Interactive Shallow Clifford Circuits: Quantum advantage against NC^1 and beyond

Daniel Grier
University of Waterloo

Luke Schaeffer
University of Waterloo

Quantum advantage with shallow circuits

Bravyi, Gosset, König (2017): There is a relation task solved by a constant-depth quantum circuit that cannot be solved by any constant-depth classical circuit with bounded fan-in gates.

→ Additional nice properties:
  Simple gate set: classically-controlled Clifford gates
  Simple circuit topology: gates are local on the 2D grid

→ No conjectures or assumptions necessary

Caveat: Bounded fan-in, constant-depth, classical circuits are weak.

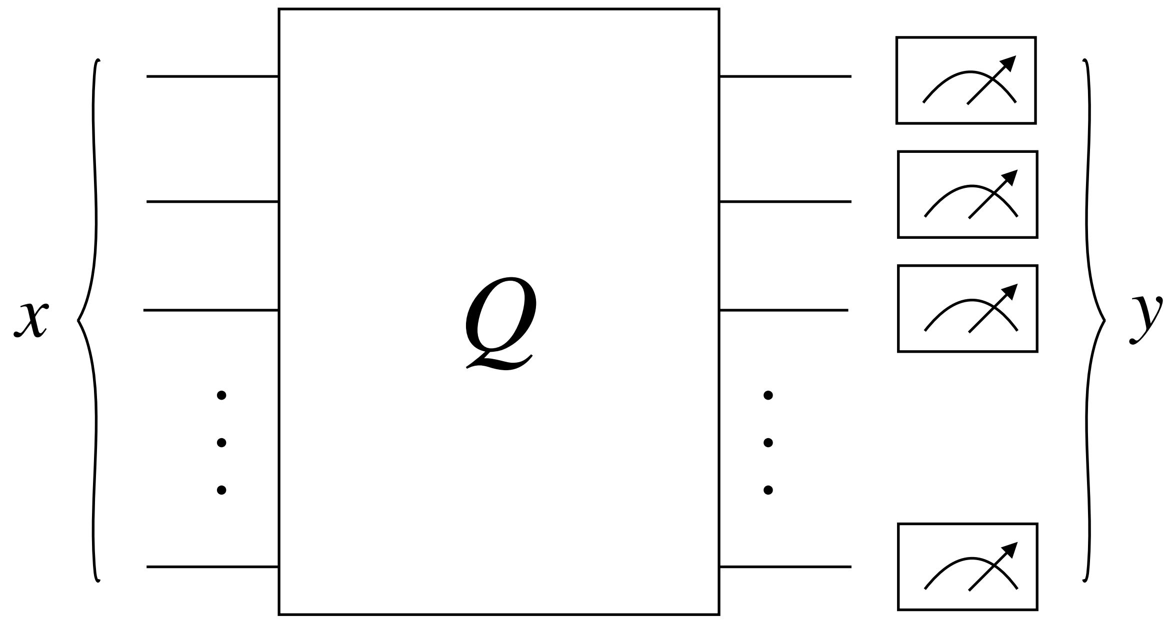
→ **Bene Watts, Kothari, Schaeffer, Tal (2019):**
Improved to *unbounded* fan-in circuits with AND, OR, and NOT gates.

BGK relation task:

Given $x \in \{0,1\}^n$

Output $y \in \{0,1\}^n$

s.t. $|\langle y | Q | x \rangle| > 0$



New separations from interactivity

Theorem: There is a 2-round *interactive* task which can be solved by a constant-depth quantum circuit that

Unconditional: Cannot be solved by constant-depth circuits with unbounded AND, OR, NOT, and PARITY gates.

Complexity-theoretic: Assuming L $\neq \oplus$L, cannot be solved by logarithmic-space Turing machines.

Morally the same problem from BGK.

