A Quantum of Quantum Computing

Cora Barrett
Om Joshi
Hyo Sun Park
Ági Villányi
Matt Yeh

IAP 2025: MIT Quantum Winter School

Contents

Entanglement

> *Anybody who's not bothered by Bell's theorem has to have rocks in his head.*
>
> -Some Princeton guy, to David Mermin

Locality and Realism

Locality: cannot influence faster than speed of light
Realism: physical properties are inherent, independent of observation or measurement. Confusing name that leads to misleading reporting in popular media. Better statement is that any apparent measurement-dependence is because we do not have all the possible information, i.e. there are *hidden variables* that obscure the "true" nature of physical system.
Non-locality: Violation of Bell's inequalities shows quantum mechanics is not locally real, i.e. local hidden variable theories do not adequately describe physics.

Loopholes

The implications of Bell's theorem cannot be understated. By providing a statistical limit on correlations possible in a local hidden variable theory, the very foundations of quantum mechanics as a nondeterministic theory can be experimentally tested. Indeed, the 2022 Nobel Prize in the Physics was awarded for significant contributions to experimental violations of Bell's inequality, convincing much of the scientific community of the invalidity of local hidden-variable theories.

However, various "loopholes" have been proposed that could "coincidentally" lead to seeming Bell inequality violations, increasingly philosophical in nature. The primary ones that experimentalists are concerned with are the "locality" and "detection" loopholes:

1. (Locality) In principle, the two recipients (detectors) could "cheat" and communicate their results to each other to spoof the quantum correlations. This loophole is closed by having the measurement settings changed randomly. Moreover, by sufficiently spatially separating the two recipients and changing the measurement settings fast enough, communication at or below the speed of light can be excluded.

2. (Detection) In principle, if the detector efficiencies are not sufficiently high, quantum correlations could be spoofed by only sampling a portion of the results (unfair sampling). This was closed after great engineering efforts in developing near-unit efficiency detectors.

The first "loophole-free" experiments were reported in 2015, although researchers continue to attempt to close more exotic loopholes and with ever greater statistical certainty.

Ekert91 Protocol for Quantum Key Distribution

Although QKD protocols like BB84 provide information-theoretic security, practical implementations may be exploited by a number of attacks. We have already discussed "intercept-and-resend," which can be detected to a certain threshold due to the no-cloning theorem. However, it is often more convenient to use attenuated laser pulses that *approximate* single photons, rather than true single photons. It can be derived that such a state, known as a "weak coherent state," follows a Poisson distribution in photon number n

$$P(n) = e^{-\langle N \rangle} \frac{\langle N \rangle^n}{n!} \tag{1}$$

where $\langle N \rangle$ is the average photon number. Thus, even when the average photon number is small ($\langle N \rangle \ll 1$) and "mostly"' single-photon, there is always a Poisson tail that includes multiphoton events. This opens up the possibility of an eavesdropper Eve peeling off and storing part of a multiphoton pulse until Alice and Bob reveal their measurement bases, at which point Eve would also be able to measure their stored part of the pulse in the correct basis.

Such a "photon number splitting" attack can be specifically mitigated by switching to true single-photon sources. However, it is illustrative that limitations in practical implementations can break down the security of QKD. More generally, discrepancies between how quantum devices are modeled to work vs how they actually operate can be exploited, i.e. small changes to device calibration (perhaps from an eavesdropper) can be hard to detect.

It may seem contrived, but Bell tests inherently provide verification of the quantum nature of the key distribution. Entanglement bounds the information that an adversary can gain, therefore embedding communication security even if the quantum devices are imperfect. Such a protocol was originally described by Artur Ekert in 1991:

1. Alice and Bob each receive one photon from an entangled photon pair in the singlet Bell state $|\Psi^-\rangle$, perhaps sourcing from a trusted third party.

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B) \tag{2}$$

2. Alice and Bob then measure their photons, picking the measurement basis randomly. For ease of visualization we use the typical polarization encoding $|0\rangle \rightarrow |H\rangle$, $|1\rangle \rightarrow |V\rangle$ so that the measurement bases correspond to polarizer angles. Then, Alice picks from the angles $\{0°, 22.5°, 45°\}$ and Bob from $\{0°, 22.5°, 67.5°\}$.

