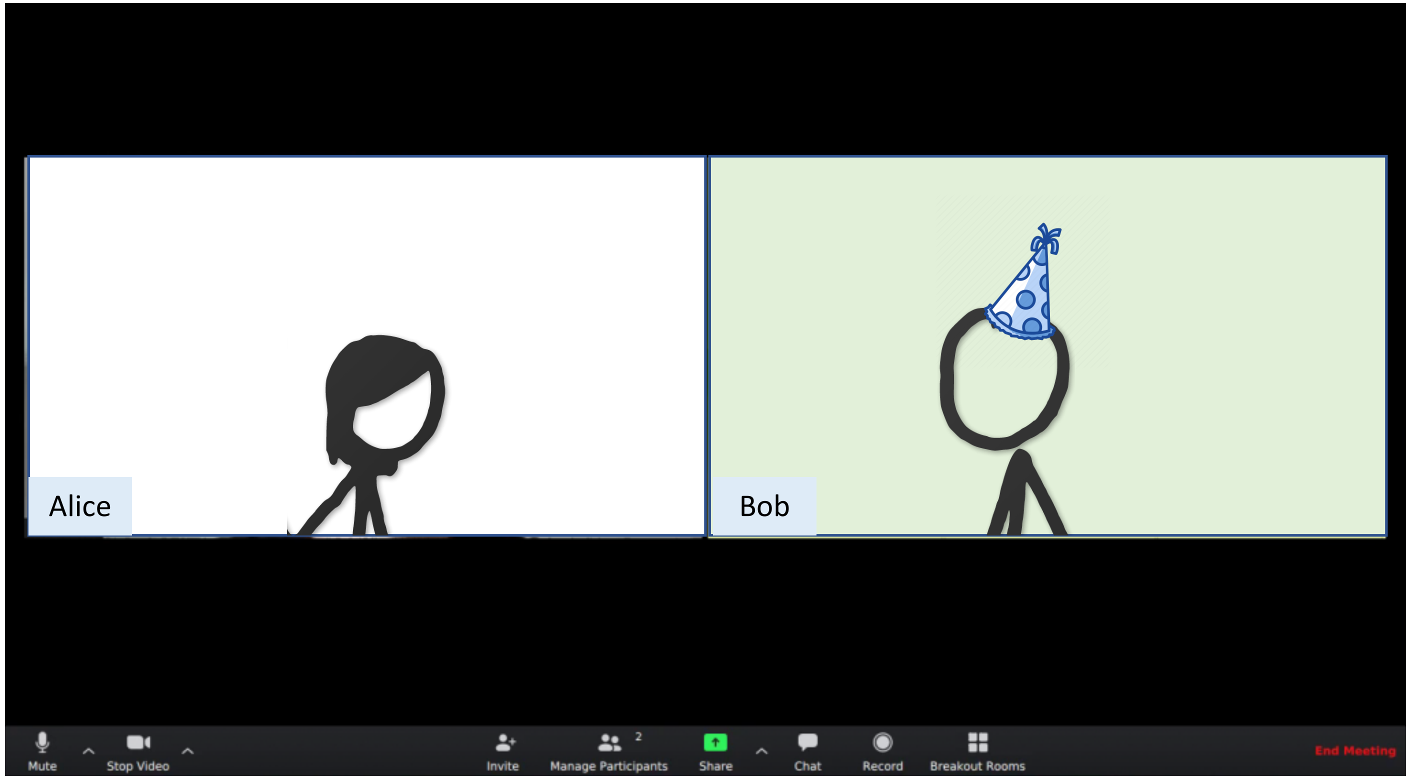
Crash Course in Quantum Computing

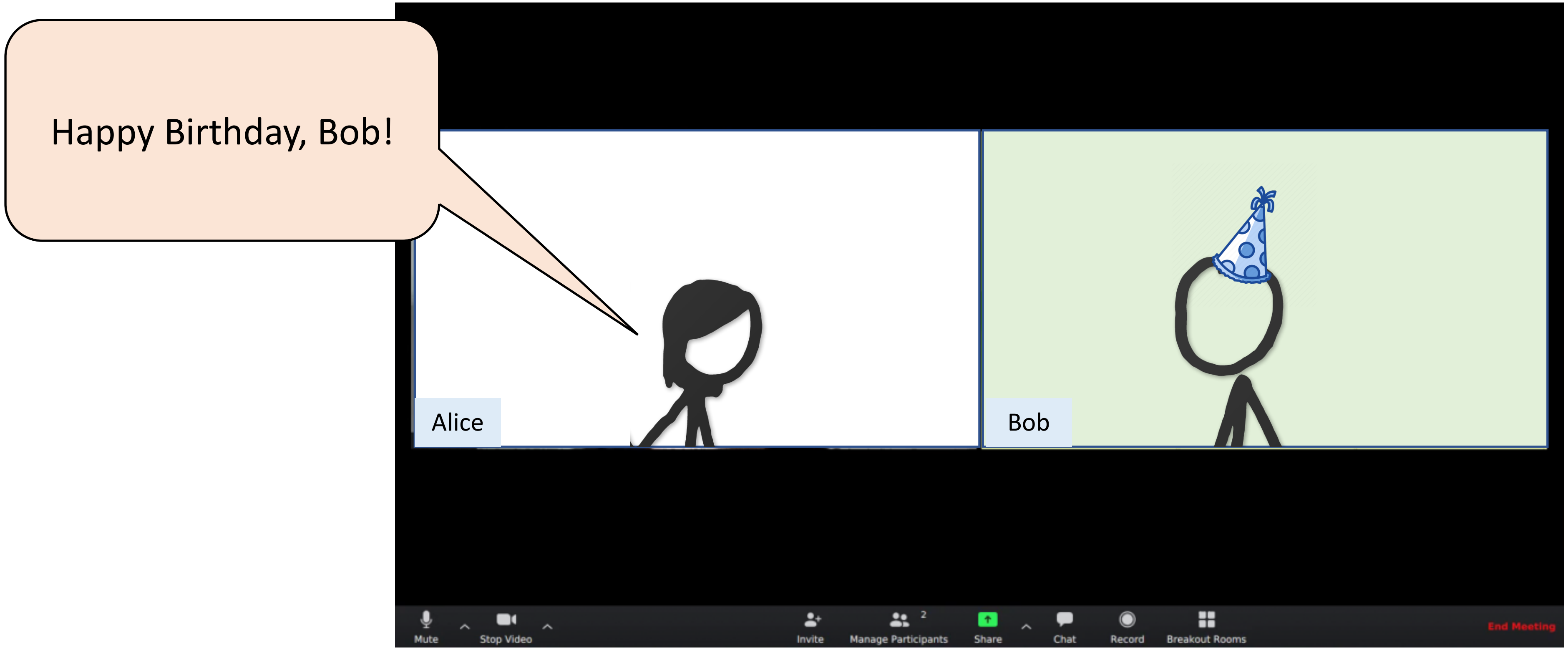
Hour 2: Quantum Computation

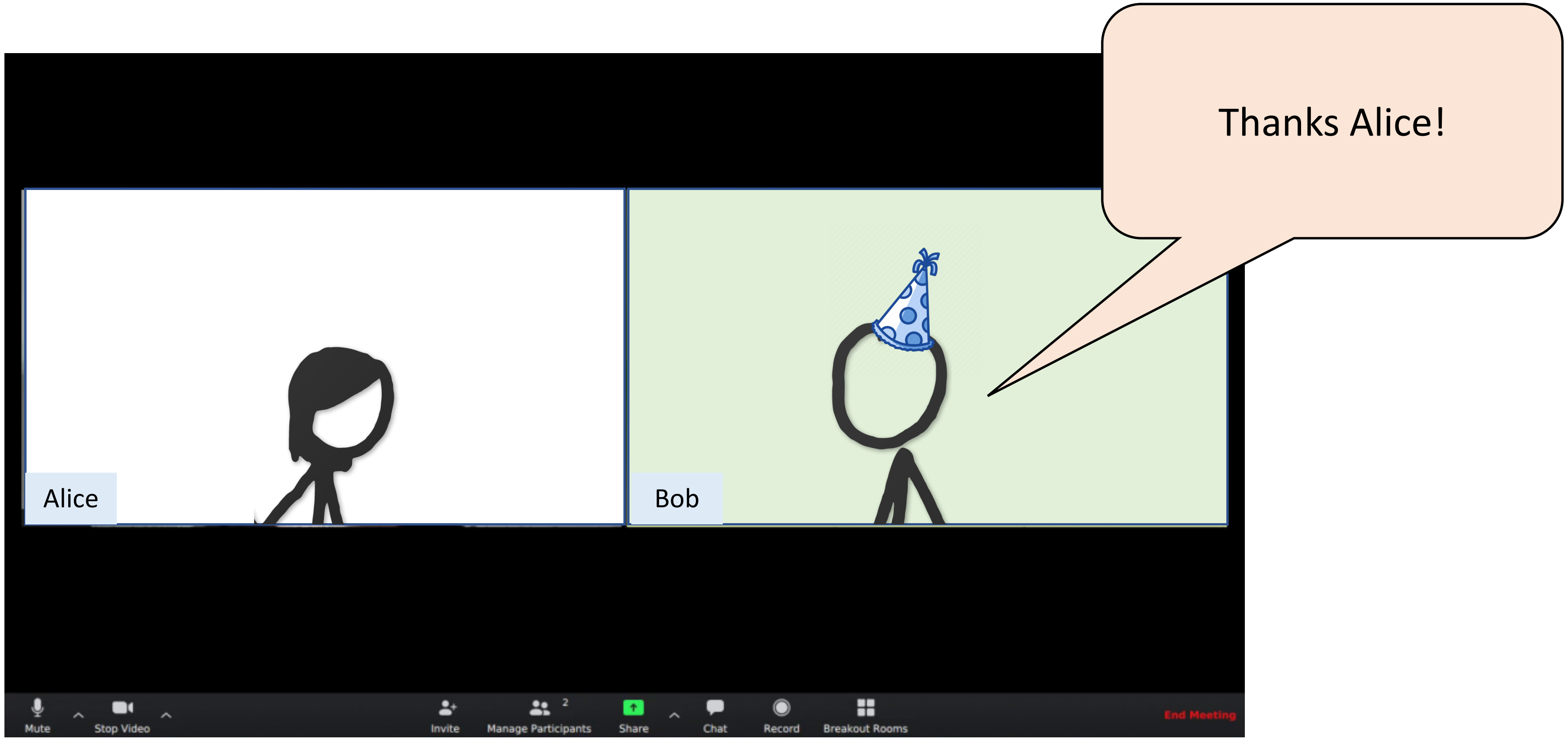
BIU Winter School on Cryptography 2021

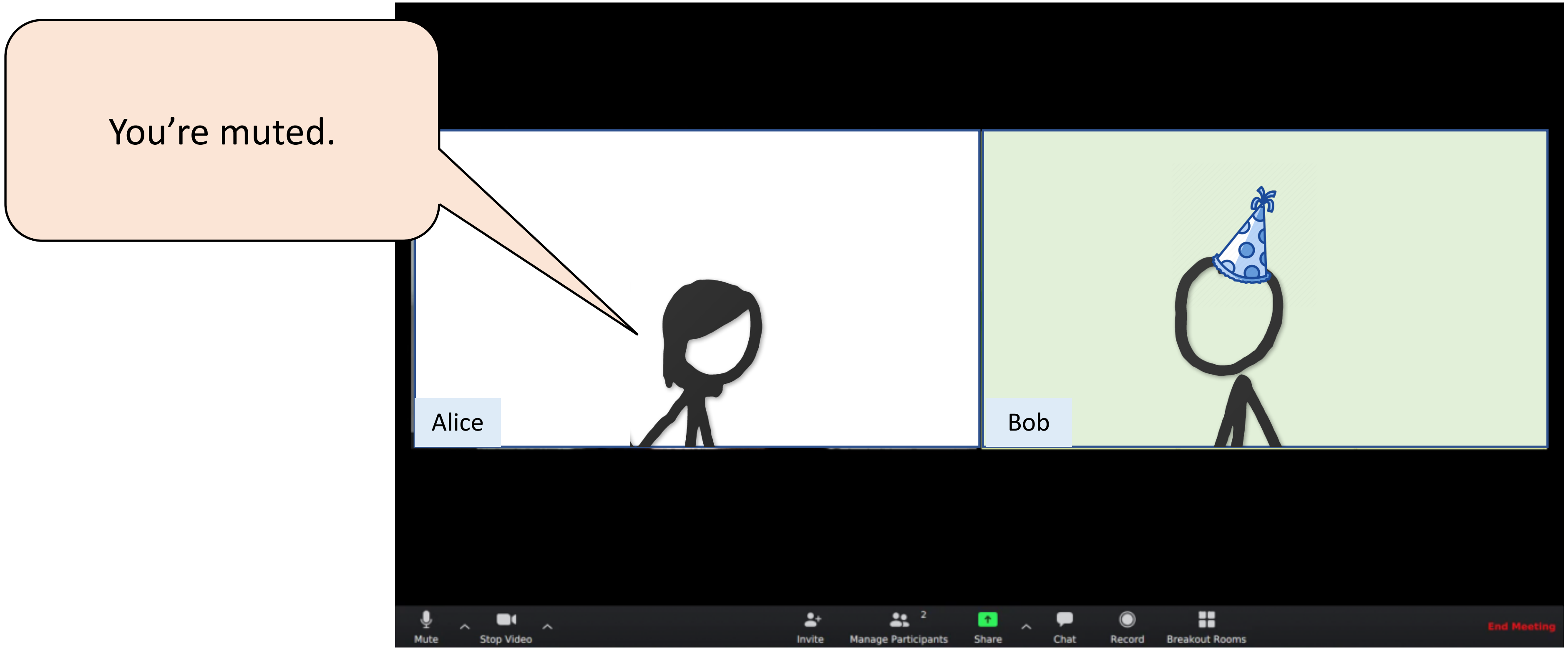
Lecturer: Henry Yuen

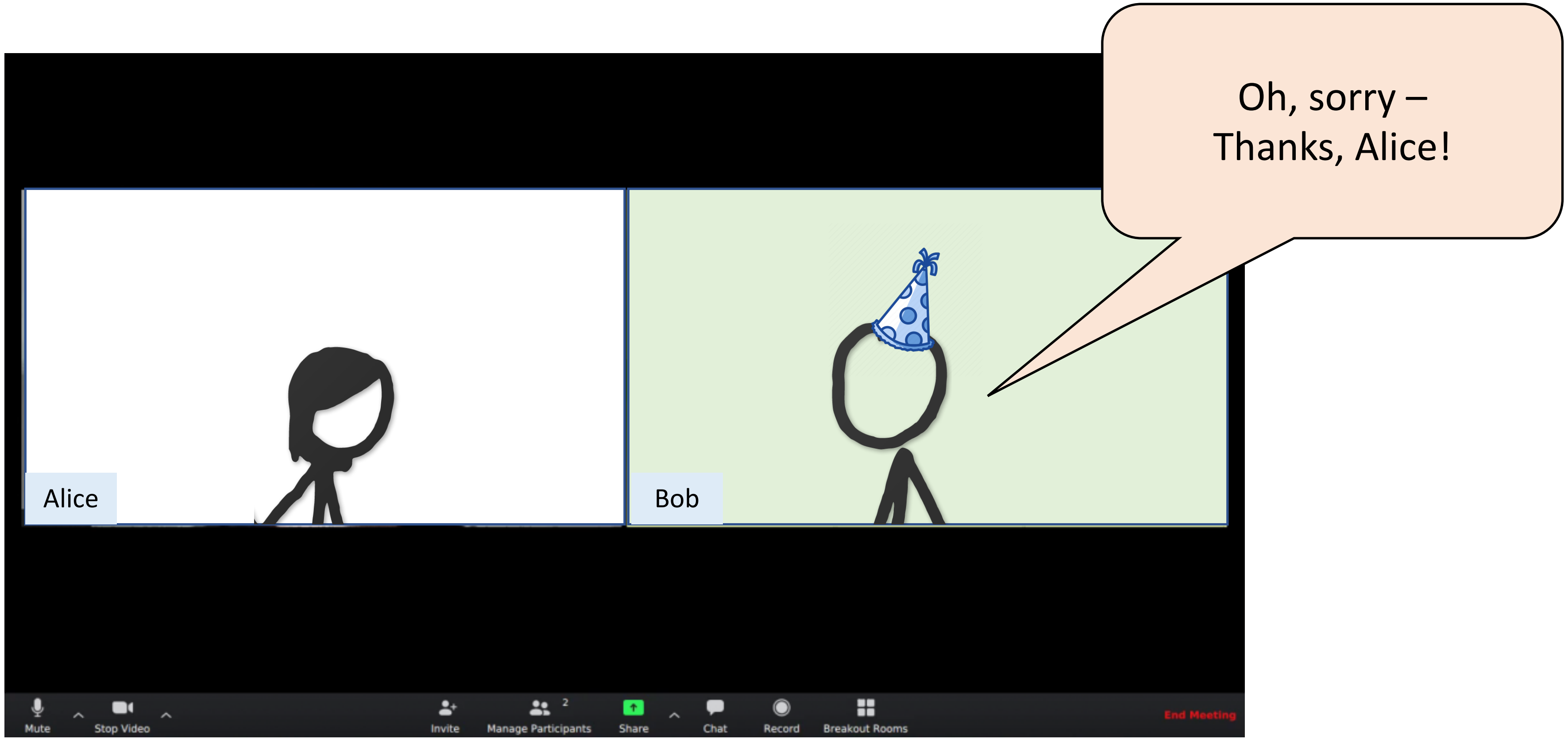


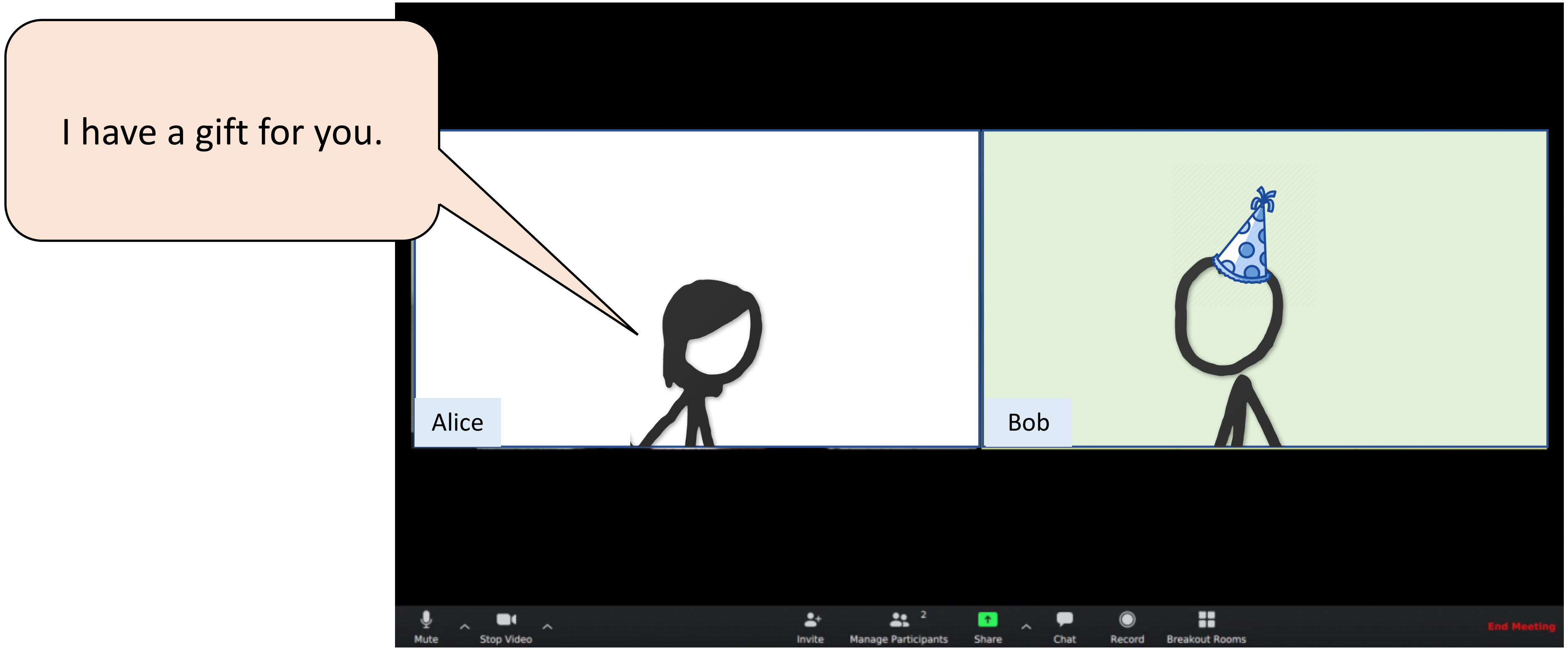
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
2
Share
Chat
Record
Breakout Rooms
End Meeting

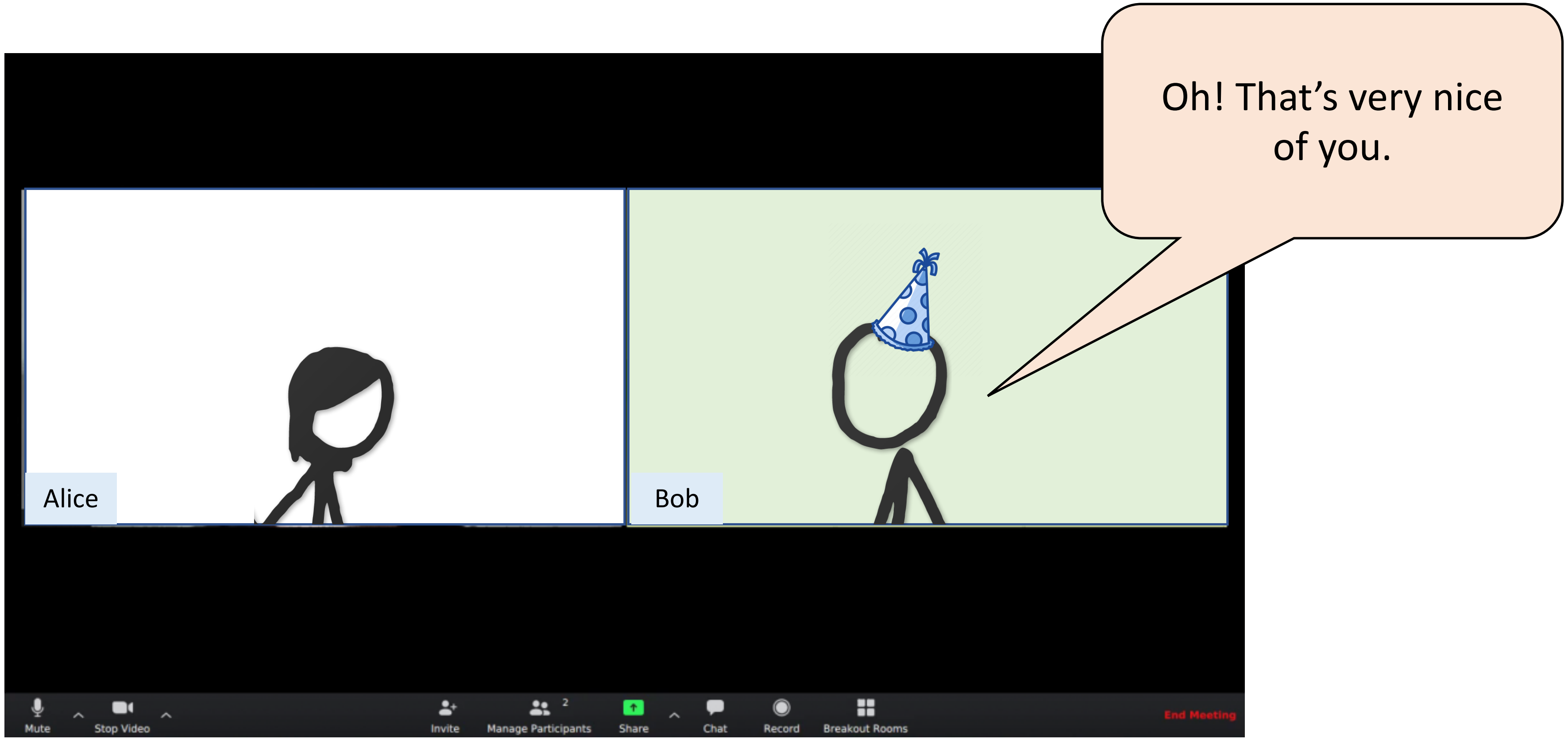

Happy Birthday, Bob!
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
Share
Chat
Record
Breakout Rooms