Small complexity classes

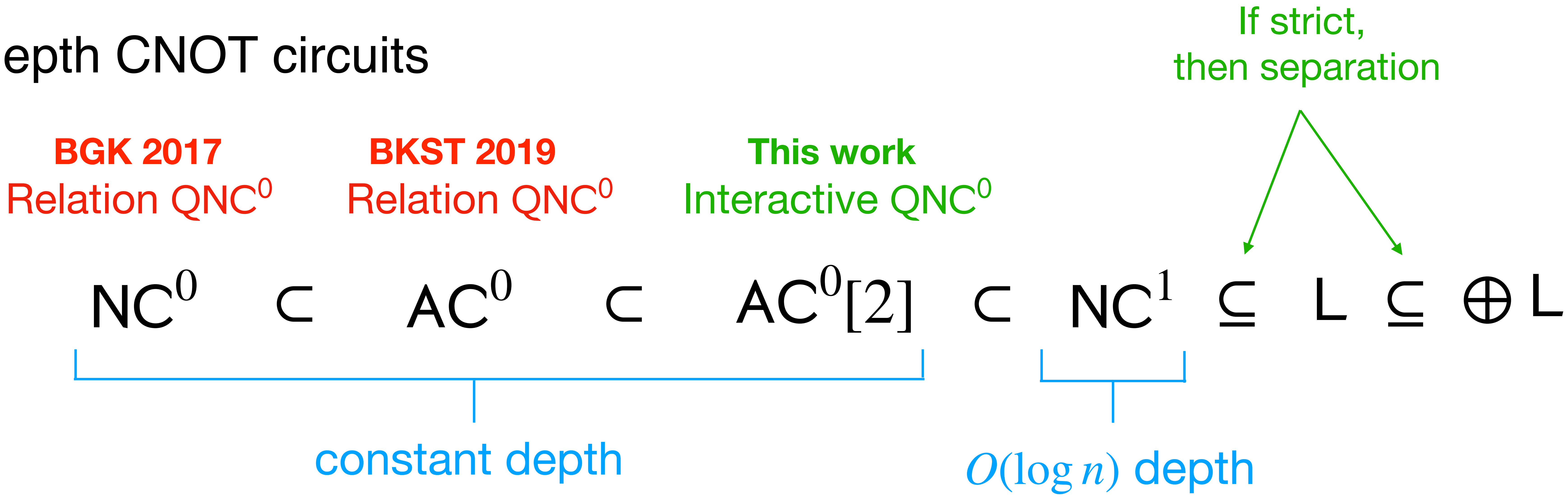
NC : bounded fan-in AND, OR, and NOT gates

