IPQI, IOP, Bhubaneswar

Quantum Computing

R. Srikanth
Poornaprajna Institute of Scietific Research,
Bangalore, India
Raman Research Institute, Bangalore, India

Plan of talk

1. Introduction: Elementary algorithms.

2. Shor's algorithm: period finding and factoring

3. Grover's search algorithm

4. Quantum error correction

5. Adiabatic QC

6. One-way or measurement-based QC

7. Physical implementation of quantum computers

Some simple algorithms

Hadamard transformation:

$$H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \; : \; \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Superposition:

$$H^{\otimes n}|x_1 \cdots x_n\rangle_n =$$
$$\frac{1}{2^{n/2}} \sum_{z=0\cdots 0}^{1\cdots 1} (-1)^{z_1 x_1 \oplus \cdots \oplus z_n x_n} |z_1 \cdots z_n\rangle_n$$
$$\equiv \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle_n \qquad (1)$$

In particular, a useful initial state:

$$H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}} \sum_j |j\rangle_n$$

Reversibility and unitarity:

$$U(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$$

Linearity, parallelism and entanglement:

$$U\left(\frac{1}{2^{n/2}}\sum_j |j\rangle_n \otimes |0\rangle\right) = \frac{1}{2^{n/2}}\sum_j |j\rangle_n |f(j)\rangle.$$

Deutsch-Josza problem

Given a function $f : \{0,1\}^n \mapsto \{0,1\}$, promised to be either balanced or constant, and an **oracle** that computes $f(x)$ in one time-step, to determine whether it is balanced or constant.

Classically, in the worst case, one needs $2^n/2 - 1$ queries. Quantumly, a single query suffices.

$$\begin{aligned} |\Psi\rangle &= \frac{1}{2^{n/2}} \sum_j |j\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &\xrightarrow{U} \frac{1}{2^{n/2}} \sum_j (-1)^{(f(j))} |j\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \equiv |\Psi'\rangle \end{aligned}$$

$$(H^{\otimes n} \otimes \hat{I})|\Psi'\rangle = \frac{1}{2^n}(-1)^{j\cdot k + f(j)}|k\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

Consider the coefficient of $|0\rangle$ in first register:
$f(j)$ balanced: equal # 0's and 1's exponent of (-1) $\Rightarrow$ 0
$f(j)$ constant: exponent of (-1) constant $\Rightarrow$ 1

Bernstein-Vazirani problem

Given an oracle O_a that evaluates $a \cdot x$ in one query for any x, to determine the n binary digits of a.

Classically, n queries of $a \cdot 2^m$ $(0 \leq m \leq n-1)$ are needed. (Nota: 2^m is an n-bit string with all 0's except at digit m).

Quantumly, a single query suffices, using the B-V algorithm. Omitting the D-J-like oracle:

$$U_{O_a}\left\{\frac{1}{2^{n/2}}\sum_j |j\rangle\right\} = \frac{1}{2^{n/2}}\sum_j (-1)^{a\cdot j}|j\rangle$$
$$\stackrel{H^{\otimes n}}{\rightarrow} \frac{1}{2^n}\sum_j\sum_k (-1)^{(a+k)\cdot j}|k\rangle.$$

Here $a+k$ is the bitwise sum, which vanishes iff $k=a$.

If $k \neq a$, then $x \equiv a + k$ is a non-zero string. Thus, $x \cdot j$ will evaluate to equal 0's and 1's in the exponent ($x \cdot j$ is the parity of the substring of j defined by x). Summing over j, we see that total amplitude $= 0$.

If $k = a$, then $x = 0$, and the amplitude of $|a\rangle$ sums to 1.

Simon's algorithm

To determine vector $\xi \in \mathbf{F}_2^n$ (group of binary n-vectors), given that $f(x) = f(y)$ iff $y = x \oplus \xi$.

Mathematically, to find the subgroup $K \equiv \{0, \xi\} \subset \mathbf{F}_2^n$ such that $f(\cdot)$ is constant on cosets of K and takes different values on different cosets.

Classically: one evaluates $f(x_1)$, $f(x_2)$, $f(x_3)$ sequentially, ruling out $\leq {}^mC_2$ possible values of a. Unlikely to hit on actual a unless ${}^mC_2$ is of the order of $2^{n/2}$.

Quantumly $O(n)$ queries suffices.

Algorithm:

$$\frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} |j\rangle|f(j)\rangle \overset{\text{Measure}}{\rightarrow} \frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus \xi\rangle).$$

$$
\begin{aligned}
& H^{\otimes n} \frac{1}{\sqrt{2}} (|x_0\rangle + |x_0 \oplus \xi\rangle) \\
& \quad = \frac{1}{2^{(n+1)/2}} \sum_y \left((-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus \xi) \cdot y} \right) |y\rangle \\
& \quad = \frac{1}{2^{(n+1)/2}} \sum_y (-1)^{x_0 \cdot y} \left(1 + (-1)^{\xi \cdot y} \right) |y\rangle \\
& \quad = \frac{1}{2^{(n-1)/2}} \sum_{\xi \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle \qquad (2)
\end{aligned}
$$

With each measurement, we obtain a random y that satisfies $\sum_j y_j \xi_j = 0$. With high probability, each measurement, possible a's is halved. We require only $O(n)$ queries to reconstruct a.

Shor's algorithm

The clue from Simon's algorithm:

(magic 1) use measurement to collapse state into a periodic superposition;

(magic 2) 'Fourier transform' this superposition into a state that yields periodicity with high probability.

A bit of number theory:

$$\frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} |j\rangle|f(j)\rangle \text{ measure 2nd register} \longrightarrow$$

$$|\psi_n\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle$$

where x_0 is smallest value x s.t $f(x_0) = f_0$ and $m = \lceil (2^n - x_0)/r \rceil$.

Quantum Fourier Transform: transforms amplitudes to their DFT value in $O(n^2)$ steps.

$$U_{\mathsf{FT}}|k\rangle = \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} e^{2\pi ijk/2^n}|j\rangle$$

where multiplication in exponent is ordinary. Applied to an arbitrary state:

$$U_{\mathsf{FT}} \left(\sum_k \gamma_k |k\rangle \right) = \sum_{k=0}^{2^n-1} \widehat{\gamma}_k |k\rangle,$$

where

$$\widehat{\gamma}_k = \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} e^{2\pi ijk/2^n} \gamma_j.$$

Classically DFT requires $O(n2^n)$ steps and is thus computationally expensive.

$$U_{\mathsf{FT}}\left(\frac{1}{\sqrt{m}}\sum_{k=0}^{m-1}|x_0+kr\rangle\right)$$
$$=\sum_{j=0}^{2^n-1}e^{2\pi i x_0 j/2^n}\frac{1}{\sqrt{m2^n}}\left(\sum_{k=0}^{m-1}e^{2\pi i k r j/2^n}|j\rangle\right)$$

Thus measurement on second register yields some j with probability

$$p(j)=\frac{1}{m2^n}\left|\sum_{k=0}^{m-1}e^{2\pi i k r j/2^n}\right|^2$$

Guided by the idea that QFT implements DFT on amplitudes, we expect that the r-periodic superposition above will lead to concentration of amplitude near multiples of $2^n/r$ consequent to QFT. This is confirmed as follows.

Consider an integer j within distance of 1 from a multiple of $2^n/r$:

$$j=h\frac{2^n}{r}+\delta,$$

for some integer h and where $|\delta| \leq \frac{1}{2}$. Evaluating the geometric series in the expression for $p(j)$, we simply find:

$$p(j) = \frac{1}{m2^n} \frac{\sin^2(\pi\delta mr/2^n)}{\sin^2(\pi\delta r/2^n)}.$$

Since m lies within a distance of 1 from $2^n/r$ and $2^n/r \gg 1$, we can set $mr/2^n := 1$ in the numerator and set the sine in the denominator equal to its argument. Then

$$\begin{aligned} p(j) &= \frac{1}{r} \frac{\sin^2(\pi\delta)}{(\pi\delta)^2} \\ &\geq \frac{1}{r} \frac{4}{\pi^2}, \end{aligned} \tag{3}$$

noting that $\sin(x) \geq x/(\pi/2)$ for $0 \leq x < \pi/2$. Since there are at least $r - 1$ such values of j (lying within distance $\frac{1}{2}$ of a intger multiple of $2^n/r$), and since $r \gg 1$, probability of obtaining such a y is $> 4/\pi^2 \approx 40\%$.

We had assumed $2^n \gg r$ (register large enough to hold several periods of b^j). We require the stronger condition that $2^n > N^2$ (enough to hold N full periods) for the following reason.

Suppose our measurement above yielded integer y that is within distance $\frac{1}{2}$ of $j2^n/r$ for some j:

$$\left|\frac{y}{2^n} - \frac{j}{r}\right| \leq \frac{1}{2^{n+1}}.$$

Since we chose $2^n > N^2$, we thus have an estimate of fraction j/r to greater accuracy than $1/2N^2$.

Since $r < N$, and any two fractions (j/r and say j'/r) with denominator less than N will differ by at least $1/N^2$ (for $\left|\frac{a}{b} - \frac{c}{d}\right| \geq \frac{1}{bd}$), our error bar of $1/2N^2$ is small enough to pin down the unique rational number j/r.

This is the reason for choosing $2^n > N^2$ rather than simply $2^n > N$, even though the latter

would have sufficed to represent several periods of b^j. The latter would have sufficed if we somehow knew that $r|2^n$. For then $y = j2^n/r$ is exact, and $y/2^n$ fully determines j/r.

When $r \not| 2^n$ (the overwhelmingly common case), we can use the method of continued fractions to efficiently determine the ratio j/r (not j and r individually).

Theorem. If x is an estimate for j/r such that

$$\left| x - \frac{j}{r} \right| \leq \frac{1}{2r^2},$$

then j/r will appear in one of the partial sums in the continued fraction expansion of x (Hardy and Wright 1965).