End Meeting

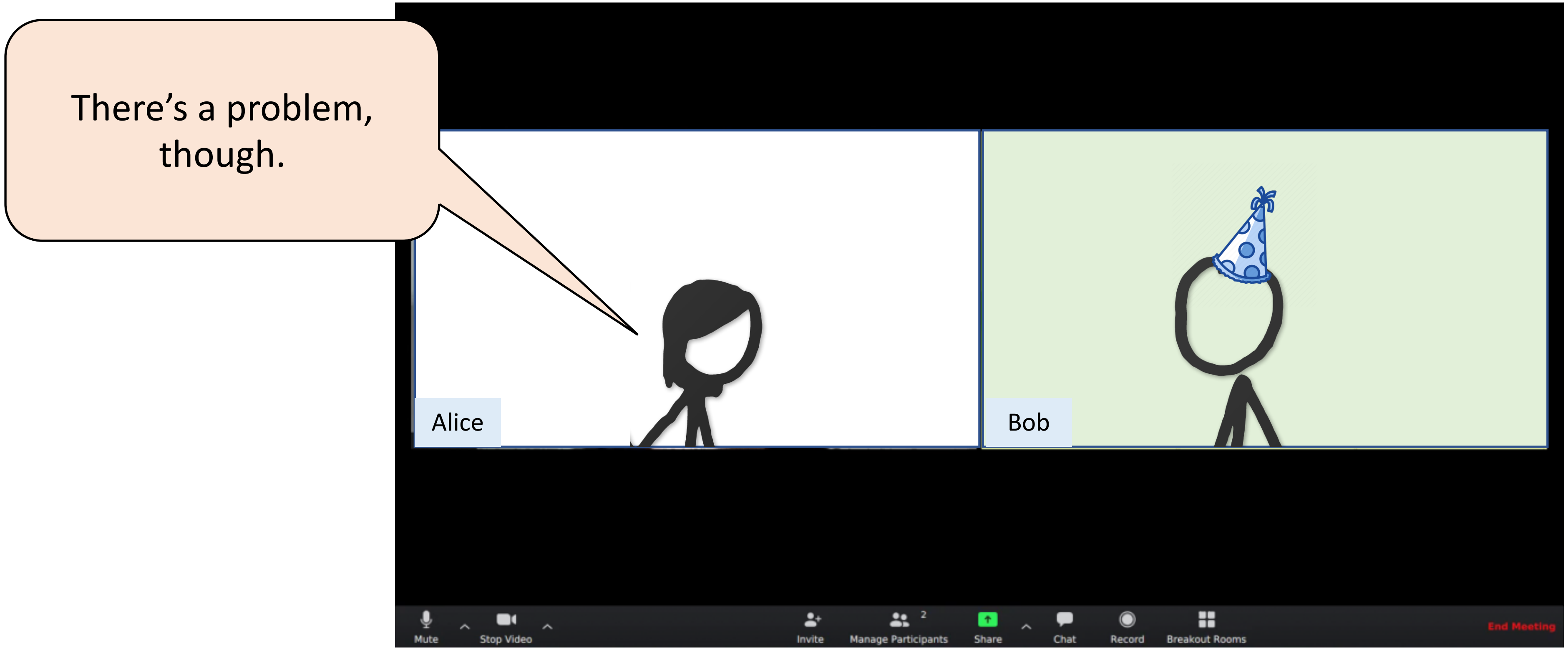

Thanks Alice!
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
Share
Chat
Record
Breakout Rooms
End Meeting


You're muted.
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
Share
Chat
Record
Breakout Rooms
End Meeting

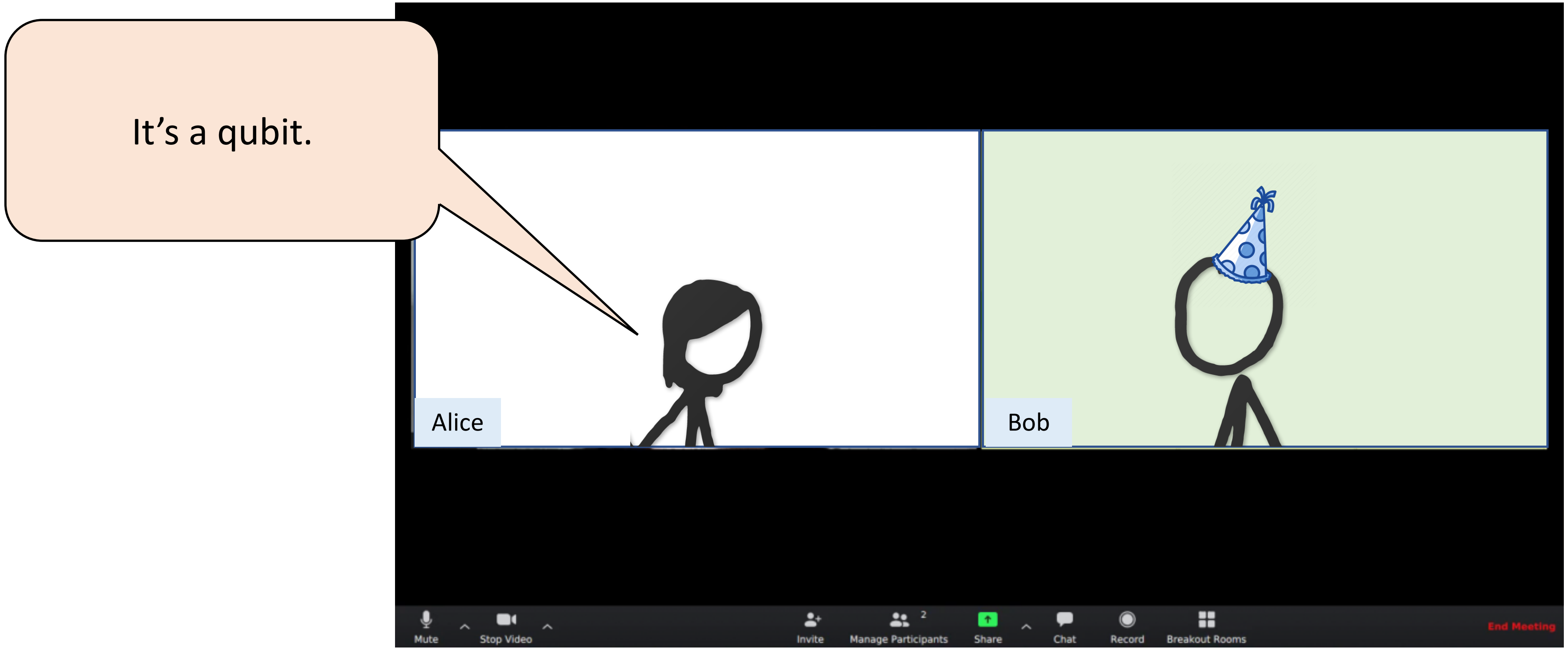

Oh, sorry –
Thanks, Alice!
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
Share
Chat
Record
Breakout Rooms
End Meeting

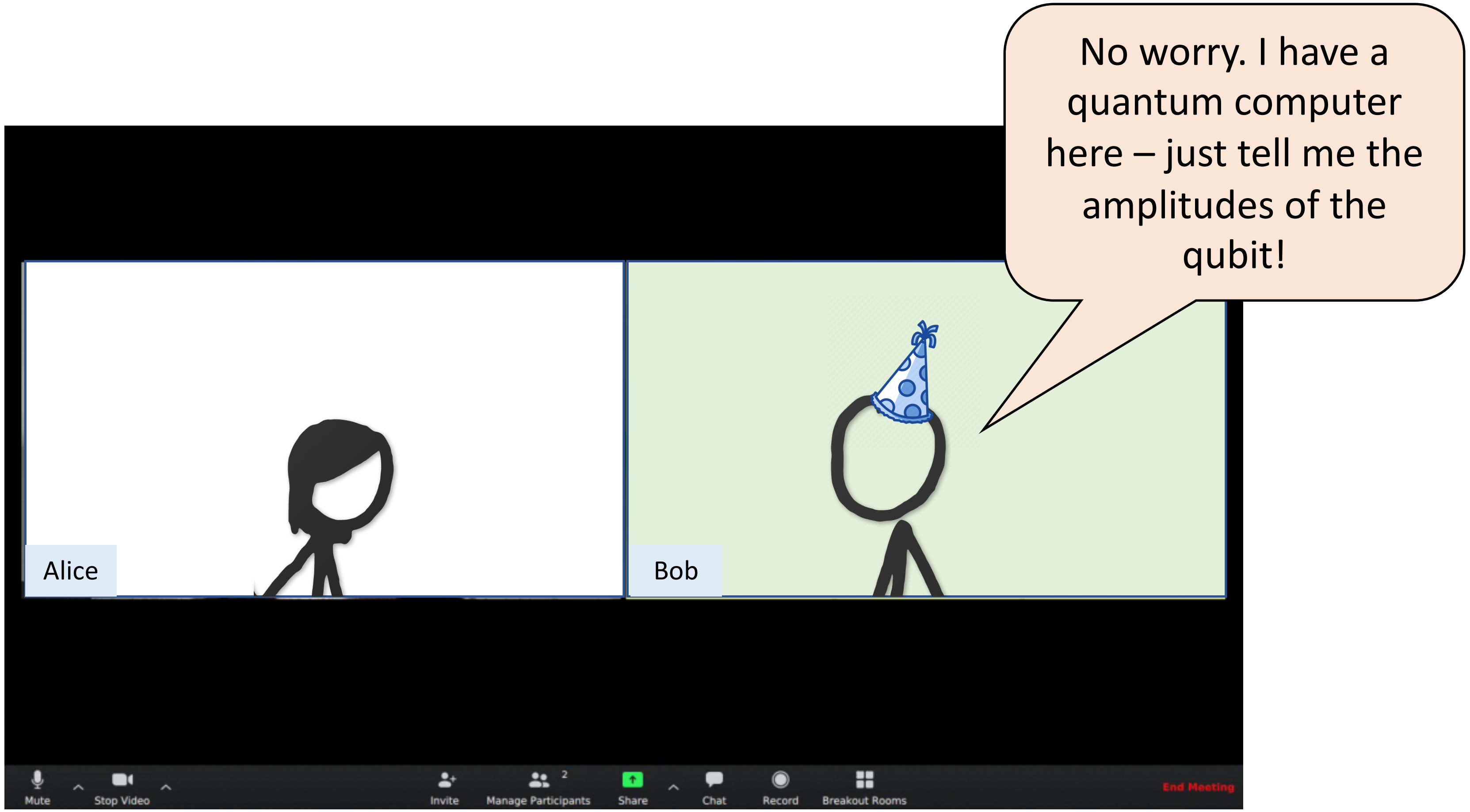

I have a gift for you.
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
2
Share
Chat
Record
Breakout Rooms
End Meeting

