ is linear map

$|w\rangle$ any $\in V$ $\longmapsto$ inner product of $|v\rangle$ with $|w\rangle$ "$\underline{v} \cdot \underline{w}$"

$\underline{v} \cdot \underline{w}$ is linear in $|w\rangle$ & antilinear in $|v\rangle$ (so linear in $\langle v|$)

If $|w\rangle = c|0\rangle + d|1\rangle$, then the inner prod of $|v\rangle$ with $|w\rangle$ is written by juxtaposing bra & ket: i.e.

$$\langle v|w\rangle = |v\rangle^\dagger |w\rangle = (a^* \; b^*)\begin{pmatrix} c \\ d \end{pmatrix} = a^*c + b^*d$$

c.f. common maths notation $(\underline{v}, \underline{w})$ inner product

→ Dirac "bra-ket" names

e.g. o.n. of $|0\rangle$ & $|1\rangle \equiv \langle i|j\rangle = \delta_{ij}$

Tensor products of vectors

For V dim m o.n. basis $|e_1\rangle, \dots, |e_m\rangle$

W dim n o.n. basis $|f_1\rangle, \dots, |f_n\rangle$

Tensor product space

$V \otimes W$ has dim mn with o.n. basis $\{|e_i\rangle \otimes |f_j\rangle\}_{j=1,\dots,n}^{i=1,\dots,m}$

($\otimes$ is bilinear)

General ket in $V \otimes W$

$$|\xi\rangle = \sum c_{ij} |e_i\rangle \otimes |f_j\rangle$$

- Natural bilinear map $f : V \times W \longrightarrow V \otimes W$

If $|\alpha\rangle = \sum a_i |e_i\rangle$, $|\beta\rangle = \sum b_j |f_j\rangle$,

then $(|\alpha\rangle, |\beta\rangle) \xrightarrow{f} |\alpha\rangle \otimes |\beta\rangle = \sum_{i,j} a_i b_j |e_i\rangle \otimes |f_j\rangle$

Note: $\otimes$ is not commutative

e.g. if $V = W$ then $|\alpha\rangle \otimes |\beta\rangle \overset{\text{gen}}{\neq} |\beta\rangle \otimes |\alpha\rangle$

($|\alpha\rangle \otimes |\beta\rangle$: cpts $a_i b_j$; $|\beta\rangle \otimes |\alpha\rangle$: cpts $b_i a_j$)

We often omit $\otimes$ & write $|\alpha\rangle \otimes |\beta\rangle$ as $|\alpha\rangle|\beta\rangle$

But the mapping f is not surjective:

Product vectors & entangled vectors.

- any $|\xi\rangle \in V \otimes W$ of form $|\xi\rangle = |\alpha\rangle \otimes |\beta\rangle$ called a product vector
- any $|\xi\rangle$ that is not a product vector is called entangled

We will mostly be concerned with tensor prods of 2-dim V_2 with itself.

For k-fold tensor power, write $\otimes^k V_2 = V_2 \otimes \cdots \otimes V_2$

- has dim 2^k and o.n. basis

$$|i_1\rangle \otimes \cdots \otimes |i_k\rangle \quad (i_1, \dots, i_k = 0, 1)$$

labelled by 2^k k-bit strings

- often write $|i_1\rangle \otimes \cdots \otimes |i_k\rangle$ as $|i_1\rangle \cdots |i_k\rangle$ or $|i_1 \cdots i_k\rangle$

Example

$|v\rangle = |00\rangle + |11\rangle$ in $V_2 \otimes V_2$

is entangled

To see this, suppose $v = (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$

RHS $= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$

compare to components of $|v\rangle$

$ac = 1,\ ad = 0,\ bc = 0,\ bd = 1$

so $abcd = (ac)(bd) = 1$

$\Rightarrow (ad)(bc) = 0$ ⁂

Can show that

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

is entangled iff $\det(a_{ij}) \neq 0$

For general dimension

$\sum_{\substack{i=1,\dots,m \\ j=1,\dots,n}} A_{ij}|i\rangle|j\rangle$ is a product vector iff matrix $[A_{ij}]$ has rank 1 (or zero)

Inner product (IP) on $V \otimes W$

- induced by IPs on V & W "applied slotwise"

For product states $|\alpha_1\rangle|\beta_1\rangle$ & $|\alpha_2\rangle|\beta_2\rangle$

I.P. is $(\langle\beta_1|\langle\alpha_1|)(|\alpha_2\rangle|\beta_2\rangle) = \langle\alpha_1|\alpha_2\rangle\langle\beta_1|\beta_2\rangle$

extend by linearity to all $|\xi\rangle \in V \otimes W$

Note (notation)

For bra vector of $|\alpha\rangle|\beta\rangle$ often reverse order & write $|\beta|\langle\alpha|$ but always important to keep track of component slots.

Sometimes include explicit labels e.g.

$|\alpha\rangle_A|\beta\rangle_B$ has bra ${}_A\langle\alpha|{}_B\langle\beta| = {}_B\langle\beta|{}_A\langle\alpha|$

Quantum principle (QM1) (physical state)

State of any (isolated) physical system S represented by unit vectors in a complex vector space V with an I.P.

$e^{i\theta}|v\rangle$ & $|v\rangle$

Simplest (non-trivial) case: $V = V_2$, 2 dim

Choose pair of o.n. vectors, label them with bit values viz $|0\rangle, |1\rangle$. Then general state

$$|\psi\rangle = a|0\rangle + b|1\rangle, \quad a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1$$

"$|\psi\rangle$ is superposition of $|0\rangle$ & $|1\rangle$ with amplitudes a, b resp"

Qubit: any quantum system with 2 dim state space and chosen o.n. basis labelled $|0\rangle, |1\rangle$

- called computational basis or standard basis ← Z-basis

Conjugate basis for a qubit

Given o.n. pair $|0\rangle$ & $|1\rangle$ we get o.n. pair

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

called conjugate basis or X-basis

(QM2) (composite system)

If system S_1 has state space V_1,
" S_2 " V_2
then joint system $S_1 S_2$ obtained by taking S_1 & S_2 together has state space $V_1 \otimes V_2$

Composite systems

S_1 quantum state space V_1

S_2 " V_2

then joint system $S_1 S_2$ has $V_1 \otimes V_2$

Basic example: n qubits

state space $V_2^{\otimes n}$, dim 2^n

computational / standard basis $|i_1 \cdots i_n\rangle$ labelled by 2^n bit strings

- n qubit state $|\psi\rangle$ is product state

  if it is tensor product of n 1-qubit states

  $|\psi\rangle = |v_1\rangle|v_2\rangle \cdots |v_n\rangle$

- otherwise $|\psi\rangle$ is entangled

Remark: in classical physics $S_1 S_2$ has state space

$V_1 \times V_2$ Cartesian product

$\rightsquigarrow$ no entangled states

Quantumly As number n of qubits grows, the full state description grows exponentially $|\psi\rangle = \sum a_{i_1 \cdots i_n} |i_1 \cdots i_n\rangle$

↑ $\exp(n)$ components

However for product states, description grows linearly in n (nK parameters, K = # params for 1 qubit)

Generally: if system S has states described by K parameters, then S_n = composite of n instances of S has

quantumly: $O(K^n)$ parameters exponential

classically: $O(n)$ parameters only linear

Dirac notation - linear maps

Consider linear maps on V_2 (higher dim similar)

with $|v\rangle = a|0\rangle + b|1\rangle$, $|w\rangle = c|0\rangle + d|1\rangle$.

Then 'ket-bra' product gives $M = |v\rangle\langle w|$.

$$M = \begin{pmatrix} a \\ b \end{pmatrix}(c^* \; d^*) = \begin{pmatrix} ac^* & ad^* \\ bc^* & bd^* \end{pmatrix} \quad (*)$$

– a linear map on V_2. for any $|x\rangle = \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$

$$M|x\rangle = (|v\rangle\langle w|)\,|x\rangle = |v\rangle\,\langle w|x\rangle$$

($|v\rangle$: 1D ring; $\langle w|x\rangle$: scalar)

in components $\underbrace{\begin{pmatrix} a \\ b \end{pmatrix}}_{(v)} \underbrace{(c^* d^*)\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}}_{c^*x_0 + d^*x_1}$

These are rank 1 mappings

For general linear map

$$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$$

note first : for basis states

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

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

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

So can express $A = a_{00}|0\rangle\langle 0| + a_{01}|0\rangle\langle 1|$

$$+ a_{10}|1\rangle\langle 0| + a_{11}|1\rangle\langle 1|$$

$$= \sum a_{ij}\,|i\rangle\langle j|$$

$\{|0\rangle\langle 0|, |0\rangle\langle 1|, |1\rangle\langle 0|, |1\rangle\langle 1|\}$ basis for $V_2 \otimes V_2^*$ (dual)

Cyclic property of trace

$$\langle v|w\rangle = \text{trace}\,(|v\rangle\langle w|) = ac^* + bd^*$$

Projection operators

Special case of (*) with $|v\rangle = |w\rangle$ (in any dim)

& $|v\rangle$ is normalised $\langle v|v\rangle = 1$

Then $\Pi_v = |v\rangle\langle v|$ is operator of proj onto 1-dim subspace spanned by $|v\rangle$.

e.g. have $\Pi_v \Pi_v = |v\rangle\langle v|v\rangle\langle v| = |v\rangle\langle v| = \Pi_v$ (① : $\langle v|v\rangle = 1$)

$$\Pi_v|v\rangle = |v\rangle\langle v|v\rangle = |v\rangle$$

$$\Pi_v|w\rangle = 0 \quad \text{if} \quad |w\rangle \perp |v\rangle \text{ i.e. } \langle v|w\rangle = 0$$

More generally, if E is any d-dim linear subspace of n-dim space V and $\{|e_1\rangle, \dots, |e_d\rangle\}$ is any o.n. basis of E, then $\pi_E = |e_1\rangle\langle e_1| + \cdots + |e_d\rangle\langle e_d|$ ← indep of choice of o.n. basis is operator of projection onto E.

Tensor products of maps

If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ are linear maps on V_2, then $A \otimes B : V_2 \otimes V_2 \to V_2 \otimes V_2$ defined by basis action

$$|i\rangle|j\rangle \mapsto (A|i\rangle)(B|j\rangle) \quad \text{\& linear extension}$$

($\otimes$ between the kets on both sides)

e.g. on any product vector $|v\rangle|w\rangle \mapsto (A|v\rangle)(B|w\rangle)$

In components, (bases $\{|i\rangle\}, \{|j\rangle\}$, & $\{|ij\rangle\}$)

$$A \otimes B = \left(\begin{array}{c|c} aB & bB \\ \hline cB & dB \end{array}\right) = \begin{pmatrix} ap & aq & \cdot \\ ar & as & \\ \cdot & & \cdot \end{pmatrix}$$

Important special cases

$I \otimes A$ & $A \otimes I$ ~ action of A on 2^{nd} (resp 1^{st}) component space of $V_2 \otimes V_2$

"local operations" on subsystems of composites

(QM3) (physical evolution of quantum systems)

any physical (finite time) evolution of a quantum system is represented by a unitary (linear) operation on vector space of states.

"our version of Schrödinger's eq^n" ~> PDE $\overset{\text{infinite}}{\underset{\text{dim}}{}}$ ~ Hamiltonian

finite dim version H hamiltonian is hermitian operator on state space, evol^n eq^n $\quad i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$

sol^n : $|\psi\rangle = e^{-i/\hbar Ht}|\psi_0\rangle$ ← initial state

↑ matrix exponential

H hermitian $\Rightarrow$ e^{iA} always unitary

Recall: U is unitary iff $U^{-1} = U^\dagger$

iff U maps any o.n. basis to an o.n. set of vectors

iff the columns (or rows) of matrix of U form an o.n. set of vectors

Partial inner products for vectors in $V \otimes W$

Any ket $|v\rangle \in V$ defines a linear map

$$V \otimes W \longrightarrow W$$

called "partial inner product with $|v\rangle$",

defined on basis vectors $|e_i\rangle|f_j\rangle \in V \otimes W$

$$|e_i\rangle|f_j\rangle \mapsto \langle v|e_i\rangle|f_j\rangle$$

(similarly for $|w\rangle \in W$ $\rightsquigarrow$ $V \otimes W \to V$ map)

- if $V = W$, important to specify which space of $V \otimes V$ is being used

Example For $V = V_2$ and $|\xi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$

Can form partial inner prod with $|0\rangle$ on either space

So first label spaces e.g. as $V_A \otimes V_B$, $V_A = V_B = V$

Then o.n. relations $\langle i|j\rangle = \delta_{ij}$ give:

$$\begin{aligned} {}_A\langle 0|\xi\rangle_{AB} &= a\,{}_A\langle 0|0\rangle_A|0\rangle_B + b\,{}_A\langle 0|0\rangle_A|1\rangle_B \\ &\quad + c\,{}_A\langle 0|1\rangle_A|0\rangle_B + d\,{}_A\langle 0|1\rangle_A|1\rangle_B \\ &= a|0\rangle_B + b|1\rangle_B \end{aligned}$$

"pick out terms of $|\xi\rangle_{AB}$ with 0 in A-slot"

$${}_B\langle 0|\xi\rangle_{AB} = a|0\rangle_A + c|1\rangle_A$$

(QM4) Quantum measurements (mmts) & Born rule

(QM4) Quantum measurement & Born Rule

Given single instance of a quantum state $|\psi\rangle$ of a physical system, state space V, dim n.

Basic Born rule – complete projective mmt (or von Neumann mmt)

Let $\mathcal{B}$ be $\{|e_1\rangle, \ldots, |e_n\rangle\}$ be any o.n. basis of V.

We can make a mmt on $|\psi\rangle$ relative to the basis $\mathcal{B}$.

$$|\psi\rangle = \sum a_i |e_i\rangle$$

Possible outcomes are $j = 1, 2, \ldots, n$

$$\text{prob}(j) = |\langle e_j|\psi\rangle|^2 = |a_j|^2$$

If outcome j seen, then after mmt the state is no longer $|\psi\rangle$, but has been "collapsed" to $|\psi_j\rangle = |e_j\rangle$.

So repeated mmt gives only the same result with certainty $(j, j, j, \ldots)$ NOT further samples of $|a_j|^2$ distribution.

"prob is squared length of projection of $|\psi\rangle$ onto the basis direction $|e_j\rangle$

& post-mmt state is that projection, renormalised"

"complete" above refers to the one-dim of orthogonal subspaces, defined by basis states

Incomplete proj mmts

Let $\{E_1, E_2, \ldots, E_d\}$ be decomposition of V into d mutually orthogonal subspaces.

$V = E_1 \oplus \cdots \oplus E_d$. Let π_i be proj onto E_i.

Then incomplete proj mmt of $|\psi\rangle$ wrt the orthogonal decomposition is the following quantum operation:

Possible outcomes are $j = 1, \ldots, d$

$$\text{prob}(j) = \| \pi_j |\psi\rangle \|^2 = \langle\psi| \pi_j |\psi\rangle$$

← recall $\pi^\dagger = \pi$, $\pi_j \pi_j = \pi_j$

$= \text{trace}(\Pi_j |\psi\rangle\langle\psi|)$

Post-mmt state is the projected "collapsed" vector renormalised

$$|\psi_j\rangle = \frac{\Pi_j|\psi\rangle}{\sqrt{\text{prob}(j)}}$$

Example: Parity mmt on 2-qubit

Parity of a 2-bit string $b_1 b_2$ is mod 2 sum $b_1 + b_2$

Parity mmt on 2 qubits is incomplete mmt with orthog decomp^n

$E_0 = \text{span}\{|00\rangle, |11\rangle\}$

$E_1 = \text{span}\{|01\rangle, |10\rangle\}$

For $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$

See 0 with $\text{pr}(0) = |a|^2 + |d|^2$

& post-mmt $\dfrac{a|00\rangle + d|11\rangle}{\sqrt{|a|^2+|d|^2}}$

Measurement of 'quantum observables'

Quantum observable Ⓜ is hermitian operator on V.