Grover algorithm

Unstructured search: in a telephone book, find a name, given number. Classically, given database of size N, we require $O(N)$ queries/steps. Quantumly, $O(\sqrt{N/M})$ queries/steps will suffice.

There is an oracle that works as in the D-J algorithm:

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

where O_G denotes the Grover oracle. Since the two registers do not entangle, we can ignore to mention the second one henceforth.

Step 0. Create a uniform superposition over $N \equiv 2^n$ states:

$$|\eta\rangle = \frac{1}{\sqrt{N}} \sum_{j=1}^{N} |j\rangle.$$

Step 1. Apply the oracle O_G.

Step 2. Apply $H^{\otimes n}$.

Step 3. Apply the conditional phase shift on all $|x\rangle$ except $x = 0$: $|x\rangle \rightarrow -(-1)^{\delta_{\alpha 0}}|x\rangle$:

$$2|0\rangle\langle 0| - I.$$

Step 4. Repeat step 2.

Step 5. After $O(\sqrt{N/M})$ steps, measure in the computational basis to find one of M solutions with high probability.

Steps 1, 2, 3 and 4 can be combined into a single operation which we may call the "Grover operator". Now, steps 2, 3 and 4 may be combined to yield

$$\left(H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}\right) O_G = (2|\eta\rangle\langle\eta| - I)\,.$$

which 'reflects amplitudes about the mean':

$$\sum_k \alpha_k |k\rangle \longrightarrow \sum \left[-\alpha_k + 2\langle\alpha\rangle\right] |k\rangle.$$

How does the algorithm work? A simple geometric picture:

Uniform superposition over solution set S:
$|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_{x\in S} |x\rangle$

Uniform superposition of non-solutions:
$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_{x\notin S} |x\rangle$.

Then:

$$\begin{aligned} |\eta\rangle &= \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle \\ &\equiv \cos(\theta/2)|\alpha\rangle + \sin(\theta/2)|\beta\rangle. \end{aligned} \quad (4)$$

In the $\{|\alpha\rangle, |\beta\rangle\}$ basis, the oracle is a reflection about vector $|\alpha\rangle$:

$$O_G \equiv |\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta| \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The operator for reflection about $|\eta\rangle$ is given by:

$$R_\eta \equiv |\eta\rangle\langle\eta| - |\eta^\perp\rangle\langle\eta^\perp| = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

The Grover operator is then defined as $G \equiv R_\eta O_G$. We have:

$$G|\eta\rangle = \cos\left(\frac{3\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{3\theta}{2}\right)|\beta\rangle.$$

Similarly:

$$G^k|\eta\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle.$$

Thus, G rotates $|\psi\rangle$ towards $|\beta\rangle$ in 2D. Since

$$\sin\theta = 2\sin(\theta/2)\cos(\theta/2) = 2\frac{\sqrt{M(N-M)}}{N},$$

we see that θ **decreases** as $M > N/2$ – a bit unintuitive. So we assume now that $M \leq N/2$ and thus $\theta \leq \pi/2$. How to handle $M > N/2$ is discussed later.

Assuming $M \ll N$ and $\theta \approx 2\sin(\theta/2) = 2\sqrt{M/N}$, the required # of iterations of G:

$$R \approx \frac{\pi/2}{\theta} = \frac{\pi}{4}\sqrt{\frac{N}{M}} \in O\left(\sqrt{\frac{N}{M}}\right).$$

We had assumed $M \leq N/2$. If this were not so:

(1) A classical computer would suffice to find a solution!

(2) Double the search data base, by adding a single qubit, such that none of N added items are solutions. In the augmented oracle, item y is marked a solution iff $y = 0x$ where x is marked by the original oracle.

II. Quantum error correction

IPQI, IOP, Bhubaneswar

Error correction is the technique of adding redundancy to our information to protect it against corruption due to unexpected and unavoidable environmental disturbances.

Classical example: a **binary symmetric channel** with error probability p per bit. Consider the code:

$$0 \longrightarrow \overline{0} \equiv 000; \qquad 1 \longrightarrow \overline{1} \equiv 111.$$

Error checking and correction effected through majority rule.

Prob(failure) = Prob(two or more flips) = $p^3 + {}^3C_2 p^2(1-p)$. Therefore, our encoding is an improvement provided $p^3 + {}^3\,C_2 p^2(1-p) < p$, or $p < 1/2$.

Hamming bound: $2^n \geq \underbrace{2^r}_{\text{message dim.}} \times \underbrace{(n+1)}_{\#\text{ possible errors}}$

Putting code rate $r = 1$, we find $n_{\text{min}} = 3$, as in the above repetition code.

Quantum error correction is different from the classical case because:

• Quantum states are more delicate.

• Measuring a quantum state (to detect error) can itself damage the state. (Seems insurmountable!)

• Not only bit flip, but also phase errors can occur.

• Even a quantum state in a finite dimensional space can suffer a continuum of errors, and thus defines digitization/discretization. (Seems insurmountable!)

Historically, on account of (2) and (4), it was thought that QEC would not be possible. Happily, this turned out to be wrong, as first shown by Shor (1995) and Steane (1995).

Let us take a closer look at quantum errors.

Decoherence

Environment-qubit interaction:

$$\begin{aligned} |e\rangle|0\rangle &\rightarrow |e_0\rangle|0\rangle + |e_1\rangle|1\rangle \\ |e\rangle|1\rangle &\rightarrow |e_2\rangle|0\rangle + |e_3\rangle|1\rangle \end{aligned} \tag{5}$$

The $|e_j\rangle$'s are not assumed to be normalized or orthogonal. This corruption of quantum states by the environment is QC's formidable adversary!

Letting $x = 0, 1$, the above two can be combined:

$$\begin{aligned} |e\rangle|x\rangle &\rightarrow ([|e_0\rangle\hat{I} + |e_1\rangle\hat{X}]\hat{P}_0)|x\rangle \\ &+ ([|e_2\rangle\hat{X} + |e_3\rangle\hat{I}]\hat{P}_1)|x\rangle \end{aligned} \tag{6}$$

where $\hat{P}_x \equiv (1 + (-1)^x\hat{Z})/2$. Noting that $\hat{Y} = \hat{Z}\hat{X}$, RHS above is rwritten as:

$$\begin{aligned} &\left(\frac{|e_0\rangle + |e_3\rangle}{2}\hat{I} + \frac{|e_0\rangle - |e_3\rangle}{2}\hat{Z} + \right. \\ &\left.\frac{|e_2\rangle + |e_1\rangle}{2}\hat{X} + \frac{|e_2\rangle - |e_1\rangle}{2}\hat{Y}\right)|x\rangle \\ &\equiv (|d\rangle\hat{I} + |a\rangle\hat{X} + |b\rangle\hat{Y} + |c\rangle\hat{Z})|x\rangle \end{aligned}$$

Thus the general error due to environment can be viewed as a superposition of no-error, bit flip, phase flip and both flips.

More generally, one can have all three errors on all n qubits of a state:

$$|e\rangle|\Psi\rangle \rightarrow \sum_{\mu_1=0}^{3} \cdots \sum_{\mu_n=0}^{3} |e_{\mu_1} \cdots e_{\mu_n}\rangle \hat{X}^{(\mu_1)} \ldots \hat{X}^{(\mu_n)} |\Psi\rangle$$

where $\hat{X}^{(0,1,2,3)} \equiv \hat{I}, \hat{X}, \hat{Y}, \hat{Z}$.

A more restricted form of error results if we assume that the environment affects the system for a short time before error checking: at most one error on the n qubits:

$$|e\rangle|\Psi\rangle \rightarrow \left(|d\rangle\hat{I} + \sum_{j=0}^{n} \left[|a_j\rangle\hat{X}_j + |b_j\rangle\hat{Y}_j + |c_j\rangle\hat{Z}_j \right] \right) |\Psi\rangle.$$

A quantum codeword $|\Psi\rangle$ is designed to ensure that each of the $1 + 3n$ error actions will take $|\Psi\rangle$ to an orthogonal subspace.

A suitable measurement ('syndrome measurement') can then collapse $|\Psi\rangle$ into one of these subspaces, where they can be identified and corrected. **Therefore it is enough to be able to correct for these discrete set of errors!**

Syndrome measurement will only reveal the error $\hat{X}_j^{(\mu)}$ that has modified the state, but nothing about the state itself. Otherwise, syndrome measurment would alter the encoded state.

The outcome of syndrome measurement (say that a bit flip has occured in qubit 5) is corrected by applying $\hat{X}_5$. This process can be automated via suitable control-gates acting from the ancillary/work qubits used to record the syndromes.

Exercise. *In general, a unitary action based on some measurement outcome can be automated in this way to eliminate measurement. Design an automated teleportation circuit.*

Another way to view our result on discretizing errors: From the general theory of quantum noise, it is known that action of noise is an arbitrary trace-preserving map

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_j E_j|\psi\rangle\langle\psi|E_j^\dagger,$$

where E_j's are the Kraus operators, which are **positive** operators that satisfy completeness: $E_j^\dagger E_j = I$. This state can be thought of as a statistical mixture of (unnormalized) states $E_j|\psi\rangle$.

Because the Pauli operators form an operator basis for 2×2 matrices, any Kraus operator can be expressed as a superposition of Pauli operators:

$$E_j = e_{j0}\hat{I} + e_{j1}\hat{X} + e_{j2}\hat{Y} + e_{j3}\hat{Z}$$

A general error, continuum error can thus be decomposed into a discrete set, provided the allowed discrete set of errors (one or more Pauli operations) drive (superposition of) code-words into orthogonal subspaces.