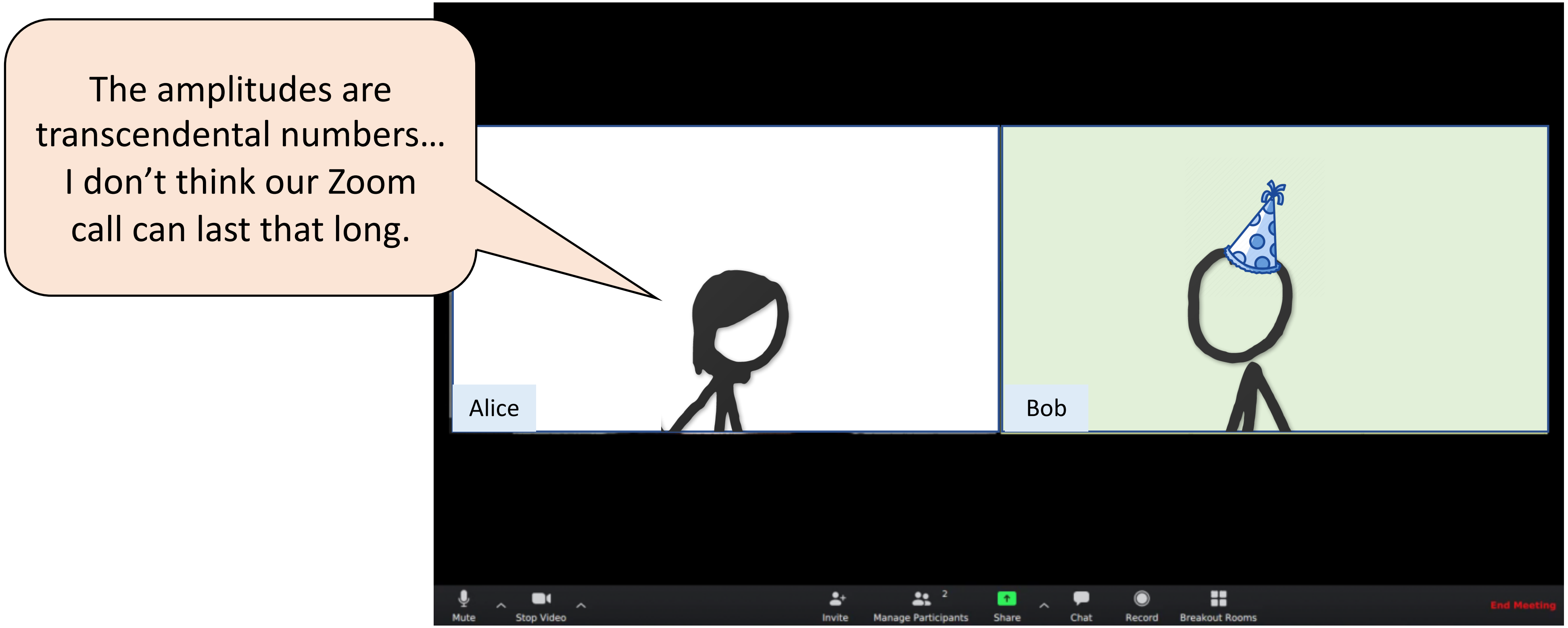

Oh! That's very nice of you.
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
2
Share
Chat
Record
Breakout Rooms
End Meeting

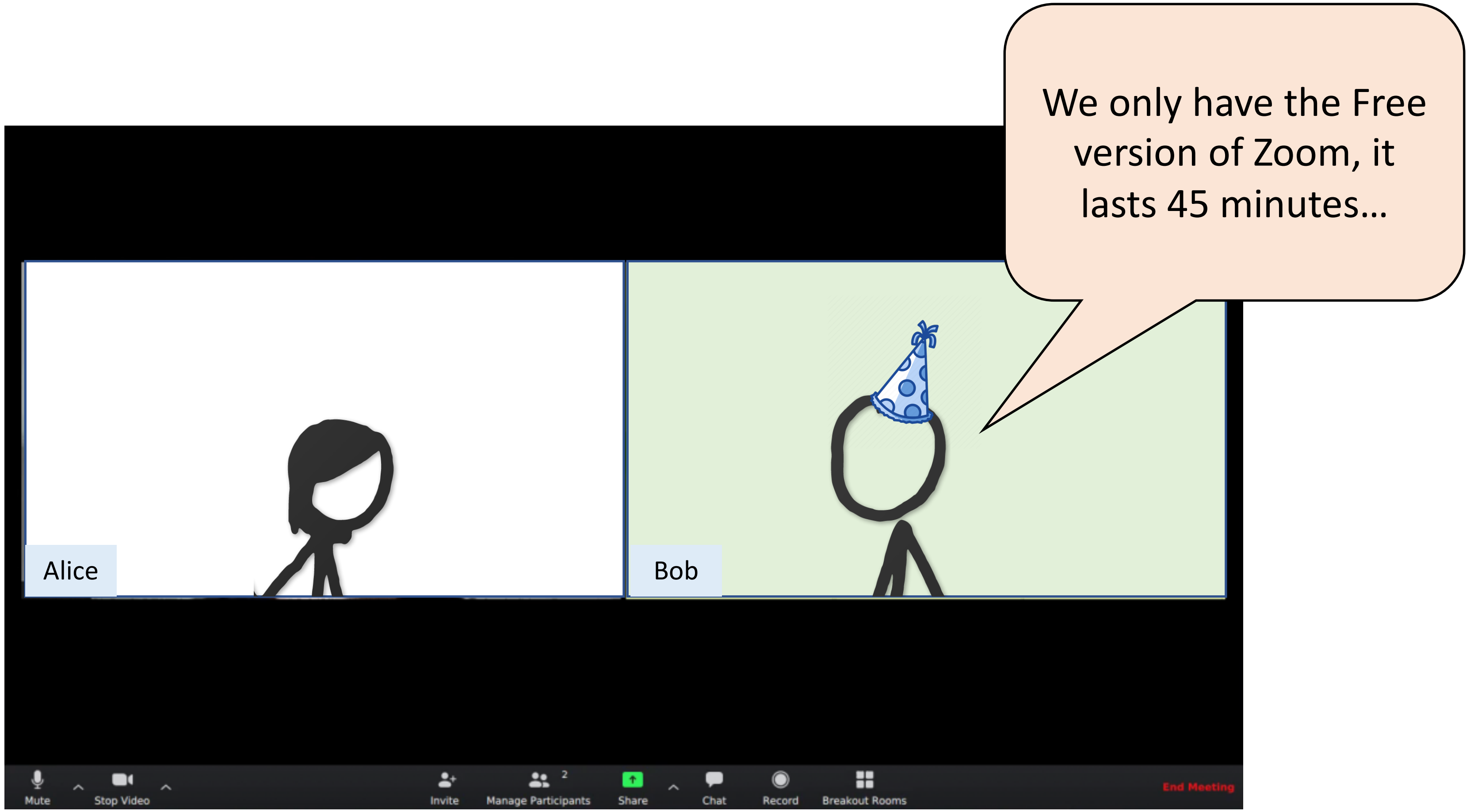


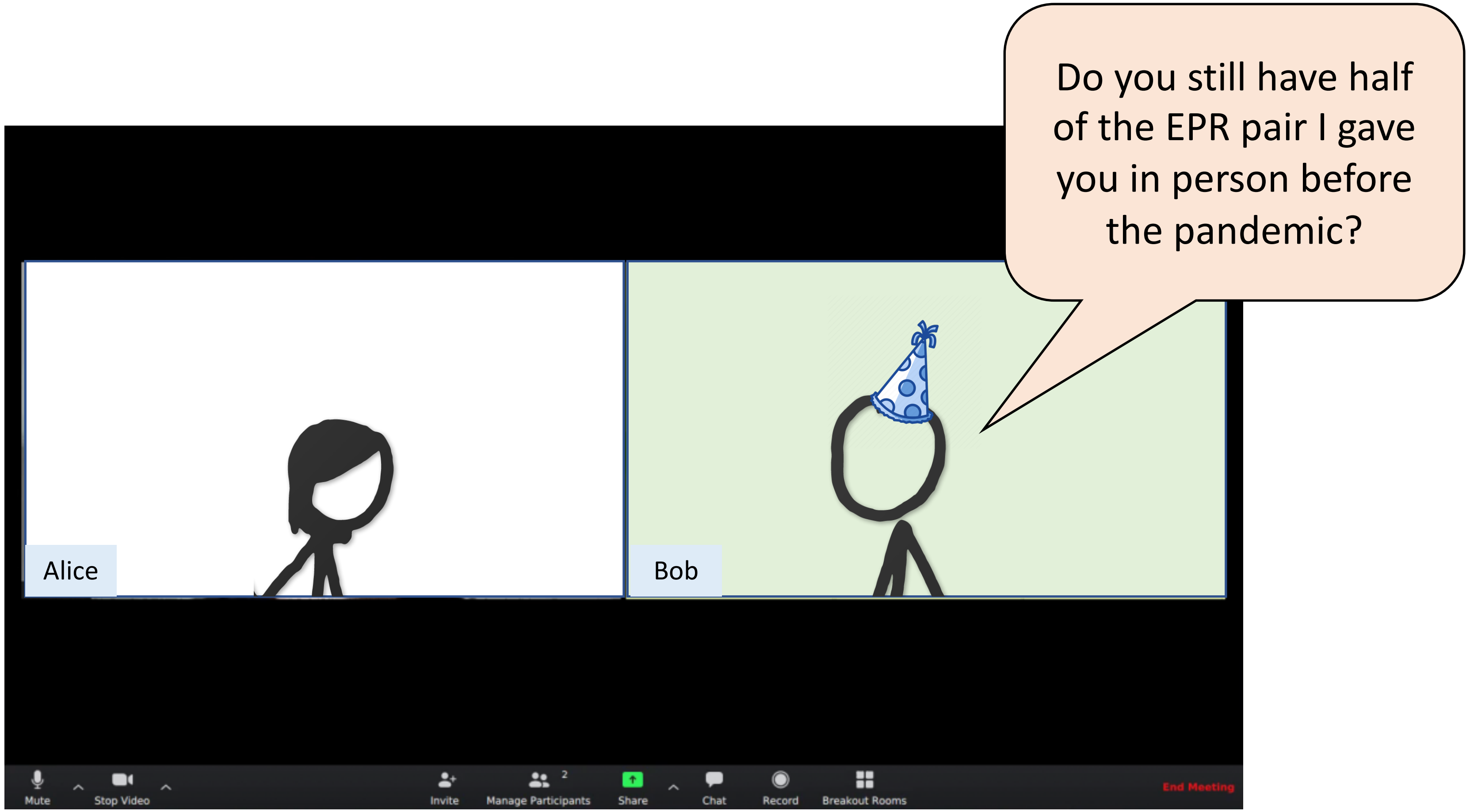
There's a problem, though.
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
Share
Chat
Record
Breakout Rooms
End Meeting


It’s a qubit.
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
Share
Chat
Record
Breakout Rooms
End Meeting

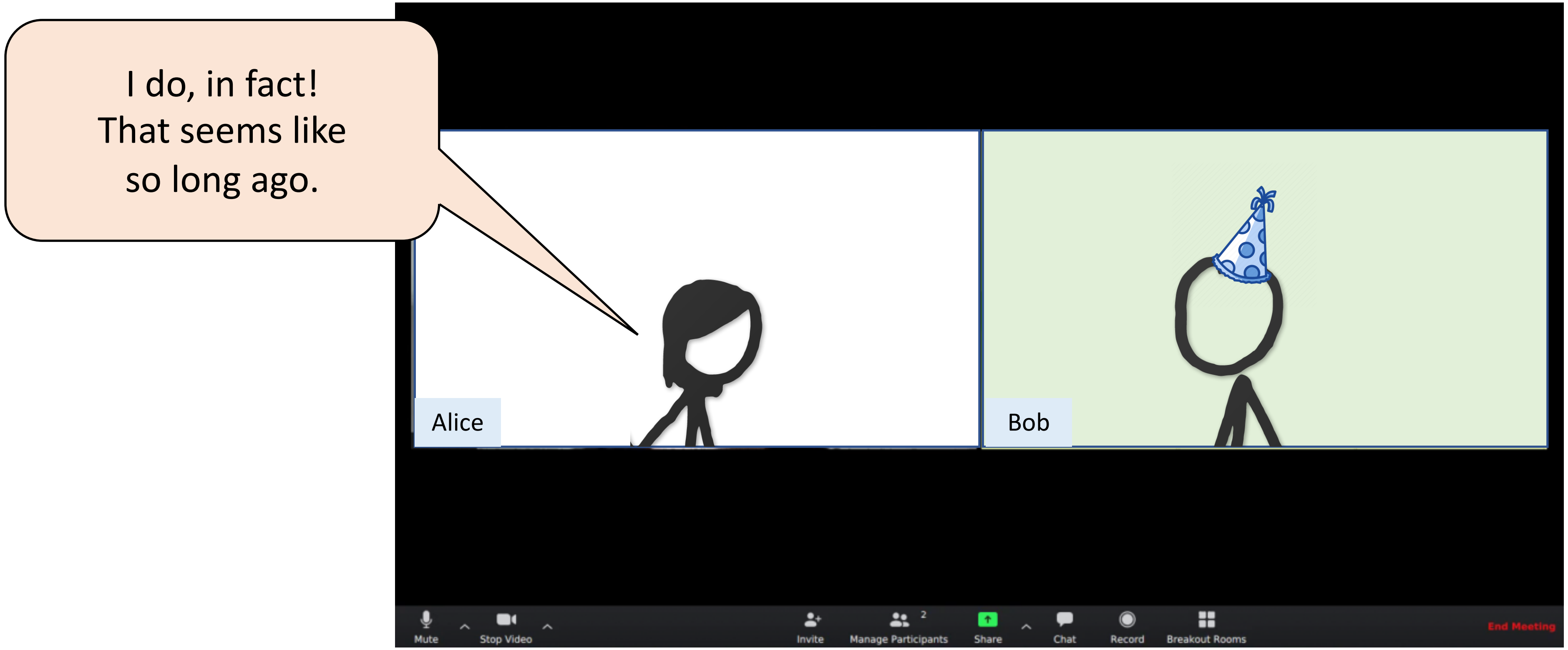

No worry. I have a quantum computer here – just tell me the amplitudes of the qubit!
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
2
Share
Chat
Record
Breakout Rooms
End Meeting


The amplitudes are transcendental numbers… I don’t think our Zoom call can last that long.
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
Share
Chat
Record
Breakout Rooms
End Meeting

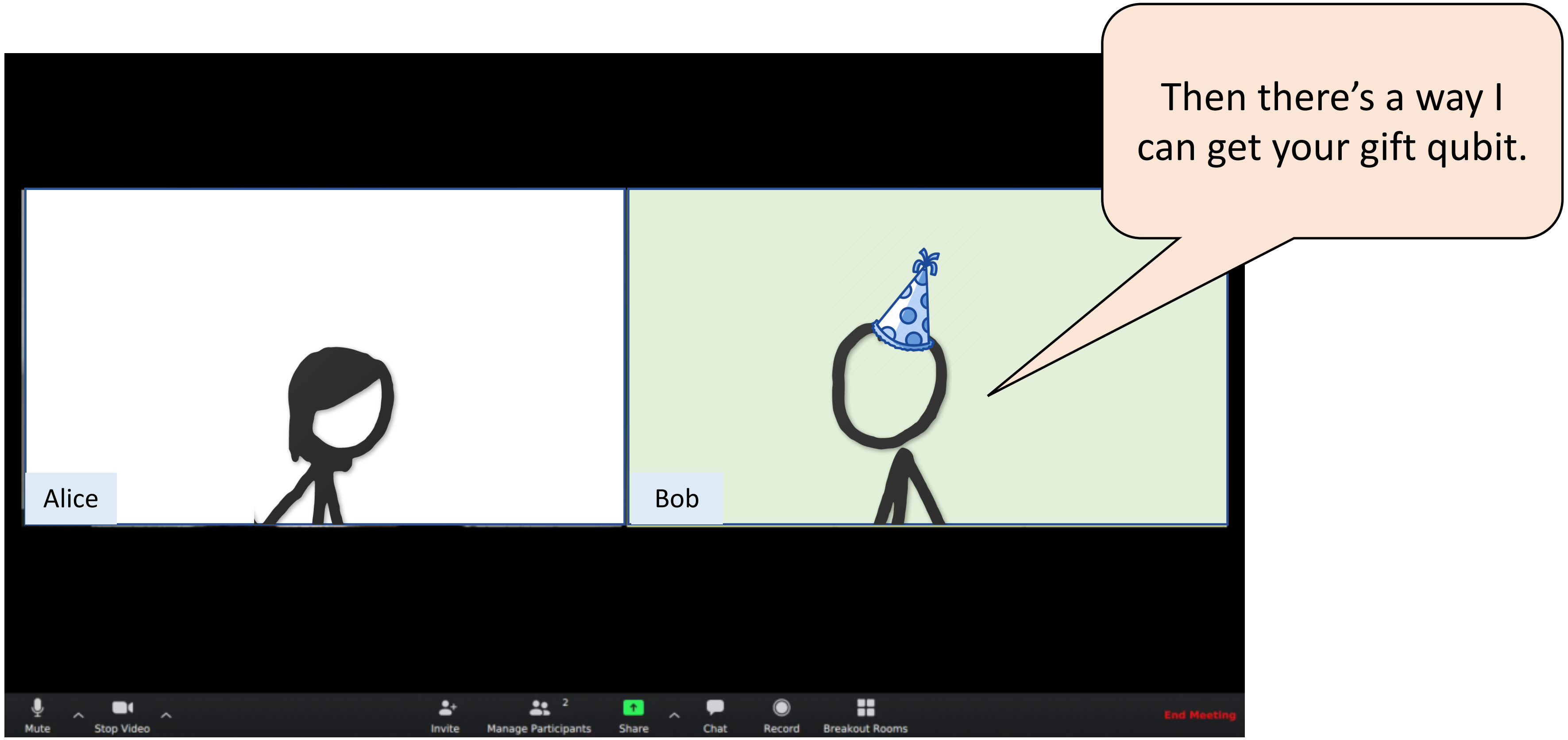

We only have the Free version of Zoom, it lasts 45 minutes…
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
2
Share
Chat
Record
Breakout Rooms
End Meeting