So Ⓜ has real eigenvalues λ_j, $j = 1, \dots, d$

orthogonal eigenspaces Λ_j, $\dim(\Lambda_j)$ = multiplicity of λ_j

and $V = \Lambda_1 \oplus \cdots \oplus \Lambda_d$

Mmt of quantum observable Ⓜ is then just incomplete mmt relative to this orthog decomposition.

Labelled by eigenvalue λ_j (not just j)

{ λ_j values ~ physical properties

{ e.g. have average value $\langle Ⓜ \rangle = \sum \lambda_j \text{prob}(j)$

But for purposes of providing information about state $|\psi\rangle$ (& post-mmt state) the choice of labelling is immaterial.

Extended Born rule

- special case of an incomplete mmt
- measuring a component part of a composite system $S_1 S_2$

Suppose $|\psi\rangle$ is state of composite system $S_1 S_2$, state space $V \otimes W$. Let $\mathcal{B}_V = \{|e_1\rangle, \ldots, |e_n\rangle\}$ be o.n. basis of V.

[$\mathcal{B}_W = \{|f_1\rangle, \ldots, |f_m\rangle\}$ o.n. basis of W]

$|\psi\rangle$ can be uniquely expanded as

$$|\psi\rangle_{VW} = \sum_i |e_i\rangle_V |\xi_i\rangle_W$$

$|\xi_i\rangle$ are generally not normalised, not orthogonal

In fact $|\xi_i\rangle_W = {}_V\langle e_i|\psi\rangle_{VW}$

$|\psi\rangle$ normalised $\Rightarrow \sum_i \langle \xi_i | \xi_i \rangle = 1$

Now e.g. we can perform a mmt of $|\psi\rangle$ relative to basis $\mathcal{B}_V$ of V ("complete mmt on V, but not on $V \otimes W$")

Outcomes $i = 1, \ldots, n$

& corresponding orthogonal subspaces (of $V \otimes W$)

$$E_i = \text{span}\{|e_i\rangle \otimes |\xi\rangle : |\xi\rangle \in W\}$$
$$= |e_i\rangle \otimes W$$

Corresponding projectors are $\Pi_i = |e_i\rangle\langle e_i| \otimes I_W$

& get $\text{prob}(i) = \langle \xi_i | \xi_i \rangle$

post-mmt state for i is $|\psi_i\rangle = \dfrac{|e_i\rangle_V |\xi_i\rangle_W}{\sqrt{\langle \xi_i, \xi_i \rangle}}$ product state

Remarks on mmts

* According to (QM4) (i.e. all mmt rules) two different states with guaranteed (prob 1) different outcomes for some mmt must lie in orthogonal subspaces, i.e. must be themselves orthog.

So non-orthogonal states, although physically different, can never be reliably distinguished ("as information") by any quantum process.

* If $|\psi\rangle$ has dim n, <u>any</u> mmt on it has at most n outcomes. But can get more outcomes by adjoining an ancilla $|A\rangle$, dim m (indep of $|\psi\rangle$)
& measure $|\psi\rangle|A\rangle$ jointly to get up to mn outcomes

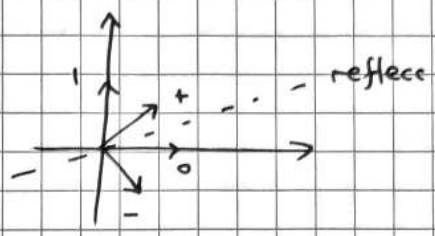
Basic unitary operations for qubits

– quantum gates

1 qubit gates

Hadamard gate $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $HH = I$

so $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$



Pauli operations / gates

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$,

$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

all unitary & hermitian

mult. (group) properties

$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I$, eigenvals $= \pm 1$

all anti-commute

$\sigma_x \sigma_y = -\sigma_y \sigma_x = i\sigma_z$ & cyclic shifts

Real versions

$X = \sigma_x$, $Z = \sigma_z$, $Y = i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

Have: $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$

← "X is quantum NOT"

i.e. $X|k\rangle = |k \oplus 1\rangle$, $k = 0, 1$

X eigenbasis is $|+\rangle$, $|-\rangle$

$Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$, $Z|k\rangle = (-1)^k|k\rangle$

Z eigenbasis is $|0\rangle$, $|1\rangle$

"X basis & Z basis"

↑ $\{|+\rangle, |-\rangle\}$ ↑ $\{|0\rangle, |1\rangle\}$

Phase gate $P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$, $(Z = P(\pi))$

2-qubit gates

controlled-X (aka controlled-NOT, CX, C-NOT)

$$CX|j\rangle|k\rangle = |j\rangle|j \oplus k\rangle$$
$$= |j\rangle X^j |k\rangle$$

so $CX|0\rangle|\alpha\rangle = |0\rangle|\alpha\rangle$

$CX|1\rangle|\alpha\rangle = |1\rangle X|\alpha\rangle$

Matrix

$$CX = \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$$

qubit 1 called control qubit

2 called target

asymmetrical roles of 2 qubits, so write CX_{12} if unclear

* write CX_{ab} for a = control qubit, b = target qubit

e.g. $CX_{21}|0\rangle_1|1\rangle_2 = |1\rangle_1|1\rangle_2$

$CX_{12}|0\rangle_1|1\rangle_2 = |0\rangle_1|1\rangle_2$

controlled-Z CZ

$$CZ_{12}|j\rangle|k\rangle = |j\rangle Z^j|k\rangle = (-1)^{jk}|j\rangle|k\rangle$$

($Z|k\rangle = (-1)^k|k\rangle$)

Note $CZ_{12} = CZ_{21}$ symmetric

Matrix

$$CZ = \begin{pmatrix} I & 0 \\ 0 & Z \end{pmatrix}$$

Quantum states as information carriers

Recall: information ~ distinguishable states of a physical system

Classically: any two different states distinguishable, in principle

Quantumly: states are distinguishable reliably iff they're orthog

qubit: simplest system that can reliably encode a classical bit

So if given quantum state $|\psi\rangle$

- impossible to identify its identity with certainty

e.g. $|0\rangle$, $|+\rangle$ as yes vs no

We call "what we get" <u>quantum information</u>

Given some quantum information $|\psi\rangle$ have 3 basic operations we can perform on it

(Ancilla): take a fixed known quantum state $|A\rangle$

& adjoin it to get $|\tilde{\psi}\rangle = |\psi\rangle|A\rangle$

$|A\rangle$ called <u>ancilla</u>

(Unitary): apply a unitary U of our choice

$|\psi\rangle$ becomes $U|\psi\rangle$

(Measure): can perform a mmt on (part of) $|\psi\rangle$

record the result & use post mmt for further q info pro that can be chosen adaptively depending on mmt outcome

- output here is generically a prob mixture over post-mmt states, prob ~ Born rule

Most general action ~ any sequence of these 3 kinds of act"

<u>The no-cloning theorem</u>

"q. info. cannot be copied or cloned"

copying of classical info is very familiar

e.g. "photocopying" or more formally <u>CNOT</u>

Bodean $b_1, b_2 \mapsto b_1, (b_1 \oplus b_2)$

$$(b)(0) \xrightarrow{\text{CNOT}} (b)(0 \oplus b) = (b)(b)$$

↑ qubit ↖ blank state ↑ the copy

More generally any "copying process" has the form

$$(b)(0)(M) \longrightarrow (b)(b)(M_b)$$

info; blank paper; initial "ready" state of copying machine; copy; final state of machine, may depend on b

Given quantum information $|\psi\rangle_A$

copy/cloning process is a quantum evolution process of ABM:

$$|\psi\rangle_A |0\rangle_B |M_0\rangle_M \longrightarrow |\psi\rangle_A |\psi\rangle_B |M_\psi\rangle_M$$

B ~ quantum register, same dim A, initially in some "blank" fixed state (ψ indep) called $|0\rangle_B$

M register is any extra space needed (~ machine) initially in some "ready"-state $|M_0\rangle$ indep of $|\psi\rangle$

Final state of $|M\rangle$ may depend on $|\psi\rangle$ too

No-cloning theorem [unitary version]

Let S be any (known) set of quantum states of A that contains at least one pair $|\xi\rangle \neq |\eta\rangle$ of non-orthogonal states.

Then no unitary process exists that achieves cloning of all states in S.

No Cloning Theorem if $|\xi\rangle \neq |\eta\rangle$ are not orthogonal
(and the set $\{|\xi\rangle, |\eta\rangle\}$ is known)
then there is no unitary cloning process as above
(for $|\psi\rangle$ being either one of $|\xi\rangle$ or $|\eta\rangle$)

Remark · If $|\xi\rangle = |\eta\rangle$ then can clone (trivially)
· If $|\xi\rangle \perp |\eta\rangle$ can clone
e.g. qubit $|0\rangle, |1\rangle$ $CX|k\rangle|0\rangle = |k\rangle|k\rangle$
but $CX(a|0\rangle + b|1\rangle)(|0\rangle) = a|0,0\rangle + b|1,1\rangle$
$\neq (a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle)$

For general $|\xi\rangle \perp |\eta\rangle$ first rotate to $|0\rangle \perp |1\rangle$ and clone as above, rotate each back.

Remark Theorem is true for general quantum processes
i.e. arbitrary alternation of (ancilla), (unitary) & (mmt)
· for (ancilla) – can just include all ancillas at the start, regard as part of M-system
· for (measure) – see notes (optional)
– need cloning to occur on all probabilistic branches
Instead of mmt collapse: introduce a further quantum register for the mmt pointer with o.n. basis labelled by mmt outcomes

Proof of no-cloning theorem
Let $|\xi\rangle, |\eta\rangle$ be two different non-orthog states.
Then the cloning process must do:

$$|\xi\rangle_A |0\rangle_B |M_0\rangle_M \longrightarrow |\xi\rangle_A |\xi_A\rangle |M_\xi\rangle_M$$
$$|\eta\rangle_A |0\rangle_B |M_0\rangle_M \longrightarrow |\zeta\rangle_A |\eta\rangle_B |M_\eta\rangle_M$$

unitary processes preserve inner products (IP)
so IP of LHS's = IP of RHS's
i.e. $\langle\xi|\eta\rangle\langle 0|0\rangle\langle M_0|M_0\rangle = \langle\xi|\eta\rangle^2 \langle M_\xi|M_\eta\rangle$
Take absolute values & use $\langle 0|0\rangle = \langle M_0|M_0\rangle = 1$
Get $|\langle\xi|\eta\rangle| = |\langle\xi|\eta\rangle|^2 |\langle M_\xi|M_\eta\rangle|$. *
Since $|\xi\rangle \neq |\eta\rangle$ & not $|\xi\rangle \perp |\eta\rangle$ have

$$0 \overset{\times}{\leq} |\langle\xi|\eta\rangle| \overset{\times}{\leq} 1$$

So can cancel

$$1 = |\langle \xi | \eta \rangle| \, |\langle M_\xi | M_\eta \rangle|$$

contradiction ✱ since

$$|\langle \xi | \eta \rangle| \leq 1 \quad \& \quad |\langle M_\xi | M_\eta \rangle| \leq 1 \qquad \square$$

Example (cloning & superluminal signaling)

No cloning thm proved in 1982 – W. Wootters & W. Zurek and D. Dieks

(also D. Park 1960 — went unnoticed)

in response to N. Herbert (1980)

- proposal for superluminal signalling in QM
- error was to assume cloning of quantum states

Herbert's method

Alice & Bob distantly separated in space & share entangled quantum state

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B \right)$$

easy to check that also

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}} \left(|+\rangle_A |+\rangle_B + |-\rangle_A |-\rangle_B \right)$$

A wants to communicate yes/no decision at noon – instantaneously

A's action for 'yes', A measures her qubit in $\{|0\rangle, |1\rangle\}$

'no', A " $\{|+\rangle, |-\rangle\}$

then Born rule ⇒ B's qubit is (instantaneously)

for 'yes' action 50/50 probability $|0\rangle$ or $|1\rangle$

'no' action 50/50 probability $|+\rangle$ or $|-\rangle$

! Fact: these yes/no preparations of # B's qubit are indistinguishable by any local action at B

– for any measurement, output probabilities are the same in 2 cases

Indeed: let π_i be projection operator for outcome i in a mmt for Bob

then in yes case: $\text{prob}_{\text{yes}}(i) = \frac{1}{2}\langle 0|\pi_i|0\rangle + \frac{1}{2}\langle 1|\pi_i|1\rangle$

$$= \text{Trace}\left[\pi_i \left(\frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \right)\right]$$

in no case $\text{prob}_{\text{no}}(i) = \text{trace}\left[\pi_i \left(\frac{|+\rangle\langle+| + |-\rangle\langle-|}{2}\right)\right]$

But (e.g. as 2×2 matrices)

$$|0\rangle\langle 0| + |1\rangle\langle 1| = |+\rangle\langle+| + |-\rangle\langle-| = I$$

So B cannot detect A's attempted signalling.

But: suppose B can clone quantum states!

Then at noon + ε he clones his qubit to make many copies (e.g. 10^6)

Now in 'yes' case

all will be $|0\rangle$ or all will be $|1\rangle$

in 'no' case

all will be $|+\rangle$ or all will be $|-\rangle$

These can now be locally distinguished by B (easily):

B measures all copies in $\{|0\rangle, |1\rangle\}$ basis

if 'yes', see $00\ldots0$ or $11\ldots1$ with prob 1

if 'no' see uniformly random bitstring $b_1 b_2 \cdots b_{10^6}$

- will be all 0 or all 1 with prob $\frac{2}{2^{10^6}} \approx 0$

Distinguishing non-orthogonal states

Given: unknown quantum state $|\psi\rangle$ (any dim d)

Promise: $|\psi\rangle$ is either $|\alpha_0\rangle$ or $|\alpha_1\rangle$ (distinct known states)

Problem: determine which, i.e. $i=0,1$ s.t. $|\psi\rangle = |\alpha_i\rangle$

Know we cannot do with certainty if $\langle\alpha_0|\alpha_1\rangle \neq 0$.

State estimation process

Given $|\psi\rangle$: · adjoin ancilla $|A\rangle$ to give $|\psi\rangle|A\rangle$
· then perform a unitary on full system
· then perform a mmt with outcomes 0 & 1 for our answer

Remark: It can be shown (as for no-cloning) that any possible sequence of (ancilla)(unitary)(measure) can be simulated by the restricted form above.

Simplifying the process

· adjoining $|A\rangle$ just changes discrimination of $|\alpha_0\rangle$ vs $|\alpha_1\rangle$ to that of $|\alpha_0\rangle|A\rangle$ vs $|\alpha_1\rangle|A\rangle$, with same inner product, just in a larger dim space

· Process M_1: "doing U, then mmt with projectors Π_0, Π_1" is equivalent to just performing M_2 ("U-rotated mmt") with projectors $\tilde{\Pi}_i = U^\dagger \Pi_i U$, $i=0,1$
as they give the same output probs on any state $|\xi\rangle$

$$\left.\begin{aligned} \text{prob}_{M_1}(i) &= (\langle\xi|U^\dagger)\Pi_i(U|\xi\rangle) \\ \text{prob}_{M_2}(i) &= \langle\xi|U^\dagger\Pi_i U|\xi\rangle \end{aligned}\right\} \text{equal}$$

· Hence our process is equivalent to just a single mmt

Given $|\alpha_0\rangle$ or $|\alpha_1\rangle$, perform a single mmt with projectors Π_i

Some mmts better than others for giving the correct answer with higher probability.

Introduce 'figure of merit' for a mmt : the success prob P_S – with no prior knowledge of which state we're getting assume prior probs of half.

Then $P_S = \frac{1}{2}$ (prob (process outputs 0 | $|\alpha_0\rangle$ input))
$+ \frac{1}{2}$ (prob (process outputs 1 | $|\alpha_1\rangle$ input))

so by Born rule

$$P_S = \frac{1}{2}\left(\langle\alpha_0|\Pi_0|\alpha_0\rangle + \langle\alpha_1|\Pi_1|\alpha_1\rangle \right)$$

Knowing $|\alpha_0\rangle$ & $|\alpha_1\rangle$ want to optimise P_S over all choices of Π_0, Π_1.