3. The key idea here is twofold. 1) The singlet state is invariant under rotations. 2) Therefore, as long as Alice and Bob match bases, their measurements will be perfectly anticorrelated. Alice and Bob thus reveal their measurement bases.

4. For the instances where Alice and Bob had mismatched measurement bases, they use their results to compute a Bell test. Hence the choice of measurement angles: $A \in \{0°, 45°\}$ and $B \in \{22.5°, 67.5°\}$ can be shown to give the biggest violation of Bell's inequality. If Bell's inequality is violated, then the measurement can be certified secure by quantum mechanics.

5. The remaining results with matched bases can then be used to compute a secret key.

Exercise for the reader: Check that the singlet state $|\Psi^-\rangle$ is invariant under rotation. Does this hold for the other Bell states?

Quantum Teleportation

Unfortunately for Mr. Einstein, Bell tests so have far have shown much greater support for "spooky action at a distance" than not. However, this would appear to conjure up an opportunity to transfer information across great spatial separations. Indeed, this forms the basis of *quantum teleportation*.

Although the name is suggestive of object transfer, it is a bit misleading. Perhaps a more precise name would be quantum *information* teleportation. The protocol is as follows:

1. Alice and Bob each receive one qubit of a Bell pair.

2. Alice wants to transfer a qubit $|\phi\rangle_A = \alpha|0\rangle + \beta|1\rangle$ to Bob, perhaps over a great spatial distance. In other words, Bob should end up with qubit

$$|\phi\rangle_B = \alpha|0\rangle + \beta|1\rangle$$

that can be manipulated, measured, etc. in the same way as Alice's qubit $|\phi\rangle_A$.

3. Because Alice has two qubits, they can perform a *Bell measurement* on them, as if one were trying to determine which of the four Bell states the two Alice qubits are in.

4. Half of the time, this turns out to send Bob's qubit into a superposition that, within a local phase flip, looks like $|\phi\rangle_A$:

$$|\phi\rangle_B = \alpha|0\rangle \pm \beta|1\rangle$$

Thus, Bob can apply a Z gate if needed to bring $|\phi\rangle_B$ to the desired superposition. What about the other half of the time? The result is a little more complicated

$$|\phi\rangle_B = \alpha|1\rangle \pm \beta|0\rangle$$

but it can be seen that with judicious application of an additional bit-flip (X gate), this becomes identical to the previous case requiring a local phase flip.

5. How does Bob know whether or not to apply an X or Z gate? It turns out that the bit-flip and relative phase depends on which of the four Bell states Alice got. Thus, Alice also needs to transfer two *classical* bits, corresponding to the measurement results from Step 3.

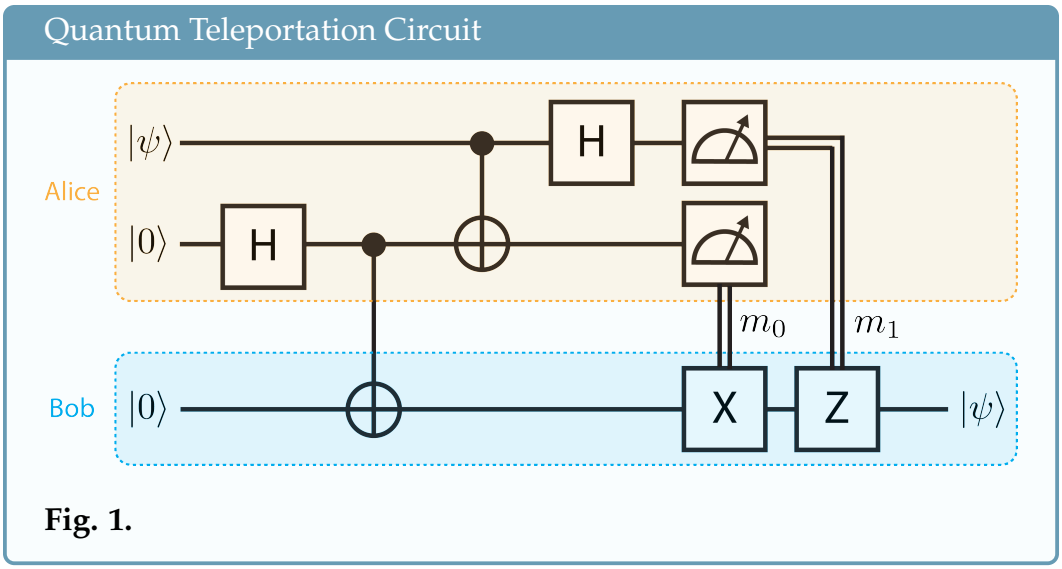

Fig. 1.