$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

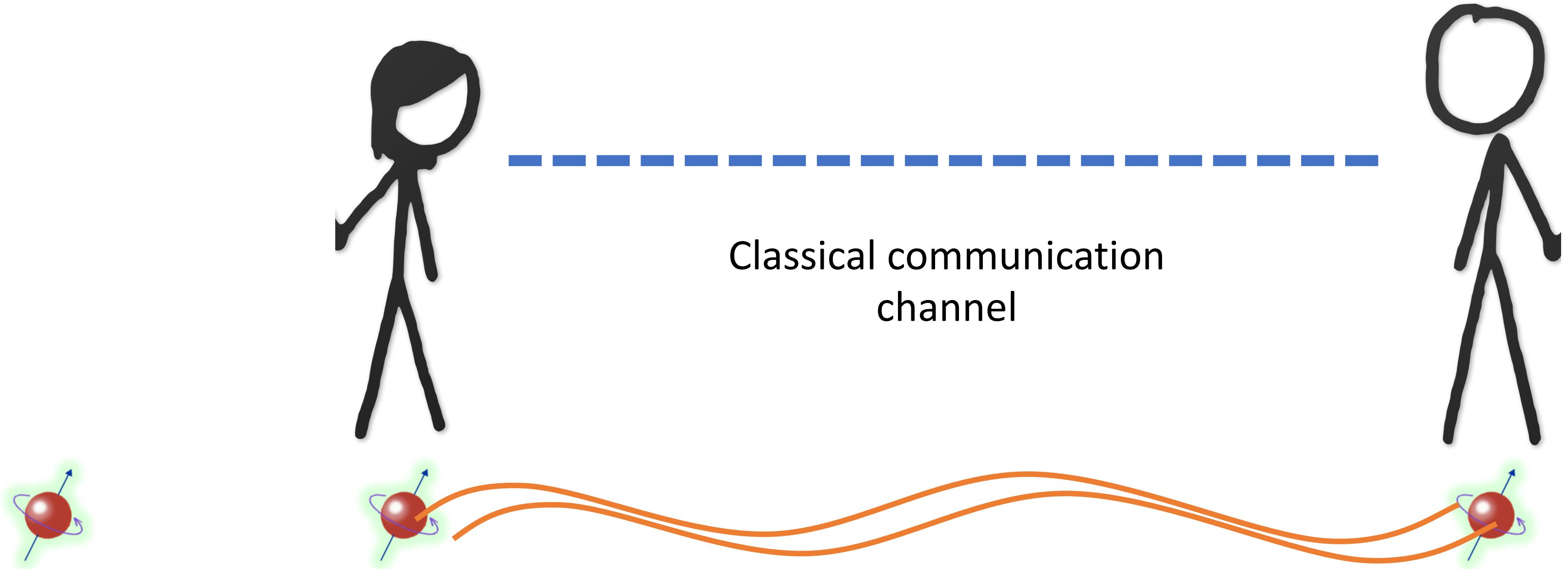


$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Quantum Teleportation



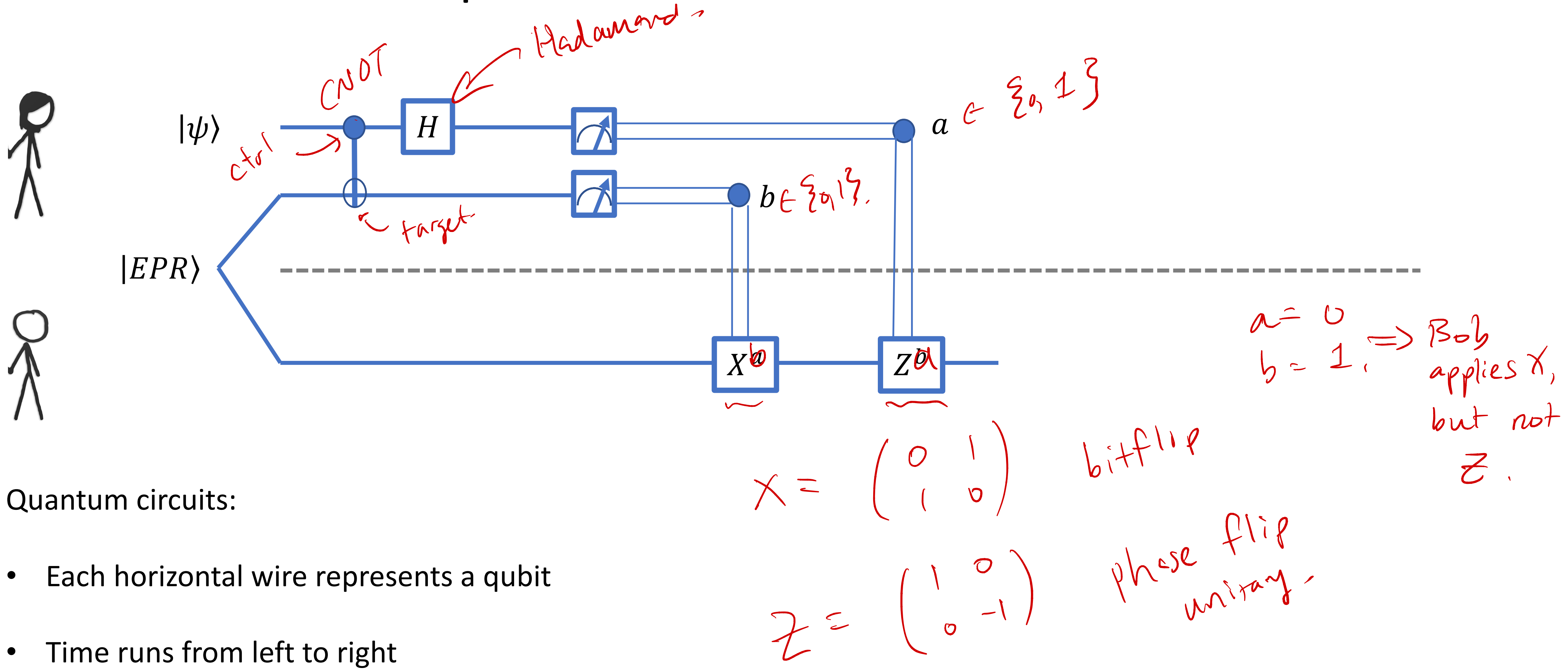
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Shared before protocol begins.

Quantum teleportation allows Alice to send $|\psi\rangle$ to Bob using preshared entanglement and classical communication.

Quantum Teleportation



Quantum circuits:

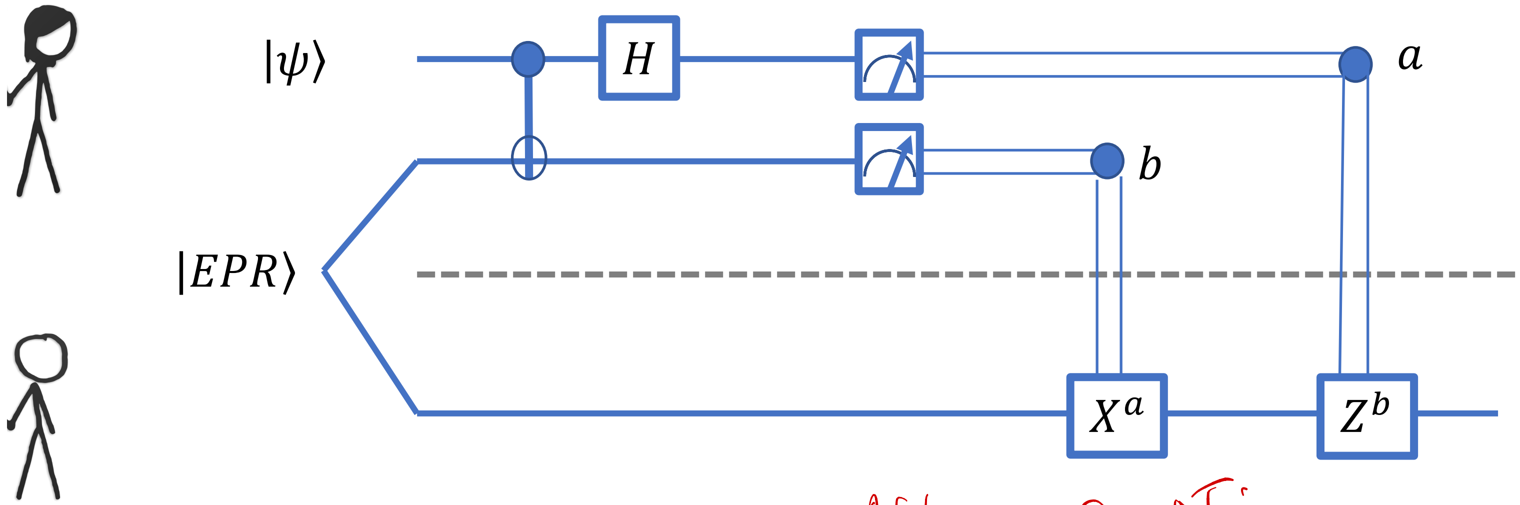
- Each horizontal wire represents a qubit
- Time runs from left to right
- Initial state of qubits is written on left hand side

Quantum Teleportation

Beginning:

$$|\psi\rangle \otimes |EPR\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) \otimes (|00\rangle + |11\rangle)$$

$$= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$



CNOT

After CNOT:

$$\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)$$

After Hadamard:

$$\frac{1}{\sqrt{2}}(\alpha|+\rangle|00\rangle + \alpha|+\rangle|11\rangle + \beta|-\rangle|10\rangle + \beta|-\rangle|01\rangle)$$

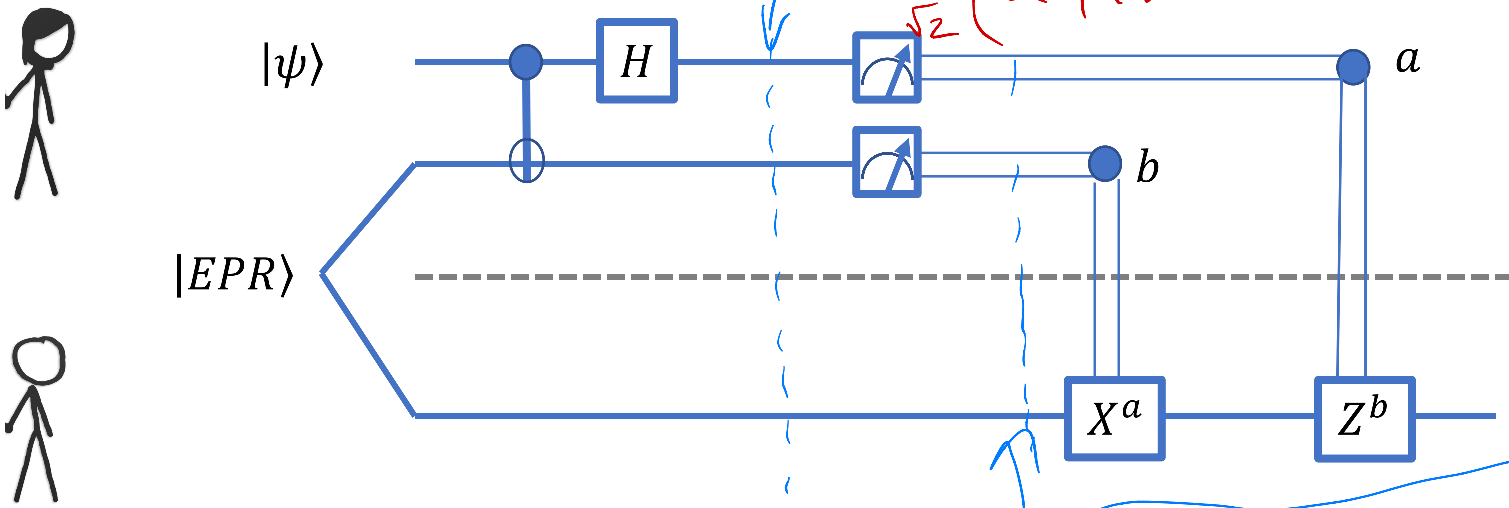
Quantum circuits:

- Each horizontal wire represents a qubit
- Time runs from left to right
- Initial state of qubits is written on left hand side

Quantum Teleportation

After Hadamard.

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



Claim: At the end of protocol, Bob has $|\psi\rangle$.

suppose $b=1$. state collapses to,

$$\alpha|+\rangle|11\rangle + \beta|-\rangle|10\rangle.$$

$$= \frac{1}{\sqrt{2}}\left(\alpha|011\rangle + \beta|010\rangle + \alpha|111\rangle - \beta|110\rangle\right)$$ Now measure first qubit.

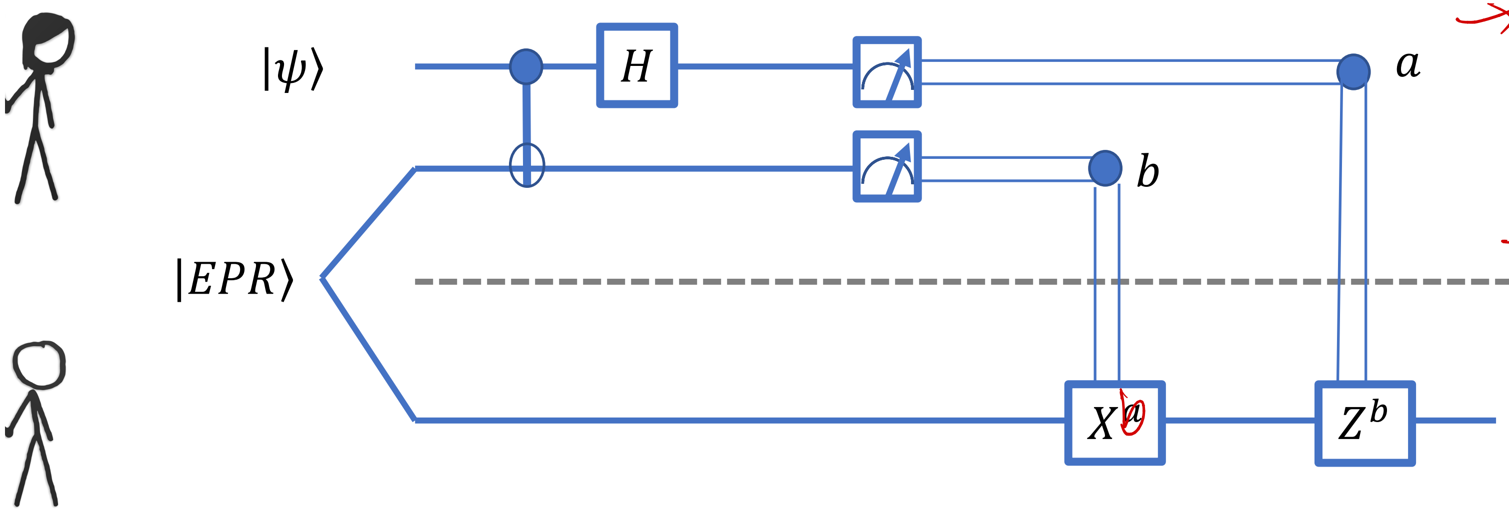
suppose $a=0$. $\rightarrow$ $\alpha|011\rangle + \beta|010\rangle = |0\rangle\otimes|1\rangle\otimes(\alpha|1\rangle + \beta|0\rangle)$.

Quantum Teleportation

In the case $a=0$, $b=1$, state after measurement is $|0,1\rangle \otimes (\alpha|1\rangle + \beta|0\rangle)$.

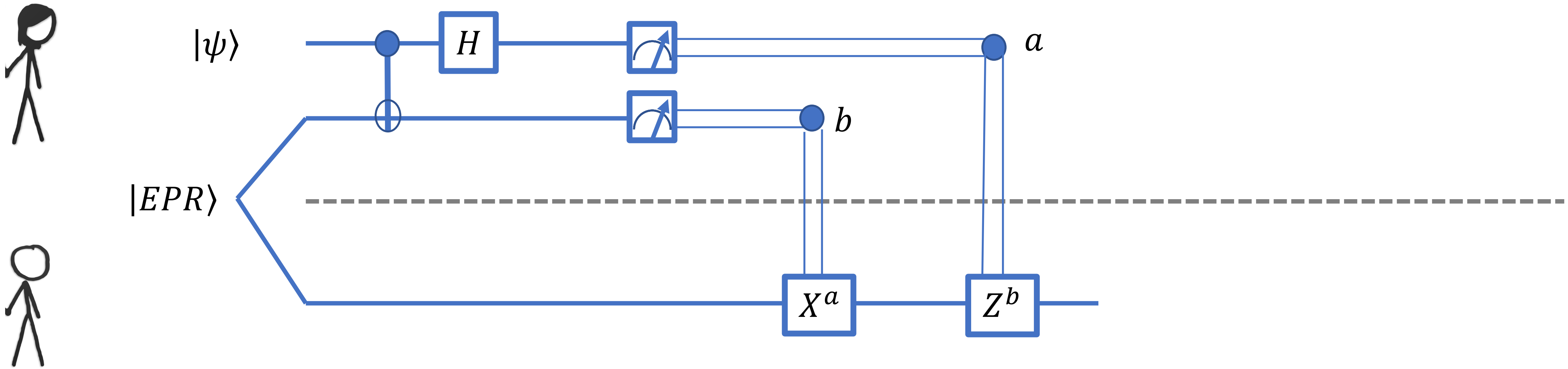
→ Bob applies X to his qubit.

→ Bob's qubit is in the state $\alpha|0\rangle + \beta|1\rangle = |\psi\rangle$.



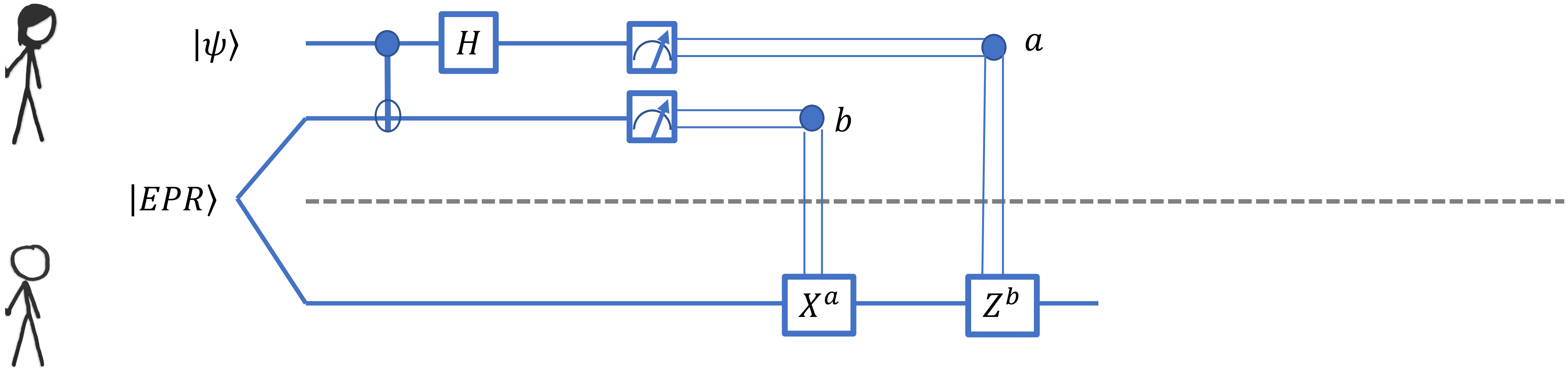
Claim: At the end of protocol, Bob has $|\psi\rangle$.