Since $\Pi_0 + \Pi_1 = I$, $\Pi_1 = I - \Pi_0$

so $P_S = \frac{1}{2}\left(1 + \langle\alpha_0|\Pi_0|\alpha_0\rangle - \langle\alpha_1|\Pi_0|\alpha_1\rangle \right)$

$$= \frac{1}{2}\left(1 + \mathrm{Tr}\left(\Pi_0 \left(|\alpha_0\rangle\langle\alpha_0| - |\alpha_1\rangle\langle\alpha_1| \right)\right)\right) \quad (*)$$

Now calculate optimal $\{\Pi_0, I - \Pi_0\}$.

Look more closely at

$$D = |\alpha_0\rangle\langle\alpha_1| - |\alpha_1\rangle\langle\alpha_1|$$

Properties : · D is hermitian, so eigenvalues real & has complete basis of o.n. eigenstates

· If $|\beta\rangle \perp |\alpha_0\rangle$ & $|\alpha_1\rangle$ then $D(|\beta\rangle) = 0$ so has only two non-zero eigenvalues & eigenvectors are in span of $|\alpha_0\rangle, |\alpha_1\rangle$

· trace $D = 0$ so non-zero eigenvalues sum to 0 write them as $+\delta$ & $-\delta$ $(\delta > 0)$ with eigenstates $|p\rangle, |m\rangle$ respectively

Hence $D = \delta|p\rangle\langle p| - \delta|m\rangle\langle m|$

· to determine δ (in terms of $|\alpha_0\rangle$ & $|\alpha_1\rangle$) work in 2-dim subspace of $|\alpha_0\rangle$ & $|\alpha_1\rangle$ & components :

Choose $|\alpha_0^\perp\rangle$ o.n. to $|\alpha_0\rangle$. In $\{|\alpha_0\rangle, |\alpha_0^\perp\rangle\}$ basis

$$|\alpha_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |\alpha_1\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = c_0|\alpha_0\rangle + c_1|\alpha_0^\perp\rangle$$

so $c_0 = \langle\alpha_0|\alpha_1\rangle$ so $|c_1| = \sin\theta$ for $\cos\theta = |\langle\alpha_0|\alpha_1\rangle|$

So $D = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(1 \;\; 0) - \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}(c_0^* \;\; c_1^*)$

$$= \begin{pmatrix} 1-|c_0|^2 & -c_0c_1^* \\ -c_0^*c_1 & -|c_1|^2 \end{pmatrix}$$

$$\therefore -\delta^2 = -|c_1|^4 - |c_0|^2|c_1|^2 = -|c_1|^2$$

$$\therefore \boxed{\delta = |c_1| = \sin\theta}$$

Finally returning to (*)

$$P_S = \tfrac{1}{2} + \tfrac{\delta}{2} \text{ trace } \Pi_0 (|p\rangle\langle p| - |m\rangle\langle m|)$$
$$= \tfrac{1}{2} + \tfrac{\delta}{2}(\langle p|\Pi_0|p\rangle - \langle m|\Pi_0|m\rangle)$$

Now for any projector Π & state $|\xi\rangle$, $0 \le \langle\xi|\Pi|\xi\rangle \le 1$

(since this is squared length of $\Pi|\xi\rangle$)

Hence P_S achieves its max value of $\frac{1}{2}(1+\delta) = \frac{1}{2}(1+\sin\theta)$
if Π_0 chosen to be any projector into a subspace
· containing $|p\rangle$ so $\Pi_0|p\rangle = |p\rangle$
& · orthogonal to $|m\rangle$ so $\Pi_0|m\rangle = 0$
(& then $\Pi_1 = I - \Pi_0$ has $\Pi_1|m\rangle = |m\rangle$)
Such a choice of Π_0 is always possible since $|p\rangle \perp |m\rangle$
The achievable bound $P_S \le \frac{1}{2}(1+\sin\theta)$
called Helstrom - Holevo bound (for pure states)
· In particular ancilla never needed, only inner product relevant
· If $|\alpha_0\rangle, |\alpha_1\rangle$ are qubit states (dim = 2)
can work entirely in their 2-dim space
& optimal discriminating mmt will be a complete projective mmt
of quantum observable $D = |\alpha_0\rangle\langle\alpha_1| - |\alpha_1\rangle\langle\alpha_1|$
i.e. mmt relative to eigenbasis of D

Theorem (Helstrom-Holevo bound)
Given one of two equally likely states $|\alpha_0\rangle, |\alpha_1\rangle$ with $|\langle\alpha_0|\alpha_1\rangle| = \cos\theta$, then the prob P_S of correctly identifying the state by any quantum process (mmt) is bounded by $P_S \leq \frac{1}{2}(1+\sin\theta)$ & bound is tight.

Remark: other discrimination scenarios possible
* unambiguous state discrimination
have mmt with 3 outcomes 0, 1, "fail"
if 0 seen: seen state certainly $|\alpha_0\rangle$
if 1 seen: state certainly $|\alpha_1\rangle$
if "fail" seen: process has failed (& generally lost all information)

The no-signalling principle

Alice & Bob distantly separated in space with local quantum systems A & B respectively. Initially AB in some joint quantum state (possibly entangled).

They can apply only local actions (on their own system)

The issue:

Suppose A does a complete mmt on her system.

By Born rule, for each mmt outcome k for A, state at B will "instantaneously" change (mmt collapse) to a corresponding post-mmt state $|\beta_k\rangle$.

Can B notice this change by just local action?

If 'yes' then get superluminal signalling!

But answer is no!

Local operations on a composite system $|\psi\rangle_{AB}$

Let $\mathcal{H}_A, \mathcal{H}_B$ be state spaces of A, B

& $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

(loc-unitary): a local unitary U by Alice resp Bob is represented on full system by $U_A \otimes 1_B$ resp $1_A \otimes U_B$

Note: local unitary operations on disjoint subsystems always commute

$$\underset{2^{nd}}{(U \otimes I)}\underset{1^{st}}{(I \otimes V)} = \underset{2^{nd}}{(I \otimes V)}\underset{1^{st}}{(U \otimes I)} = \underset{\text{simult}}{U \otimes V}$$

(loc-ancilla): Alice & Bob can adjoin local ancilla systems A', B', which just enlarges their locally held system

(loc-measure): if Alice performs mmt on A with orthogonal subspaces E_a, projectors Π_a, outcomes a (so $\mathcal{H}_A = \oplus_a E_a$) then on full space it is represented by subspaces $E_a \otimes \mathcal{H}_B$, projectors $\Pi_a \otimes 1_B$ on $\mathcal{H}_{AB}$

Thus even a complete mmt on A (i.e. 1-dim E_a's) will be incomplete mmt on AB (d-dim subspaces, $d = \dim \mathcal{H}_B$).

If Bob also does a local mmt (subspaces F_b, proj's Π_b, outcomes b) on B then by Born rule, the joint probs $p(a,b)$ obtained by performing both mmts is independent of who goes first, or whether they measure simultaneously.
(orthog subspaces $E_a \otimes F_b$)
Since $(\Pi_a \otimes I)(I \otimes \Pi_b) = (I \otimes \Pi_b)(\Pi_a \otimes I) = \Pi_a \otimes \Pi_b$

No-signalling theorem / principle

Suppose Alice & Bob have access only to subsystems A & B of a joint state $|\psi\rangle_{AB}$. Then Alice cannot convey any information to Bob by performing local operations.
i.e. no local action by Alice can change the output prob. distribution of any local quantum process by Bob.

Proof (consider key main case)

Consider basic case of B performing a complete mmt w.r.t. basis $\{|b\rangle_B\}$ outcomes b,
& first: A does nothing.
Using this basis in $\mathcal{H}_B$ can write:

$$|\psi\rangle_{AB} = \sum_b |\xi_b\rangle_A |b\rangle_B \qquad (*)$$

Here $|\xi_b\rangle_A = \langle b|\psi\rangle_{AB}$ subnormalised states, sum of squared lengths $= 1$
– called "conditional state of A given b"
or "relative state" (rel. to b)
and Born rule $\text{prob}(b) = \langle \xi_b | \xi_b \rangle$.

Now suppose Alice first does a complete mmt wrt basis $\{|a\rangle\}$, outcomes a, projs $\Pi_a = |a\rangle\langle a|$. Then first, using $(*)$

$$\text{prob}(a) = \| \sum_b (\Pi_a |\xi_b\rangle)_A |b\rangle_B \|^2$$

& post-mmt for outcome a

$$|\psi_a\rangle_{AB} = \frac{1}{\sqrt{\text{pr}(a)}} \sum_b (\Pi_a |\xi_b\rangle)_A |b\rangle_B \qquad (\dagger)$$

If now B does his mmt (& supposing A got a)

$pr(b|a)$ = length sq of proj of (†) onto $|b\rangle_B$
i.e. just the b term in sum

$$= \frac{\| \Pi_a |\xi_b\rangle \|^2}{pr(a)} = \frac{\langle \xi_b | \Pi_a | \xi_b \rangle}{pr(a)}$$

So $$pr(b) = \sum_a pr(a)\, pr(b|a)$$

$$= \sum_a \langle \xi_b | \Pi_a | \xi_b \rangle$$

$$= \langle \xi_b | \xi_b \rangle \quad \ddot{\smile}$$

Remarks on other local actions

- clearly generalizes to incomplete A mmts, c.f. $\sum \Pi_a = 1_A$
- if A performs local unitary U_A first then by (*) this just changes $|\xi_b\rangle_A \longmapsto |\xi_b'\rangle_A = U_A |\xi_b\rangle_A$
  & $\langle \xi_b' | \xi_b' \rangle = \langle \xi_b | \xi_b \rangle$
  so again B's probabilities are unchanged
- if A & B include local ancillas this just enlarges local spaces & shared state $|\varphi_{AB}\rangle \longmapsto |\tilde{\varphi}\rangle_{(AA')(BB')}$
  above arguments then still apply in enlarged scenarios

Quantum dense coding

Journal paper 1992 : C. Bennett & S. Wiesner

· a single sent qubit can reliably encode only 1 classical bit

! But if qubit is entangled with a second qubit already held by the receiver then can double classical info. capacity to 2 bit.

Introduce Bell states , Bell basis for 2 qubits

$$|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\varphi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

easy to check : orthonormal

Bell bassis $\mathcal{B} = \{|\varphi^+\rangle, |\varphi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ for 2 qubits.

$$|\varphi^+\rangle = I \otimes I |\varphi^+\rangle$$
$$|\varphi^-\rangle = Z \otimes I |\varphi^+\rangle = I \otimes Z |\varphi^+\rangle$$
$$|\psi^+\rangle = X \otimes I |\varphi^+\rangle = I \otimes X |\varphi^+\rangle$$
$$|\psi^-\rangle = Y \otimes I |\varphi^+\rangle = -I \otimes Y |\varphi^+\rangle$$

$Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

In fact (exercises):

U any 1-qubit gate, $U \otimes I |\varphi^+\rangle = I \otimes U^T |\varphi^+\rangle$

$U \otimes U |\psi^-\rangle = (\det U) |\psi^-\rangle$ ($\det U$: phase)

$U \otimes U |\varphi^+\rangle = |\varphi^+\rangle$ if U = real rotation, then $U^{-1} = U^T$

Can also make Bell states from comp basis:

$|0\rangle|0\rangle \xrightarrow{H \otimes I} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \xrightarrow{CX_{12}} |\varphi^+\rangle$

$|0\rangle|1\rangle$ " $|\psi^+\rangle$

$|1\rangle|0\rangle$ " $|\varphi^-\rangle$

$|1\rangle|1\rangle$ " $|\psi^-\rangle$

do CX_{12} then $H \otimes I$

Quantum dense coding protocol

A & B distantly separated in space, each possesses one qubit of a $|\varphi^+\rangle$ state. A wants to send 2 bits of info to B:

A applies I, Z, X or Y to her qubit respectively
giving $|\varphi^+\rangle, |\varphi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$
for messages 00, 01, 10, 11 resp

A sends her qubit to B & B does a Bell mmt on the 2 qubits

Quantum teleportation

a protocol in "LOCC" paradigm
← local operations & classical communication

Alice & Bob distantly separated in space
- They can communicate classically
- They share entangled $|\varphi^+\rangle$ state
- Suppose A has another qubit in some state $|\alpha\rangle$ (possibly unknown to her)

They want to transfer this qubit to B.
- We know she cannot identify $|\alpha\rangle$ & tell him classically
- Suppose space in between is 'hostile'

Teleportation process:

A can transfer $|\alpha\rangle$ to B intact using the entanglement of $|\varphi^+\rangle$ "without the state having passed through the space in between" - in sense - transference unaffected by any physical action in the intervening space

Let qubit 1, 2, 3 be respectively:
Alice's input qubit $|\alpha\rangle$, Alice's qubit of $|\varphi^+\rangle$, Bob's qubit of $|\varphi^+\rangle$
So initial state is

$$|\alpha\rangle_1 |\varphi^+\rangle_{23}$$ A has 12, B has 3

Write $|\alpha\rangle = a|0\rangle + b|1\rangle$. Then

$$|\alpha\rangle|\Phi^+\rangle = (a|0\rangle + b|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$= \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|100\rangle + \frac{b}{\sqrt{2}}|111\rangle \qquad (*)$$

Then quantum teleportation protocol comprieses 5 steps (or (3)+2 steps i.e. '3' steps):

(i) A applies CX_{12} to her qubits 12

(ii) A applies H_1 to qubit 1

(iii) A measures her 2 qubits in computational basis obtaining a 2 bit string 00, 01, 10 or 11

Note (i)(ii)(iii) together ≡ Bell mmt on 12

Calculate effects of (i), (ii)(iii) on (*)

$$(*) \longrightarrow \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|110\rangle + \frac{b}{\sqrt{2}}|101\rangle \qquad (CX_{12})$$

$$\longrightarrow \frac{a}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|00\rangle + \frac{a}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|11\rangle$$
$$+ \frac{b}{\sqrt{2}}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|10\rangle + \frac{b}{\sqrt{2}}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|01\rangle \qquad (H_1)$$

$$\overset{\text{collect in 12}}{=} \frac{1}{2}\Big[|00\rangle(a|0\rangle+b|1\rangle) + |01\rangle(a|1\rangle+b|0\rangle)$$
$$+ |10\rangle(a|0\rangle-b|1\rangle) + |11\rangle(a|1\rangle-b|0\rangle)\Big]$$

$$\overset{!}{=} \frac{1}{2}\Big[|00\rangle I|\alpha\rangle + |01\rangle X|\alpha\rangle + |10\rangle Z|\alpha\rangle + |11\rangle XZ|\alpha\rangle\Big]$$

So by Born rule,

outcome	post mmt state	prob
0 0	$\|00\rangle I\|\alpha\rangle$	1/4
0 1	$\|01\rangle X\|\alpha\rangle$	1/4
1 0	$\|10\rangle Z\|\alpha\rangle$	1/4
1 1	$\|11\rangle XZ\|\alpha\rangle$	1/4
i j	$\|ij\rangle X^i Z^j\|\alpha\rangle$	1/4

end me

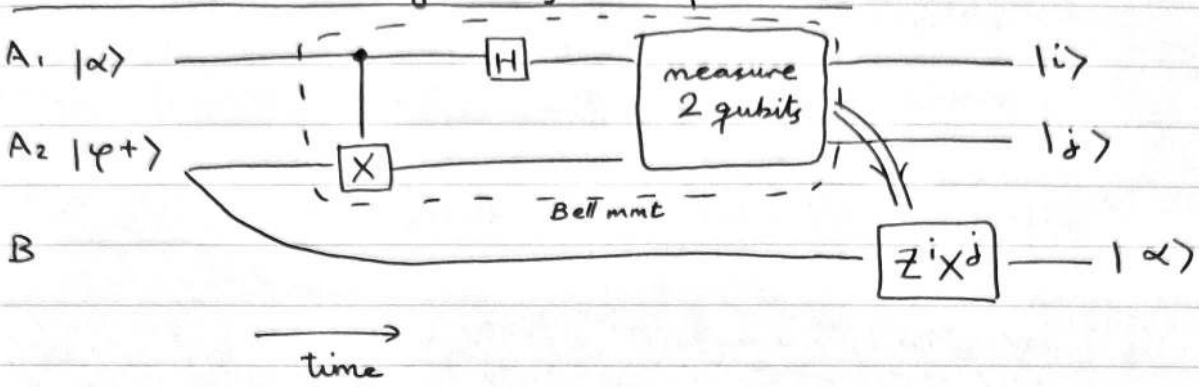
Then after (i)(ii)(iii):

