Introduction to Quantum Computation

Richard Jozsa
University of Bristol UK

Outline

Lecture 1: Basic quantum formalism
(states, operations, measurements), entanglement.
Quantum interference, nonlocality, teleportation.

Lecture 2: Quantum computation - circuit model
Quantum time complexity, oracle problems
Some basic quantum algorithms

Lecture 3: Quantum computing and NP.
Grover's quantum searching algorithm & generalisations

Lecture 4: Classical simulation of quantum computation.
(classical vs quantum computing power)
Clifford circuits. Matchgate circuits.

Why quantum computing?

What is computation? - "processing of information?"

Information: bit strings! A bit is 0 or 1?..

"Information is physical!" "No information without representation!"

So processing is physical evolution, So:

Possibilities of storage/processing/communication of information must rest on laws of physics! ~~classical~~ → now quantum!

Quantum physics/computing: cannot compute Turing-uncomputable tasks

but appear to get exponential benefits in complexity of computation!

(for some problems...)

Also: "Moore's law" - miniaturisation of computing components

- will soon reach sub-atomic sizes!..

Rules of quantum mechanics ("CS version")

(I) States of a physical system are represented by unit vectors in a complex vector space (we'll use finite dimensions) with an inner product.

Dirac notation: ket vector $|v\rangle$, bra vector $\langle w|$, inner prod $\langle w|v\rangle$.

Physically distinguishable states will correspond to orthogonal vectors (cf measurements later)

Simplest non-trivial system: qubit

2-dimensional state space. Chosen basis $|0\rangle$, $|1\rangle$

General qubit state $|\psi\rangle = a|0\rangle + b|1\rangle$ $\quad |a|^2 + |b|^2 = 1$

"superposition of 0 & 1"

Coefficients a & b called (probability) amplitudes.

(Actual physical systems exist for any finite dimension)

(II) Composite systems:

If $(S_1) \sim$ unit vectors in V_1

$(S_2) \sim$ unit vectors in V_2

Then composite system $(S_1 S_2)$

$\sim$ unit vectors in tensor product $V_1 \otimes V_2$

Remarks

1) Entanglement e.g. 2 qubit general state is

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

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$$

write $|0\rangle \otimes |0\rangle$ as $|00\rangle$ etc.

Basis of tensor prod space = tensor prod of bases.

$\dim(V_1 \otimes V_2) = (\dim V_1) \cdot (\dim V_2)$

Special case:

product states $(s|0\rangle + t|1\rangle) \otimes (x|0\rangle + y|1\rangle)$

$$= sx|00\rangle + sy|01\rangle + tx|10\rangle + ty|11\rangle$$

But not all $|\psi\rangle$'s factorise like this!

Non-product def entangled state

Individual qubits not describable by unit vectors!

"Whole is greater than the sum of parts."

~ "quantum correlations"

Fact: $|\psi\rangle$ above is product state iff $ad - bc = 0$.

Similarly for 3 or more qubits: entangled if $|\psi\rangle \neq |v_1\rangle|v_2\rangle \ldots |v_n\rangle$ for 1-qubit $|v_i\rangle$'s.

2) Compare classical physics! —

Systems S_1, S_2 state spaces S_1, S_2

Composite (S_1, S_2) has state space $S_1 \times S_2$ cartesian product!

"Individual component systems always in definite individual states!"

If classical S described by k parameters then $(\underbrace{S \ldots S}_{n})$ described by nk parameters — linear growth with n.

If quantum S has k dim's ($O(k)$ parameters) then $(\underbrace{S \ldots S}_{n})$ has dim k^n — exponential growth with n!

e.g. n qubits $\sim 2^n$ dimensions/components.

If number of parameters $\sim$ ability to represent information then quantum system is exponentially better than classical system of comparable size!

(III) Physical evolution of state vector

is always a linear unitary transformation.

conjugate transpose

U unitary: preserves all inner products or $UU^\dagger = U^\dagger U = I$

or columns of matrix of U are orthonormal set of vectors.

- If U is applied to subsystem S_1 of composite (S_1, S_2) then its action is $U_{S_1} \otimes I_{S_2}$ on full state vector $|\psi\rangle \in V_1 \otimes V_2$

Calculation of tensor products of states and of operations easy to perform with components/matrices ...