AC : unbounded fan-in AND, OR, and NOT gates

AC[2] : unbounded fan-in AND, OR, NOT, and PARITY gates

L : Log-space Turing machines

$\oplus$ L : poly-depth CNOT circuits



If strict,
then separation

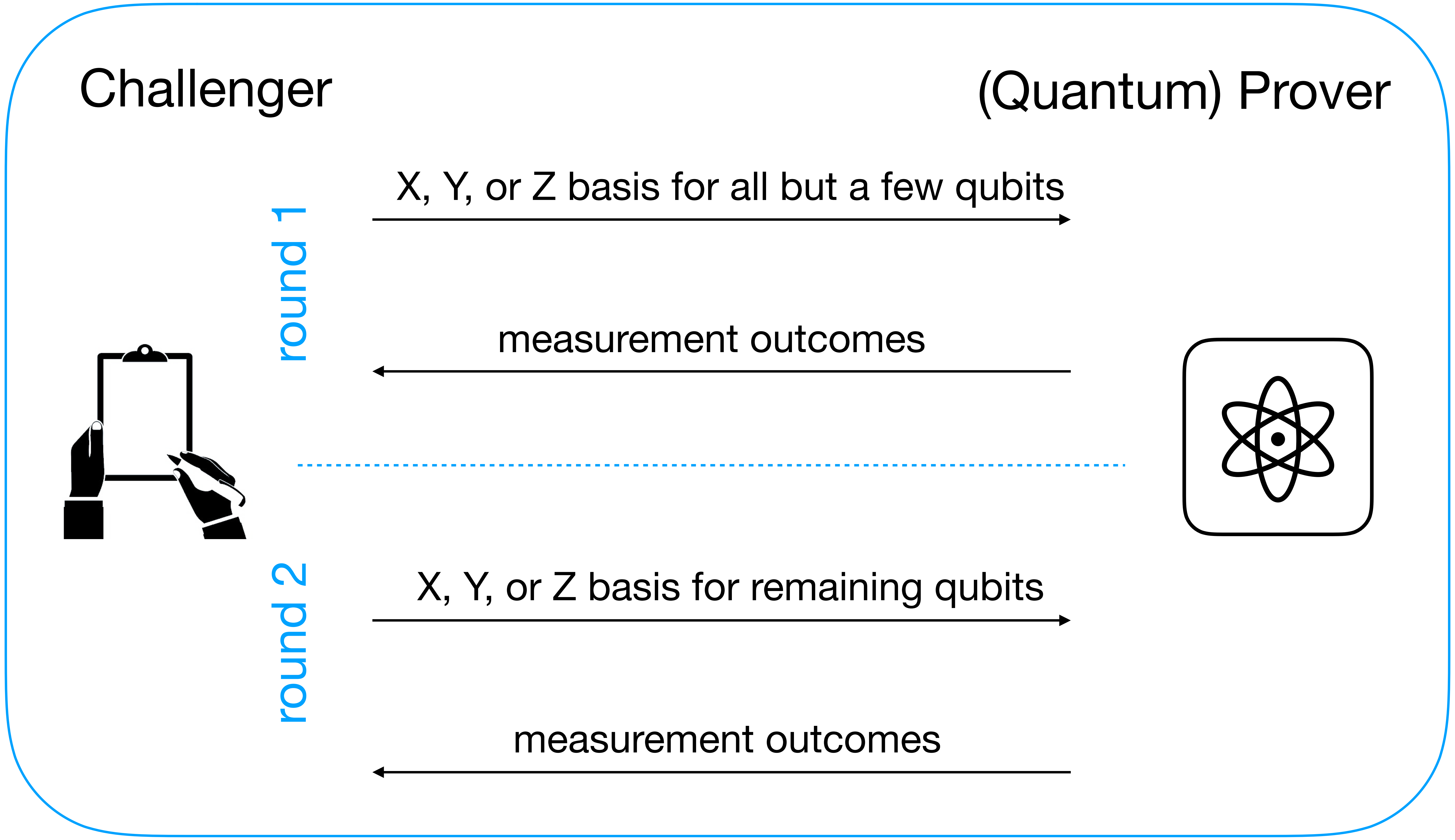
BGK 2017
Relation QNC^0

BKST 2019
Relation QNC^0

This work
Interactive QNC^0

$$\underbrace{\mathrm{NC}^0 \subset \mathrm{AC}^0 \subset \mathrm{AC}^0[2]}_{\text{constant depth}} \subset \underbrace{\mathrm{NC}^1}_{O(\log n)\text{ depth}} \subseteq \mathrm{L} \subseteq \oplus \mathrm{L}$$