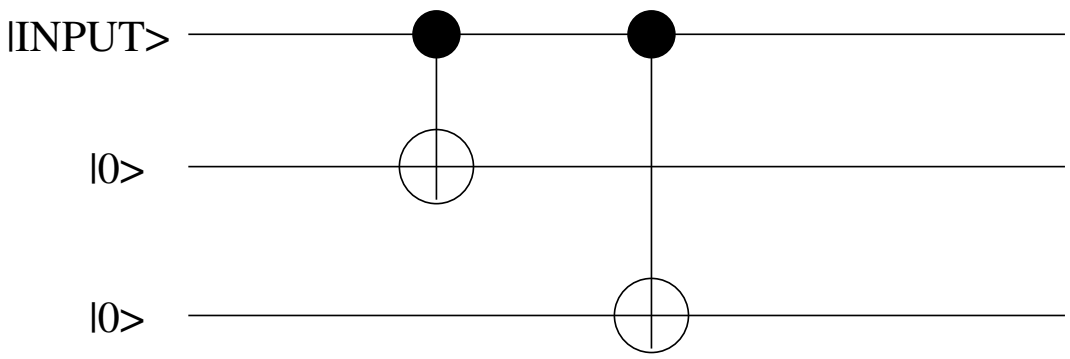
Code protecting against 1-qubit bit flip error

Suppose we have a (classical-like) bit flip channel:

$$|0\rangle \rightarrow |\overline{0}\rangle \equiv |000\rangle; \quad |1\rangle \rightarrow |\overline{1}\rangle \equiv |111\rangle$$

Thus

$$\begin{aligned} \alpha|0\rangle + \beta|1\rangle &\rightarrow |\Psi\rangle \equiv \alpha|\overline{0}\rangle + \beta|\overline{1}\rangle \\ &\equiv \alpha|000\rangle + \beta|111\rangle. \end{aligned}$$



Circuit for encoding a 3-qubit code that protects against a single qubit bitflip error.

Assuming single qubit errors, the post-error state could be one of:

$$\begin{aligned} |\Psi_0\rangle &= \hat{X}_0|\Psi\rangle = \alpha|001\rangle + \beta|110\rangle \\ |\Psi_1\rangle &= \hat{X}_1|\Psi\rangle = \alpha|010\rangle + \beta|101\rangle \\ |\Psi_2\rangle &= \hat{X}_2|\Psi\rangle = \alpha|100\rangle + \beta|011\rangle. \end{aligned} \quad (7)$$

Exercise. *Describe the noise process that characterizes the bit flip channel (in terms of Kraus operators).*

Main observation: $|\Psi\rangle, |\Psi_j\rangle$ $(j = 0, 1, 2)$ all lie in mutually orthogonal subspaces. Thus, in principle, they can be distinguished by measurement.

Eg., the following scheme of **incomplete** and **commuting** measurement does the job:

$$\begin{aligned} \hat{P}_0 &\equiv |000\rangle\langle 000| + |111\rangle\langle 111| \\ \hat{P}_1 &\equiv |100\rangle\langle 100| + |011\rangle\langle 011| \\ \hat{P}_2 &\equiv |010\rangle\langle 010| + |101\rangle\langle 101| \\ \hat{P}_3 &\equiv |001\rangle\langle 001| + |110\rangle\langle 110| \end{aligned}$$

The state $\alpha|010\rangle + \beta|101\rangle$ makes $\langle \hat{P}_2 \rangle = 1$ but 0 for the other $\hat{P}_j$'s. This reveals a bitflip error in the second qubit, without revealing anything about α, β.

Error recovery is then implemented by applying $\hat{X}_2$.

Exercise. *Adding redundant qubits makes more systems available that can be affected by error. What is the largest error rate for which the above code improves performance?*

But the above measurements require 3-qubit operations. The following, alternative, 2-qubit syndrome measurements equally well do the job.

An incomplete measurement of relative parity of qubits 1, 2:

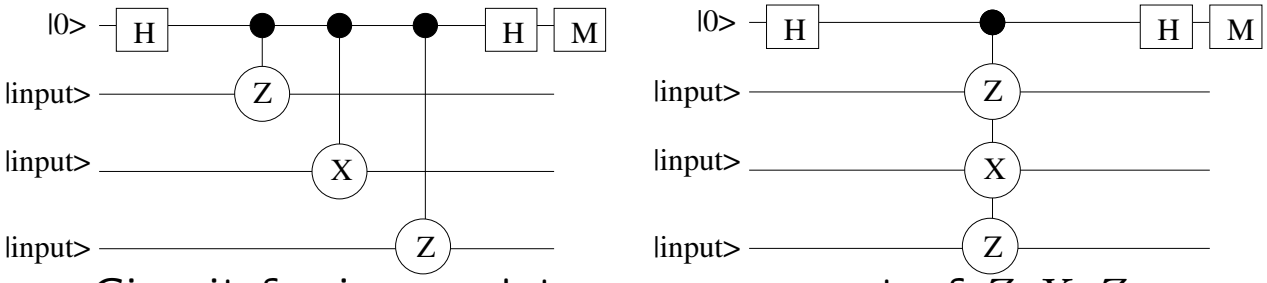
$$(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes \hat{I} - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes \hat{I} = Z_1 Z_2.$$

and an incomplete measurement of relative parity of qubits 2, 3:

$$\hat{I} \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|) - \hat{I} \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|) = Z_2 Z_3$$

Note that $Z_1 Z_2$ is an incomplete measurement with 2 (not 4!) possible outcomes. Measuring Z_1 and Z_2 individually will destroy the state, of course.

The following kind of (equivalent) circuits implement such incomplete measurements. Suppose one wants to measure $M \equiv Z_1 X_2 Z_3$. Note that $M^2 = \pm 1$.



Circuit for incomplete measurement of $Z_1X_2Z_3$.

This is also a state for preparation of an eigenstate of $Z_1X_2Z_3$, by inputting (say) $|000\rangle$.

Exercise. *Verify that the left side circuit implements the above measurement, and that the two circuits are equivlent.*

Code protecting against 1-qubit phase flip error

The above code is powerless against a phase error,

$$G(\phi) \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

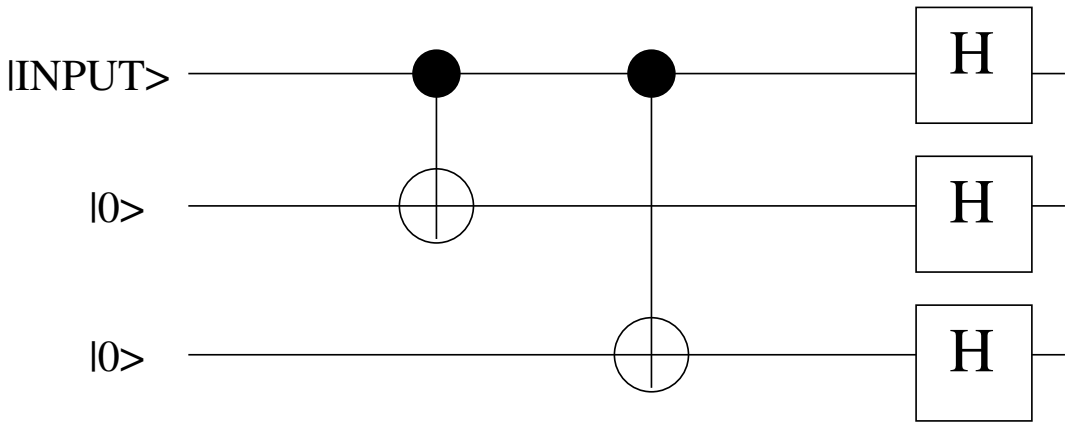
acting on a single qubit. There's a happy escape from this situation. Since phase flips act like bit flips in the X basis, we work in this basis. Thus:

$$|0\rangle \rightarrow |\overline{0}\rangle \equiv |+++\rangle; \quad |1\rangle \rightarrow |\overline{1}\rangle \equiv |---\rangle,$$

where $|\pm\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ are the eigenstates of $\hat{X}$.

Thus

$$\begin{aligned} \alpha|0\rangle + \beta|1\rangle &\rightarrow |\Phi\rangle \equiv \alpha|\overline{0}\rangle + \beta|\overline{1}\rangle \\ &\equiv \alpha|+++\rangle + \beta|---\rangle. \end{aligned}$$



Circuit for encoding a 3-qubit code that protects against a single qubit phase error.

Assuming single qubit $G(\pi) = \hat{Z}$ phase errors, the post-error state will be one of:

$$\begin{aligned} |\Phi_0\rangle &= \hat{Z}_0|\Psi\rangle = \alpha|+++\rangle + \beta|---\rangle \\ |\Phi_1\rangle &= \hat{Z}_1|\Psi\rangle = \alpha|+-+\rangle + \beta|-+-\rangle \\ |\Phi_2\rangle &= \hat{Z}_2|\Psi\rangle = \alpha|-++\rangle + \beta|+--\rangle, \end{aligned} \quad (8)$$

having orthogonal support.

As before, the following scheme of **incomplete** and **commuting** measurement can identify all

the above 1-qubit errors:

$$\begin{aligned}
\hat{P}_+ &\equiv |+++\rangle\langle+++| + |---\rangle\langle---| \\
\hat{P}_- &\equiv |-++\rangle\langle-++| + |+--\rangle\langle+--| \\
\hat{P}_2 &\equiv |+-+\rangle\langle+-+| + |-+-\rangle\langle-+-| \\
\hat{P}_3 &\equiv |++-\rangle\langle++-| + |--+\rangle\langle--+|
\end{aligned}$$

As with the bit flip channel, here too, an alternative, 2-qubit syndrome measurements equally well do the job.