Of course, one could conceive of simply sending a $|\phi\rangle$ encoded photon to Bob. The key is that with quantum teleportation, Alice never even has to do that! Remember, the Bell pair could be coming from someone else entirely, a third party. Instead, Alice only ever needs to transmit classical information to Bob (which unfortunately, does limit the communication to the speed of light).

It might seem like this protocol appears out of nowhere. The key intuition here is that the four Bell states form a complete basis for a two-qubit composite system. Thus, even though Alice's qubits may not be in a maximally-entangled state, they can always be decomposed into a superposition of Bell states. Roughly speaking, this suggests the full Alice-Bob three-qubit composite system may be able to be factorized as a tensor product of the Alice Bell-state decomposition, times Bob's qubit, with weights related to $|\phi\rangle_A$. Measurement then projects Bob's qubit into the desired state.

Mathematically, this is not precisely the case, but it is quite related. Suppose the shared entangled state is the Bell state $|\Phi^+\rangle$. Then the full composite system is given by:

$$|\phi\rangle_A |\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(\alpha |0\rangle_A \pm \beta |1\rangle_A)(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) \tag{3}$$

where the subscripts indicate whom the qubits belong to. Then, decompos-

ing Alice's qubits in the Bell basis, we obtain

$$\begin{aligned}|\phi\rangle_A |\Phi^+\rangle_{AB} = \frac{1}{2}[&|\Phi^+\rangle_A (\alpha |0\rangle_B + \beta |1\rangle_B) \\ &+ |\Phi^-\rangle_A (\alpha |0\rangle_B - \beta |1\rangle_B) \\ &+ |\Psi^+\rangle_A (\alpha |1\rangle_B + \beta |0\rangle_B) \\ &+ |\Psi^-\rangle_A (\alpha |1\rangle_B - \beta |0\rangle_B)] \end{aligned} \tag{4}$$

In both a mathematical and physical sense, the probability amplitudes of $|\phi\rangle_A$ "transfer over" to Bob's qubit. It is clear then that each Bell state is associated with a particular Bob qubit state that needs to be communicated to ensure the proper phase relation between $|0\rangle_B$ and $|1\rangle_B$.

We summarize the four possible Bell state measurement results for Alice and Bob's required manipulations in the following table:

Alice's Result	Bob's state	Bob's state (in terms of $\|\psi\rangle$)	Bob applies
$\|\Phi^+\rangle$ (00)	$\alpha\|0\rangle + \beta\|1\rangle$	$\|\psi\rangle$	$\mathbb{1}$
$\|\Psi^+\rangle$ (01)	$\alpha\|1\rangle + \beta\|0\rangle$	$X\|\psi\rangle$	X
$\|\Phi^-\rangle$ (10)	$\alpha\|0\rangle - \beta\|1\rangle$	$Z\|\psi\rangle$	Z
$\|\Psi^-\rangle$ (11)	$\alpha\|1\rangle - \beta\|0\rangle$	$XZ\|\psi\rangle$	ZX

Entanglement Swapping

Is quantum teleportation really useful for anything? Again, surely it would be easier to just directly transmit a photonic qubit between Alice and Bob.

Alas, reality is often disappointing. The biggest limiting factor in quantum communication is transmission loss, which grows exponentially with distance. Although amazing work has been done to make optical fiber low-loss (another Nobel prize!), the transmission still drops by 50% every 15 km. At a certain point, there are essentially zero photons being detected per unit time, which would appear to severely limit the distances over which quantum information can practically be shared and networked.