(iv) A sends the 2 bit outcome ij to B

(v) On receiving ij, Bob applies unitary operation $Z^i X^j$ (inverse)

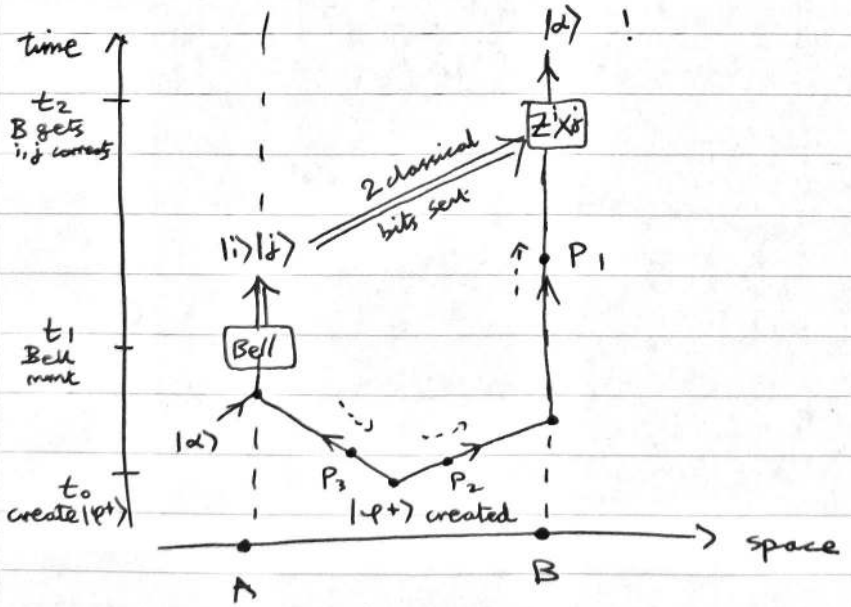
Then guaranteed for B to have state $|\alpha\rangle$.

Quantum circuit diagram for teleportation



Remarks

- After teleportation, A left with 2 qubit state $|00\rangle$ or $|01\rangle$ or $|10\rangle$ or $|11\rangle$ chosen uniformly at random
  i.e. no information about $|\alpha\rangle$ remains with A
  Thus process is consistent with no-cloning theorem (in strong sense)
- Before A's mmt, B's qubit is right half of $|\Phi^+\rangle$ state
  Can show: for any complete mmt on it, any outcome has probability $\frac{1}{2}$. After A's mmt, B's qubit is in a state that's an equal (probs $\frac{1}{4}$) mixture of $|\alpha\rangle$, $X|\alpha\rangle$, $Z|\alpha\rangle$, $XZ|\alpha\rangle$
  Averaging over these we know that outcome of any complete mmt has prob $\frac{1}{2}$, as before.
  So teleportation is consistent with no signalling theorem



· physical system embodying $|\alpha\rangle$ not transfered
- only state identity / information - reconstructed exactly in another physical system

· How did information get across ?
only 2 classical bits sent but $|\alpha\rangle$ depends on continuous parameters

1 qubit gate U applied at P_1 or P_2 or P_3 :

~~at P_1~~ Suppose Bell mmt gave $|00\rangle$ i.e Bob needs no correction

at P_1 : get $U|\alpha\rangle$ at B [telep calculation with $|\varphi^+\rangle$ replaced by $I\otimes U|\varphi^+\rangle$]

at P_2 : get $U|\alpha\rangle$ at B [" "]

at P_3 : get $U^T|\alpha\rangle$ at B [telep calc with $|\varphi^+\rangle$ replaced by $U\otimes I|\varphi^+\rangle = I\otimes U^T|\varphi^+\rangle$]

This is correct time reversed action of U on time reversed state $|\alpha\rangle$.

Ref M. Laforest, J. Baugh, R. Laflamme arxiv quant-ph/0510048

$|\alpha\rangle \rightsquigarrow$ separated into 2 parts, each totally random
- classical bits i, j
- quantum preparation of equal mixture of $|\alpha\rangle$, $X|\alpha\rangle$, $Z|\alpha\rangle$, $XZ|\alpha\rangle$

[Classical : bit b, random bit $r \rightarrow (b\oplus r, r)$
both fully random & get b back by $(b\oplus r)\oplus r = b$]

Quantum cryptography BB84 quantum key distribution (QKD)

Recall: use of non-orthogonal states to encode messages:

* receiver cannot read message reliably
* any attempt to read message cause irreversible damage
!* same applies to any evaesdropper (Eve, E)
* can use this to get unconditionally secure communication (QKD)

we'll discuss only one: Bennett - Brassard 1984 scheme

Context: secure communication (classically)

very long history ~ Caesar 100BC

substitution cipher

More generally: permutation cipher
↑ of the alphabet

Feature: . receiver & sender need to share a secret (i.e. the permutation)
· but all such schemes are insecure;
hard to guess permutation but compute table of frequency of symbols ~ characteristic of language

Still more sophisticated schemes...

- none provably secure except so-called one-time pad

Remark - public key crypto systems

- classical schemes (Diffie-Hellman scheme, RSA, elliptic curve crypto)
- currently used widely

advantages no need for shared secret!

receiver can openly publish encryption method, "public key", but only receiver can decrypt (having knowledge of "secret key"

Main disadvantage security relies on unproven (but widely believed) computational hardness assumptions - c.f. lecture 1

So (?) . in future better faster algorithm?.

* quantum computing provides new kinds of algorithms

The one-time pad (classical)

Assume message is bitstring M of length n

For encryption / decryption A & B need to share secret private key K which is a uniformly random bitstring of length n too, known only to them.

A's encryption : add K to M bitwise mod 2

This gives cypherlext (cryplext $C = K \oplus M$

which A sends to B.

B's decryption : on receiving C he computes $C \oplus K = M$

Note : If K uniformly random then so is C

So any eavesdropper learns nothing (beyond the length n) of the message M by looking at C.

Important for security that key K used only once ; hence "one-time pad"

e.g. if used trice to encode $C_1 = M_1 \oplus K$

$C_2 = M_2 \oplus K$

then $C_1 \oplus C_2$ (available to Eve) $= M_1 \oplus M_2$

~ has info about M_1 & M_2 & hence also about K

Quantum key distribution (QKD)

A method for separated parties to establish a shared secret key over public classical & quantum channels. No need for intermediary / meeting

BB84 : 4 signal states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$
B92 : uses 2 non-orthogonal states (see sheet 2)
E91 : uses an entangled pair (e.g. $|\Phi^+\rangle$)
in place of BB84 states

BB84 QKD

A & B distantly separated in space
can communicate over classical & quantum channels
Eavesdropper E also has access to these channels

For quantum transmission we'll use for qubit states

$|\psi_{00}\rangle = |0\rangle$ $\quad |\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$|\psi_{10}\rangle = |1\rangle$ $\quad |\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

giving 2 o.n. bases $B_0 = Z$ eigenbasis $\{|0\rangle, |1\rangle\}$
$B_1 = X$ eigenbasis $\{|+\rangle, |-\rangle\}$

a.k.a. conjugate bases // mutually unbiased bases

Bit value 0 will be encoded as $|0\rangle$ or $|+\rangle$ (randomly)
" 1 " $|1\rangle$ " $|-\rangle$ (")

↑ basis 0 ↑ basis 1

so $|\psi_{ij}\rangle \sim$ bit value i encoded in basis j

Remark on MUBs (optional)

- set of MUBs in $\mathbb{C}^d$: set of o.n. bases s.t. any vector of a basis is an equally weighted superpos^n in any other basis:
  $|\langle e_i | f_j \rangle|^2 = \frac{1}{d}$ all i,j all pairs of bases $\{|e_i\rangle\text{'s}\}$ $\{|f\rangle\text{'s}\}$

* Let N = max # MUBs in dim d

e.g. $d=2$, Z, X, Y - bases $N = 3 = d+1$

Known: if d = prime power then $N = d+1$

!* for any non-prime power d, N is <u>unknown</u> !

e.g. $d=6$ smallest such number d

Know only $3 \leq N \leq 7$

* arbitrary $d = p_1^{n_1} \cdots p_k^{n_k}$, $p_1 < \cdots < p_k$

known $p_1^{n_1} + 1 \leq N \leq d+1$

BB84 QKD protocol

<u>BB84 step 1</u> A generates two uniformly random binary strings of length m,

$X = x_1 x_2 \cdots x_m$, $Y = y_1 y_2 \cdots y_m$, $x_i, y_i \in \{0,1\}$

Then she prepares m qubit states

$|\psi_{x_1 y_1}\rangle \; |\psi_{x_2 y_2}\rangle \cdots |\psi_{x_m y_m}\rangle$

and sends them (in order) over to B.

- sometimes called (q) <u>conjugate coding</u>

<u>BB84 step 2</u> When B receives the m qubits they may no longer be in states $|\psi_{x_i y_i}\rangle$ that A sent because

- channel may be noisy
- eavesdropping may have occurred

Let's assume first: channel noiseless & no eavesdropping

i.e. B receives precisely the $|\psi_{x_i y_i}\rangle$ that A sent

then B generates a uniformly random string

$Y' = y_1' \cdots y_m'$, $y_i' \in \{0,1\}$

and measures qubit i in basis $B_{y_i'}$ to get a result x_i'
i.e. y_i' is B's guess at A's encoding basis y_i
Let $X' = x_1' x_2' \cdots x_m'$ be string of B msmt outcomes.
Note If $y_i' = y_i$ (B correctly chooses A basis)
then $x_i' = x_i$ too.
But if $y_i' \neq y_i$, then x_i' is completely uncorrelated to x_i
* $y_i' = y_i$ happens with prob $1/2$ = prob 2 bits chosen at random are equal, i.e. 00 or 11 & not 01 or 10

BB84 Step 3 Next A & B publicly reveal & compare their choices of bases i.e. strings Y & Y' (but keep secret X and X' strings)
They discard all bits x_i & x_i' for which $y_i \neq y_i'$ leaving shorter strings of expected length $m/2$.
Call these strings $\tilde{X}$ & $\tilde{X}'$.
Under assumption of no noise & no eavesdropping these bits would provide the desired shared secret key.

In reality: always noise & possible eavesdropping too.
So have 2 further steps - purely classical.
BB84 Step 4 "information reconciliation"
A & B want to estimate bit error rate (BER)
i.e. number of bits in $\tilde{X}'$ that differ from those in $\tilde{X}$
- they publicly compare a random sample of their strings — say half of the bits at randomly chosen positions
& discard all announced bits
& assume remaining bits have about same proportion of errors (albeit at unknown positions)

Next they want to correct these errors to obtain 2 strings that agree in high % of positions with high probability.
! — possible - sacrificing more bits, without giving everything away, if BER is not too large

BB84 Step 5 "privacy amplification"

From BER, A & B can estimate max amount of information that an eavesdropper can have about the remaining bits

From this information estimate they use classical techniques of privacy amplification with public discussion to obtain even shorter strings about which E can have practically no knowledge at all (with high prob.)

Many possible (quantum) eavesdropping strategies for E, including

* intercept - resend attack

E intercepts each passing qubit separately, measures it in some basis to try to acquire info about it & sends post-mmt state on to B.

* general coherent attack

E has a (large) quantum probe system & unitaryly interacts it with each passing qubit

Finally E can measure the proble to obtain (possibly joint) info about A's bits,

even postpone this until after listening to A & B's subsequent public discussion in steps 3, 4, 5

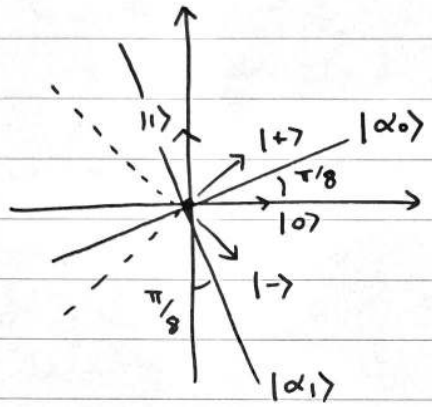
Example of intercept-resend attack

Assume quantum channel is noiseless but E intercepts each qubit & measures it in Breidbart basis:

$|\alpha_0\rangle = \cos\pi/8\,|0\rangle + \sin\pi/8\,|1\rangle$ → E concludes A's bit was 0

$|\alpha_1\rangle = -\sin\pi/8\,|0\rangle + \cos\pi/8\,|1\rangle$ " 1

This is good choice – simultaneously "closest" to both BB84 encoding states for each bit value.



sq. overlaps of both $|0\rangle$ & $|+\rangle$ with $|\alpha_0\rangle$ are $= \cos^2\pi/8$

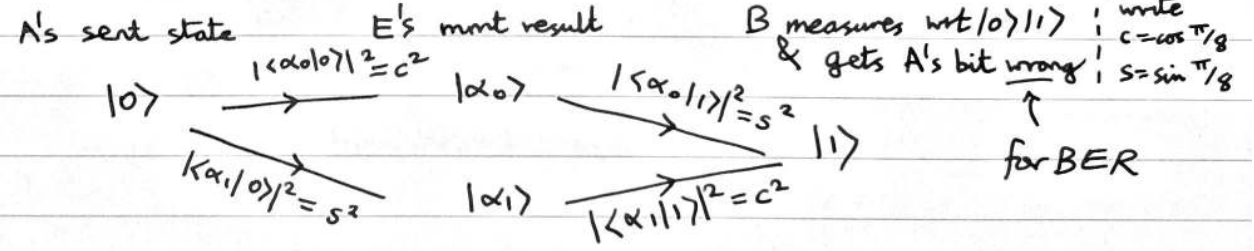
sim. for $|1\rangle$ & $|-\rangle$ for $|\alpha_1\rangle$

So in every case E's mmt result will correctly be A's bit with prob $\cos^2\pi/8 \cong 0.85 = \frac{1+\frac{1}{\sqrt{2}}}{2}$

Now calculate BER in $\tilde{X}$ vs $\tilde{X}'$ strings resulting from E's actions: we know B is measuring in same basis that A used to encode.

Four cases: of A sending $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$ (each prob $\frac{1}{4}$)

(a) Suppose A sent $|0\rangle$. Then have probabilistic branching tree:



So in this case, pr(bit error) $= c^2s^2 + s^2c^2$

$= \frac{1}{2}(4c^2s^2)$

$= \frac{1}{2}\sin^2\left(\frac{2\pi}{8}\right)$

$= \frac{1}{4}$

Other cases (A sends $|1\rangle$, $|+\rangle$, $|-\rangle$) give same BER $1/4$

So BER = $1/4$ overall

Example: idea of information reconciliation method
Book: S. Loepp & W. Woothers Cha 5
Knowing BER estimate.
1) apply a (public) random permutation to both strings
(randomise position of errors)
2) A & B break strings into blocks of suitable length (determined by BER) so it's unlikely that block contains 2 errors.
3) For each block A & B compute parity (bit sum mod 2)
- blocks with agreeing parity tentatively accepted as correct
(could still have 2 errors..)
4) For blocks with disagreeing parities, must have 1 or 3.. errors
- most likely 1
Break into 1st half / 2nd half blocks & repeat till 'offending' block is a single bit. Then B flips that erroneous bit.
5) Then A & B repeat the above many times, gradually reducing BER so block sizes increase
→ do until block length in 2) ≃ length of whole string
Note: more information is leaked to E i.e. parities
but for block length k have $\sim \log_2 k$ halvings (parity values)
- exponentially less than block size k

Example - of privacy amplification
A & B share 3-bit string $x_1 x_2 x_3$
Suppose E knows 1 bit & nothing else
Fact: if E knows bit x but not bit y
then $x \oplus y$ is unif random to E
More generally if E knows some, but not all, bits of a set, then she has no knowledge of parity of that set.