An incomplete measurement of relative parity of qubits 1, 2:

$$(|++\rangle\langle++| + |--\rangle\langle--|) \otimes \hat{I} - (|+-\rangle\langle+-| + |-+\rangle\langle-+|) \otimes \hat{I} = X_1 X_2.$$

and an incomplete measurement of relative parity of qubits 2, 3:

$$\hat{I} \otimes (|++\rangle\langle++| + |--\rangle\langle--|) - \hat{I} \otimes (|+-\rangle\langle+-| + |-+\rangle\langle-+|) = X_2 X_3 \quad .$$

Exercise. *Construct a circuit that measures this syndrome. Construct another that uses only c-phase and H gates.*

Consider the action of a general phase error $G(\phi)$ on say qubit #2. In the $\hat{X}$ basis representation, $G(\phi)$ takes the form:

$$G'(\phi) \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1+e^{i\phi} & 1-e^{i\phi} \\ 1-e^{i\phi} & 1+e^{i\phi} \end{pmatrix}$$

One directly checks that

$$G'(\phi)|\Phi\rangle = \frac{1+e^{i\phi}}{2}|\Phi\rangle + \frac{1+e^{-i\phi}}{2}|\Phi_1\rangle.$$

Measuring the error syndrome collapses this to $|\Phi\rangle$ with probabilty $(1+\cos\phi)/2$, requiring no error recovery, or to $|\Phi_1\rangle$ with probabilty $(1-\cos\phi)/2$, requiring Z_2 by way of recovery.

Quantum Hamming bound:

$$2^n \geq 2(3n+1)$$

That is, the full space of dimension 2^n must be able to accomodate $3n+1$ orthogonal 2-D spaces. **Therefore the smallest code that can protect against an arbitrary 1-qubit error is a 5-qubit code.**

More generally:

$$2^n \geq 2^k \sum_{j=0}^{t} \left(\begin{array}{c} n \\ j \end{array} \right) 3^j.$$

The 5-qubit error correcting code

Two codewords: logical 0, logical 1– $|\overline{0}\rangle$, $|\overline{1}\rangle$.

To be distinguished: $1 + (5 \times 3) = 16$ mutually $\perp$ 2-D subspaces. We require 4 **commuting** syndrome measurement operators that square to 1, since they would then have 2 eigenvalues ± 1 and $2^4 = 16$.

$$\begin{aligned} M_0 &= ZXXZI \\ M_1 &= ZIZXX \\ M_2 &= XZIZX \\ M_1 &= XXZIZ \end{aligned} \tag{9}$$

All of them commute with each other (since they 'nontrivially' differ in even # of places, and $XZ = -ZX$.)

$$|\overline{0}\rangle = \frac{1}{4}(1+M_0)(1+M_1)(1+M_2)(1+M_3)|0\rangle^{\otimes 5}$$
$$|\overline{1}\rangle = \frac{1}{4}(1+M_0)(1+M_1)(1+M_2)(1+M_3)|1\rangle^{\otimes 5}$$

Each codeword has 16 terms in the computational basis. Because M_j's, M_jM_k's and $M_jM_kM_l$'s all have even # of X's, the terms in the $|\overline{0}\rangle$ ($|\overline{1}\rangle$) superposition will have odd number of 0's (1's) in the computational basis. Thus the codewords are orthogonal, as they should be.

Since # odd number of 0's (1's) patterns from five bits is ${}^5C_1 + {}^5C_3 + {}^5C_5 = 16$, $|\overline{0}\rangle$ ($|\overline{1}\rangle$) is a superposition of all odd 0 (1) patterns.

Exercise. *Write out the two codewords* $|\overline{0}\rangle$ *and* $\overline{1}\rangle$ *in full.*

Since $M_j^2 = I$, and the M_j's commute with each other:

$$\begin{aligned} M_1|\overline{0}\rangle &= \frac{1}{4}(1+M_0)M_1(1+M_1)(1+M_2)(1+M_3)|000000\rangle \\ &= \frac{1}{4}(1+M_0)(M_1+1)(1+M_2)(1+M_3)|000000\rangle \\ &= 1\cdot|\overline{0}\rangle. \end{aligned}$$

Similarly one can show that $|\overline{0}\rangle$, $|\overline{1}\rangle$ and their superpositions

$$|\zeta\rangle \equiv \alpha|\overline{0}\rangle + \beta|\overline{1}\rangle,$$

are eigenstates of each M_j with eigenvalue $= +1$. Thus codewords form a basis for the $+1$ degenerate subspace of the syndrome operators.

The $15 = 2^4 - 1$ possible 1-qubit corruptions are also eigenstates, with other sets of eigenvalues ± 1. To see this note that each X_j, Y_k, Z_l either commutes or anticommutes with each M_j. Therefore $X_j|\zeta\rangle$, $Y_j|\zeta\rangle$ and $Z_j|\zeta\rangle$ are all eigenstates of each M_j with eigenvalue $\pm$.

Thus, given a state $|\psi\rangle \equiv \alpha|0\rangle + \beta|1\rangle$, it is encoded as ζ above. When any of the allowed errors P_j (a Pauli operator at site j) occur, the resultant state $P_j|\zeta\rangle$ remains an eigenstate of the M_j's, but the spectral signature of the syndrome measurement will change from $\{+1, +1, +1, +1\}$ to some other characteristic pattern, such that a measurement of all M_j's will tell us which error occured.

operator	$X_1X_2X_3X_4X_5$	$Y_1Y_2Y_3Y_4Y_5$	$Z_1Z_2Z_3Z_4Z_5$	1
M_0	$+-++-$	$+----$	$++--+$	$+$
M_1	$-+-++$	$-+---$	$+++--$	$+$
M_2	$+-+-+$	$--+--$	$-+++-$	$+$
M_3	$++-+-$	$---+-$	$--+++$	$+$

Syndrome signature for different errors on 5-qubit code. Here "+" ("−") indicates "+1" ("−1").

Encoded operations.

The operations:

$$\overline{\mathbf{Z}} \equiv ZZZZZ; \quad \overline{\mathbf{X}} \equiv XXXXX$$

commute with all M_j's because each of these differs 'nontrivially' from each M_j at exactly two places. Thus:

$$\begin{aligned}
\overline{Z}|\overline{0}\rangle &= \frac{1}{4}(1+M_0)(1+M_1)(1+M_2)(1+M_3)(Z|0\rangle)^{\otimes 5} \\
&= +|\overline{0}\rangle. \\
\overline{Z}|\overline{1}\rangle &= \frac{1}{4}(1+M_0)(1+M_1)(1+M_2)(1+M_3)(Z|1\rangle)^{\otimes 5} \\
&= -|\overline{1}\rangle.
\end{aligned}$$

Further

$$\begin{aligned}
\overline{X}|\overline{0}\rangle &= \frac{1}{4}(1+M_0)(1+M_1)(1+M_2)(1+M_3)(X|0\rangle)^{\otimes 5} \\
&= |\overline{1}\rangle. \\
\overline{X}|\overline{1}\rangle &= \frac{1}{4}(1+M_0)(1+M_1)(1+M_2)(1+M_3)(X|1\rangle)^{\otimes 5} \\
&= |\overline{0}\rangle.
\end{aligned}$$

Thus, the encoded $\overline{Z}$ and $\overline{X}$ operations act on the 'logic basis' states $\overline{0}, \overline{1}$ just as Z and X act on the computational basis states $|0\rangle, |1\rangle$. This

is important from a practical point of view, because it implies that these encoded operations on encoded states can be performed via single qubit operations.

Unfortunately, the same can't be said for other important single qubit operations. In particular, defining $\overline{H} = HHHHHH$, it can be shown that:

$$\overline{H}|\overline{x}\rangle \neq \frac{1}{\sqrt{2}}(|\overline{0}\rangle + (-1)^x|\overline{x}\rangle).$$

The 7-qubit code, devised by Steane, though less ideal in terms of encoding, allows simple encoded operations, and in this sense is more **fault tolerant**.

The 7-qubit error correcting code

Altho less ideal than the 5-qubit code, encoded operations are straightforward to perform in the 7-qubit Steane code.

Syndrome measurement are mutually **commuting** operators:

$$M_0 = XIIIXXX; \quad N_0 = ZIIIZZZ;$$
$$M_1 = IXIXIXX; \quad N_1 = IZIZIZZ;$$
$$M_2 = IIXXXIX; \quad N_2 = IIZZZIZ;$$

The 7-qubit codewords are:

$$|\overline{0}\rangle = 2^{-3/2}(1+M_0)(1+M_1)(1+M_2)|0\rangle^{\otimes 7}$$
$$|\overline{1}\rangle = 2^{-3/2}(1+M_0)(1+M_1)(1+M_2)\overline{X}|0\rangle^{\otimes 7}$$

where $\overline{X} \equiv X^{\otimes 7}$.

The syndromes are measured according to the pattern indicated earlier.

Since each M_j flips 4 qubits, and $\overline{X}$ flips all 7, $|\overline{0}\rangle$ ($|\overline{1}\rangle$) is a superposition of terms with odd (even) # of 0's.

Because all M_j's commute and $M_j(1+M_j) = 1+M_j$, $|\overline{0}\rangle$ and $|\overline{1}\rangle$ lie in the +1 eigenspace of the M_j's.

Further, since N_j's commute with M_j's and with $\overline{X}$ and $|0000000\rangle$ lies in their +1 eigenspace, $|\overline{0}\rangle$ and $|\overline{1}\rangle$ lie also in the +1 eigenspace of the N_j's.

A general state lying in the +1 eigenspace of the syndrome operators

$$|\Psi\rangle \equiv \alpha|\overline{0}\rangle + \beta|\overline{1}\rangle$$

under corruption assumes the form

$$|e\rangle|\Psi\rangle \rightarrow \left(|d\rangle\mathbf{1} + \sum_{i=1}^{7}[|a_i\rangle X_i + |b_i\rangle Y_i + |c_i\rangle Z_i]\right)|\Psi\rangle.$$

The $21 = 3 \times 7$ possible corruptions are also eigenstates of each M_j and N_j because each X_j, Y_j, Z_j commutes or anticommutes with the each M_j and N_j.

Thus, these allowed errors remain within the eigenspace of the M_j's and the N_j's. However, the pattern of outcomes of the 6 syndrome measurements will be different.