Unitary evolution $\Rightarrow$ No-cloning theorem:

Given an unknown $|a\rangle$ (and standard state $|0\rangle$)

there is no physical process that will copy $|a\rangle$:

$$|a\rangle \rightsquigarrow |a\rangle|a\rangle \quad !$$

Quantum gates (on 1 or 2 qubits)

(will replace basic classical Boolean gates for computing)

Some 1-qubit gates

Pauli matrices: $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

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

Phase gate $P_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$

Some 2-qubit gates

CNOT or CX: $|i\rangle|j\rangle \to |i\rangle|j \oplus i\rangle$

control qubit ↗ ↖ target qubit

"if 1st qubit is 0, do nothing (I)

if 1st qubit is 1, apply X to 2nd qubit."

Similarly "controlled-U" for any 1-qubit U.

(IV) Quantum measurements (Born rule)

~ classical output of a quantum computational process.

Example 1: Given (unknown) 1-qubit state $|\psi\rangle = a|0\rangle + b|1\rangle$

apart from unitary evolution, only allowed operation is "make a measurement" or "perform a test" to see if $|\psi\rangle$ is 0 or 1.

Then see

outputs	0	with prob	$p_0 = \|a\|^2$	and post-mmt state is	$\|0\rangle$
	1	(Born rule)	$p_1 = \|b\|^2$		$\|1\rangle$

"collapse of state" non-unitary!

i.e. can sample $\{|a|^2, |b|^2\}$ probability distribution only <u>once</u>! (recall no-cloning...)

So: get very little information about state identity & rest is destroyed!

cf classical states – can in principle measure fully (to any desired precision) & state left intact.

Quantum measurement intrusive – unavoidable destruction of state!

If $|\alpha\rangle$ & $|\beta\rangle$ orthogonal, can distinguish/identify them with certainty (first unitarily rotate to standard $|0\rangle, |1\rangle$ position & measure.)

If $|\alpha\rangle$ & $|\beta\rangle$ not orthogonal then cannot be distinguished with certainty by any physical process.

(even though distinct as math. descriptions!)

Example 2 Measure some qubits of a multi-qubit state

natural generalisation of the above.

- See a corresponding bit-string as output
- Post-mmt state = coeff vector (re-normalised) for that bit string in given state
- Prob. of outcomes = squared lengths of coeff. vectors. ("Extended Born rule")

eg measure 1st qubit of

$$|\psi\rangle = \frac{3}{10}|000\rangle - \frac{4}{10}|010\rangle + \frac{i}{2}|011\rangle - \frac{1}{2}|100\rangle + \frac{1+i\sqrt{3}}{2}|111\rangle$$

Write $|\psi\rangle$ as

$$|0\rangle\left[\frac{3}{10}|00\rangle - \frac{4}{10}|10\rangle + \frac{i}{2}|11\rangle\right] + |1\rangle\left[-\frac{1}{2}|00\rangle + \frac{1+i\sqrt{3}}{2}|11\rangle\right]$$

$$\equiv |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle$$

Then

outcomes	with probs		and post-mmt states	
0		$p_0 = \langle\psi_0\|\psi_0\rangle$		$\|0\rangle\|\psi_0\rangle/\sqrt{p_0}$
1		$p_1 = \langle\psi_1\|\psi_1\rangle$		$\|1\rangle\|\psi_1\rangle/\sqrt{p_1}$

Here endeth the rules of quantum mechanics!

Quantum Interference

how to think of $a|0\rangle + b|1\rangle$?