Quantum Teleportation



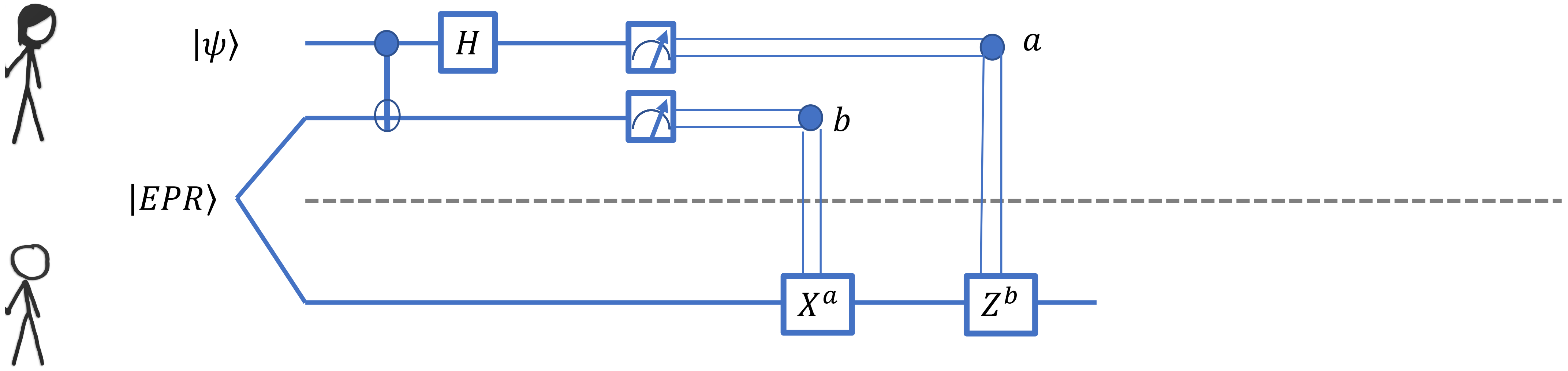
Claim: At the end of protocol, Bob has $|\psi\rangle$.

Quantum Teleportation



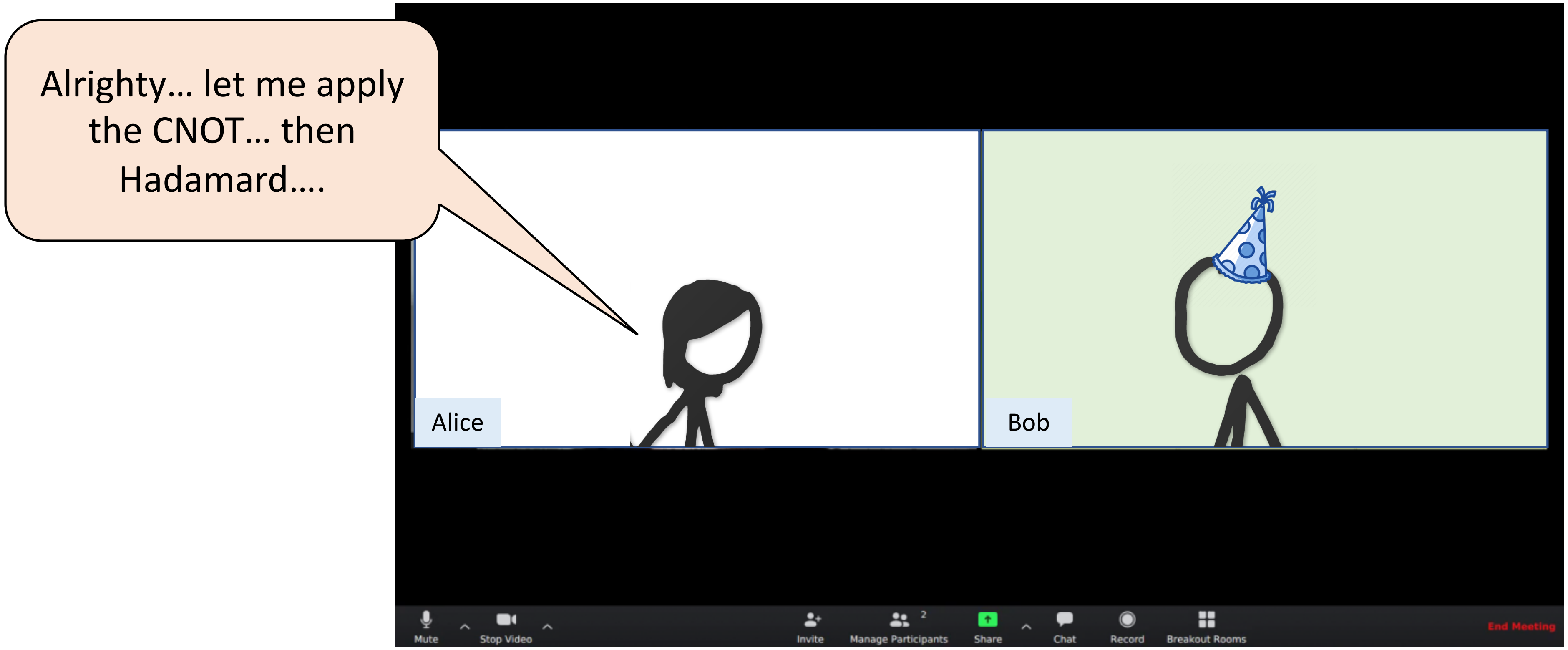
Claim: At the end of protocol, Bob has $|\psi\rangle$.

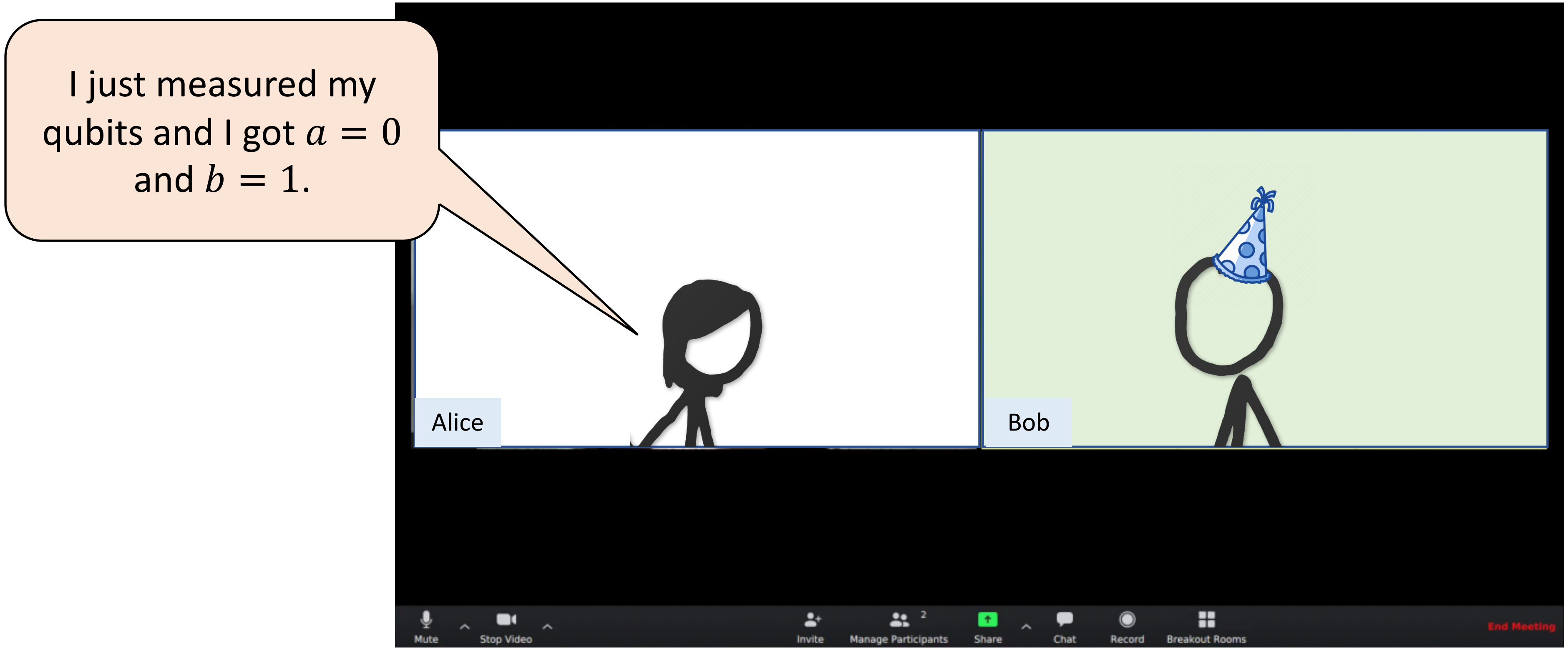
Quantum Teleportation

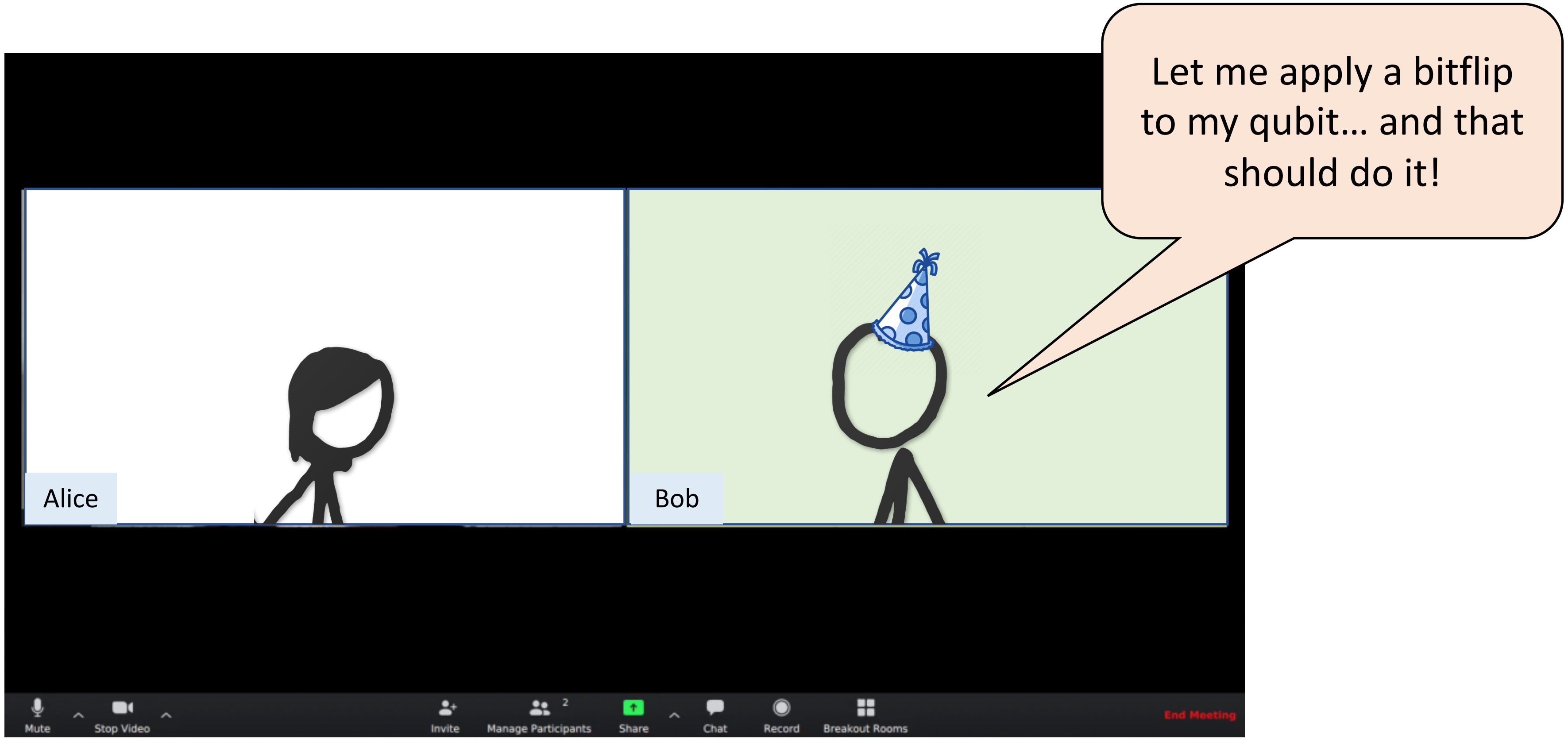


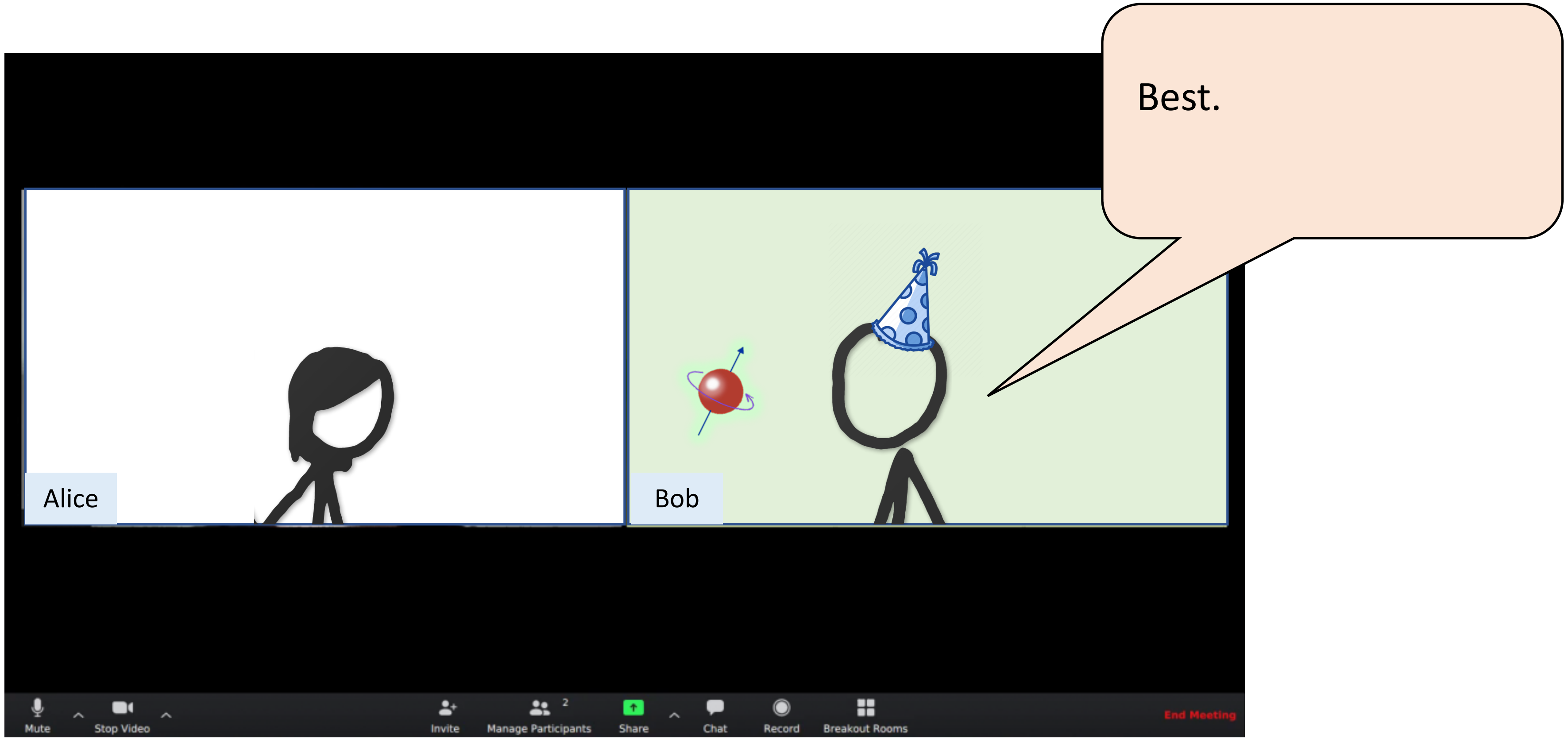
Claim: At the end of protocol, Bob has $|\psi\rangle$.