Now consider 2-bit strings y_1, y_2:

$y_1 = x_1 \oplus x_3$, $\quad y_2 = x_2 \oplus x_3$

Then have table:

x	000	001	010	011	100	101	110	111
y	00	11	01	10	10	01	11	00

Then for any fixed value of any x_i, e.g. $x_2 = 0$
corresponding 4 y's always are 00, 01, 10, 11
i.e. E has no knowledge of y's.

[Also: consider $x = x_1x_2x_3x_4$ & E knows 2 bits
Try $y_1 = x_1 \oplus x_2 \oplus x_3$, $\quad y_2 = x_2 \oplus x_3 \oplus x_4$,
$y_1 \oplus y_2 = x_1 \oplus x_4$, E will know this if her 2 bits are x_1, x_4]

Back to $x_1 x_2 x_3$

Can write $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}}_{G} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \equiv Gx$

Rows of G define subsets of bits for parity sums

More generally can show

Thm If E knows k bits of n (& nothing else)
then $m \times n$ $(m < n)$ Boolean matrix G will produce
secret y's (m of them) iff
min Hamming weight of code generated by G
is strictly $> k$

- code $\equiv$ linear subspace of $(\mathbb{Z}_2)^n$, $\dim = k \leq n$
  $\equiv$ span of k basis codewords in $(\mathbb{Z}_2)^n$
  given by rows of G (non-zero)
- min weight of code = least Hamming weight of any $c \in C$
- Hamming distance of 2 codewords $c_1, c_2 \in C$
  = # places in which they differ
  = Hamming weight $c_1 \oplus c_2 \geq$ min wt w

Can extend these ideas to cover all kinds of E's into

Universal hashing: given n bit string choose $m < n$ determined by BER, & random Boolean $m \times n$ G ($\sim m$ random subsets of n bits)

then w.h.p. E will have no info about m bit string $y = Gx$

↑ with high probability

Computation & basic notions of computational complexity theory

Write $B = B_1 = \{0,1\}$, $B_n = \{$ all n-bit strings $\}$

$B^* =$ set of all finite length bit strings $= \bigcup_n B_n$

Computational task

- input: bit string $x = i_1 \cdots i_n \in B_n$
* input size $= n =$ length of input
- language $L \subseteq B^*$ (e.g. primes in binary)
* Decision problem: given $x \in B^*$, is $x \in L$
  ↖ 1 bit output

Computational model (classical)

many possible choices

important feature: a process with discrete steps, each requiring a fixed constant effort/resource to implement – not growing with n

e.g. elementary 1 or 2 bit Boolean gates

Circuit model (or gate array model)

For input $x = i_1 \cdots i_n$ extend with extra 0 bits
↖ "extra working space"

$i_1 \cdots i_n 0 \cdots 0$

basic comp step: specified AND, OR, NOT gate applied to specified bits in list.

Note: these gates are universal i.e. any $f: B_n \to B_n$ can be constructed by a sequence of these steps

Computation is prescribed sequence C_n of these steps for each input size n.

Output is value of some designated bit(s) after final step.

C_n called Boolean circuit

In all, have circuit family $(C_1, C_2, C_3, \ldots)$

Randomised (probabilistic) classical computation

As above, but initially extend $x = i_1 \cdots i_n$ also by a sequence of random bits $r_1 \cdots r_k$. So start now with

$$i_1 \cdots i_n r_1 \cdots r_k 00 \cdots 0$$

Each time circuit C_n is run, random bits are newly set initially uniformly at random

Output is probabilistic.

Then usually require output to be correct with "suitably good probability", as desired.

Complexity of a computational task

"consumption of resources as a function of n"

Resource taken to be

time $T(n)$ = number of computational steps
= circuit size = # of gates

space $Sp(n)$ = amount of memory / workspace needed

We'll consider time only.

* Main question: Does $T(n)$ grow polynomially or exponentially (super-poly) with n?

· poly-time: write $T(n) = O(\text{poly}(n))$ or $O(n^k)$, some k
i.e. $\exists n_0$ & true const c such that $T(n) < cn^k$ for all $n > n_0$

Poly Time computations are "tractable / feasible in practice"

exponential (superpoly) time: "computable in principle but but no feasible / computable in practice

$n^{\log n} = 2^{(\log n)^2}$
or $2^{\sqrt{n}} < c^n$ any $c > 0$

* poly vs expn time makes notion of complexity robust against details of model used

e.g. binary vs decimal representation of inputs

· circuits vs TMs

· choice of universal gate set

· also has good properties for complexity considerations since sums & products of polys are still polys

Complexity classes of decision problem

P (poly time) - class of decision problems having (deterministic) poly-time algorithms

BPP (bounded error, probab, poly time) - class of decision problems with probabilistic poly-time algorithms, such that for every input x Prob(answer correct) $> \frac{2}{3}$

($x \in L$: $Pr(\text{output} = 1) > \frac{2}{3}$
$x \notin L$: $Pr(\text{output} = 1) < \frac{1}{3}$)

"bounded error": $\frac{2}{3}$ bounded away from $\frac{1}{2}$

* efficient algorithm ≡ poly-time algorithm

Fact: can replace $2/3$ here by any const $\frac{1}{2}+\delta$, $0<\delta<1/2$ & class BPP is same

Idea: if have $(\frac{1}{2}+\delta)$ algorithm, (δ small say) repeat it K times, take majority vote as final answer

KIMI GA SHINE

Chernoff bound of prob theory

$\Rightarrow$ prob(maj vote correct) $> 1 - e^{-2\delta^2 K}$

so can be $>$ any $1-\varepsilon$ for suitable const K

(solve $e^{-2\delta^2 K} < \varepsilon$)

& $K \times$ poly = a poly so "K-runs" process is still poly time

[Nielsen & Chuang book p154]

* BPP ~ classically feasible computations

"computable in practice"

clearly $P \subseteq BPP$ but unknown if $P = BPP$ or not

Poly time algorithms, classes P & BPP

Example primality testing

input: is integer N in binary

input size $n = \log_2 N$

Naive test-divide algorithm – not poly time

↑ try divide by $2, 3, 4, \ldots, \sqrt{N}$ ⇒ at least $\sqrt{N} = 2^{n/2}$ steps

if $N = ab$, a or b must be $\leq \sqrt{N}$

Known: primality testing is in BPP – Solovay-Strassen algorithm 1977

shown to be in P in 2004

Many more complexity classes

NP – see later

PSPACE: deterministic algorithms with poly space

i.e. length of input $i_1 \cdots i_n 0 \cdots 0$

← bounded → by poly(n)

Clearly $P \subseteq PSPACE$

Easy to see:

inclusions $P \subseteq NP \subseteq \begin{matrix} \updownarrow ? \\ BPP \end{matrix} \subseteq PSPACE$

None of the inclusions known to be strict

Quantum computation – circuit model

For input $x = i_1 \cdots i_n \in B_n$ start with qubits

$|i_1\rangle |i_2\rangle \cdots |i_n\rangle |0\rangle \cdots |0\rangle$

Computational steps are quantum gates on designated (few) qubits each. Commonly use

$H, X, Z, \quad P(\varphi) = \begin{pmatrix} 1 & \\ & e^{i\varphi} \end{pmatrix}, \quad CX, CZ$

output: quantum measurement in $\{|0\rangle, |1\rangle\}$ basis only on specified qubits

Universal sets of gates

General U on n qubits ~ continuous parameters

so no finite quantum gate set can be (exactly) universal

(finite circuits of finite set of gates ⇝ finite strings from finite alphabet ⇝ countably many)

So ask for

Approximate universality of a gate set $\mathcal{G}$:

For any $\varepsilon > 0$ & any W on n qubits there is a circuit $\tilde{W}$ of gates from $\mathcal{G}$ such that

$$\|W - \tilde{W}\| < \varepsilon \qquad \text{Here } \|A\| \overset{\text{def}}{=} \max_{\text{normalised } |\psi\rangle} \|A|\psi\rangle\|$$

($\|A\|$: operator norm; $\|A|\psi\rangle\|$: vector norm)

$$\max_{|\psi\rangle} \|W|\psi\rangle - \tilde{W}|\psi\rangle\|$$

Size of circuit $\tilde{W}$ generally exponential in # qubits n of W.

For dependence on accuracy:

Solovay – Kitaev theorem

For each fixed n, there is a poly P such that for all W on n qubits, size of circuit $\tilde{W}$ is bounded by $P(\log 1/\varepsilon)$

i.e. poly in # digits of accuracy

[Proof: Nielsen & Chuang appendix]

Facts: $\mathcal{G} = \{CX, \text{all 1-qubit gates}\}$ infinite set is exactly universal.

$$\mathcal{G} = \{H, CX, P(\tfrac{\pi}{4}) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}\}$$

is approx universal

(See N&C §4.5)

Complexity class BQP (bounded error quantum poly time)
~ class of all decision problems that can be solved with poly-sized quantum circuit family, having prob(answer correct) at least $2/3$ in every case
"problems feasible/computable in practice on a quantum computer"
- BQP unchanged if $2/3 \rightsquigarrow$ any $\frac{1}{2} < x < 1$
- BQP is indep of choice of approx universal gate set (see ExSh 3...)
- $BPP \subseteq BQP$ "quantum computing at least as strong as class"
- Is $BPP \subsetneq BQP$? Unproven, but believed.

Reversible version of any Boolean function $f : B_m \to B_n$

For any $f : B_m \to B_n$, $x \mapsto f(x) = y$, $x \in B_m$, $y \in B_n$
Consider $\tilde{f} : B_{m+n} \to B_{m+n}$

$$(x, y) \longmapsto (x, y \oplus f(x))$$

(x: called input register; y: output register)

* $f \leftrightarrow \tilde{f}$ easily either way
$\oplus$ is addition of n-bit strings bitwise i.e. $\oplus$ in $(\mathbb{Z}_2)^n$

e.g. $\begin{array}{r} 011 \\ 110 \\ \hline 101 \end{array} \oplus$ $\qquad x \oplus x = 0 \ \forall x$

Lemma $\tilde{f}$ always reversible, actually self-inverse

Proof recall $x \oplus x = 0 \ \forall x$
then $(x, y) \xrightarrow{\tilde{f}} (x, y \oplus f(x)) \xrightarrow{\tilde{f}} (x, y \oplus \underbrace{f(x) \oplus f(x)}_{0})$
$= (x, y)$

i.e. $\tilde{f} = (\tilde{f})^{-1}$. $\square$

Now if $g : B_k \to B_k$ is any invertible Boolean function then the linear map on k qubits defined on basis by

$$A_g : |x\rangle \mapsto |g(x)\rangle$$

is unitary.

$\leftarrow$ $|x\rangle = |i_1\rangle \cdots |i_k\rangle$, $|g(x)\rangle = |j_1\rangle \cdots |j_k\rangle$ for $f(i_1 \cdots i_k) = j_1 \cdots j_k$

For $\tilde{f}$ write $A_{\tilde{f}}$ as U_f.

$U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ on $(m+n)$ qubits

used to represent Boolean f's f in quantum computing.

Computation by quantum parallelism

Have $|x\rangle|0\cdots0\rangle \xrightarrow{U_f} |x\rangle|f(x)\rangle$

(m qubits, n qubits)

So by linearity

$$\left(\frac{1}{\sqrt{2^m}} \sum_{\text{all } x} |x\rangle\right) |0\cdots0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^m}} \sum_{\text{all } x} |x\rangle|f(x)\rangle \equiv |f\rangle$$

* one run of U_f gives a state $|f\rangle$ all (expon many) values of f!
* Furthermore although $|\psi\rangle = \frac{1}{\sqrt{2^m}} \sum_{\text{all } x} |x\rangle$ has expon many terms it can be made easily by poly(m) (linear) effort – use m H's $\quad |0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$$\text{So } |0\rangle\cdots|0\rangle \xrightarrow{H^{\otimes m}} \frac{1}{\sqrt{2^m}} (|0\rangle+|1\rangle) \cdots (|0\rangle + |1\rangle) \equiv |\psi\rangle$$

Query complexity / promise problems

Instead of input $x = i_1 \cdots i_n \in B_n$ or $|i_1\rangle \cdots |i_n\rangle$, have:

* input is a given black box / oracle $\mathcal{O}_f$ that computes some boolean function $f : B_m \to B_n$ (or U_f in quantum case)
  - each use of oracle counts as one computational step
  - may have a priori promise on form of f
  - Problem: want to determine some property of f

* only access to f is via queries (inputs) to oracle
• computation starts on $0\ldots0$ or $|0\rangle\ldots|0\rangle$

Query complexity number of times that the oracle needs to be queried to solve the problem

Total time complexity total size of circuit, counting each oracle use as one gate.

Example (balanced vs constant problem)

Input: black box / oracle for a Boolean $f: B_n \to B = B_1$

Promise: f is either (a) a const function, $f(x) = 0 \ \forall x$ or $= 1 \ \forall x$

(b) 'balanced' i.e. exactly half of its 2^n values are 0 and 1

Problem: determine if f is (a) or (b) with certainty

classically: $2^n/2 + 1$ queries are necessary & sufficient to solve with certainty

sufficiency: clear

necessary: suppose we have a deterministic classical algorithm $\mathcal{C}$ claimed to work for any such f with $K \leq 2^n/2$ queries.

Then an adversary A can make $\mathcal{C}$ fail:

when $\mathcal{C}$ run with A, A has not yet chosen f but simply answers 0 to any query

At the end: it must correctly output 'balanced' or 'const'. But A has his f^n now specified on $K \leq 2^n/2$ xs (all 0s) so is free to extend f to all x to be balanced or const to make $\mathcal{C}$'s output wrong

quantumly: 1 query suffices!