Interactive task



Challenger

(Quantum) Prover

round 1

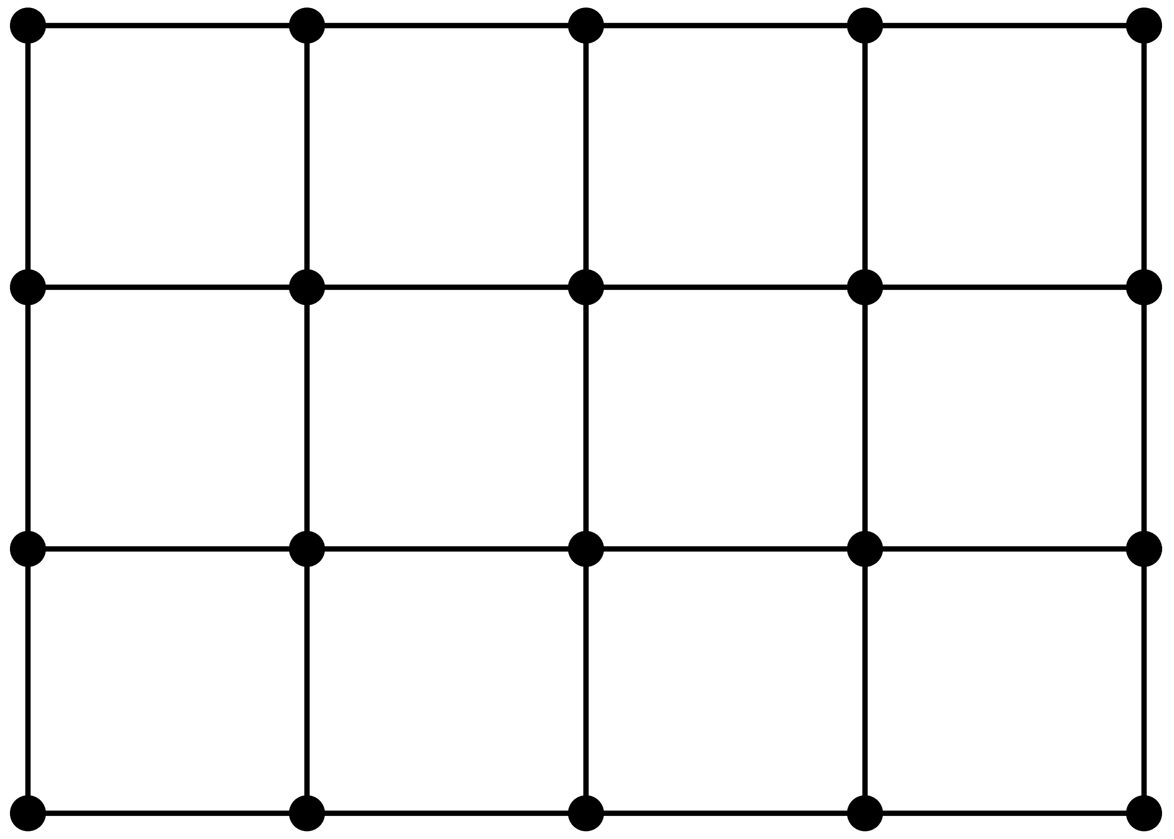
X, Y, or Z basis for all but a few qubits