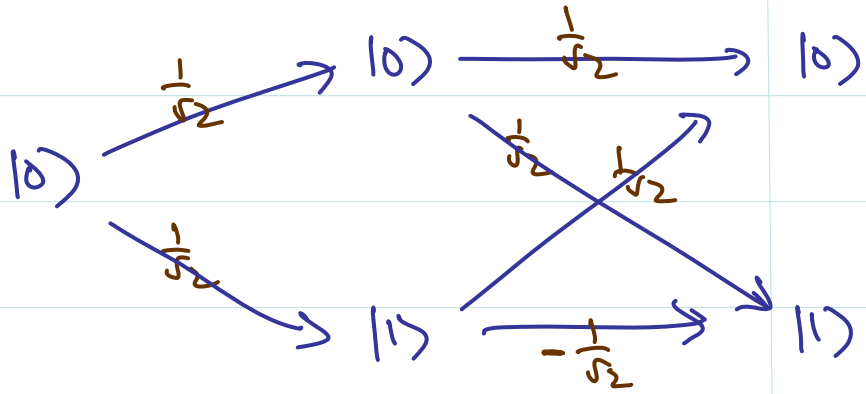
e.g. $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ same as random bit for measurement purposes

but <u>not</u> so for unitary evolution! – 0 & 1 are "simultaneously present."

Consider process: apply H to $|0\rangle$, then apply H again:

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{H} \frac{1}{\sqrt{2}}\left[\begin{array}{l} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array}\right] = |0\rangle$$

Depict as branching process relative to the basis & write amplitudes on arrows:



Note: 50/50 probab. mixture of $|0\rangle, |1\rangle$.

If apply H & measure, will see 0 or 1 with 50/50 probability – <u>no</u> "interference".

Feynman "sum over paths" rules:

For final amplitude of $|0\rangle$ (or $|1\rangle$)

look @ all paths from start to $|0\rangle$

- multiply amplitudes along path
- add up all paths
- final prob = $|\text{final amplitude}|^2$

} just like branching probability rules but here can have +ve & -ve (even complex) path contributions!

e.g. for HH $|0\rangle$ process

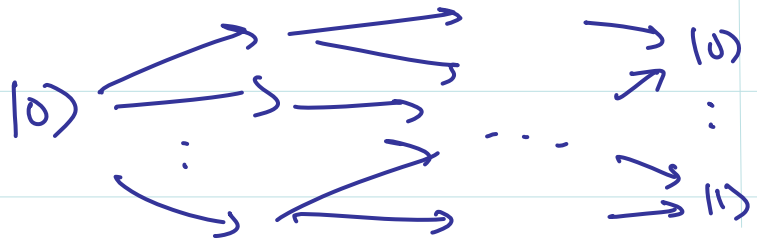
$|0\rangle \rightsquigarrow |1\rangle$ has two non-zero paths yet they cancel and this transition is forbidden! "destructive interference" $\frac{1}{2} - \frac{1}{2} = 0$, prob = 0

$|0\rangle \rightsquigarrow |0\rangle$ has two paths with amplitudes $\frac{1}{2} + \frac{1}{2} = 1$

so prob = $1^2 = 1$ "constructive interference".

↖ cannot simulate like probs, by making successive branch choices... !

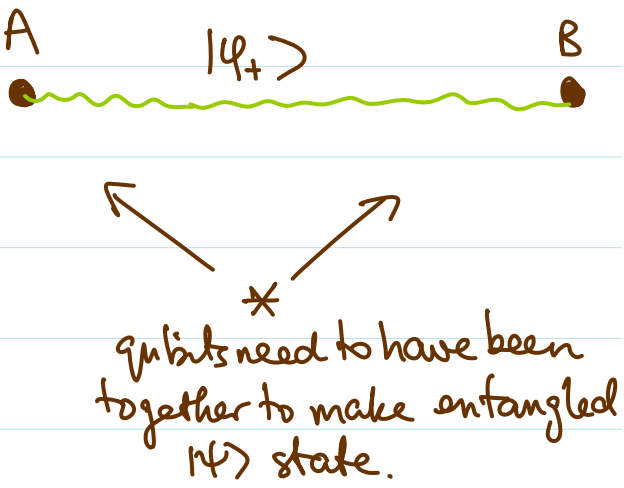
Similarly for any process of a sequence of gates



"many worlds"? ...

Quantum non-locality

$|\psi_+\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right]$



A measures her qubit:

outcome	prob.	post-mmt state (instantaneous!)
0	$\frac{1}{2}$	$\|0\rangle\|0\rangle$
1	$\frac{1}{2}$	$\|1\rangle\|1\rangle$

- So B's mmt outcome then fixed to be same as what A got!
- If A does not measure, B sees 0/1 with probs $\frac{1}{2}/\frac{1}{2}$. (ie a random bit)

So whether or not A measures, B locally sees same output!

ie. "non-signalling" – although description of B's state changes, no local physical effects change.