Deutsch–Jozsa algorithm (DJ) (1992)

Have $U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

We use "phase kick back" to encode f^n values as $\pm$

rather than ↑ 0/1s

$$|a\rangle\left(e^{i\theta}|b\rangle\right) = \left(e^{i\theta}|a\rangle\right)|b\rangle$$

! set output register (1 qubit) to $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = H|1\rangle$
$= HX|0\rangle$

Then note

$$|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{U_f} |x\rangle \left[\frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right]$$

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

$$= (-1)^{f(x)} |x\rangle|-\rangle$$

Now do in superposition over all x's

$$\frac{1}{\sqrt{2^n}} \sum_{\text{all } x} |x\rangle|-\rangle \xrightarrow{U_f} \underbrace{\left(\frac{1}{\sqrt{2^n}} \sum_{\text{all } x} (-1)^{f(x)} |x\rangle\right)}_{\text{call } |\xi_f\rangle} (|-\rangle)$$

↘ discard (unentangled)

So 1 query gives $|\xi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_{\text{all } x} (-1)^{f(x)} |x\rangle$

Key observation. f const vs f balanced

all signs same — exactly half ± signs

so $|\xi_{f\,\text{const}}\rangle \perp |\xi_{f\,\text{bal}}\rangle$

orthog: ⇒ can perfectly distinguish with a quantum mmt

But: we allow mmt only in standard basis

Recall: $|0\rangle \cdots |0\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2}} \sum_{\text{all } x} |x\rangle \xrightarrow{H^{\otimes n}} |0\rangle \cdots |0\rangle$
as $HH = I$

so write $|\eta_f\rangle = H \otimes \cdots \otimes H |\xi_f\rangle$

then $|\eta_{f\,\text{const}}\rangle \perp$ any $|\eta_{f\,\text{bal}}\rangle$

and f const: $|\eta_f\rangle = \pm |0\rangle \cdots |0\rangle$

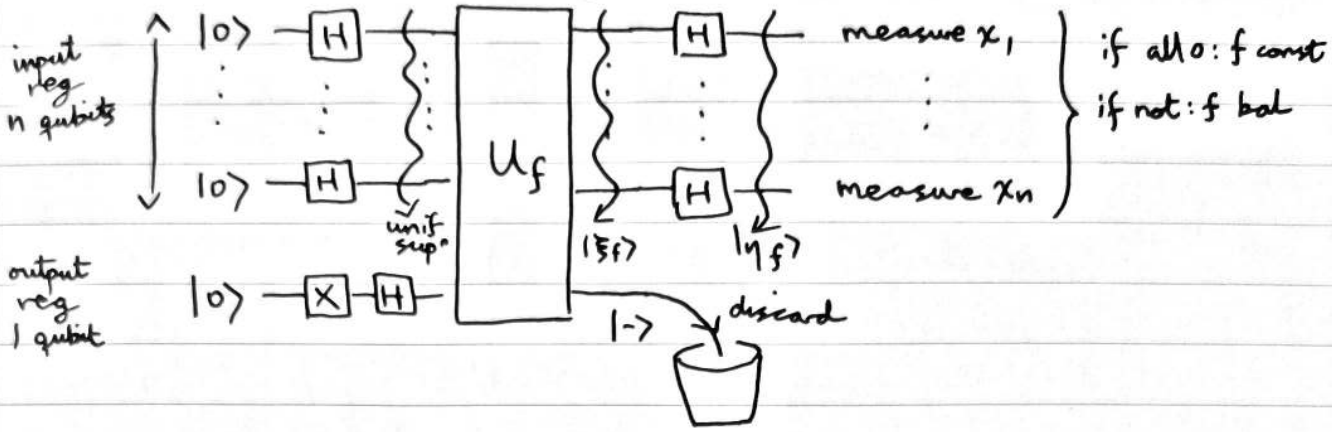
f bal: $|\eta_f\rangle = \sum_{\substack{x \in B^n \\ x \neq |0\rangle \ldots |0\rangle}} a_x |x\rangle$ ← some ampl

So mmt of n qubits of $|\eta_f\rangle$ distinguishes f const (mmt gives

$0 \cdots 0$ with certainty)

from f_{bad} (mmt gives <u>some</u> $x \in B_n$ but never $x = 0 \cdots 0$)

Circuit diagram for DJ algorithm



$$|\xi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} |-1)^{f(x)} |x\rangle$$

Uses one query + $O(n)$ processing.

Remarks

(1) For some special balanced f's ($2^n - 1$ of all ${}^{2^n}C_{2^{n-1}}$ bal. functions), f_a labelled by $a \in B_n$, $a \neq 00\cdots0$ get $|\eta_{f_a}\rangle = |a\rangle$ so final mmt gives a with certainty.
In fact $f_a(x) = a \cdot x = a_1 x_1 \oplus \cdots \oplus a_n x_n$
→ see ExSh3 Bernstein-Vazirani problem / algorithm

(2) Can we decide <u>any</u> yes/no question about $f: B_n \to B_1$ by q. algorithm on $|f\rangle$ or few (poly(n)) queries to U_f?
<u>No!</u> e.g. SAT problem (NP complete)
given $f: B_n \to B_1$, (no promise)
is there an x with $f(x) = 1$?
Can prove: any q. algorithm solving this with prob $1-\varepsilon$ (any $\varepsilon > 0$) needs at least $O(\sqrt{2^n})$ queries to f.
(any classical algorithm needs at least $O(2^n)$ queries)

(3) If tolerate error in bal vs const problem i.e. answer correct with prob $1-\varepsilon$ (any $\varepsilon > 0$)
DJ still applies ⇝ 1 query solution.

But now there is classical randomised algorithm with const # queries ($O(\log(1/\varepsilon))$) so lose exponential separation of quantum over classical.

Classical algorithm

choose K (fixed) x values $x_1, \ldots, x_K$ uniformly at random, & evaluate $f(x_1), \ldots, f(x_K)$ (K queries)

If all same: output "const"

If not: output "balanced"

If f was const: answer correct prob 1

If f was bal: each $f(x_i) = 0/1$ prob $1/2$ each

so prob (all 0 or all 1) $= 2/2^K =$ prob (wrong)

then $\frac{2}{2^K} < \varepsilon$ if $K > \log_2(1/\varepsilon) + 1$

But Simon's algorithm/problem (1994) → ExSh 3

→ a provable exponential separation of query complexity with bounded error

Oracle: $f : B_n \to B_n$

Promise: f either (a) f one-to-one

(b) f two-to-one such that there is $\xi \in B_n$ s.t. $f(x \oplus \xi) = f(x) \quad \forall x$

(recall $\xi \oplus \xi = 00\ldots0$)

Sheet 3 → quantum algorithm with $O(n)$ queries.

DJ → Simon's → Shor's factoring algorithm

(4) oracle problem "no access to inside/workings" of oracle

- unrealistic?
- would like a standard comp. task ...
- none (provably) known!

Quantum Fourier Transform & periodicities

Def QFT mod N (or QFT_N or QFT)

N-dim state space, basis $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ labelled by $\mathbb{Z}_N$

often 2^n $\quad QFT: |a\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} e^{2\pi i ab/N} |b\rangle$

$a, b = 0, 1, \ldots, N-1$

Matrix entries: $[QFT] = \frac{1}{\sqrt{N}} \omega^{ab}, \quad \omega = e^{2\pi i/N}$

$a, b = \underline{0}, 1, \ldots, N-1$

row/column labels from $\underline{0}$ ...

The matrix $\sqrt{N}QFT$ is:

- symmetric
- 1st row/col always all 1's
- each row/col is geometric sequence $1, r, r^2, \ldots, r^{N-1}$, $r = \omega^k$ for k^{th} row/col
- QFT mod 2 = H
- QFT mod 4 $\neq H \otimes H$,

$(\mathbb{Z}_2)^n$ (group) $\longrightarrow H \otimes \cdots \otimes H$ is "Boolean FT" on n

$\neq$ QFT mod 2^n

Prop: QFT is unitary

Use basic fact $1 + r + r^2 + \cdots + r^{N-1} = \begin{cases} \frac{1-r^N}{1-r} & \text{if } r \neq 1, \\ N & \text{if } r = 1. \end{cases}$

If $r = \omega^k$ get $\begin{cases} 0 & \text{if } k \text{ not mult of } N \\ N & \text{if } k \text{ is mult of } N \ (\text{or } 0) \end{cases}$

Then see $QFT^\dagger QFT = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & \omega^a & \cdots \\ & \uparrow & \\ & a^{th} \text{ row} & \end{pmatrix} \frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ \omega^b \\ \vdots \\ \uparrow \\ b^{th} \text{ col} \end{pmatrix} = I$

$(ab)^{th}$ entry $= 1 + r + r^2 + \cdots + r^{N-1}$, $r = \omega^{b-a}$

Periodicity problem

Given $f: \mathbb{Z}_N \to Y$ (oracle, but can be formula too)

Promise f is periodic $f(x+r) = f(x)$, least r, all x
($+$ mod N)

(so r divides N: $N = Ar$, integer A = # periods)

will also require that f is 1-1 in each period

$f(x_1) \neq f(x_2)$, $0 \leq x_1 < x_2 < r$

Problem find r (with any const level of probability $1-\varepsilon$, $\varepsilon > 0$ indep of N)

Note generally r can be $O(N)$ as N increases

Fact classically $O(\sqrt{N})$ queries are necessary and sufficient
~ "collision problem"

! will show: quantumly $O(\log\log N)$ queries
$+ O(\text{poly}(\log N))$ further processing steps suffice.

Later: will reduce factoring of integer K to periodicity problem with $N \simeq K^2$, so input size $n = O(\log K)$ for factoring so above algorithm is poly-time in n.

Quantum algorithm for periodicity determination

Have quantum oracle for $f: \mathbb{Z}_N \to \mathbb{Z}_M$

$U_f |x\rangle|y\rangle = |x\rangle|y + f(x) \bmod M\rangle$

1) Make $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ (e.g. $QFT_N|0\rangle$ gives this)

2) Use 1 query to get

$$|f\rangle = \frac{1}{\sqrt{N}} \sum_{\text{all } x} |x\rangle|f(x)\rangle$$

Now recall $r|N$, $N = Ar$, A = # periods

3) Measure 2nd register, see some value $y = f(x_0)$ with x_0 least x with $f(x) = y$ i.e. in 1st period

So one such x value in each period

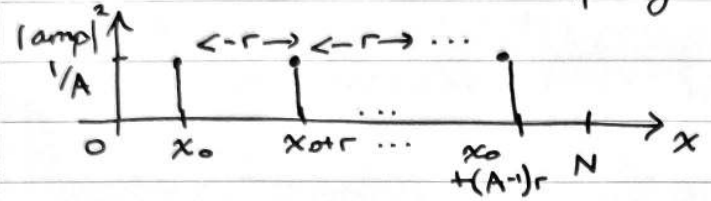
$x_0, x_0+r, x_0+2r, \ldots, x_0+(A-1)r$

So 1st register collapsed to

$$|\text{per}\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle$$

* here x_0 has been chosen unif at random from $0, 1, \ldots, r-1$ i.e. in 1st period

since all f^{th} values occur equally often



? If we measure $|per\rangle$ we select a random j value $\Rightarrow x_0 + jr$ so get a random element x_0^{th} of a random period (j^{th})
$\equiv$ uniformly random x in $0, 1, \ldots, N-1$ i.e. useless!

Resolution: apply QFT_N first!

4) Apply QFT to $|per\rangle$

Recall QFT: $|x\rangle \rightsquigarrow \frac{1}{\sqrt{N}} \sum_y \omega^{xy} |y\rangle$, $\omega = e^{2\pi i/N}$

So $$QFT|per\rangle = \frac{1}{\sqrt{NA}} \sum_{j=0}^{A-1} \left[\sum_{y=0}^{N-1} \omega^{(x_0+jr)y} |y\rangle \right]$$

$$= \frac{1}{\sqrt{NA}} \sum_{y=0}^{N-1} \omega^{x_0 y} \left[\sum_{j=0}^{A-1} \omega^{jyr} \right] |y\rangle$$

Now look at last $[\ldots]$

$[\ldots]$ is geom series $1 + \alpha + \cdots + \alpha^{A-1}$, $\alpha = \omega^{yr} = e^{2\pi i ry/N}$
$= (e^{2\pi i/A})^y$

If $\alpha \neq 1$, (i.e. iff y is not a multiple of A) ↖ $\alpha^A = 1 \ \forall y$

$$[\ldots] = \frac{1-\alpha^A}{1-\alpha} = 0$$

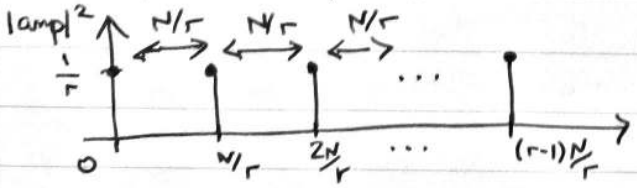
If $\alpha = 1$, (i.e. iff y is mult of A)

$$[\ldots] = A$$

So $$QFT|per\rangle = \sqrt{\frac{A}{N}} \sum_{k=0}^{r-1} \omega^{x_0 k(N/r)} \left| k\tfrac{N}{r} \right\rangle$$

↖ $\frac{1}{\sqrt{r}}$

Random shift x_0 now in phase not in labels, so $|amp|^2$ indep of x_0!



5) Now measure label: will obtain c which is a multiple $k_0 N/r$
$0 \le k_0 \le r-1$ chosen unif at random

$$c = k_0 \frac{N}{r}$$

unknown, but unif random k_0 ← want

$$\frac{k_0}{r} = \frac{c}{N}$$

c ← know, N ← know

6) To get r, use some (purely classical) number theory:

* suppose (by good luck) k_0 coprime to r
then we cancel c/N to lowest terms $\tilde{c}/\tilde{r}$
[Euclid's algorithm for hcf, & divide it out, all in poly$(\log N)$ time]
& read off r as resulting denominator $\tilde{r}$

how likely to be so lucky? Quote / use:

Thm (coprimality)
The # integers $< r$ that are coprime to r
grows as $O\left(\frac{r}{\log\log r}\right)$ [$\sim e^{-\gamma} r/\log\log r$] as $r \to \infty$

$$\gamma = \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \log n\right)$$

↑ woopsie!

So if k_0 chosen unif at random $< r$,
prob (k_0 coprime to r) $\sim O\left(\frac{1}{\log\log r}\right) > O\left(\frac{1}{\log\log N}\right)$

* can check if $\tilde{r}$ is true period:
evaluate $f(0)$ & $f(\tilde{r})$, see if same
(if k_0 was not coprime then $\tilde{r} < r$ ($\tilde{r}$ a factor of r)

So get period r with prob $\left(O\left(\frac{1}{\log\log N}\right)\right.$ & 3 queries

Lemma (basic prob theory)
If an event has success prob p & given any $0 < 1-\varepsilon < 1$
then for M trials, prob(at least one success) $> 1-\varepsilon$
if $M = -\log \varepsilon / p$ i.e. $O(1/p)$ for const. ε

Proof want prob(all fail) $= (1-p)^M < \varepsilon$
so $M > -\log\varepsilon / -\log(1-p) \gtrsim -\log \varepsilon / p$

So repeat q. algorithm $O(\log \log N)$ times
(& check each time $\tilde{r}$ value)
will get r with any const level $1-\varepsilon$ of prob e.g. 0.9999
Each repeat uses 3 queries ($|F\rangle$, $f(0)$, $f(\tilde{r})$)

Fact: QFT mod N can be implemented in poly(n) time

e.g. have:

Theorem QFT mod 2^n can be implemented by circuit of size $O(n^2)$

Proof: see notes § 9.3 (optional)

Based on fact:

$$QFT_{2^n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i xy/2^n} |y\rangle \qquad x = 0, 1, \ldots, 2^n-1$$

is always a product state of n 1-qubit states

Quantum algorithms for search problem (Grover's algorithm)

Search problems: search for "good" item in a (large) search space. 2 features:

① given any item "easy" (poly-time) to check if it's good or not

② "exponentially many" items in search space

Basic examples

· simultaneous constraint satisfaction e.g. timetabling

* Boolean satisfiability SAT:

Given: boolean formula $f: B_n \to B_1$ (poly(n) time computable), n boolean variables

Problem: is there a satisfying assignment?

i.e. input $x = x_1 \cdots x_n$ with $f(x) = 1$

Formalised in complexity class NP

"non-deterministic poly time" NO PROBABILITY

Intuitively: class of languages L which may be hard to decide (e.g. $L \notin P$) but if $x \in L$ then can check/certify membership in poly time

More formally: 2 definitions:

1st defn of NP Language L is in NP if:

there is a computation $V(x, c)$ called "poly time verifier" with 2 inputs x & c such that

(a) V runs in poly $|x|$ time

* (b) (i) if $x \in L$ then for some c, $V(x,c)$ halts with "accept"

(ii) if $x \notin L$ " all " "reject"

i.e. (i) c is certificate / proof of membership
& checkable in poly time

(ii) if x not true member, cannot be fooled into accepting it

Clearly $P \subseteq NP$

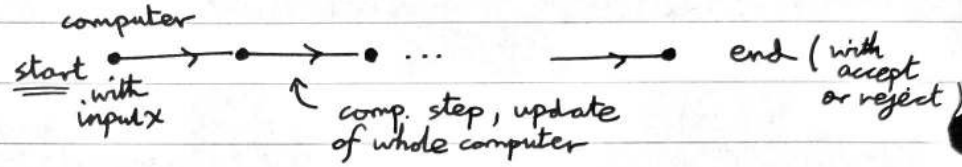
$SAT \in NP$

Note: asymmetric in $x \in L$ vs $x \notin L$!