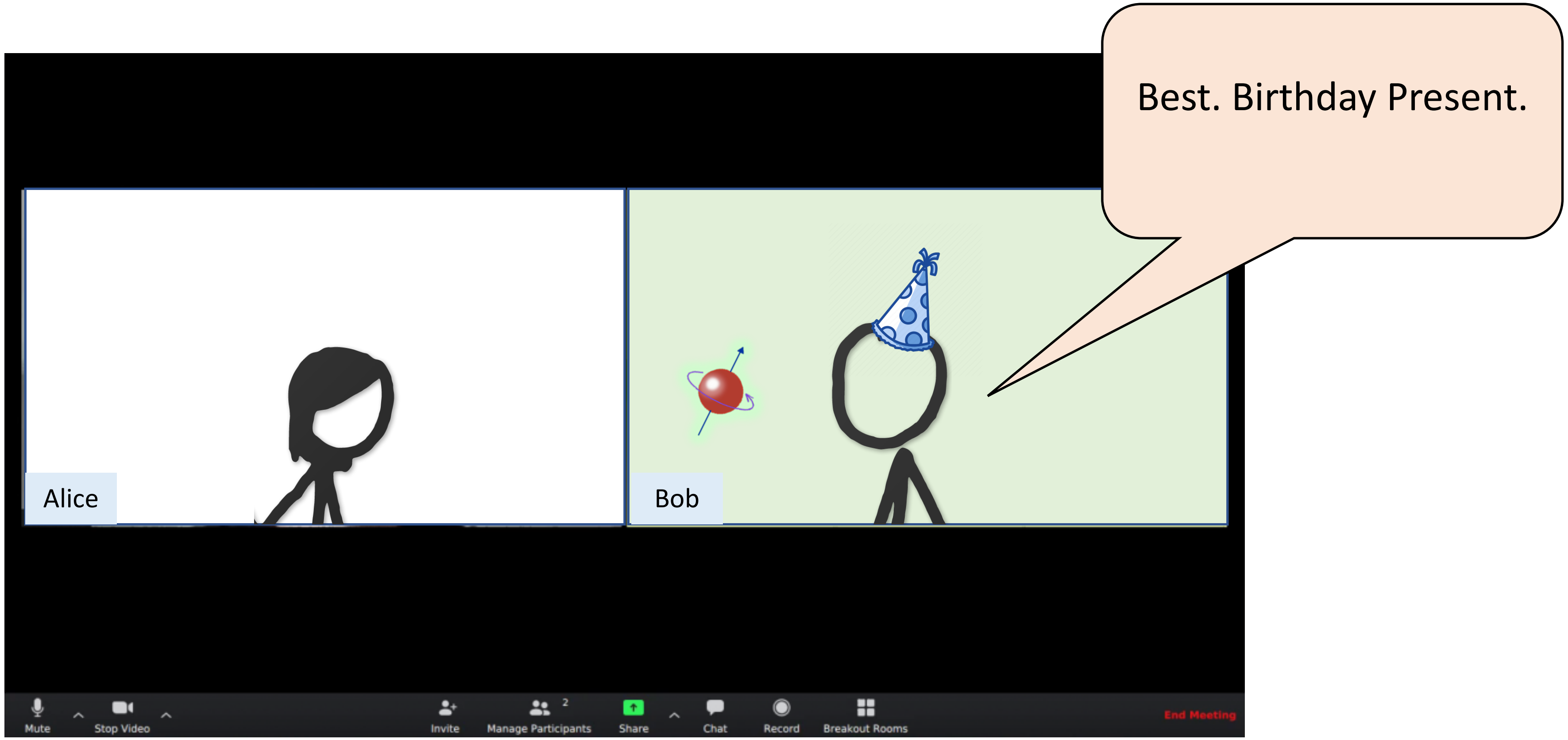
Quantum teleportation does not allow Alice to instantaneously send $|\psi\rangle$ to Bob.
Alice needs to communicate classical bits to Bob!

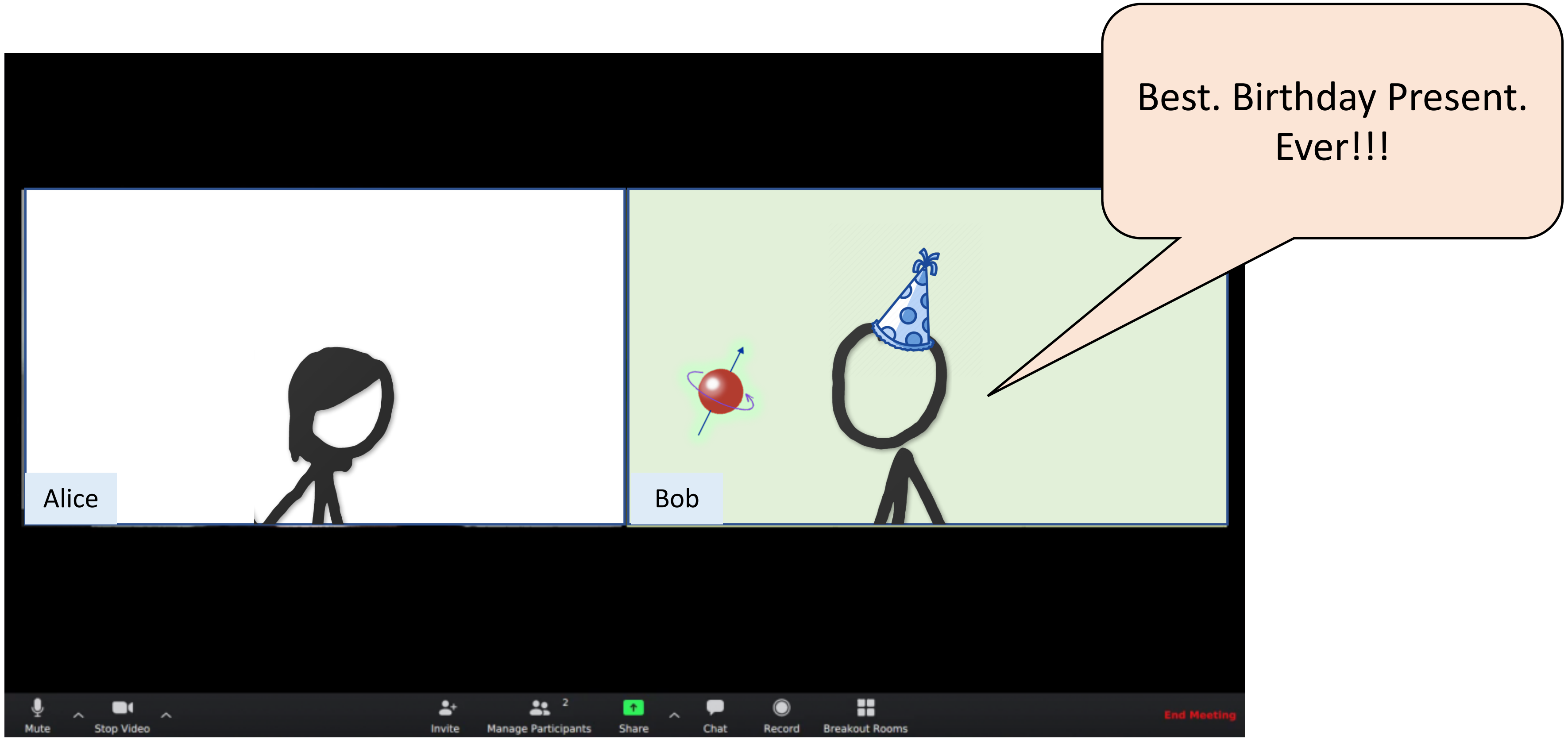

Alrighty… let me apply the CNOT… then Hadamard….
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
2
Share
Chat
Record
Breakout Rooms
End Meeting


I just measured my qubits and I got $a = 0$ and $b = 1$.
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
Share
Chat
Record
Breakout Rooms
End Meeting


Let me apply a bitflip to my qubit… and that should do it!
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
Share
Chat
Record
Breakout Rooms
End Meeting


Best.
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
2
Share
Chat
Record
Breakout Rooms
End Meeting


Best. Birthday Present.
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
Share
Chat
Record
Breakout Rooms
End Meeting


Best. Birthday Present. Ever!!!
Alice
Bob
Mute
Stop Video
Invite
Manage Participants
Share
Chat
Record
Breakout Rooms
End Meeting

FIN

Quantum Circuit Model

Quantum gates

- A k qubit-*quantum gate* is a $2^k \times 2^k$ unitary matrix U

- Common single-qubit quantum gates:
  - I – identity
  - X – bitflip: $|0\rangle \leftrightarrow |1\rangle$
  - H – Hadamard: $|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

    $|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Phase gates

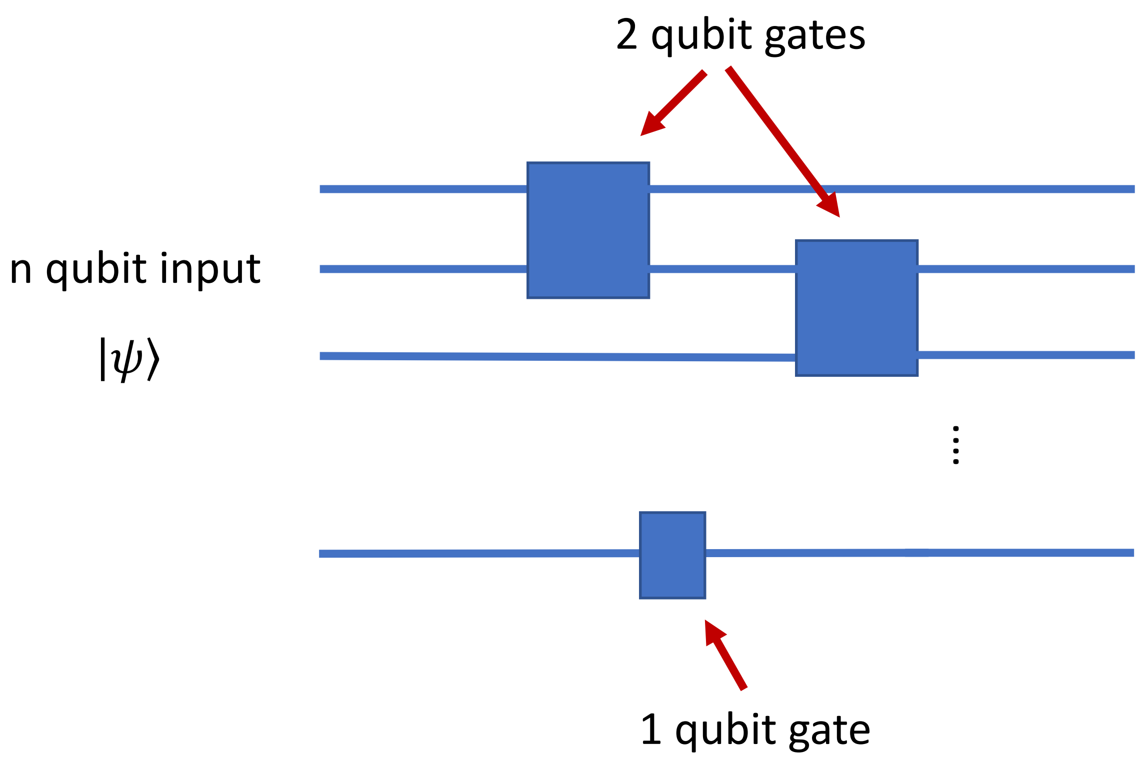
Z: $|0\rangle \mapsto |0\rangle$, $\quad |1\rangle \mapsto -|1\rangle$

P: $|0\rangle \mapsto |0\rangle$, $\quad |1\rangle \mapsto i|1\rangle$

T: $|0\rangle \mapsto |0\rangle$, $\quad |1\rangle \mapsto e^{\frac{2\pi i}{8}}|1\rangle$

- Two-qubit gates:
  - $CNOT$ – controlled NOT operation: $CNOT|x, a\rangle = |x, a \oplus x\rangle$

Quantum circuits

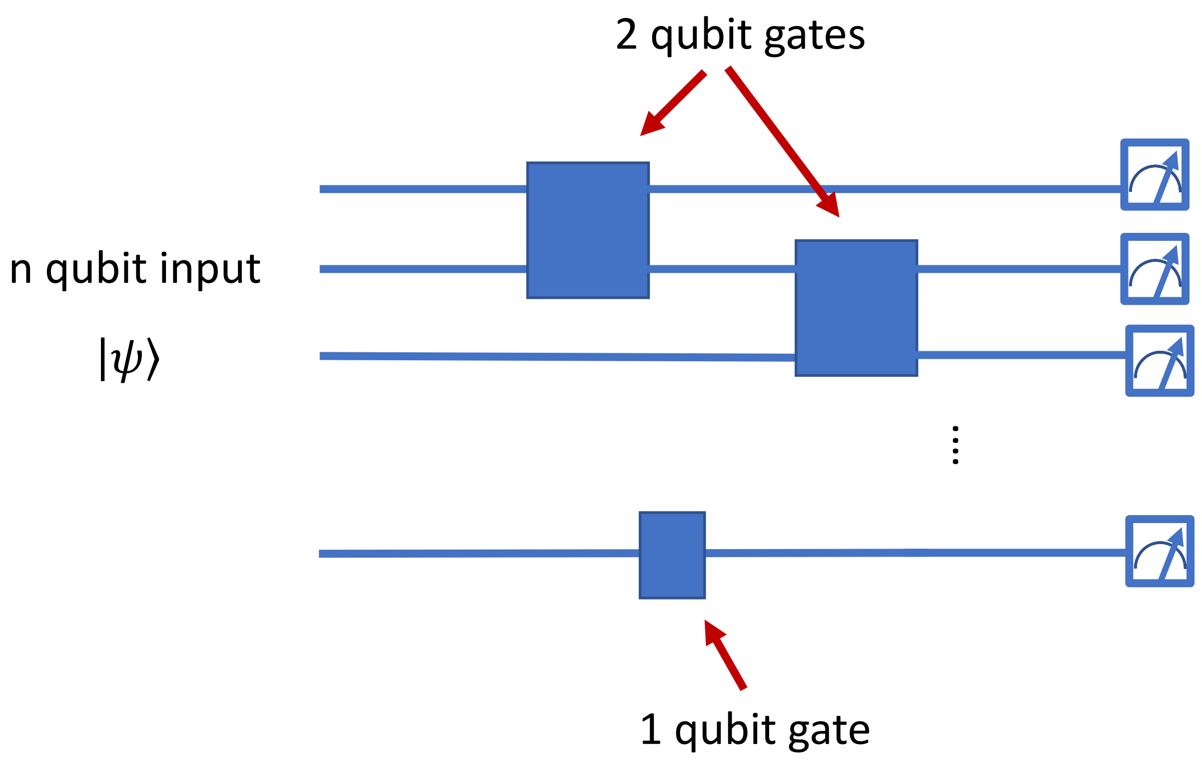


- A quantum circuit F consists of an ordered collection of 1- and 2-qubit gates $G_1, G_2, \ldots$ applied to subsets of qubits.

- Output of circuit F on input $|\psi\rangle$ is equal to

$$G_m \cdots G_2 G_1 |\psi\rangle$$

Measurements



- At end of computation, if final state is

$$|\varphi\rangle = \sum \beta_x \, |x\rangle$$

can perform **measurement** to get classical outcome of computation.

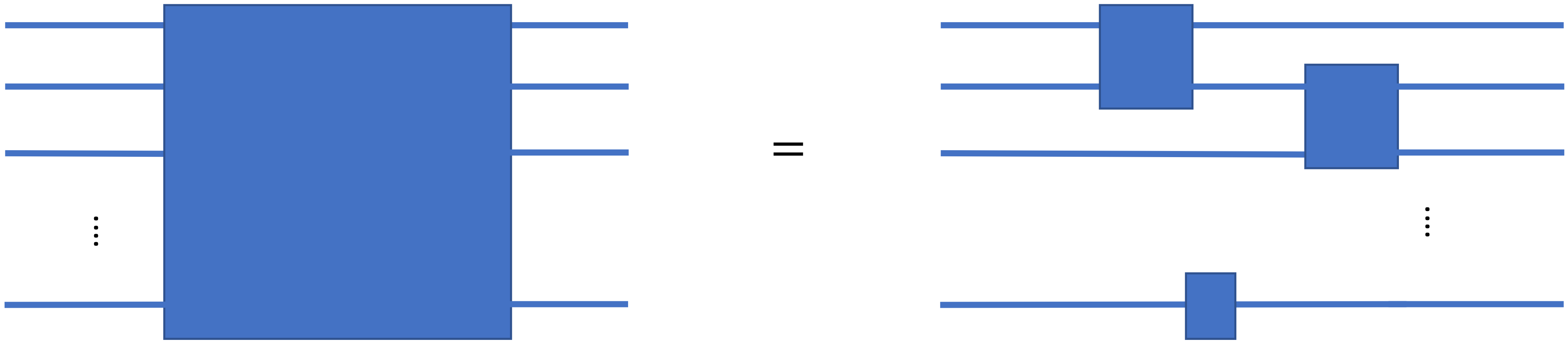
- Measurement is probabilistic: obtains outcome $x \in \{0,1\}^n$ with probability $|\beta_x|^2$.

- Measurement is **destructive**: measuring in middle of quantum computation will disturb the state.

We can also allow intermediate measurements (like in quantum teleportation), but for now let's assume that measurements happen at the very end.

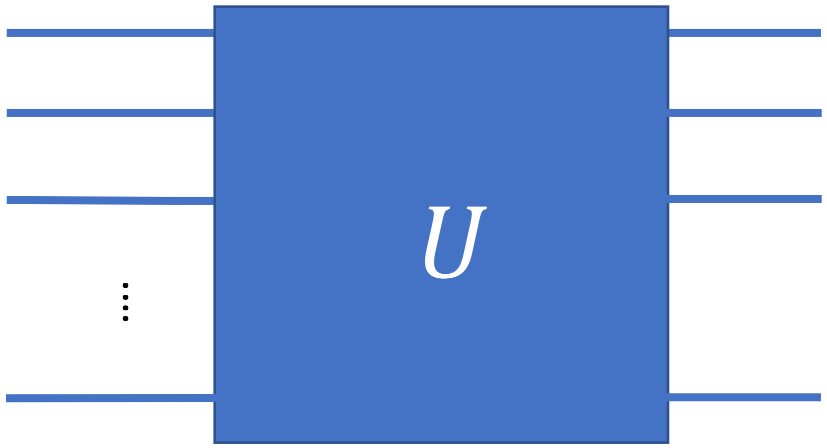
Universal and non-universal gate sets

- Every n-qubit unitary U can be implemented as a quantum circuit consisting of single-qubit gates and CNOT.
- In worst case, such a circuit requires $\approx 4^n$ gates.
- Can use arbitrary single-qubit gates $G \in \mathbb{C}^{2\times 2}$.