Is this a genuine non-local action? .... hmm..mm..um..

No! — can claim:

- Quantum state description is just a mathematical artifice
  - not physically "real" (after all, cannot measure identity of an unknown quantum state!)
- When particles were together they were given a perfectly correlated random bit (local h.v.) which is then output upon measurement!
  - explains all observed aspects of experiment and no non-local influences!

But: more complicated situation! ... —

In their separate labs A & B can apply $U(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ to their qubit before making measurements.

$M_A(\alpha)$: A applies $U(\alpha)$ and then measures.

$M_B(\beta)$: B applies $U(\beta)$ and then measures.

Easy calculation:

$$|\varphi_{\alpha\beta}\rangle \equiv U(\alpha)\otimes U(\beta)|\varphi_+\rangle = \frac{1}{\sqrt{2}}\left[\cos(\alpha-\beta)|00\rangle - \sin(\alpha-\beta)|01\rangle + \sin(\alpha-\beta)|10\rangle + \cos(\alpha-\beta)|11\rangle\right]$$

Then Born rule gives:

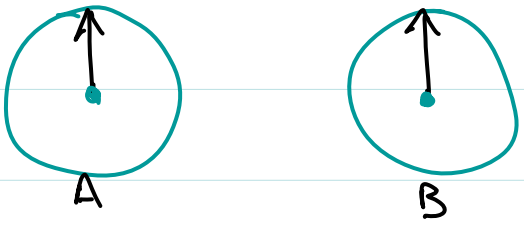
Fact 1: Measuring either qubit of $|\varphi_{\alpha\beta}\rangle$ gives 0 or 1 with probs $\frac{1}{2}, \frac{1}{2}$.

Fact 2: If measure both qubits of $|\varphi_{\alpha\beta}\rangle$ (either order, or simultaneously) then Prob(outcomes differ) = Prob(01 or 10) = $\sin^2(\alpha-\beta)$.

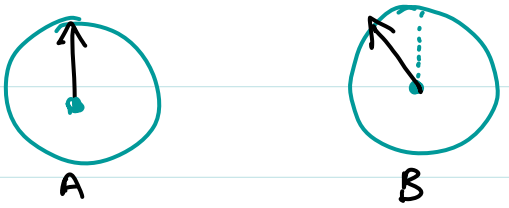
Now use only $\alpha, \beta = 0°, \pm 30°$

Do long sequence of experiments. A & B get strings of measurement outcomes.

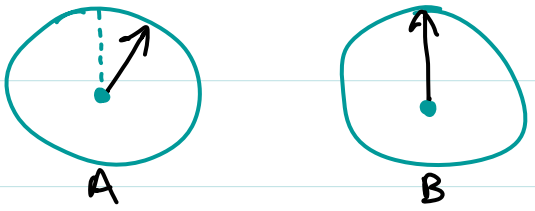
$M_A(0°)\ M_B(0°)$ $\quad Pr(\text{differ}) = 0$



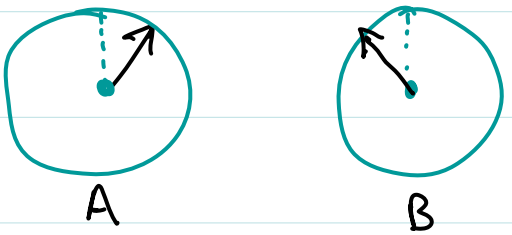
$M_A(0°)\ M_B(-30°)$ $\quad Pr(\text{differ}) = \frac{1}{4}$



$M_A(30°)\ M_B(0°)$ $\quad Pr(\text{differ}) = \frac{1}{4}$



$M_A(30°)\ M_B(-30°)$ $\quad Pr(\text{differ}) = \frac{3}{4}$



Locality assumption: mmt outcomes at A (resp. B) are not influenced by the mere choice of settings at B (resp. A).

- inconsistent with above data!
- actually observed in real experiments.