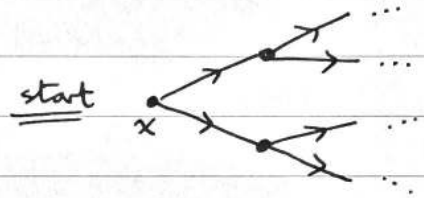
2nd def of NP ~ non-deterministic computation

Pictorially

deterministic:



non-deterministic:



* at each stage computer can branch into 2 different computational paths / step

* all branches done in ||el (NOT probab choice)

so after k steps, can have 2^k computations running in ||el

(unphysical comp. model)

Poly time: all paths run in poly time

- each halting with accept or reject
- may get both answers for x, on different paths

Definition: the computation accepts x if at least one path accepts
rejects if all paths reject

2nd def of NP: NP = class of languages accepted by a non-deterministic poly-time computation ← clearly $P \subseteq NP$

Thm def 1 equivalent to def 2

Proof idea poly-time verifier $V(x,c)$ ⇝ non-det poly-time computation N

- V runs in poly $|x|$ time ⇒ at most poly $|x|$ bits of c can be relevant

So on input x, N 1st branches into $2^{\text{poly}|x|}$ branches,
each path writing a c-string next to x
then N just runs $V(x, c)$ in each path ✓

poly-time non-det N $\longrightarrow$ poly time $V(x, c)$
if $x \in L$, then $\exists$ branch of N that accept
& $x \notin L$, all branches reject
so label paths by bit strings $b_1 b_2 \cdots b_k$, k = depth of tree
$b = 0 \rightarrow$ "go up", $b = 1 \rightarrow$ "go down"
Let c = label of any path
Then $V(x, c)$ is poly time <u>det</u> computation that runs the single c^{th} branch of N on x

NP to quantum computing

Computing in quantum superposition looks (superficially) like non-deterministic computation!

but mmt theory causes a problem

e.g. SAT for $f : B_n \to B_1$

easy accessed to exponential "quantum branching"

$$|0\rangle \cdots |0\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} |x\rangle$$

then get $|f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} |x\rangle |f(x)\rangle$

But cannot easily decide SAT from $|f\rangle$

e.g. $f_0(x) = 0$ for all x

vs $f_1(x) = \begin{cases} 0 & \text{all } x \neq x_1 \\ 1 & x = x_1 \text{ (unique)} \end{cases}$

STA reject f_0, accept f_1

Then $|f_0\rangle$ & $|f_1\rangle$ exponentially close as vectors

$$\| |f_0\rangle - |f_1\rangle \| \sim 1/\sqrt{2^n}$$

so output prob distributions for any mmt expon. close too

$\Rightarrow$ need expon many samples to distinguish them

will see: for SAT: classically $O(2^n)$ queries neces & suff

quantumly $O(\sqrt{2^n})$ "

Structured vs unstructured search

Searching can be greatly helped by structuring the search space

e.g. finding an item in a linearly ordered database, size 2^n

- classically n queries necessary & sufficient

by binary search

[Quantumly: optimal no. queries not known: but know

$0.220n \leq$ # q. queries $\leq 0.526n$

unstructured search: if we query any x in database, then get no info about goodness/badness of any other y in database

Unstructured search problem for a unique good item

Given: unstructured database with $N = 2^n$ items containing unique good item [or no good item]

Problem: find good item [or determine if one exists] with prob $1-\varepsilon$ any const $\varepsilon > 0$

Classically $O(N)$ queries are necessary & sufficient

[can assume good item has been uniformly at random

So in k queries $\Pr(\text{good seen}) = k/N$ so $k = O(N)$ to make prob const.]

Quantumly: Grover's algorithm: $O(\sqrt{N})$ queries suffice (Grover 1996) & $O(\sqrt{N})$ are necessary [many proofs, first 1994]

Database will be represented by oracle $f: B_n \to B_1$

a lookup / good-bad test $\equiv$ a query

Promise: there is unique $x_0 \in B_n$ with $f(x_0) = 1$

$$(\& f(x) = 0 \text{ for all } x \neq x_0)$$

Problem: find x_0

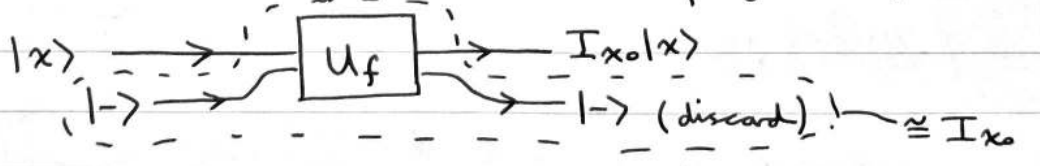
Usual quantum oracle $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ on $(n+1)$ qubits

We'll use instead I_{x_0} on n qubits

$$I_{x_0}|x\rangle = \begin{cases} |x\rangle & \text{if } x \neq x_0, \\ -|x\rangle & \text{if } x = x_0, \end{cases}$$

formula $I_{x_0}|x\rangle = I|x\rangle - 2|x_0\rangle\langle x_0|x\rangle$

Implement: one use of I_{x_0} from one query to U_f



More generally we'll need reflections

For any state $|\alpha\rangle$

$\Pi_{|\alpha\rangle} = |\alpha\rangle\langle\alpha|$ is proj^{n} onto 1-dim subspace of $|\alpha\rangle$

$I_{|\alpha\rangle} =: I - 2|\alpha\rangle\langle\alpha|$ is reflection in mirror hyperplane $\perp |\alpha\rangle$

$I_{|\alpha\rangle}|\alpha\rangle = -|\alpha\rangle$ ($|\alpha\rangle \perp$ mirror)

& any $|\beta\rangle \perp |\alpha\rangle$: $I_{|\alpha\rangle}|\beta\rangle = |\beta\rangle - 2|\alpha\rangle\langle\alpha|\beta\rangle$ (zero)

↖ i.e. in mirror $= |\beta\rangle$

For computational basis states of n qubits,

write $I_{|x\rangle}$ as I_x

$I_{|0\cdots0\rangle}$ as $I_{0\ldots0}$ or just I_0

$H_n = H \otimes \cdots \otimes H$, $N = 2^n$

Grover's algorithm

quantum searching

work on n qubits

- start with $|\psi_0\rangle = H_n|0\cdots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{\text{all } x} |x\rangle$

! - consider Grover iteration operator on n qubits

$$Q = -H_n I_0 H_n I_{x_0}$$

↑ x_0 unknown; 1 query to oracle needed for I_{x_0}

($|\psi_0\rangle$ & Q have only real components/entries so will get direct geom interpretation in Euclidean $\mathbb{R}^N$)

Will show: Let $P(x_0)$ = (real) plane of $|x_0\rangle$ & $|\psi_0\rangle$

↑ initially unknown!

Then

* (Q1): In $P(x_0)$, Q is rotation through 2α with $\sin\alpha = 1/\sqrt{N} = \langle x_0|\psi_0\rangle$

(Q2): In orthogonal complement $P(x_0)^\perp$, $Q = I$

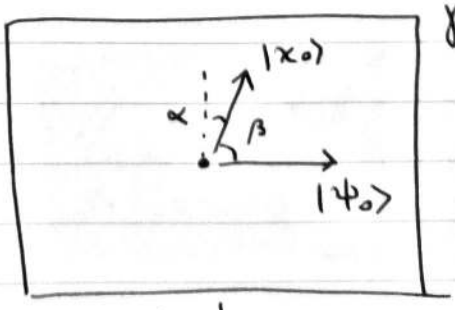
So: * repeatedly apply Q to $|\psi_0\rangle$ to rotate it near to x_0 (in $P(x_0)$) & then measure

Initial angle:

$\cos\beta = \langle x_0|\psi_0\rangle = \frac{1}{\sqrt{N}}$ (indep of $|x_0\rangle$)

so # iterations $= \frac{\arccos\left(\frac{1}{\sqrt{N}}\right)}{2\arcsin\left(\frac{1}{\sqrt{N}}\right)} = \frac{\beta}{2\alpha}$

Generally not an integer, so



$\cos\beta = \frac{1}{\sqrt{N}} = \sin\alpha = \langle\psi_0|x_0\rangle$

use nearest integer, then $|\psi_0\rangle$ will be rotated within angle $\pm\alpha$
so most gives x_0 with prob $\sim 1 - O(\frac{1}{N})$ since α small,

$\sin\alpha \approx \frac{1}{\sqrt{N}}$ ↗ $\cos^2\alpha \approx 1 - \frac{1}{N}$

For large N, $\beta \approx \frac{\pi}{2}$, $\alpha \approx \frac{1}{\sqrt{N}}$ ($\sin\alpha \approx \alpha$ small α)

$$\#\text{ iterations} \approx \frac{\pi/2}{2(1/\sqrt{N})} = \frac{\pi}{4}\sqrt{N}$$

Example $N=4$ $(n=2)$

initial angle $\cos\beta = \frac{1}{\sqrt{4}} = \frac{1}{2}$ so $\beta = \pi/3$

$2\alpha = 2\arcsin\left(\frac{1}{2}\right) = 2\,\pi/6 = \pi/3$!

So 1 iteration of Q will map $|\psi_0\rangle$ exactly onto $|x_0\rangle$! i.e. can find 1 in 4 with certainty with only one query !

To prove claimed properties of Q

· Note first: for any U, $I_{|\psi\rangle} = I - 2|\psi\rangle\langle\psi|$

$$U I_{|\psi\rangle} U^\dagger = \underbrace{UIU^\dagger}_{I} - 2\,U|\psi\rangle\underbrace{\langle\psi|U^\dagger}_{(U|\psi\rangle)^\dagger}$$

$$= I_{U|\psi\rangle}$$

Now $H_n = H_n^\dagger$ & $|\psi_0\rangle = H_n|0\cdots0\rangle$

So $Q = -H_n I_0 H_n I_{|x_0\rangle} = -I_{|\psi_0\rangle} I_{|x_0\rangle}$

· Next note for any $|\psi\rangle, |\xi\rangle$

$I_{|\psi\rangle}|\xi\rangle = |\xi\rangle - 2|\psi\rangle\langle\psi|\xi\rangle$

modifies $|\xi\rangle$ by some mult of $|\psi\rangle$

So $Q|\xi\rangle = -I_{|\psi_0\rangle} I_{|x_0\rangle}|\xi\rangle$ modifies $|\xi\rangle$ first by a mult of $|x_0\rangle$, then by a mult of $|\psi_0\rangle$

So if $|\xi\rangle \in \mathcal{P}(x_0)$ then $Q|\xi\rangle \in \mathcal{P}(x_0)$ too

i.e. Q preserves $\mathcal{P}(x_0)$

Action of Q in $\mathcal{P}(x_0)$:

In 2 dim $\mathcal{P}(x_0)$

$I_{|x_0\rangle}$ is reflection in mirror line $\perp |x_0\rangle$

$I_{|\psi_0\rangle}$ " $\perp |\psi_0\rangle$

Facts about 2D Euclidean geome

① If R is reflection in mirror M along $|M\rangle$, then $-R$ is reflection in mirror $M^\perp$ along $|M^\perp\rangle$

⌜ any vector $\sim a|M\rangle + b|M^\perp\rangle$

R: $a \mapsto a$, $b \mapsto -b$ so $-R$: $a \mapsto -a$, $b \mapsto b$ $\equiv$ refl in $M^\perp$ ⌟

· f is 1-1 in each period

· f is efficiently computable in poly (# digits of k)

- $f(k) = a^k$ not by $a^k = \underbrace{a \times a \times \cdots \times a}_{k}$!

see sheet 3 Q2

· classically - hard to find r even though we have very simple formula

Legendre (~1800): knowing $r \rightsquigarrow$ can factor N

Suppose we can find r & suppose r is even

Then $(a^r - 1) \equiv (a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \mod N$

so N exactly divides the product,

not all into 1st (i.e. $a^{r/2} - 1$) as r was least

So if N does not all go into $(a^{r/2} + 1)$

then $\text{hcf}(N, a^{r/2} \pm 1)$ are non-trivial factors of N

↖ Euclid again

So need (1) r even & (2) $a^{r/2} \not\equiv -1 \mod N$

Theorem: if N is odd & not a prime power

and $a < N$ chosen unif at random,

then prob (① & ② hold) $\geq \frac{1}{2}$ (actually $\geq 1 - \frac{1}{2^{m-1}}$, $m = \#$ distinct prime divisors of N)

Proof - see 3 refs in notes

. So repeat K times $\rightarrow$ Prob(fail to get factor) $< \frac{1}{2^K}$

expon small in K

· If $N = c^l$, $c, l \geq 2$ then there's a poly-time classical algorithm that computes c.

How to find r? - use q. period finding algorithm

$f(k) = a^k \mod N$ periodic on $\mathbb{Z}$ - infinite domain !

Need to work on finite domain but don't know r.

- so f will not be exactly periodic on a truncated domain.

Will work on

$D = \{0, 1, \ldots, 2^m - 1\} = \mathbb{Z}_{2^m}$

for 2^m = least power of 2 $> N^2$ (!!)

then have $2^m = Br + b$, $0 \le b < r$

so have $B > N$ full periods (as $r < N$)

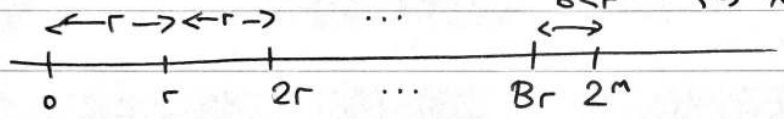
& 1 "corrupt" one of length b.

Now analyse effect of this "corruption" on the period finding algorithm:

Make $|f\rangle = \frac{1}{\sqrt{2^m}} \sum |x\rangle|f(x)\rangle$ & measure value

get $|per\rangle = \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |x_0 + kr\rangle$,

$A = B$ or $B+1$ depending on random x_0 vs b



Then (as before)

$$QFT_{2^m} |per\rangle = \sum_{c=0}^{2^m - 1} \tilde{f}(c)|c\rangle$$

Recall $$QFT_{2^m} |x_0 + kr\rangle = \frac{1}{\sqrt{2^m}} \sum_{\text{all } c \in \mathbb{Z}_{2^m}} e^{2\pi i (x_0 + kr)c/2^m} |c\rangle$$

so get $$\tilde{f}(c) = \frac{\omega^{cx_0}}{\sqrt{A}\sqrt{2^m}} \left[1 + \alpha + \cdots + \alpha^{A-1}\right] \quad \text{with} \quad \omega = e^{2\pi i/2^m}, \quad \alpha = e^{2\pi i c r/2^m}$$

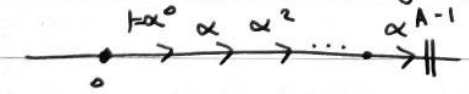
Now if measure: which c's will we get with "good probability"?