Eg., suppose the error is: Z_5. Since this error operator commutes with the N_j's and with $M_1 = IXIXIXX$, each of these measurements will yield +1. But $M_0 = XIIIXXX$ and $M_2 = IIXXXIX$ anticommute, and hence yield outcome -1, since:

$$\begin{aligned} M_1 Z_5 |\Psi\rangle &= M_1 Z_5 (\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle) \\ &= -Z_5 M_1 (\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle) \\ &= -Z_5 |\Psi\rangle \end{aligned}$$

Exercise. *Using the above recipe, derive the 21 possible error syndromes. Show that each allowed error produces a unique syndrome. Noting that # possible measurement outcome patterns* $2^6 = 64 > 21$*, indicate what patterns are not legitimate syndrome patterns.*

The operations:

$$\overline{\mathbf{Z}} \equiv ZZZZZZZ; \quad \overline{\mathbf{X}} \equiv XXXXXXX$$

commute with all M_j's, the former because each of these differs 'nontrivially' from each M_j at even # of places, the latter trivially.

Thus:

$$\begin{aligned} \overline{Z}|\overline{0}\rangle &= 2^{-3/2}(1+M_0)(1+M_1)(1+M_2)(Z|0\rangle)^{\otimes 7} \\ &= +|\overline{0}\rangle. \\ \overline{Z}|\overline{1}\rangle &= 2^{-3/2}(1+M_0)(1+M_1)(1+M_2)(Z|1\rangle)^{\otimes 7} \\ &= -|\overline{1}\rangle. \end{aligned}$$

Further

$$\begin{aligned}
\overline{X}|\overline{0}\rangle &= 2^{-3/2}(1+M_0)(1+M_1)(1+M_2)(X|0\rangle)^{\otimes 7} \\
&= |\overline{1}\rangle. \\
\overline{X}|\overline{1}\rangle &= 2^{-3/2}(1+M_0)(1+M_1)(1+M_2)(X|1\rangle)^{\otimes 7} \\
&= |\overline{0}\rangle.
\end{aligned}$$

Thus, the encoded $\overline{Z}$ and $\overline{X}$ operations act on the 'logic basis' states $\overline{0}, \overline{1}$ just as Z and X act on the computational basis states $|0\rangle, |1\rangle$.

Unlike the 5-qubit code, the encoded Hadamard $\overline{H} \equiv HHHHHHHH$ also acts in the same way. One way to show this is by demonstrating that $\langle \overline{x}|\overline{H}|\overline{x}\rangle = \frac{1}{\sqrt{2}}$.

Since $HX = ZH$, $\overline{H}M_j = N_j\overline{H}$. Thus:

$$\begin{aligned}
\langle \overline{x}|\overline{H}|\overline{x}\rangle &= 2^{-3/2}\langle \overline{x}|(1+N_0)(1+N_1)(1+N_2)\overline{H}|x\rangle^{\otimes 7} \\
&= 2^{-3/2}\langle \overline{x}|(1+N_0)(1+N_1)(1+N_2)|\pm\rangle^{\otimes 7} \\
&= 2^{-(3/2)+3}\langle \overline{x}|\pm\rangle^{\otimes 7} \\
&= 2^{-3/2}(2^3 \cdot 2^{-3/2} \cdot 2^{-7/2}) \\
&= 2^{-1/2}.
\end{aligned}$$

where the kets on the right take $|+\rangle$ or $|-\rangle$ values depending on whether $x = 0$ or 1, and where we make use of the fact that $|\pm\rangle^{\otimes 7}$ represented in computational basis will contain kets of given parity will have the same sign, and the codewords $|\overline{x}\rangle$ are superposition of kets with fixed parity.

Exercise. *Prove that $H^{\otimes 5}$ does not work like an encoded Hadamard in the case of the 5-qubit code.*

III. Measurement-based quantum computers

IPQI, IOP, Bhubaneswar

In conventional cirtuit or gate array model of QC, computational steps are unitary operations, that lead to a large entangled state, which is finally measured.

In measurement-based QC, one begins with a **fixed entangled state**, possibly of many qubits. Computational steps are a sequence of measurements on designated qubits in designated bases. The choice of basis for later measurements may depend on ealier measurement outcomes. The final result is determined from the classical data of all measurement outcomes.

There are two principal schemes of measurement-based QC: teleportation-based QC (TQC) and the cluster-model or one-way QC (1WQC).

TQC was developed by Nielsen (2001) and Leung (2001) based on the idea teleporting quantum gates (Gottesman and Chuang 1999). 1WQC

was developed by Raussendorf and Briegel (2001; 2002; 2003).

All the models are equivalent to each other, and can perform universal quantum computation.

In some case, eg., parallelizability of algorithms, measurement-based models offer an advantage over the ciruit model.

R. Josza, quant-ph/0508124;

Teleportation-based QC

We represent Bell-states by the notation:

$$|B_{cd}\rangle = Z^c X^d \otimes I |B_{00}\rangle,$$

where $|B_{00}\rangle \equiv \frac{1}{\sqrt{2}}|00\rangle + |11\rangle)$. Measurement in the standard Bell basis teleports state $|\psi\rangle_1 = \sum_j \alpha_j |j\rangle_1$ on particle 1 to particle 3, where particles 2 and 3 share entanglement.

Standard teleportation: The projection of $|\alpha\rangle_1 |\phi\rangle_{23}$ onto $|\phi\rangle_{12}$ results in $\frac{1}{d}|\alpha\rangle_3$. To see this: let $|\alpha\rangle \equiv \sum_j a_j |j\rangle$. Then the projection is:

$$\frac{1}{d}\left(\sum_i \langle i|\langle i|\right)\left(\sum_{jk} a_j |j\rangle|k\rangle|k\rangle\right)$$
$$= \frac{1}{d}\sum_{ijk} a_j \delta_{ij}\delta_{ik}|k\rangle = \frac{1}{d}\sum_k a_k |k\rangle.$$

Define 'rotated Bell basis':

$$|\phi(U)\rangle \equiv U^\dagger \otimes I|B_{cd}\rangle$$

produces state $U|\psi\rangle$ at particle 3. Similarly, it can be shown that teleportation in the rotated basis, involving projection of $|\alpha\rangle_1|\phi\rangle_{23}$ onto $|\phi(U)\rangle_{12}$ results in $\frac{1}{d}U|\alpha\rangle_3$.

Exercise. *Verify this claim!*

In general, in d dimensions, we will seeks a set of d^2 unitaries such that $U_j \otimes I|\phi\rangle$ will yield an orthonormal basis for the space of particles 1 and 2. In standard teleportation, the operators are $\{I, X, Y, Z\}$. In 'rotated' teleportation, they are $\{U, XU, YU, ZU\}$. As a result, note that particle 3 is left in the state $X^d Z^c U|\psi\rangle$ ($c, d \in \{0, 1\}$), requiring 2 bits of classical communication to complete teleportation.

2-qubit operations

By this same method, we can also apply 2-qubit gates such as cZ (controlled-Z) via teleportation in dimension $d = 4$. Eg., using $|B_{00}\rangle|B_{00}\rangle$ and the unitaries $U_{ij} = (P_i \otimes P_j)(CZ)$, where P_k ranges over all Pauli operators, it may be checked that $\{(U_{ij}^\dagger \otimes I)cZ|\phi\rangle\}$ is an orthonormal set and that output is $(P_i \otimes P_j)cZ|\psi\rangle$ for arbitrary $|\psi\rangle$.

Exercise. *Verify this claim!*

That is: qubits 1a and 1b are the input, that are measurement jointly with a 4-qubit (rotated) Bell state measurement along with qubits 2a and 2b, with the output appearing in 3a and 3b.

d^2 operators $\{U_i\}$ will make $|\phi(U_i)\rangle \equiv (U_i \otimes I)|\phi\rangle$ orthonormal iff $\mathrm{Tr}(U_i U_j^\dagger) = \delta_{ij}$, i.e., $\{U_i\}$ forms an operator basis. For any dimension d, many such sets exist, each corresponding to a teleportational scheme.

For the rotated basis, we can choose any $n \geq d^2$ operators U_i such that

$$|\phi(U_j)\rangle\langle\phi(U_j)| = I_d \otimes I_d.$$

Thus the set $\{k_i|\phi(U_j)\rangle\langle\phi(U_j)|\}$ forms the elements of a rank 1 POVM (positive operator valued measure).

- Consider the gates:

$$\begin{aligned} R_x(\theta) &= e^{-i\theta X}; \quad R_z(\theta) = e^{-i\theta Z}; \\ W(\theta) &= \begin{pmatrix} 1 & e^{i\theta} \\ 1 & -e^{i\theta} \end{pmatrix} = H \begin{pmatrix} 1 & 0 \\ 0 & -e^{i\theta} \end{pmatrix} \end{aligned}$$

where the last quantum operation is the phase gate.

Any 1-qubit gate (upto overall phase) can be decomposed as:

$$U = R_x(\zeta) R_z(\eta) R_x(\xi)$$

for some ζ, η, ξ and also as:

$$U = W(0) W(\theta_1) W(\theta_2) W(\theta_3)$$

for some $\theta_{1,2,3}$.

Since cZ and 1-qubit gates are universal for QC, either of

$$\{cZ, R_x(\zeta) R_z(\eta) R_x(\xi) \quad \forall \zeta, \eta, \xi\} \quad \{cZ, W(\theta) \quad \forall \theta\}$$

is universal.

The reason for the choice of this particular set of universal gates is now clarified.

Adaptive measurements

In trying to implement $\cdots U_3 U_2 U_1 |\psi\rangle$, we actually implement $P_3 U_3 P_2 U_2 P_1 U_1 |\psi\rangle$. It turns out, if we choose the U's carefully enough, we can propagate all the Pauli operators to the left without changing the U's 'too much'.

The universal set we chose have the following propagation relations:

$$\begin{aligned} R_x(\theta)X &= XR_x(\theta); \quad R_x(\theta)Z = ZR_x(-\theta); \\ R_z(\theta)X &= XR_z(-\theta); \quad R_z(\theta)Z = ZR_z(\theta); \\ W(\theta)X &= ZW(-\theta); \quad W(\theta)Z = XW(\theta) \end{aligned}$$

Suppose we want to prepare: $\cdots R_Z(\beta)R_x(\alpha)|\psi\rangle$.