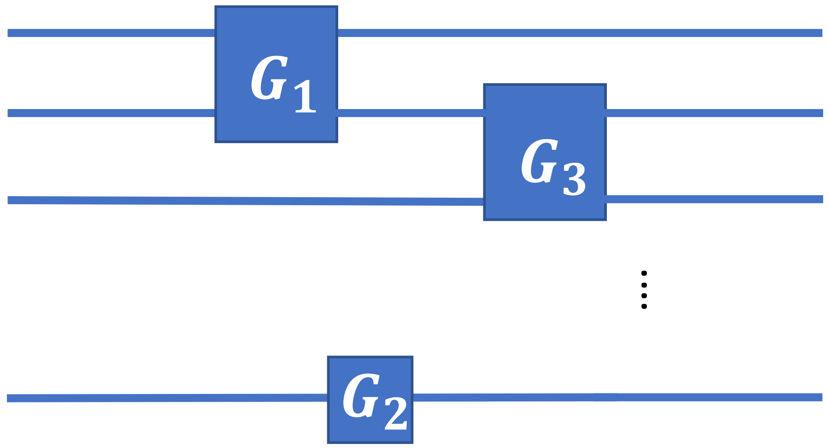


Universal and non-universal gate sets

- In practice, we can only use gates from a fixed, finite set (depending on your hardware).
- A set Λ of gates is ***universal*** if any unitary (on any number of qubits) can be approximated arbitrarily well by a circuit consisting of gates from Λ.
- A unitary U ϵ-approximates another unitary V if: $\max_{|\psi\rangle} \| U|\psi\rangle - V|\psi\rangle \| \leq \epsilon$



$\approx$



$G_1, G_2, G_3, \ldots \in \Lambda$

Universal and non-universal gate sets

- **Ex**: $\Lambda = \text{Clifford} \cup \{T\}$ is a universal gate set!
  - Clifford$=$ gates generated by $\{H, P, CNOT\}$

Non-Clifford

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{8}} \end{pmatrix}$$

Clifford gates

$CNOT$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Universal and non-universal gate sets

- **Ex**: $\Lambda =$ Clifford is *not* universal gate set.
  - Clifford= gates generated by $\{H, P, CNOT\}$

Fact #0: Clifford circuits are not even universal for *classical* computation.

Fact #1: Clifford circuits (with all zeroes input) can be efficiently simulated on classical computers (Gottesman-Knill Theorem).

$CNOT$

Clifford gates

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Universal and non-universal gate sets

- **Ex**: $\Lambda =$ Clifford is *not* universal gate set.
  - Clifford= gates generated by $\{H, P, CNOT\}$
- Pauli = gates generated by $\{X, Z\} \subseteq$ Clifford
- n-qubit Pauli unitaries: tensor products of $\{I, X, Y, Z\}$

Clifford gates

$CNOT$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

Pauli gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

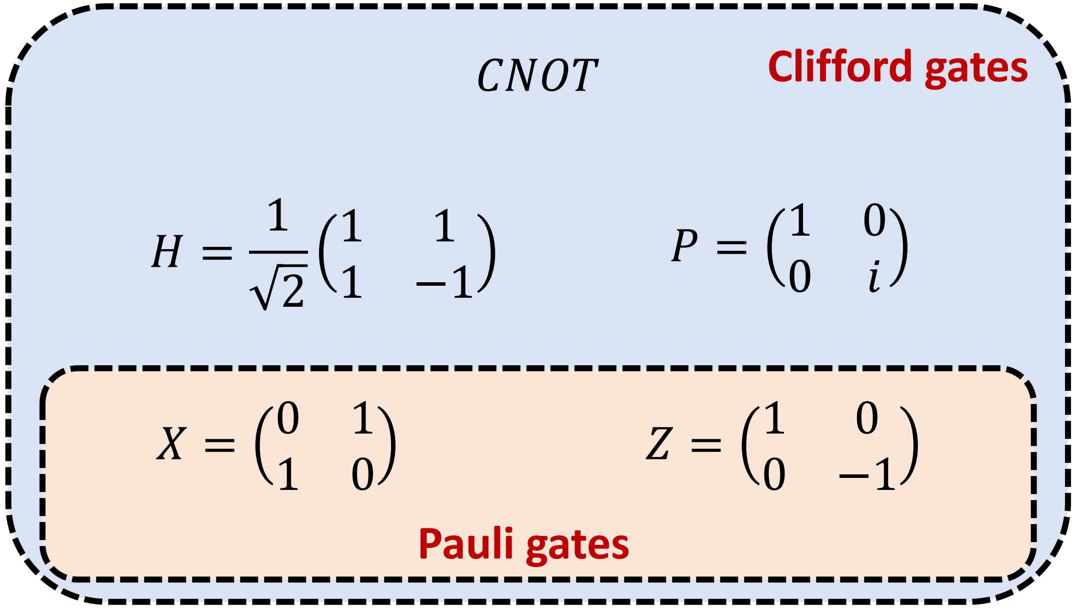
Fact #2: Clifford circuits/unitaries are equivalently defined in terms of their behavior on ***Pauli matrices***.

$X \otimes X$

$X \otimes Z \otimes I \otimes \cdots$ } Pauli

Universal and non-universal gate sets

- **Ex**: $\Lambda =$ Clifford is *not* universal gate set.
  - Clifford= gates generated by $\{H, P, CNOT\}$
- Pauli = gates generated by $\{X, Z\} \subseteq$ Clifford
- n-qubit Pauli unitaries: tensor products of $\{I, X, Y, Z\}$



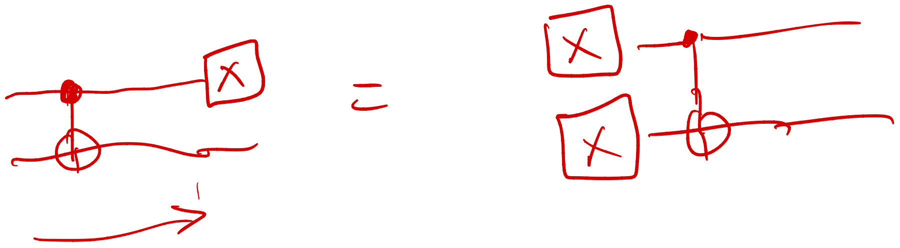
Fact #2: Clifford circuits/unitaries are equivalently defined in terms of their behavior on ***Pauli matrices***.

For all Pauli unitaries $W = W_1 \otimes W_2 \otimes \cdots \otimes W_n$

for all n-qubit Clifford unitaries C, there exists another Pauli unitary $W' = W_1{}' \otimes W_2{}' \otimes \cdots \otimes W_n{}'$ such that

$$WC = CW'$$

Ex: $XH = HZ$



Computing classical functions, quantumly

How to compute $f: \{0,1\}^n \to \{0,1\}^m$ using a quantum circuit?

Can call classical functions as a subroutine using ***classical oracles***: define the unitary U_f on $n + m$ qubits: for all $x \in \{0,1\}^n, b \in \{0,1\}^m$,

$$U_f|x, b\rangle = |x, b \oplus f(x)\rangle$$

} is a unitary.

bitwise XOR.

Ex: $f = \text{AND}, f = \text{NOT}$

$$U_{AND}|a,b,c\rangle = |a,b,c \oplus ab\rangle.$$

$$U_{NOT} = \text{CNOT}.$$

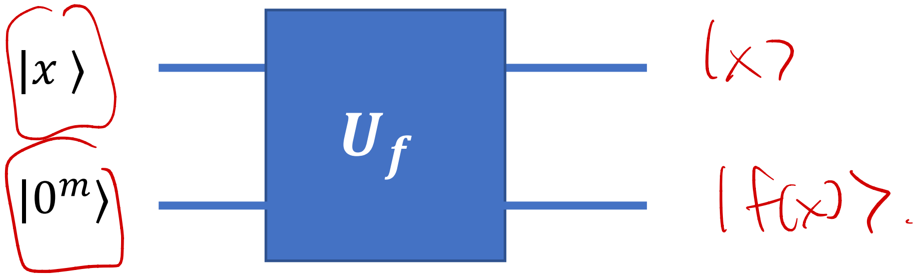
Computing classical functions, quantumly

How to compute $f: \{0,1\}^n \to \{0,1\}^m$ using a quantum circuit?

Can call classical functions as a subroutine using ***classical oracles***: define the unitary U_f on $n + m$ qubits: for all $x \in \{0,1\}^n, b \in \{0,1\}^m$,

$$U_f|x, b\rangle = |x, b \oplus f(x)\rangle$$

Ex: $f = \text{AND}, f = \text{NOT}$



Computing classical functions, quantumly

How to compute $f: \{0,1\}^n \to \{0,1\}^m$ using a quantum circuit?

Can call classical functions as a subroutine using ***classical oracles***: define the unitary U_f on $n + m$ qubits: for all $x \in \{0,1\}^n, b \in \{0,1\}^m$,

$$U_f|x, b\rangle = |x, b \oplus f(x)\rangle$$

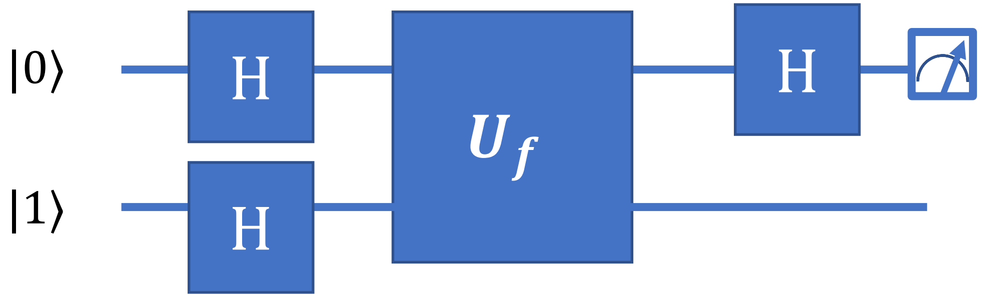
Size s classical circuit computing $f \implies$ There is a size $O(s)$ quantum circuit computing U_f.

Computing classical functions, quantumly

Magic starts happening when classical oracles are queried on a ***superposition*** of inputs.

Deutsch's Problem: Given $f: \{0,1\} \rightarrow \{0,1\}$, determine using one quantum query to U_f whether

- <u>YES case:</u> $f(0) \neq f(1)$
- <u>NO case:</u> $f(0) = f(1)$



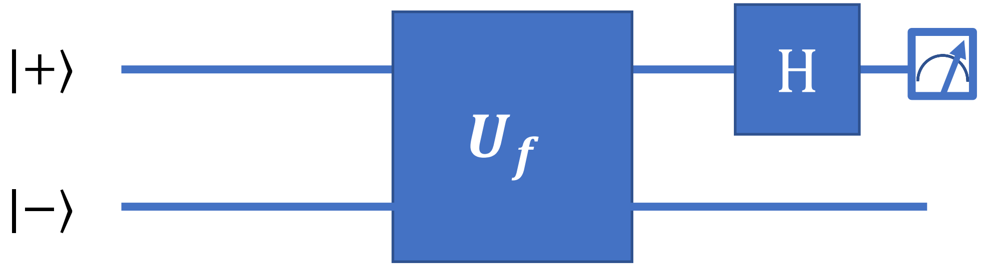
Computing classical functions, quantumly

Magic starts happening when classical oracles are queried on a ***superposition*** of inputs.

Deutsch's Problem: Given $f: \{0,1\} \to \{0,1\}$, determine using one quantum query to U_f whether

- YES case: $f(0) \neq f(1)$
- NO case: $f(0) = f(1)$

circuit equivalent to



Computing classical functions, quantumly

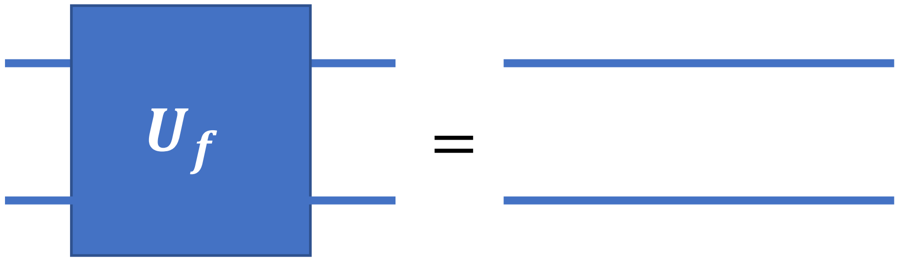
Magic starts happening when classical oracles are queried on a ***superposition*** of inputs.

Deutsch's Problem: Given $f: \{0,1\} \rightarrow \{0,1\}$, determine using one quantum query to U_f whether

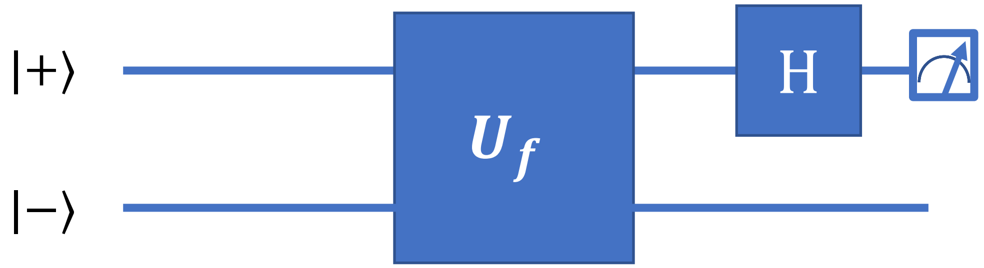
- <u>YES case:</u> $f(0) \neq f(1)$
- <u>NO case:</u> $f(0) = f(1)$

circuit equivalent to

Case 1: $f(0) = f(1) = 0$



Computing classical functions, quantumly



Case 1: $f(0) = f(1) = 0$

circuit equivalent to

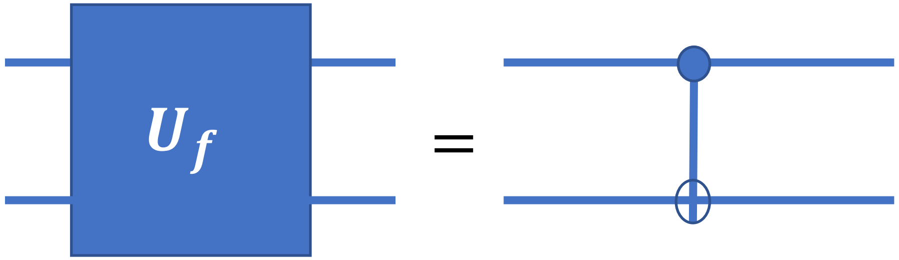
Computing classical functions, quantumly

Magic starts happening when classical oracles are queried on a ***superposition*** of inputs.

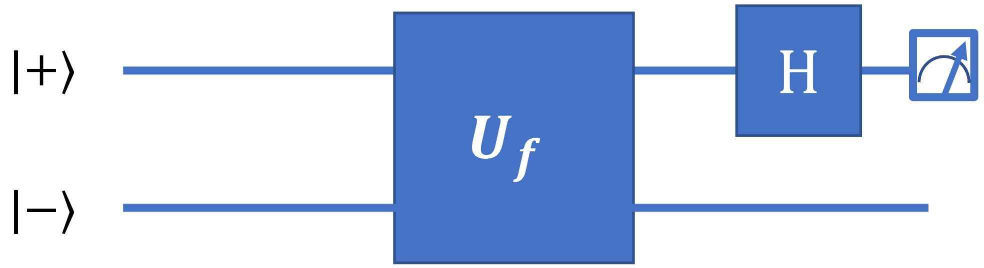
Deutsch's Problem: Given $f: \{0,1\} \to \{0,1\}$, determine using one quantum query to U_f whether

- YES case: $f(0) \neq f(1)$
- NO case: $f(0) = f(1)$

Case 2: $f(0) = 0, f(1) = 1$

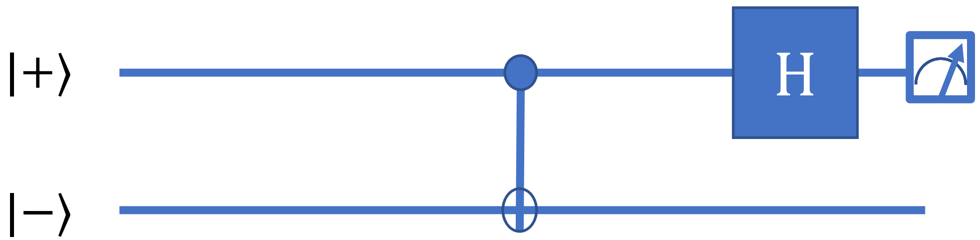


Computing classical functions, quantumly



Case 2: $f(0) = 0, f(1) = 1$

circuit equivalent to



Grover Search

Unstructured search

Search problem: Given black-box access to $f: \{0,1\}^n \rightarrow \{0,1\}$, find x such that $f(x) = 1$.

Classical query complexity: $\Omega(2^n)$

Quantum query complexity: $O(\sqrt{2^n})$

Unstructured search

Search problem: Given black-box access to $f: \{0,1\}^n \rightarrow \{0,1\}$, find x such that $f(x) = 1$.

For boolean functions, we can use different oracle (called *phase* oracle): for all $x \in \{0,1\}^n$

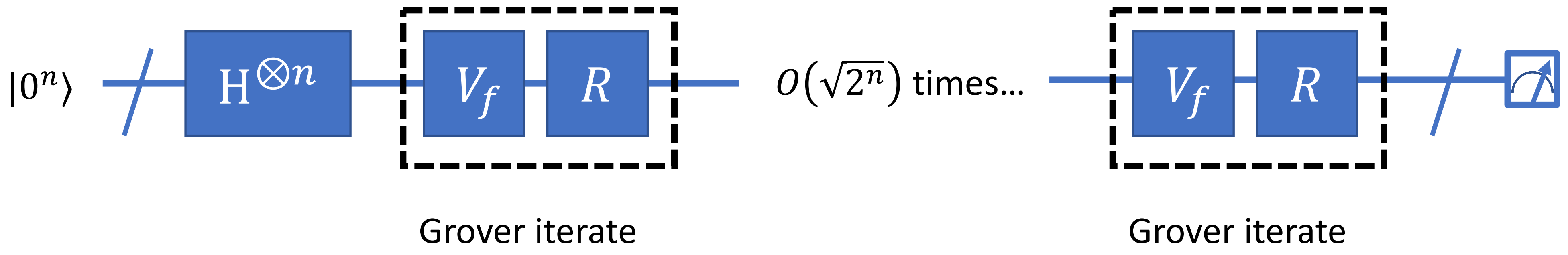
$$V_f|x\rangle = (-1)^{f(x)}|x\rangle$$

XOR oracles and phase oracles are equivalent!