measurement outcomes

round 2

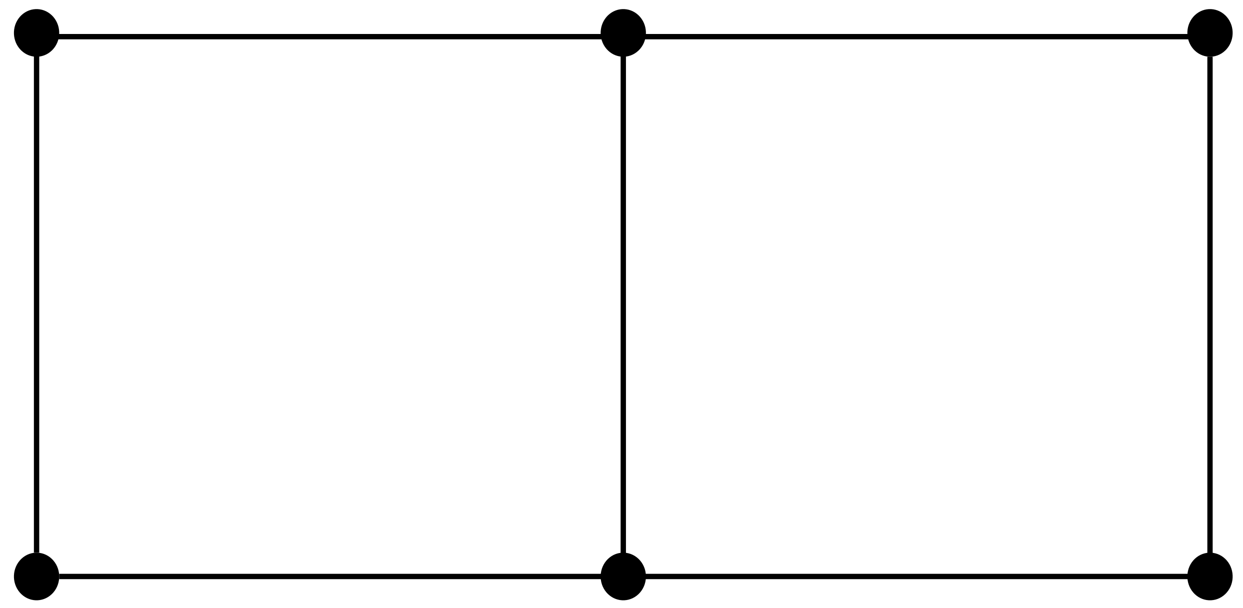
X, Y, or Z basis for remaining qubits