$Z^c X^d R_z(\beta) Z^a X^b R_x(\alpha)|\psi\rangle = (-1)^{\delta_{ad}} Z^{a+c} X^{b+d} R_z((-1)^b \beta) R_x(\alpha)|\psi\rangle.$

So in step 2, we teleport the gate $R_z((-1)^b\beta)$ instead of $R_z(\beta)$.

Continuing this way:

$$\cdots X_2^{m_2} Z_2^{n_2} X_1^{m_1} Z_1^{n_1} (\text{the required } U)|\psi\rangle.$$

With cZ, the situation is even better, in that it does not need to be adapted under Pauli propagation:

$$cZ(Z \otimes I) = (Z \otimes I)cZ; \quad cZ(X \otimes I) = (X \otimes Z)cZ,$$

and similarly for X and Z acting on the other qubit, since cZ's action is symmetric.

The accumulated Pauli operators propagated to the left are easily handled: in measuring in computational basis, Z's can be ignored; X's merely serve to 'interchange' outcome label.

Clifford group

Operations like cZ, which do not require adaptivization, are called Clifford operators. More specifically:

Define $\mathcal{P}_n$ Pauli group generated by n-fold tensor products of $\pm I$, $\pm iI$, X, Z. E.g., $X \otimes Z \otimes Z, -iZ \otimes Y \otimes I, I \otimes I \otimes X \in \mathcal{P}_3$.

A Clifford operator C is defined as one for which

$$C\mathcal{P}_n C^\dagger = \mathcal{P}_n, \quad \text{i.e.,} C\mathcal{P}_n = \mathcal{P}_n C.$$

That is, for every Pauli operator $P \in \mathcal{P}_n$, there is (possibly another) P' such that

$$CP = P'C.$$

An array of Clifford operations of the form $C_k \cdots C_1 |\psi\rangle$ can be implemented with only 1

parallel measurement layer (for we get an output of the form $P_k C_k \cdots P_k C_1 |\psi\rangle$. Commuting out the Pauli opertors we get

$$X^{a_n} Z^{b_n} \cdots X^{a_1} Z^{b_1} C_k \cdots C_1 |\psi\rangle$$

If we could not commute them out, then the measurements would have had to be done, and their outcomes used to determine the subsequent measurements and qubits.)

It turns out that any Clifford operator can be constructed by Z, Hadamard H , $(\pi/4)$-phase-gate $P_{\pi/4} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, and cX acting in some combination on n qubits.

Therefore, it suffices to verify for the propagation of X and Z to check for the Clifford property.

We saw that cZ is a Clifford operator. The Clifford property of H is demonstrated by the fact that:

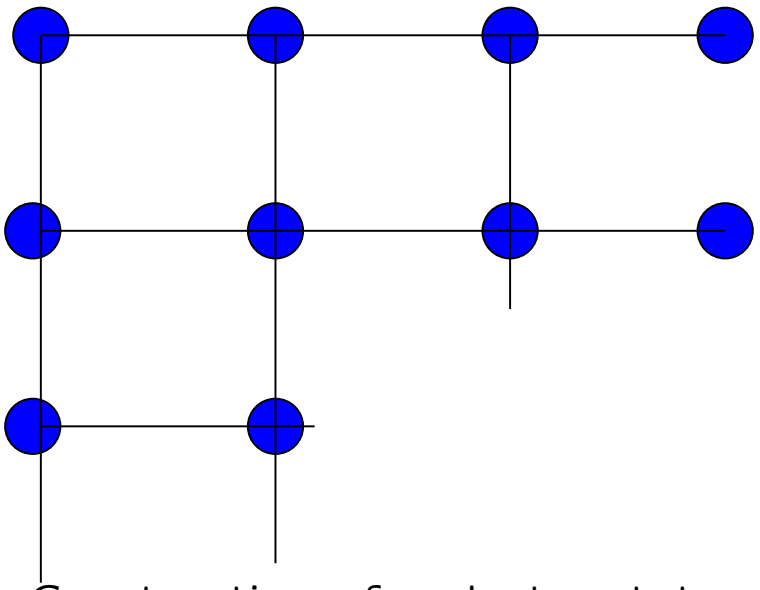
$$HX = ZH; \quad HZ = XH.$$

The group formed by Clifford operator, generated by the above 4 operations, is called the Clifford group.

In TQC, the collection of maximally entangled states in all the teleportations can be manufactured in parallel (eg., by applying cX on many $|+,+\rangle$'s). So the entire process requires only a constant amount of quantum parallel time, in contrast to the corresponding gate array in the circuit model, whose depth generally increases with n.

1-way quantum computation

Cluster state: A state obtained by mapping a 2-dimensional grid as follows. At each node, place a $|+\rangle$ state. Apply cZ to each nearest neighbour pair (in horizontal and vertical directions). These CZs all commute so for any grid size they can all be applied in parallel, as a process of constant quantum depth.



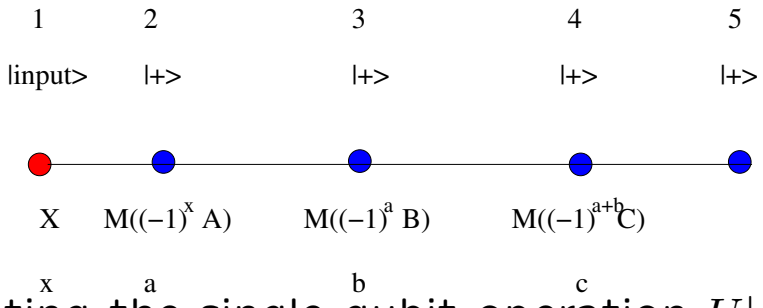
Construction of a cluster state.

A one-dimensional cluster state is constructed in the same way, but beginning from a 1-D array of $|+\rangle$ states.

There is no unitary evolution: the only measurements used are measuring in the computational basis $\{|0\rangle, |1\rangle\}$ and in the bases $\{|0\rangle \pm e^{i\theta}|1\rangle\}$.

As in TQC, subsequent measurements will be adaptive, and operations are implemented upto Pauli corrections.

The name "one-way" arises from the fact that an initial resource cluster state is, with each layer of measurement, irreversibly degraded.



Implementing the single-qubit operation $U|\psi\rangle$, taking $U = R_x(A)R_z(B)R_x(C)$. Qubit 5 is left in the state $X^{a+c}Z^{x+b}U|\psi\rangle$.

Alternative representation:

$$|\psi\rangle|+\rangle^{\otimes 4} \xrightarrow{XM((-1)^x A)M((-1)^a B)M((-1)^{a+b}C)} X^{a+c}Z^{x+b}U|\psi\rangle.$$

One way to see this is to reorder the operation as follows: (entangle 1-2, measure 1), (entangle 2-3, measure 2) etc. This works because both measurement on 1 and the 1-2 entangling operation both commute with all subsequent measurements and entangling operations.

In particular one can verify that:

$$|\psi\rangle|+\rangle \overset{M^{(1)}(\theta)}{:\longrightarrow} X^m W(-\theta)|\psi\rangle,$$

where m is the outcome of $M^{(1)}(\theta)$, the measurement of $M(\theta)$ on particle 1.

Exercise. *Verify the claim!*

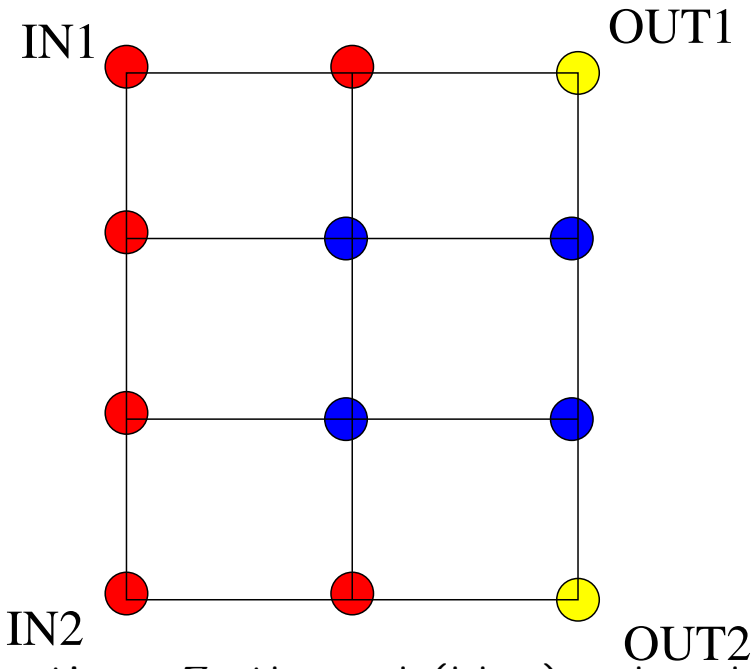
Therefore the above scheme will give us, apart from Pauli corrections, the effective gate

$$HW(A)W(B)W(C) = U,$$

as desired, for some suitably chosen A, B, C.

Implementing c-Phase

For implementing universal computation, cZ and arbitrary singly qubit gates suffice. cZ employs a 2-dimensional grid:

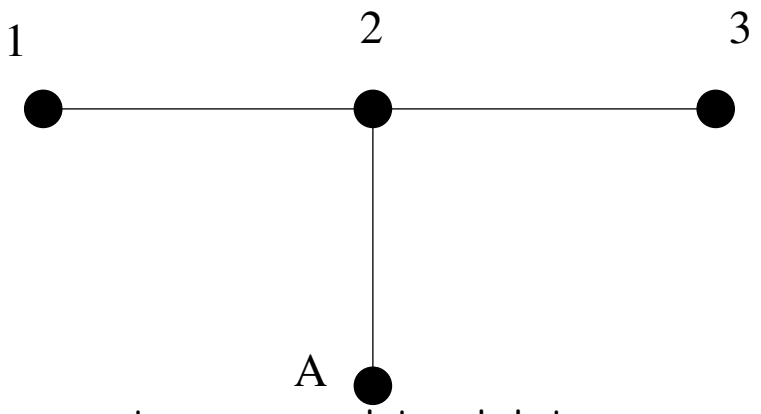


Implementing cZ: the red (blue) colored vertices denote an X (Z) operation. $|\psi\rangle$ is input (extracted) at vertices labelled IN (OUT).