Teleportation provides an out. The key insight is that there's no particular reason state teleportation only has to occur between two parties, i.e. Alice transmits a qubit to Bob. If a third person in the middle could teleport an entire entangled pair, shared between Alice and Bob, then that could cut the required transmission distance in half. Repeat this *ad infinitum*, and any distance can be crossed to distribute entanglement. In essence, the person in the middle acts as a *quantum repeater*, refreshing the entanglement every so often.

The way this is implemented uses a very similar strategy to the standard teleportation protocol.

1. Alice and Bob each prepare a Bell pair and sends one of their qubits to a Repeater.

2. The Repeater performs a Bell measurement, and transmits the results classically to Alice and Bob.

3. Within a local rotation (informed by the previous results), the qubits that Alice and Bob held onto are now entangled in the desired Bell state.

Entanglement swapping

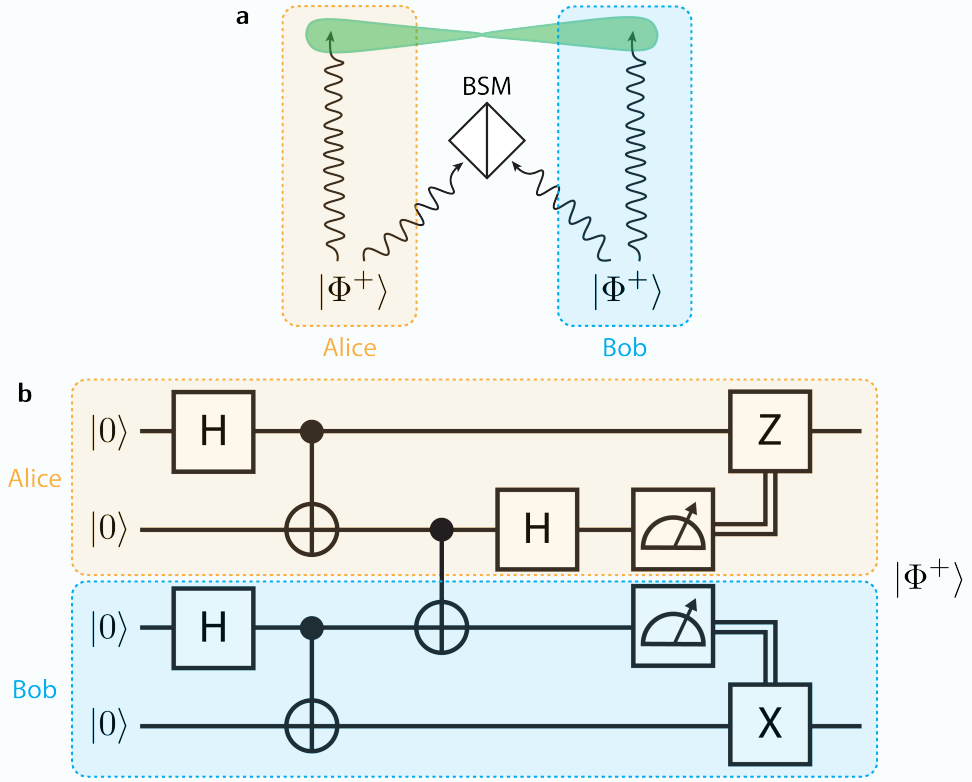

Fig. 2.

Once again, by performing a Bell measurement, Alice and Bob's qubits get projected into the desired state–an entangled pair. Because Alice and

Bob can now share entanglement despite their qubits having never interacted before, this is known as *entanglement swapping*.

Exercise for the reader: Verify the entanglement swapping protocol mathematically. Start with Alice and Bob each having Bell states $|\Phi^+\rangle_A$, $|\Phi^+\rangle_B$.

Measurement-based Quantum Computation

> *I would like to thank A. White, whose constant discourse on "mode-matching" formed a primary source of irritation for this work.*
>
> -Terry Rudolph, *Resource-Efficient Linear Optical Quantum Computation*

So far we have been concerned with quantum teleportation as a means of information transfer. None of this, however, strictly is concerned with computation. In this section, we will introduce an alternate strategy to achieve a universal quantum computer. While circuit models of quantum computing typically apply a series of gates serially, generating entanglement as needed, *measurement-based quantum computing* instead seeks to start with a large entangled state as a resource. Measurements are then applied to certain qubits in the large-scale entangled state, destroying them. The output is the quantum state that the remaining qubits are left in.