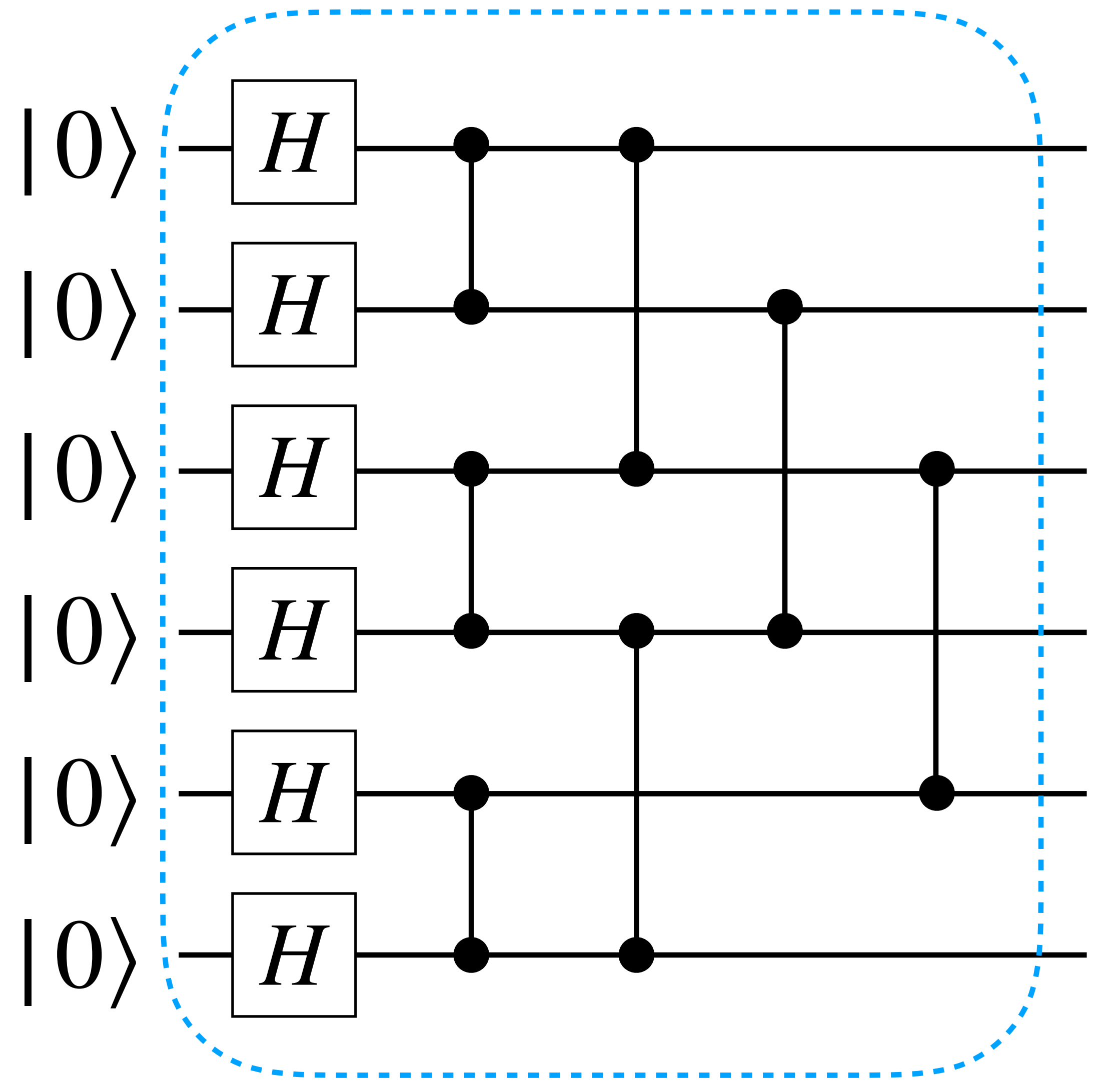
measurement outcomes



$$\sum_{x} \prod_{(i,j)\in E} (-1)^{x_i x_j} |x\rangle$$