Exercise. *Verify the claim!*

Remark 1. 1-dimensional cluster states can be efficiently (i.e., in polynomial time) simulated classically (Nielsen 2005), so we don't expect it to be universal.

Remark 2. Note that we can start from a standard cluster state by eliminating the input state $|\psi\rangle$, and transfering it to the cluster by using an appropriate 1-qubit measurement at the beginning of the computation.



Z measurements are used to delete unwanted sites.

Since cZ requires a 2-D grid but 1-qubit gates require only 1-D clusters, there will in general be some extraneous sites not used in the measurement patterns. Z-measurements are used to delete such extraneous sites.

Because $[cZ_{12}, Z_A] = [cZ_{23}, Z_A] = 0$, we can perform cZ_{2A} and then Z_A before cZ_{12} and cZ_{23}. If k_A is the measurement outcome of Z_A, then qubits 1, 2 and 3 are left in the state $|+\rangle|(-1)^{k_A}\rangle|+\rangle$. Thus deleting sites only addes a Z^{k_A} correction to neighboring sites over the Pauli corrections arising from the measurement patterns.

A further paralellizability result:

It turns out that any polynomially sized quantum gate array can be implemented in 1WQC using at most a polynomial number of measurement layers. (A Clifford array requires only a single layer.)

One may ask: which classes of quantum gate arrays can be implemented in 1WQC using at most 1 or 2 or logarithmic number of measurement layers.

One result known, due to Raussendorf and Briegel (2001): Any gate array using gates from the set $\{cX, R_x(\theta)\forall\theta\}$ or from the set $\{cX, R_z(\theta)\forall\theta\}$ can be implemented with just 2 measurement layers.

(Note that neither of these sets is universal, though $\{cX, R_y(\theta)\forall\theta\}$ is.

Proof sketch. $R_x(\theta)$ can be implemented according to the following measurement scheme:

$$|\psi\rangle_1|+\rangle_2|+\rangle \overset{X,M(-\theta)}{:\longrightarrow} X^{s_2}Z^{s_1}R_x((-1)^s_1)|\psi\rangle,$$

where the hyphen indicates $cZ_{12}cZ_{23}$. Given a gate array $G_n \cdots G_1$ with $G_j \in \{cX, R_x(\theta)\forall\theta\}$:
Layer I: Measure all cX's and X's of the above $R_x(\theta)$ measuerment scheme.
Layer II: Propagate the resultant Pauli corrections to the left. They may adaptively alter only the $M(\theta)$ measurements (cX being Clifford). Measure the adapted $M(\theta)$ measurement.

Similarities/differences between 1WQC and TQC

– Both are measurement-based, and require Pauli corrections.

– But: TQC uses Bell-state meaurements on 2 or more qubits, whereas 1WQC uses only 1-qubit measurements.

– And: 1WQC starts in a std. cluster states, whereas TQC starts with Bell pairs.

Different broad ways have been proposed to relate them. As one example: suitable pairs of consecutive 1-qubit measurements of 1WQC are like teleportation in TQC (Aliferis and Leung 2004). Eg.,

$$|\psi\rangle|+\rangle|+\rangle \stackrel{X_1 X_2}{:\longrightarrow} Z_3^{s1} X_3^{s2} |\psi\rangle_3.$$

However, in general, not all consecutive 1-qubit measurements can be fused to form a Bell-state measurement.

Measurement-based models and computational complexity

The measurement-based models provide a novel way of looking at QC. However, they are polynomial-time equivalent to the standard circuit model i.e. each model can simulate the other with only a polynomial (i.e. modest) overhead of resources (number of qubits and computational steps).

Intuitively:
To see how QC ciruit model can efficiently simulate a 1WQC computer, we note that a measurement and an adaptive action at some site can be replaced by an ancillary qubit with an appropriate control-action that effects the outcome-based unitary operation in 1WQC.

Conversely, any quantum circuit can be simulated by a 1WQC computer using a two-dimensional

cluster state as the resource state, by laying out the circuit diagram on the cluster; Z measurements delete unnecessary physical qubits from the cluster, while $M(\theta)$ measurements (in the X-Y plane) teleport the logical qubits along the "wires" and perform the required quantum gates (Briegel and Raussendorf 2003).

This can be shown to be also polynomially efficient, as the required size of cluster scales as the size of the circuit (qubits $\times$ time steps), while the number of measurement time steps scales as the number of circuit timesteps.

III(b) Quantum Computation by Adiabatic Evolution

This model of computation is different from the circuit model and the measurement-based models discussed above. It is based on the idea of a so-called ground-state oracle , the power of a system to somehow locate its ground state.

$|\psi\rangle$ evolves according to a Hamiltonian that varies smoothly from an initial Hamiltonian, whose ground state is easy to construct to a final Hamiltonian, whose ground state encodes the (possibly) satisfying assignment.

To ensure that the evolution satisfies the adiabatic condition, the evolution time must be large enough. This time depends inversely on the minimum energy difference between the two lowest states of the time-dependent Hamiltonian.

Farhi, Gutmann, Sipser quant-ph/0001106

The n-bit instance of Satisfiability (SAT) is the formula:

$$C_1 \wedge C_2 \wedge \cdots \wedge C_M$$

where C_j is a Boolean clause, that is True or False, depending on the value of a subset of the n Boolean variables.

It may not be difficult to devise a method or device that obtains a value assignment that satisfies a given clause. The difficulty lies finding out if there is an assignment that satisfies all clauses.

Algorithm, specified on the Hilbert space of n qubits, evolves the state according to Schrödinger equation governed by Hamiltonian of the form

$$H(t) = H_{C_1}(t) + H_{C_2}(t) + \cdots + H_{C_M}(t). \ (0 \leq t \leq T)$$

where H_{C_j} depends only on clause C_j and acts on bits contained in C_j.

$H(t)$ varies slowly in time.

The initial state, which is always easy to construct, is the ground state of $H(0)$.

For each j, the ground state of $H_{C_j}(T)$ encodes the satisfying assignments of clause C_j. The ground state of $H(T)$ encodes the intersection of the satisfying assignments of all clauses.

According to the adiabatic theorem, if T is large enough, $|\psi(T)\rangle$ will be close to the g.s of $H(T)$, as required.

For this algorithm to be successful, we require $T = \text{poly}(n)$.

Nota: quantum adiabatic evolution as used here is different from simulated annealing, a classical algorithm to determine the g.s of $H(T)$ by cooling the system from a Boltzmann distribution ($\propto e^{-\beta T}$).

The Adiabatic theorem

The theorem tells us how Schrödinger equation:

$$i\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle = H(t)|\psi(t)\rangle.$$

guides the evolution of system when $H(t)$ varies slowly. Reparametrize: $\tilde{H}(s)$, $0 \leq s \leq 1$, and let

$$H(t) = \tilde{H}(t/T)$$

so that T controls H's rate of change. Instantaneous eigenstates:

$$\tilde{H}(s)|l;s\rangle = E_l|l;s\rangle$$

with

$$E_)(s) \leq E_1(s) \leq \cdots \leq E_{N-1}(s)$$

where N is Hilbert space dimension. Designate initial ground state by:

$$|\psi(0)\rangle \equiv |l=0;s=0\rangle.$$

The adiabatic theorem says that if $E_1(s) - E_0(s) > 0$ for all s, then:

$$\lim_{T\to\infty} |\langle l = 0; s = 1|\psi(T)\rangle| = 1.$$

Define minimum gap:

$$g_{\min} \equiv \min_{0\le s\le 1} (E_1(s) - E_0(s)).$$

More particularly, the theorem tells that taking

$$T \gg \frac{\mathcal{E}}{g_{\min}^2},$$

where

$$\mathcal{E} = \max_{0\le s\le 1} \left| \left\langle l = 1; s \left| \frac{\mathrm{d}\tilde{H}}{\mathrm{d}s} \right| l = 0; s \right\rangle \right|$$

can make

$$|\langle l = 0; s = 1|\psi(T)\rangle|$$

arbitrarily close to 1. For our purposes, $\mathcal{E}$ is of the order of a typical eigenvalue of H and is not too big. Size of T thus governed by $g_{\min}^2$.

The Satisfiability problem

Many computationally interesting problems can be recast into an equvialent problem of finding an assignment of variables that minimizes an 'energy function'. Consider 3-SAT (where each clause is a disjunction of at most 3 literals/bits). Let the bits that appear in clause C be i_C, j_C, k_C. For each clause define the energy function:

$$h(z_{i_C}, z_{j_C}, z_{k_C}) = \begin{cases} 0 & \text{if } (z_{i_C}, z_{j_C}, z_{k_C}) \text{ satisfies } C \\ 1 & \text{else} \end{cases}$$

Total energy:

$$h = \sum_{C=1}^{M} h_C.$$

Clearly $h \geq 0$, and $h(z_1, z_2, \cdots, z_n) = 0$ if and only if $(z_1, z_2, \cdots, z_n)$ satisfies all of the clauses. Thus finding the minimum energy configuration of h tells us if the formula has a satisfying assignment.

(Conventionally, only the OR function of constituent variables in the clause is computed, but for our purpose more general functions may conveniently considered.)

The problem Hamiltonian H_P

The Hilbert space is spanned by the $N = 2^n$ basis vectors $|z_1\rangle|z_2\rangle \cdots |z_n\rangle$. Clause C associated with operator $H_{P,C}$ satisfying the e.v equation:

$$H_{P,C}(|z_1\rangle|z_2\rangle \cdots |z_n\rangle) = h_C(z_{i_C}, z_{j_C}, z_{k_C})|z_1\rangle|z_2\rangle \cdots |z_n\rangle$$

which acts on a fixed number of bits. The full Hamiltonian is

$$H_P \equiv \sum_C H_{P,C}$$

By construction, ($\langle\psi|H_P|\psi\rangle \geq 0 \forall\psi$, and $H_P|\psi\rangle = 0$ iff $|\psi\rangle$ is a superposition of states $|z_1\rangle|z_2\rangle \cdots |z_n\rangle$ s.t. $z_1, z_2, \cdots z_n$ satisfy all the clauses.