Unstructured search

Search problem: Given black-box access to $f: \{0,1\}^n \to \{0,1\}$, find x such that $f(x) = 1$.

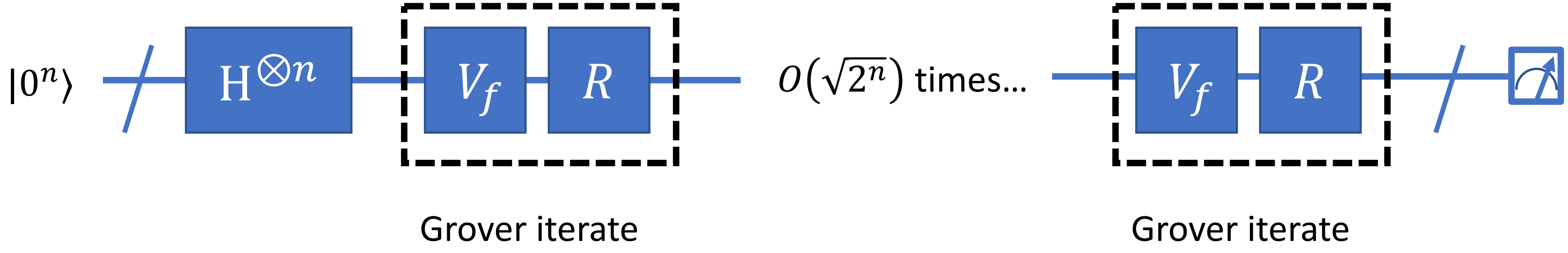
Assume there exists a unique x^* such that $f(x^*) = 1$.

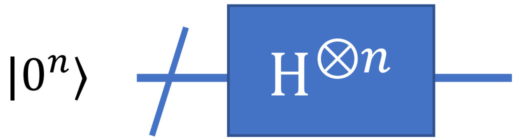


Unstructured search

Search problem: Given black-box access to $f:\{0,1\}^n \rightarrow \{0,1\}$, find x such that $f(x) = 1$.

Assume there exists a unique x^* such that $f(x^*) = 1$.



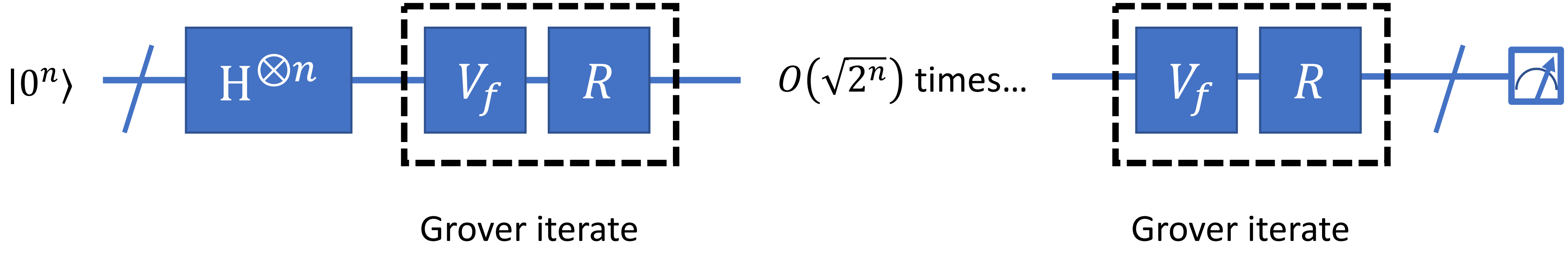


$= \; |+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \Big\} \; |s\rangle.$

Unstructured search

Search problem: Given black-box access to $f: \{0,1\}^n \rightarrow \{0,1\}$, find x such that $f(x) = 1$.

Assume there exists a unique x^* such that $f(x^*) = 1$.



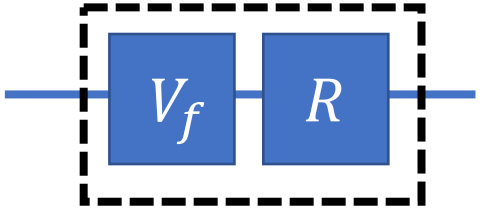
”diffusion operator”, “inversion about the mean”,…

$= 2|s\rangle\langle s| - I$ } unitary

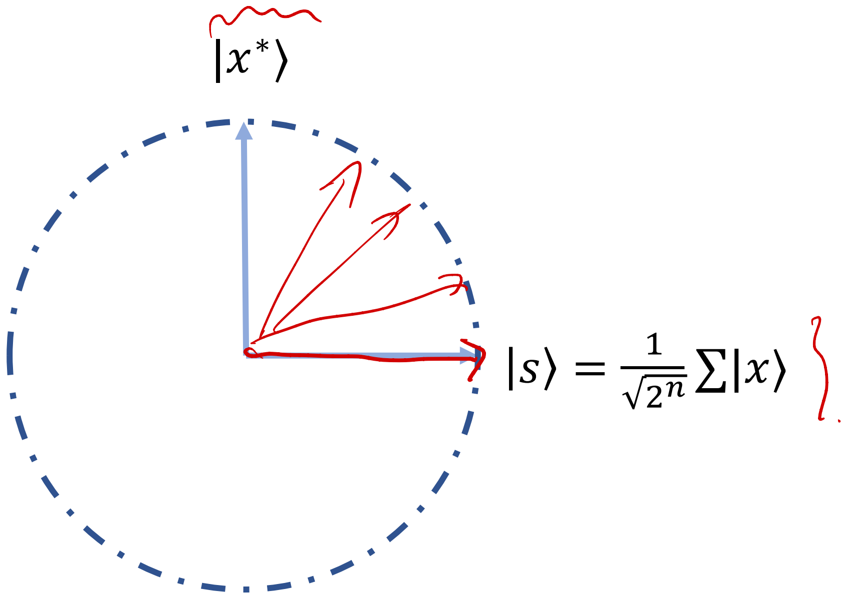
Unstructured search

Search problem: Given black-box access to $f: \{0,1\}^n \rightarrow \{0,1\}$, find x such that $f(x) = 1$.

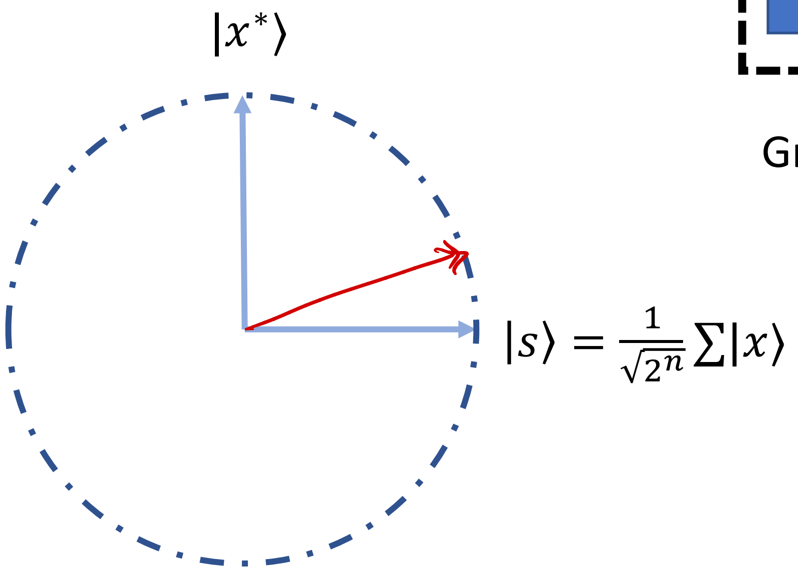
Assume there exists a unique x^* such that $f(x^*) = 1$.



Grover iterate



Starting state of algorithm

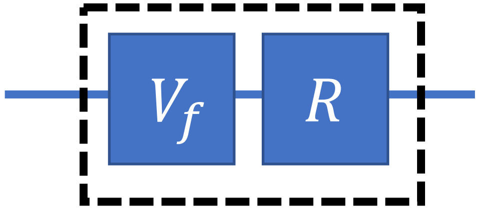


After one Grover iterate

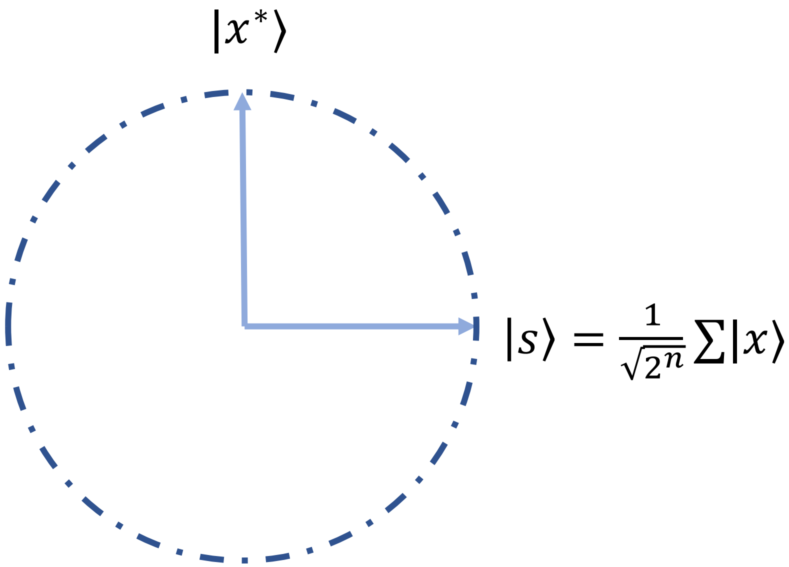
Unstructured search

Search problem: Given black-box access to $f: \{0,1\}^n \rightarrow \{0,1\}$, find x such that $f(x) = 1$.

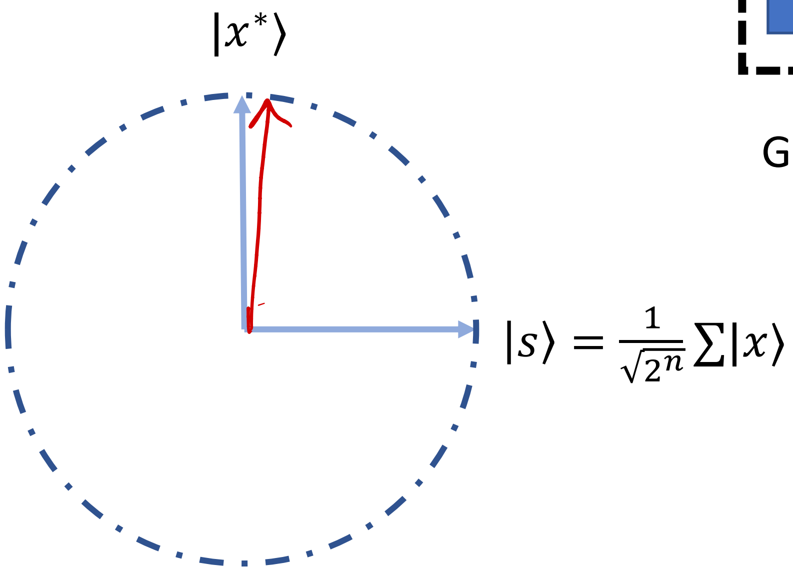
Assume there exists a unique x^* such that $f(x^*) = 1$.



Grover iterate



Starting state of algorithm



after $O\left(\sqrt{2^n}\right)$ iterates

Unstructured search

Search problem: Given black-box access to $f: \{0,1\}^n \rightarrow \{0,1\}$, find x such that $f(x) = 1$.

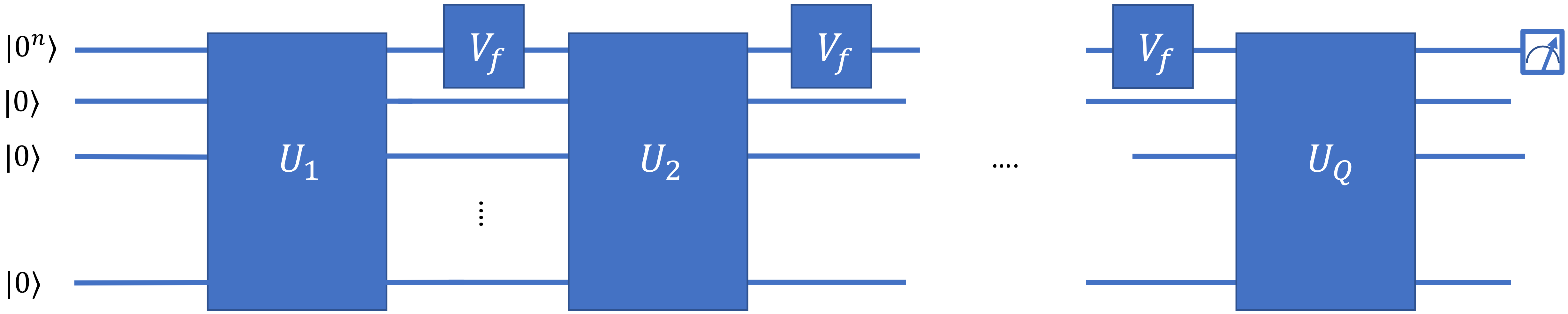
What if there are T solutions x such that $f(x) = 1$?

- If T is known before hand, run $O\left(\sqrt{\frac{2^n}{T}}\right)$ queries.
- If T is unknown, then using more clever algorithm, can still find solution in $O\left(\sqrt{\frac{2^n}{T}}\right)$ queries!

Quantum lower bound for unstructured search

Grover's algorithm is optimal (in terms of query complexity) for solving the unstructured search problem: $\Omega(\sqrt{2^n})$ queries are needed!

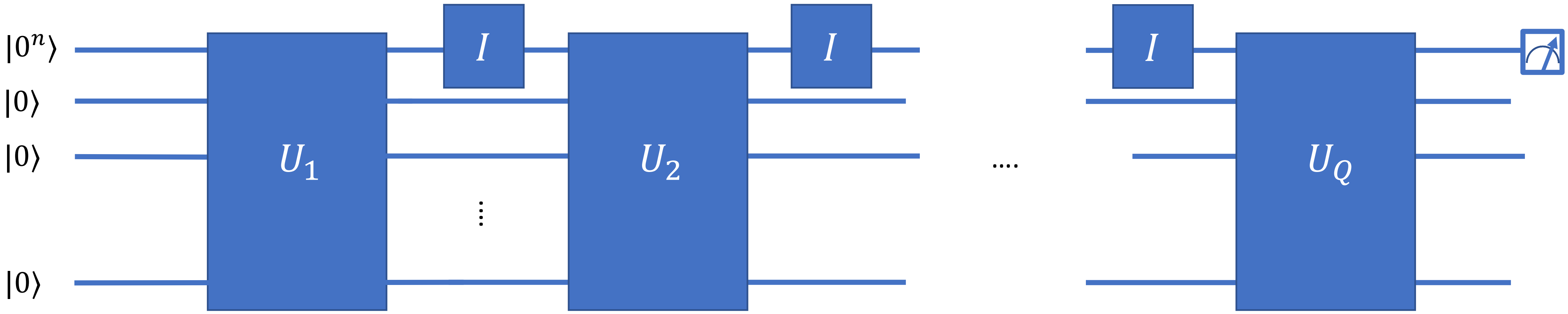
Bennett, Brassard, Bernstein, Vazirani proved this using a *hybrid argument*. Suppose there was a Q-query algorithm for unstructured search, for $Q \ll \sqrt{2^n}$.



Quantum lower bound for unstructured search

Grover's algorithm is optimal (in terms of query complexity) for solving the unstructured search problem: $\Omega(\sqrt{2^n})$ queries are needed!

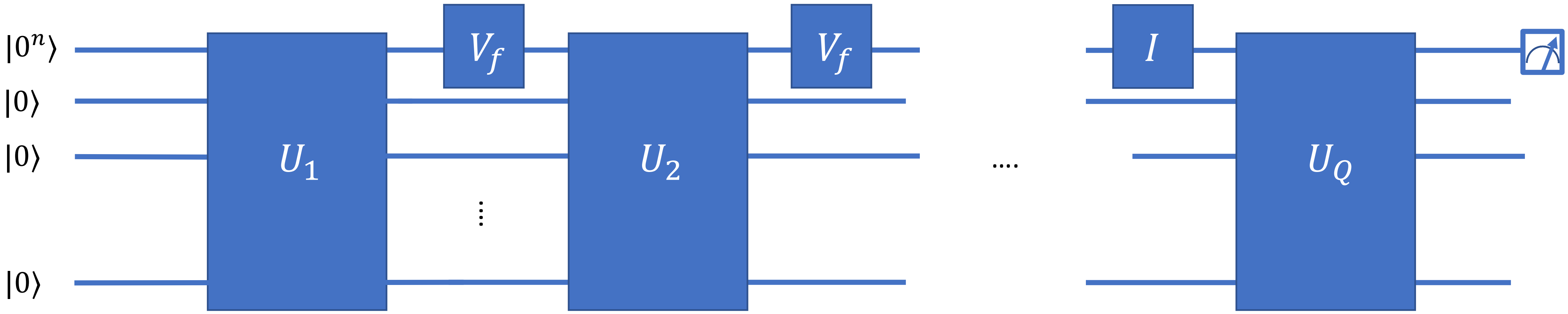
Bennett, Brassard, Bernstein, Vazirani proved this using a *hybrid argument*. Suppose there was a Q-query algorithm for unstructured search, for $Q \ll \sqrt{2^n}$.



Quantum lower bound for unstructured search

Grover's algorithm is optimal (in terms of query complexity) for solving the unstructured search problem: $\Omega(\sqrt{2^n})$ queries are needed!

Bennett, Brassard, Bernstein, Vazirani proved this using a *hybrid argument*. Suppose there was a Q-query algorithm for unstructured search, for $Q \ll \sqrt{2^n}$.



Generalizations of Grover search

- Quantum Counting

- Amplitude Amplification