It turns out that this approach can exactly simulate quantum circuits. Thematically, the secret is once again quantum teleportation–the action of measuring a qubit in different bases ripples across the entire entangled state.

We begin with the following circuit, which nominally looks similar to the teleportation circuit, except there are only two qubits involved:

One bit teleportation

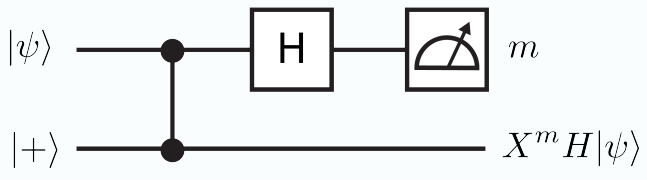

Fig. 3.

Remarkably, the output state is related (up to a unitary transformation) to $|\psi\rangle$–teleportation! If that were it though, we would not have much to build a quantum computer off of. The key is to add an additional rotation, $R_z(\theta)$, that changes the basis we measure the first qubit in.

Generalizing one-bit teleportation

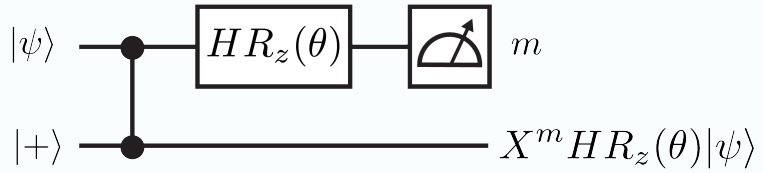

Fig. 4.

Evidently, doing so acts that unitary transformation on the second qubit. And because we already started with large-scale entanglement as a resource, we essentially have met our universal gate set criteria of single-qubit unitaries and an entangling gate.

Let's reinforce this notion by building up the example of simulating a single qubit quantum circuit. Consider the following:

Simulating quantum circuits with one-bit teleportation

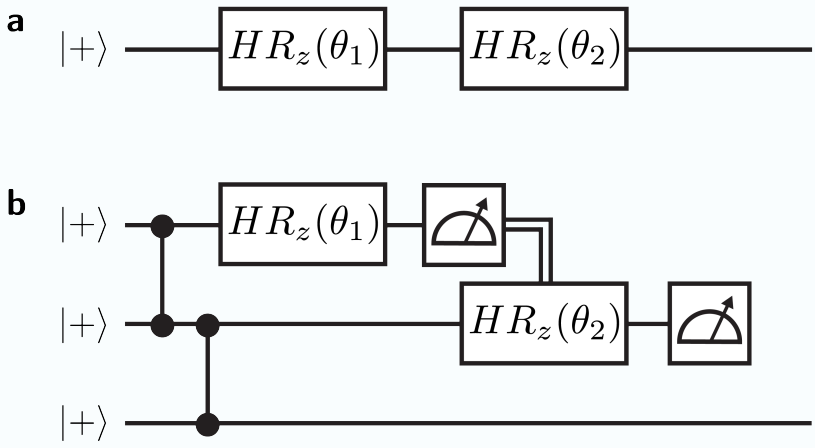

Fig. 5.

This circuit is equivalent to breaking apart the two single-qubit gates into two single-qubit teleportations. To convert this into a measurement-based computation on a single graph state, we note that we may commute the controlled-phase gates so that these entangling operations occur at the very beginning of the operation.