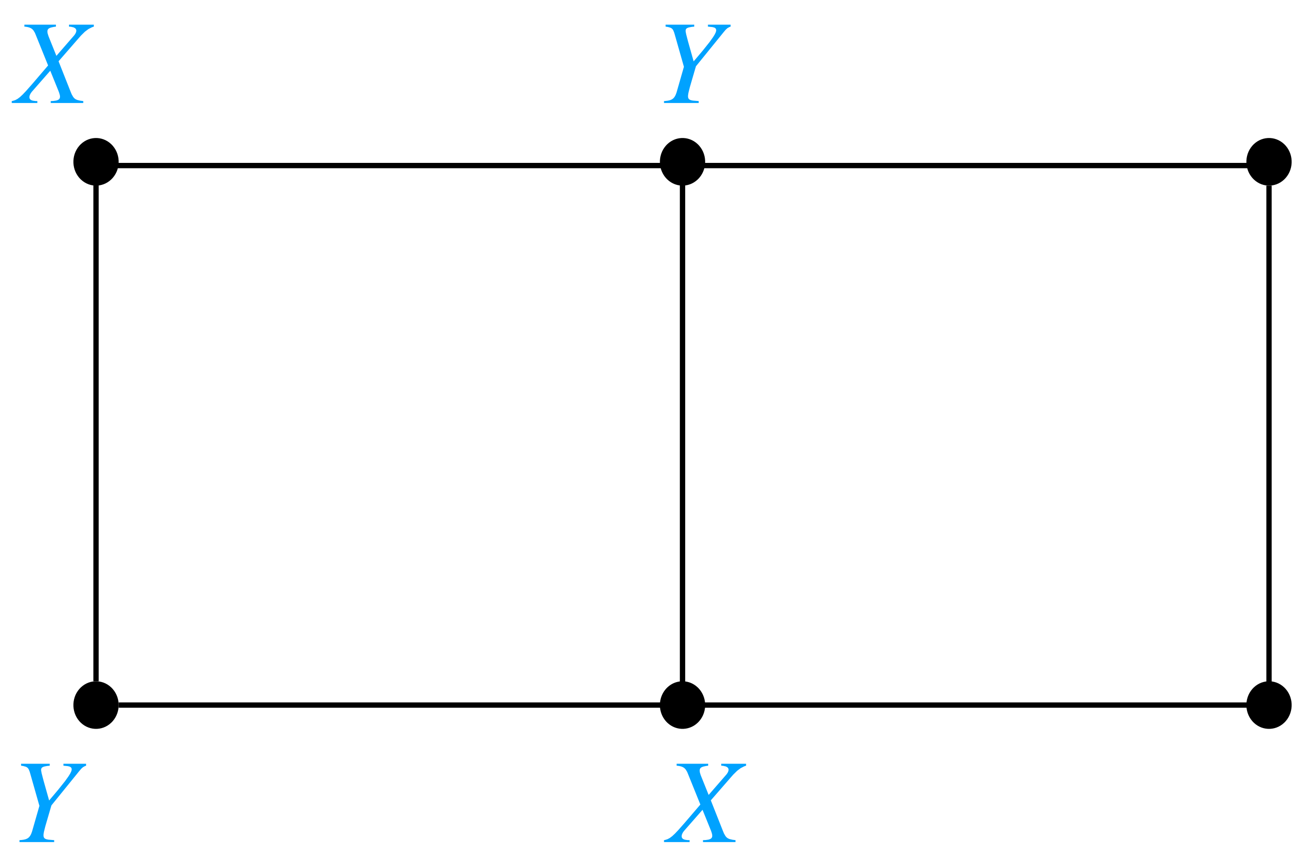
Interactive quantum task - Example

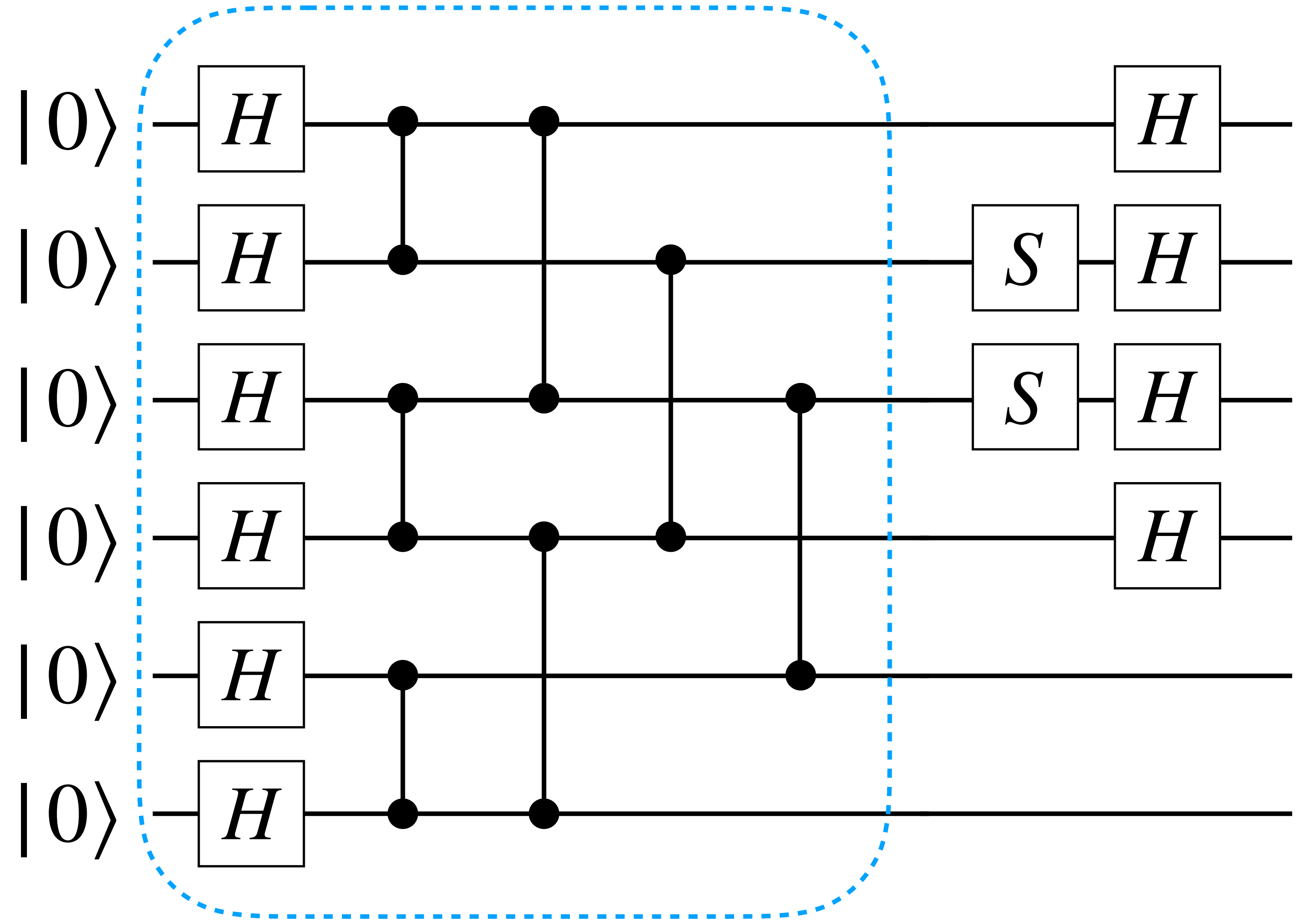