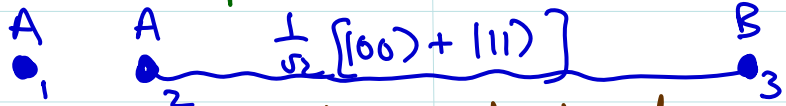
so even if quantum theory is "wrong", nonlocal (but non-signalling) influences are a feature of actual physical reality!

Really? May still object! –

needed counterfactual arguments, and could demand–

"unperformed experiments have no outcomes!"

Quantum teleportation



$|\alpha\rangle = a|0\rangle + b|1\rangle$

unknown qubit state

shared entanglement

A wants to transmit $|\alpha\rangle$ to B.

- 2-qubit orthonormal Bell basis:

$$|\phi_\pm\rangle = \frac{1}{\sqrt{2}}\left[\,|00\rangle \pm |11\rangle\,\right]$$

$$|\psi_\pm\rangle = \frac{1}{\sqrt{2}}\left[\,|01\rangle \pm |10\rangle\,\right]$$

- Bell measurement on qubits 1 & 2:

Apply $CNOT_{12}$, then H_1, then measure both qubits → output $i\,j$.

rotates Bell basis into standard basis.

Quantum teleportation protocol

1) A performs Bell mmt on her two qubits
2) A sends her 2-bit classical outcome ij to B
3) B applies $U = X^j Z^i$ to his qubit.

ij always uniformly random 2-bit string for any $|\alpha\rangle$!

Then B's qubit is in state $|\alpha\rangle$ with certainty!

A is left with no info about $|\alpha\rangle$ at all only a uniformly random $|00\rangle, |01\rangle, |10\rangle$ or $|11\rangle$ state.

c.f. no cloning. (stronger form...)

Proof – easy direct calculation:

$$|\alpha\rangle|\phi_+\rangle = (a|0\rangle + b|1\rangle)\left(\tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|11\rangle\right)$$

$$= \tfrac{1}{\sqrt{2}}\left[a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\right]$$

$\xrightarrow{\text{CNOT}_{12}\text{ then }H_1 \text{ \& re-arrange}}$

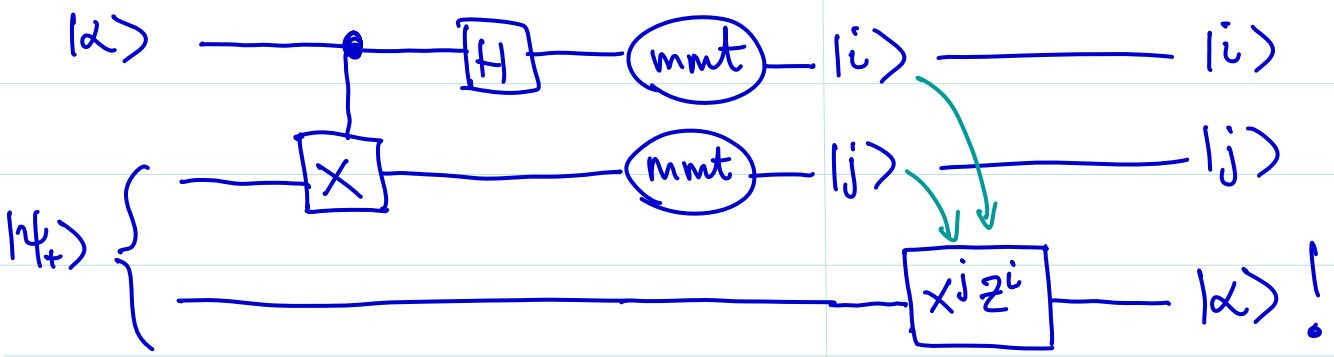
$$\tfrac{1}{2}\Big[|00\rangle(a|0\rangle+b|1\rangle) + |01\rangle(b|0\rangle+a|1\rangle) + |10\rangle(a|0\rangle-b|1\rangle) + |11\rangle(-b|0\rangle+a|1\rangle)\Big]$$