Equivalency to measuring an initial graph state

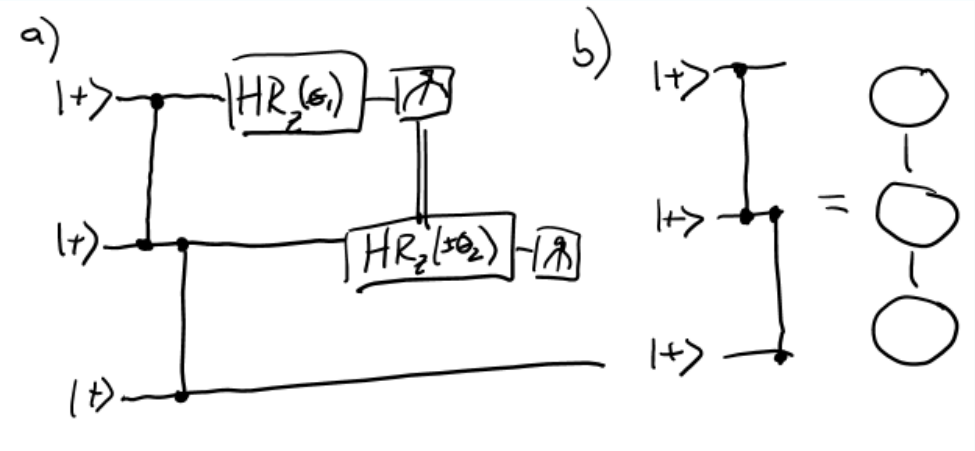

Fig. 6.

The measurements can then be seen as acting on an initial large-scale entangled state. We can map this to a so-called *graph state*: each vertex is a qubit in the $|+\rangle$ state, and each edge corresponds to a controlled-phase operation. The single-qubit circuit can then be realized as a time-ordered series of measurements (marked by labels t_i) on vertices of the graph state.

Measurement-based quantum computation

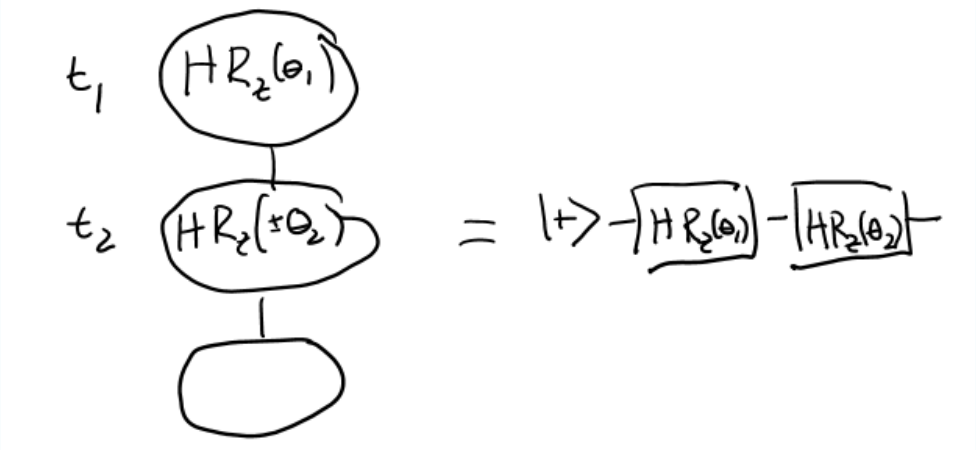

Fig. 7. text here

This method is not restricted to single-qubit operations. We leave the multi-qubit generalization as an exercise for the reader.

Entropy

Relationships are going toward entropy.

-Taylor, *Love is Blind*, Season 7

At this point we have introduced many examples of how to manipulate quantum information. But it is worth stopping for a moment to ask ourselves, "How do we actually quantify how much information we can encode and convey?" This is the field of *information theory*.

Let's start with an everyday example. It is spring time in Boston, and someone comes to visit you. They say, "It is raining today."

As the adage goes, "April showers bring May flowers" – it is not really surprising to you that it is raining in spring in New England. The person might as well not have said anything; not much information was conveyed.

However, what if it was in the middle of summer and sunny outside? The same person says "It is raining today". You get the sense that maybe a weird weather pattern is coming in, or you realize you didn't check the weather in the morning, or you regret not bringing an umbrella. In other words, you are surprised, and as a result more information has been transferred by the same number of words.

To turn this into a quantifiable measure of information, we need to be more precise. Why were the same words more surprising in the second case? It is because *the probability is lower* that it would be raining in the middle of summer. We should then strive to find a mathematical function that monotonically increases as the probability goes lower. It turns out that a mathematically convenient function that does precisely this is the logarithm

$$S \propto \log 1/p. \tag{5}$$

We call this measure of information the *entropy*, denoted here by S. Incidentally, this gives an alternative perspective on such statements you might have heard like "Entropy always increases." By definition, things are more likely to settle into their most probable state.

Bibliography