Thus, solving a 3-SAT problem $\equiv$ finding the ground state of a Hamiltonian. Specifying H_P is easy, but finding its g.s is in general difficult.

The initial Hamiltonian H_B

Specifying both H_B and its g.s are easy, by design. To bit i assign Hamiltonian:

$$H_B^i = \frac{1}{2}(1 - X^{(i)}),$$

with 'eigenset' $\{(0, |x = 0\rangle), (1, |x = 1\rangle)\}$. Define:

$$H_{B,C} = H_B^{i_C} + H_B^{j_C} + H_B^{k_C}$$

and

$$H_B = \sum_{C=1}^{M} H_{B,C} = \sum_{j=0}^{n-1} d_j H_B^{(j)},$$

where d_j is # clauses in which bit j appears in the instance of 3-SAT being considered. The g.s is immediately seen to be:

$$|x_1 = 0\rangle |x_2 = 0\rangle \cdots |x_n = 0\rangle = 2^{-n/2} \sum_{i=0}^{2^n - 1} |j\rangle.$$

Adiabatic evolution

Adiabatic evolution is used to go from H_B to H_P:

$$H(t) = \left(1 - \frac{t}{T}\right) H_B + \frac{t}{T} H_P.$$

That is,

$$\begin{aligned} \tilde{H}(s) &= (1-s)H_B + sH_P \\ &= \sum_C (1-s)H_{B,C} + sH_{P,C} \\ &= \sum_C \tilde{H}_C(s). \end{aligned}$$

$g_{\min}$, $\mathcal{E}$ and T

We have:

$$\frac{\mathrm{d}\tilde{H}}{\mathrm{d}s} = H_P - H_S.$$

Since $H_P = \sum_C H_{P,C}$, the spectrum of H_P is contained in $\{0, 1, 2, \cdots, M\}$. Since $H_B = \sum_{j=1}^{n} d_j H_B^{(j)}$, the spectrum of H_B is contained in $\{0, 1, 2, \cdots, d\}$, where $d = \sum_j d_j$. For 3-SAT, $d \leq 3M$.

Since we are interested only in $M \in$ poly(n), therefore $\mathcal{E} \in$ poly(n), and $g_{\min}$ alone determines whether T is polnomial or exponential in n.

Typically, we don't expect $g_{\min}$ to vanish. $g_{\min} = 0 \Rightarrow \exists_s(E_0(s) = E_1(s))$. For a 2×2 Hamiltonian

$$H \equiv \begin{pmatrix} a(s) & c(s) + id(s) \\ c(s) - id(s) & b(s) \end{pmatrix},$$

this happens only if $c(s) = d(s) = 0$ and $a(s) = b(s)$. This seems unlikely, unless H has some symmetry properties.

Eg., if H is known to commute with (say) σ_x, then $a(s) = b(s)$ and $d(s) = 0$. As s varies, it would not surprising to see $c(s)$ cross 0. However, in a general $N \times N$ Hamiltonian of practical interest, such symmetries are probably unlikely. Hence we expect that $g_{\min}$ will not vanish, and hence T will be finite.

The adiabatic quantum algorithm

A review of the algorithm for solving SAT problems:

(1) An easily constructable initial state, g.s of H_B.

(2) A time-dependent Hamiltonian $H(s)$ that is easily constructable from the given instance of the problem.

(3) Schrödinger evolution of the system for time $T \gg \mathcal{E}/g^2_{\text{min}}$.

(4) The final state $|\psi(T)\rangle$, that for big enough T, will be very nearly the g.s of H_P.

(5) Measurement of $|\psi(T)\rangle$ in the computational basis will yield a state that minimizes energy (# of violated clauses). Iff this energy is zero, a satisfying assignment exists. The resultant state will encode one such assignment.

An example with 3 bits

Consider an instance of 2-SAT with three Boolean variables (bits):

(z_1 implies z_2) AND (z_1 and z_3 disagree)
AND (z_2 and z_3 agree)

Knowing that the indiv. clauses satisfy (00?, 01?, 11?), (1?0, 0?1) and (?00, ?11), it is easy to write down H_P

$$H_P = H^{12}_{\text{imply}} + H^{13}_{\text{disagree}} + H^{23}_{\text{agree}}.$$

without (in general) knowing whether a satisfying assignment exists (tho in this 3-bit case one can quickly solve the problem classically.)

$$H_B = \left(H^1_B + H^2_B\right) + \left(H^1_B + H^3_B\right) + \left(H^2_B + H^3_B\right),$$

where $H^j_B = \frac{1}{2}(1 - \sigma^{(j)}_x)$.

Starting the system in the g.s of H_B, $|x_1 = 0\rangle|x_2 = 0\rangle|x_3 = 0\rangle = \frac{1}{\sqrt{8}}\sum_{j=0}^{7}|j\rangle$, and evolving via $H(s)$, we will reach $|0,1,1\rangle$, the g.s of H_P with e.v $= 0$.

Measuring it in the compu. basis, we conclude that $z_1 = 0, z_2 = 1, z_3 = 1$ is a satisfying assignment.

The crucial problem is estimating $g_{\min}$ and thus $T = T(n)$ for arbitrary n. No case is known where T is estimated to be sufficiently small as to give exponential speedup over classical algorithms.

In fact, one can prove (Lloyd 1998) that the conventional circuit model can **efficiently** simulate quantum computation based on adiabatic evolution, implying that a latter is no more powerful.

Thank you

IV. Physical implementation of computers

In a good physical realization of a quantum computer, one must have the ability to:

(1) robustly represent quantum information
(2) perform a universal family of unitary operations
(3) to prepare of a suitable initial state.
(4) Measure the output result.

Typically a qubit is represented by a spin (Nuclear Magnetic Resonance [NMR], ion traps), by charge (quantum dots, SQUID), photon (cavity QED), etc.

Optical photon quantum computer

An illustrative, rather than practical, implementation.

Qubit representation: Location of a photon between two optical cavity modes.

$$|\overline{0}\rangle \equiv |01\rangle; \quad |\overline{1}\rangle \equiv |10\rangle,$$

and polarization.

Initial state preparation. Create single photon states typically by attenuating a laser, which is described by a coherent state:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle.$$

Average photons per state $\langle\alpha|\hat{n}|\alpha\rangle = |\alpha|^2$.

For better synchronicity while manipulating multiple photons, use 'heralded photons' from parametric downconversion via nonlinear optical media such as KH_2PO_4.

Unitary operations: phase gate. Passing through a transparent medium of RI $\nu > \nu_0$. Relative phase shift is given by $e^{i(\nu-\nu_0)L\omega/c}$, where L is medium's thickness.

Unitary operations: beam splitters. Given by the Hamiltonian $i\theta(ab^\dagger - a^\dagger b)$. Its action on the mode operators is to produce the transformation:

$$B \equiv \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \equiv e^{i\theta Y}.$$

Beam splitters and phase shifters are sufficient to implement any single qubit operation.

Two-qubit gates. Via cross phase modulation in a nonlinear Kerr medium. Classically, the optical Kerr effect:

$$\nu(I) = \nu + \nu_2(I).$$

When two equal-intensity beams are passes thru a nonlinear Kerr medium, each will experience an extra phase shift $e^{in_2 IL\omega/c}$.

Quantum mechanically: $H_{\text{Xpm}} = -\chi a^\dagger a b^\dagger b$ giving the unitary operation $K = e^{i\chi L a^\dagger a b^\dagger b}$, where χ is related to n_2 and nonlinear susceptibility $\chi^{3)}$. One can then construct a c-phase gate using K:

$$\begin{aligned} K|00\rangle &\rightarrow |00\rangle \\ K|01\rangle &\rightarrow |01\rangle \\ K|10\rangle &\rightarrow |10\rangle \\ K|11\rangle &\rightarrow -|11\rangle \end{aligned}$$

c-Phase and single qubit operations are universal for QC.

Drawbacks. Getting photons to interact is usually very difficult. Nonlinear media tend to be highly absorptive.

Optical cavity QED

The nonlinear medium of the optical quantum computer is replaced by individual atoms trapped in a cavity of high Q (low mode leakage). Because only 1 or 2 modes exist in a cavity, and they have high electric field strength, dipole coupling between atom and light is very strong.

Qubit representation. Location of single photon between two modes $|01\rangle$ and $|10\rangle$, and polarization.

Unitary evolution: single qubit operations. Phase shifters ($R_z(\theta)$ and beam-splitters ($R_z(\theta)$.

Unitary evolution: 2-qubit operations. Atom-light interaction via the dipole-field interaction:

$\mathbf{d}\cdot\mathbf{E}$. In the 'rotating wave approximation', this leads to the Hamiltonian:

$$H = \frac{\hbar\omega_0}{2}Z + \hbar\omega a^\dagger a + g(a^\dagger\sigma_- + a\sigma_+).$$

whose eigenstates are:

$$|\chi_n^\pm\rangle \equiv \frac{1}{\sqrt{2}}(|n,1\rangle \pm |n-1,0\rangle),$$

with eigenvalues $\pm g\sqrt{n+1}$, where the notation is $|\text{field},\text{atom}\rangle$.

When two light modes (distinguished by small difference in frequency) are input into the cavity, because of interaction with the atom, it can be shown that the following interaction arises:

$$K = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\phi_a} & 0 & 0 \\ 0 & 0 & e^{i\phi_b} & 0 \\ 0 & 0 & 0 & e^{i\phi_a + i\phi_b = \Delta} \end{bmatrix}$$

which can be used to realize a c-phase gate.