$I|\alpha\rangle$ $X|\alpha\rangle$ $Z|\alpha\rangle$ $ZX|\alpha\rangle$

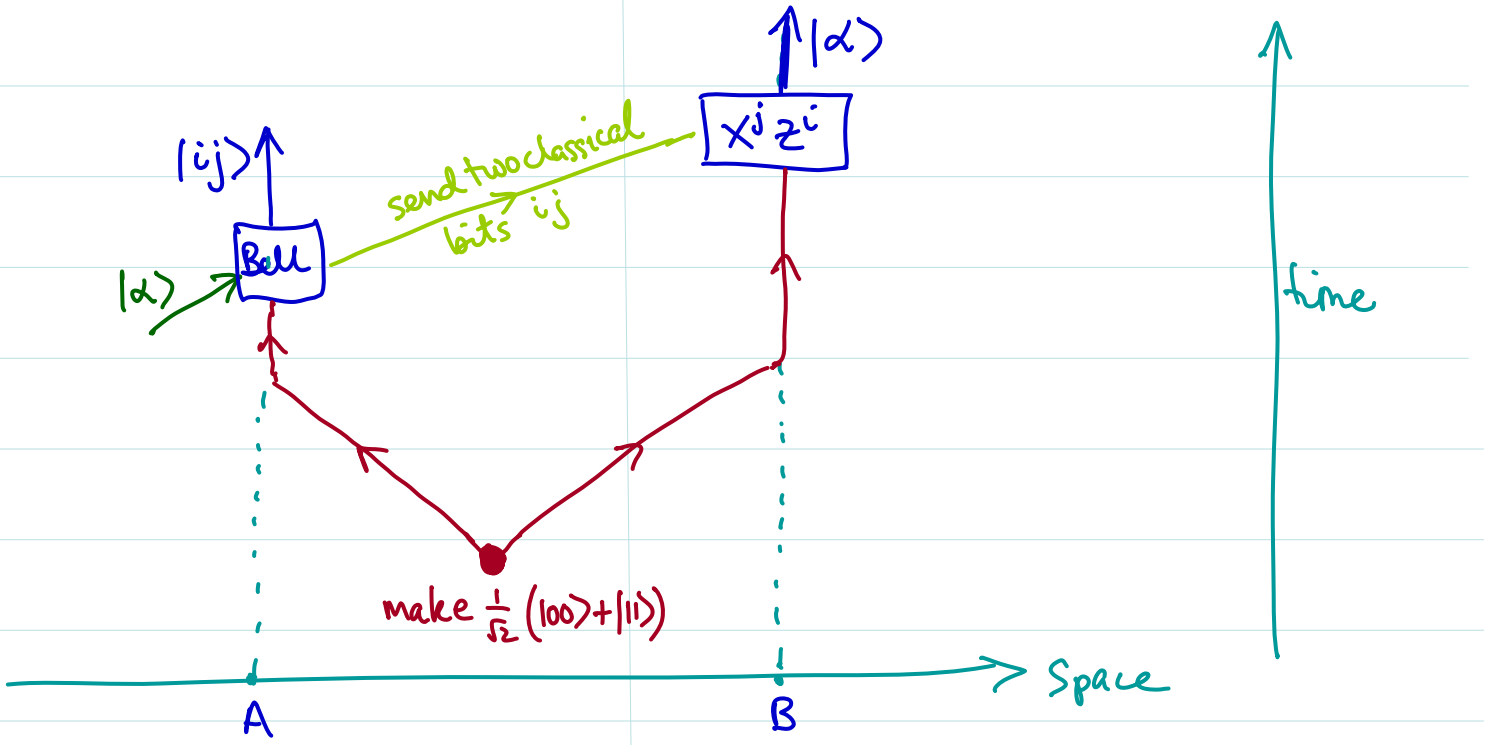
$$= \frac{1}{2}\sum_{i,j} |ij\rangle_{12} Z^i X^j |\alpha\rangle_3$$

So B should then apply $(Z^i X^j)^{-1} = X^j Z^i$.

Teleportation as a circuit diagram



Teleportation — spacetime diagram



How does $|\alpha\rangle$ get across? Cannot measure $|\alpha\rangle$ but can have verifier/preparer...

Channel for its propagation? 2-bits not enough!...

Backwards in time? — Backward propagated state is totally random, so not inconsistent!... hmm...