Intuition

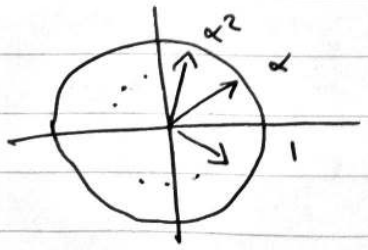
Previously for exact periodicity $\frac{2^m}{r} = A$ was integer

& all $\tilde{f}(c) = 0$ except c = mults of $(2^m/r)$

For them: $\alpha = 1$ & get constructive add^n of terms



For other c's, sum cancels exactly to 0, α = any A^{th} root of unity not 1 so $1 + \alpha + \alpha^2 + \cdots + \alpha^{A-1} = 0$



← get perfect cancellation

For inexact case:

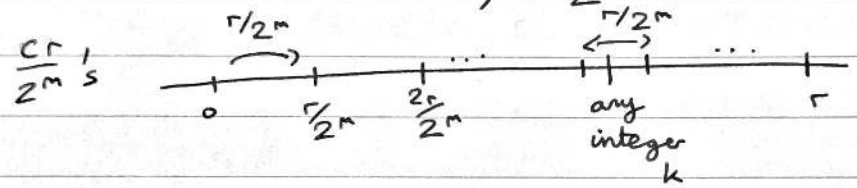
Expect constructive addition in geom series for those c's such that phase (α) small (α's nearest the real axis)

As $c: 0 \to 2^m - 1$ have $\frac{cr}{2^m}: 0 \to \approx r$ & want those c's having $\alpha = e^{2\pi i c r/2^m}$

$\frac{cr}{2^m}$ nearest to integers $k = 0, 1, \ldots, (r-1)$ (*)

& powers $1, \alpha, \ldots, \alpha^{A-1}$ don't spread too far around circle, so avoid cancellation

As c increases $0 \to 2^m - 1$, $\frac{cr}{2^m}$ increments by $\frac{r}{2^m}$'s (small $\frac{cr}{2^m}$'s)



So amongst all 2^m c's, have special c_k's (only r of them) with $c_k r/2^m$ nearest to integers $k = 0, 1, \ldots, r-1$:

i.e. $\left| \frac{c_k r}{2^m} - k \right| \leq \frac{1}{2} \frac{r}{2^m}$ (†)

i.e. $\left| c_k - k\frac{2^m}{r} \right| \leq \frac{1}{2}$

For these c_k's, $\frac{c_k r}{2^m} = k + \xi$, $|\xi| \leq \frac{1}{2}\frac{r}{2^m}$

so $\alpha^A = e^{2\pi i c_k r A/2^m} = e^{2\pi i (k+\xi) A} = e^{2\pi i \xi A}$, with $\xi A \sim \frac{r}{2^m} \cdot \frac{2^m}{r} \sim \frac{1}{2}$

Recall $A \sim 2^m/r$ & $|\xi| < \frac{1}{2}\frac{r}{2^m}$ so $\alpha^A \sim e^{\pm i\pi}$

i.e. $1, \alpha, \alpha^2, \ldots, \alpha^{A-1}$ all in UHP or all in LHP, so sum $1 + \alpha + \cdots + \alpha^{A-1}$ cannot cancel (in imaginary parts)

Doing the algebra (cf notes) get

Theorem Suppose $QFT(|a_r\rangle)$ is measured.

Then for any c_k as above, satisfying (+),

$$\text{Prob}(c_k) > \frac{\gamma}{r}, \quad k = 0, 1, \ldots, r-1 \quad \& \quad \gamma = \frac{4}{\pi^2} \simeq 0.4$$

* so mmt will give some c_k with const prob > 0.4 //

algebra here:

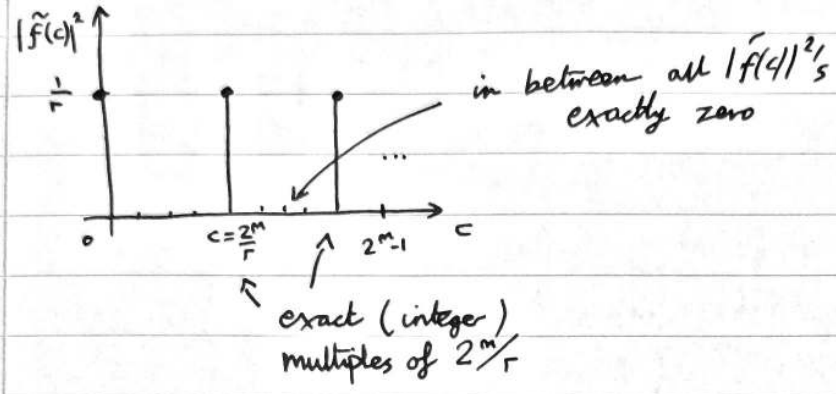
geom series $|\tilde{f}(c)|^2 = \frac{1}{A 2^m} \left| \frac{1 - \alpha^A}{1 - \alpha} \right|^2$, $A \approx 2^m/r$

$A > 2^m/r - 1$

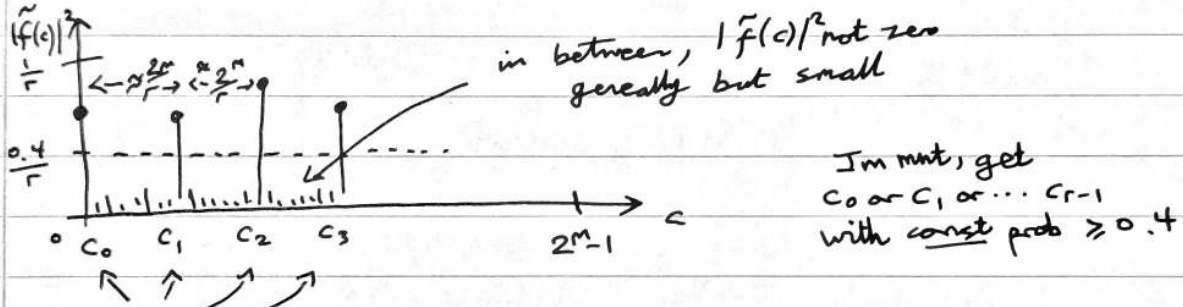
$\alpha = e^{i\theta_c}$, $|\theta_c| < \pi r/2^m$ (small)

$\Rightarrow |\tilde{f}(c)|^2 > \frac{\gamma}{r}$

exact periodicity $2^m/r$ = exact integer



inexact periodicity $2^m/r$ not exact integer



Im mnt, get c_0 or c_1 or $\cdots$ c_{r-1} with const prob ≥ 0.4

$$\left| c_k \frac{r}{2^m} - k \right| < \frac{1}{2}\frac{r}{2^m} \quad \text{(phase nearest Re-axis)}$$

$$\text{i.e. } \left| c_k - \frac{k2^m}{r} \right| < \frac{1}{2}$$

How to get r from c_k?

Have $\left| \frac{c_k}{2^m} - \frac{k}{r} \right| < \frac{1}{2^{m+1}} < \frac{1}{2N^2}$ (*) (& $r<N$)

$\frac{c_k}{2^m}$: know, know; $\frac{k}{r}$: want!, not known

Claim there it as most one fraction $\frac{k'}{r'}$ with denom $<N$ that satisfies (*). So (*) does uniquely determine k/r.

Proof $\left| \frac{k'}{r'} - \frac{k''}{r''} \right| = \frac{|k'r'' - r'k''|}{r'r''} \geq \frac{1}{r'r''} > \frac{1}{N^2}$

(k', r' different from k'', r'')

Hence cannot both be within $\frac{1}{2N^2}$ of any number. //

* This is why we chose $2^m > N^2$!

Introduce: "good" c_k value $\equiv$ k coprime to r

so prob(good c_k) $= O\left(\frac{0.4}{\log\log r}\right) > O\left(\frac{1}{\log\log N}\right)$

and by above it will determine r itself

How to get r from good c-value

Could (?!) try all fractions k'/r' with $k' < r' < N$

& find closest to $c/2^m$.

But: $O(N^2)$ fractions to try & want poly $(\log N)$ time computation

Theory of continued fractions (CFs)

any rational s/t $(s<t)$ has CF expression

$$\frac{s}{t} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 \ddots + \frac{1}{a_L}}}}$$

← if $s > t$, then $a_0 + a_1 + \dots$

$a_1, a_2, \dots, a_L$ all positive integers, finite list

since $(s<t)$ $\frac{s}{t} = \frac{1}{\frac{t}{s}} = \frac{1}{a_1 + \frac{s_1}{t_1}}$, $t_1 = s$, $s_1 < t_1$

$= \frac{1}{a_1 + \frac{1}{\frac{t_1}{s_1}}} = \dots$

each bottom line = prev top line $<$ prev bottom line

So seq of denominators are strictly decreasing seq of integers, so must terminate.

Notation: $\cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \frac{1}{a_L}}} = [a_1, a_2, \dots, a_L] = \frac{s}{t}$

* k^{th} convergent of $\frac{s}{t}$ is $\frac{p_k}{q_k} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \frac{1}{a_k}}} = [a_1, \dots, a_k]$

So $\frac{p_1}{q_1} = [a_1] = \frac{1}{a_1}$, $\frac{p_2}{q_2} = [a_1, a_2] = \frac{1}{a_1 + \frac{1}{a_2}} = \frac{a_2}{a_1 a_2 + 1}$ etc

$\frac{p_L}{q_L} = \frac{s}{t}$

Example $\frac{29}{51} = [1,1,3,7]$ cgts are
$[1]=1$, $[1,1]=\frac{1}{2}$, $[1,1,3]=\frac{4}{7}$,
$[1,1,3,7]=\frac{29}{51}$

* we will want to compute all convergents of
$\frac{s}{t} = \frac{c}{2^m}$

Lemma (recurrence relation)
For $a_1,\dots,a_l$ any +ve real numbers
set $p_0=0$, $q_0=1$, $p_1=1$, $q_1=a_1$ ||
(a) then $[a_1,\dots,a_k] = p_k/q_k$ where
$p_k = a_k p_{k-1} + p_{k-2}$, $q_k = a_k q_{k-1} + q_{k-2}$, $k \geq 2$
(b) $q_k p_{k-1} - p_k q_{k-1} = (-1)^k$, $k \geq 1$
(c) $hcf(p_k, q_k) = 1$, $k \geq 1$ ← if a_i are integers?

Proof (sketch) (a) induction $[a_1, a_2, \dots, a_{k+1}] = [a_1, \dots, a_k + \frac{1}{a_{k+1}}]$
($a_1,\dots,a_{k+1}$: $k+1$; $a_1,\dots,a_k+\frac{1}{a_{k+1}}$: k)

(b) induction, (c) easy from (b)

Theorem If $s<t$ are m-bit integers (coprime) then
$CF(\frac{s}{t}) = [a_1,\dots,a_l]$ has length $l = O(m)$
and all convergents $\frac{p_k}{q_k} = [a_1,\dots,a_k]$, $k=1,\dots,l$
can be computed in $O(m^3)$ time.

Proof a_k's ≥ 1, p_k, q_k's ≥ 1
Have recurrence relation
$p_k = a_k p_{k-1} + p_{k-2}$, $q_k = a_k q_{k-1} + q_{k-2}$
so $p_k > p_{k-1} > p_{k-2}$ increasing so by · again $p_k \geq 2p_{k-2}$
So p_k's grow exponentially with # steps
($\gtrsim$ double every 2 steps)
So $O(m)$ of these will get to m-bit s.
Similarly for q_k's.
& addition/mult of m-bit integers $\sim O(m^2)$ time. =
Hence can compute all convergents in time $O(m)O(m^2) = O(m^3)$. ✓

Main CF theorem

For any (rational) $0 < x < 1$,
if $|x - \frac{p}{q}| < \frac{1}{2q^2}$
then $\frac{p}{q}$ is a convergent of $CF(x)$.

Proof (optional) – see notes

Remark CFs also work for irrational x too e.g. $x \in (0,1)$

$$x = \frac{1}{\frac{1}{x}} = \frac{1}{a_1 + x_1} = \frac{1}{a_1 + \frac{1}{\frac{1}{x_1}}} \to \cdots = \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots}}}$$

a_1, a_2 integers as before but now need not terminate

e.g. golden ratio $\gamma = \frac{\sqrt{5}+1}{2}$, $\gamma^2 - \gamma - 1 = 0$ so $x = 1 + \frac{1}{x}$

so $\gamma = [1; 1, 1, 1, \ldots]$ $= 1 + \frac{1}{1 + \frac{1}{x}}$

convergents are quotients of successive Fibonacci

$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \ldots$ $= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \cdots}}}$

$$(\sqrt{2}-1) \cdot \frac{\sqrt{2}+1}{\sqrt{2}+1} = \frac{1}{\sqrt{2}+1} = \frac{1}{2 + (\sqrt{2}-1)} = [2, 2, \ldots]$$

so $\sqrt{2} = [1; 2, 2, \ldots]$

Periodic CF: initial finite block, then repeating finite block

Thm (Lagrange) x has periodic CF iff x is irrational sol^n of a quadratic with integer coeffs

Can show (Euler)

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]$$

Also (Euler)

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{2}{3 + \cfrac{3}{4 + \cfrac{4}{5 + \ddots}}}}}$$

Back to getting r from good c value (k & r coprime)
& satisfying $\left|\frac{c}{2^m} - \frac{k}{r}\right| < \frac{1}{2N^2} < \frac{1}{2r^2}$ as $r < N$

so by CF $\frac{k}{r}$ must be a cgt of $CF(c/2^m)$
(*) i.e. out of all $O(N^2)$ $\frac{k}{r}$'s with denom $< N$
we need to consider only l = length $(CF(c/2^m)) = O(m) = O(\log N)$ of them

Can compute all convergents in $O(m^3)$ time $= O((\log N)^2)$ time
& check which (unique) one of these is within $1/2N^2$ of $c/2^m$ to give k/r.
This achieves factoring in $O((\log N)^3)$
! slowest part of algorithm is classical post-processing of period-finding algorithm output.

Example Factor $N = 39$. Have chosen $a = 7 < 39$ coprime
r = period of $f(x) = 7^x \bmod 39$
will compute f for $x: 0 \rightsquigarrow$ "$2^m > N^2$"
$N^2 = 1521 > 1024$ but $N^2 < 2048 = 2^{11}$
so $m = 11$, use 11 qubits in x register
· Suppose mmt of QFT_{2^m} (per) yields $c = 853 \in \mathbb{Z}_{2^m}$
so by theory c has cont's prob ≈ 0.4 to satisfy

$$\left|\frac{853}{2^m} - \frac{k}{r}\right| < \frac{1}{2^{m+1}} = \frac{1}{2^{12}} < \frac{1}{2N^2}$$

and with 'good' prob $> O\left(\frac{1}{\log\log N}\right)$, k coprime to r

* here $c = 853$ chosen to have these properties, with k, r coprime
Now $\left|\frac{853}{2048} - \frac{k}{r}\right| < \frac{1}{2^{12}}$ for unique $\frac{k}{r}$ with $r < N$
To find $\frac{k}{r}$, calculate $CF\left(\frac{853}{2048}\right)$ & convergents.

$$\frac{853}{2048} = \frac{1}{\frac{2048}{853}} \quad \Big\} \; 2 + \frac{342}{853}$$

$$= 2 + \frac{1}{\frac{853}{342}} \quad \Big\} \; 2 + \frac{169}{342}$$

$$= 2 + \frac{1}{\frac{342}{169}} \quad \Big\} \; 2 + \frac{4}{169}$$

$$= 2 + \frac{1}{\frac{169}{4}} \quad \Big\} \; 42 + \frac{1}{4}$$

$$= 42 + \frac{\frac{1}{4}}{1} \; \checkmark$$

so $CF = [2,2,2,42,4]$

Convergents are

$[2] = \frac{1}{2}$, $[2,2] = \frac{2}{5}$, $[2,2,2] = \frac{5}{12}$,

$[2,2,2,42] = \frac{212}{509}$, $[2,2,2,42,4] = \frac{853}{2048}$

Check: only $\frac{5}{12}$ is within $\frac{1}{2^{12}}$ of $\frac{853}{2048}$

$$\left| \frac{5}{12} - \frac{853}{2048} \right| = 0.000163\ldots < \frac{1}{2^{12}} = 0.000244\ldots$$

So $\frac{5}{12}, \frac{10}{24}, \frac{15}{36}$ are possible $\frac{k}{r}$'s with $r < 39$.

but k, r coprime $\Rightarrow r = 12$

Indeed check $7^{12} \equiv 1 \mod 39$ ✓

Then $39 \mid (7^6+1)(7^6-1)$

& hope / expect it goes into both partially

Compute $7^6+1 = 117650 = 26 \mod 39$

$7^6-1 = 117648 = 24 \mod 39$

Euclid: $\text{hcf}(26,39) = 13$

$\text{hcf}(24,39) = 3$

giving factors 13 & 3 of 39.

Shor's algorithm: technique generalises to other problems –

① discrete logs (ExSh 4)

② hidden subgroup problem

group G, size $|G|$

· given oracle for $f: G \to$ some Y

· promise: there is a subgp $H < G$ s.t. f is constant & distinct on cosets of H in G

· problem: "find" H

& do it all in poly $\log |G|$ time

Example $f: \mathbb{Z}_N \to \mathbb{Z}$ period r

$G = (\mathbb{Z}_N, +)$, $H = \{0, r, \ldots, (A-1)r\}$