prepare cluster state

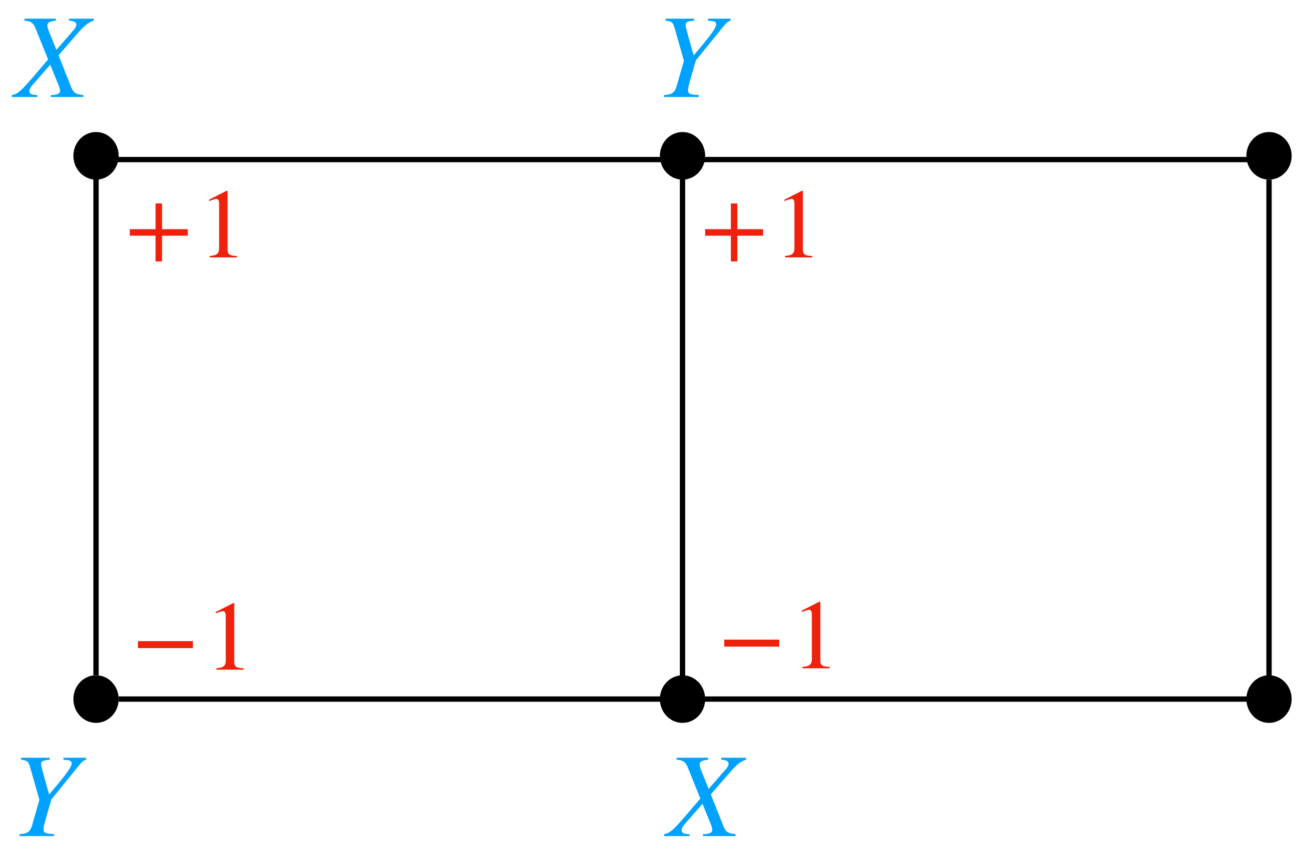
Interactive quantum task - Example

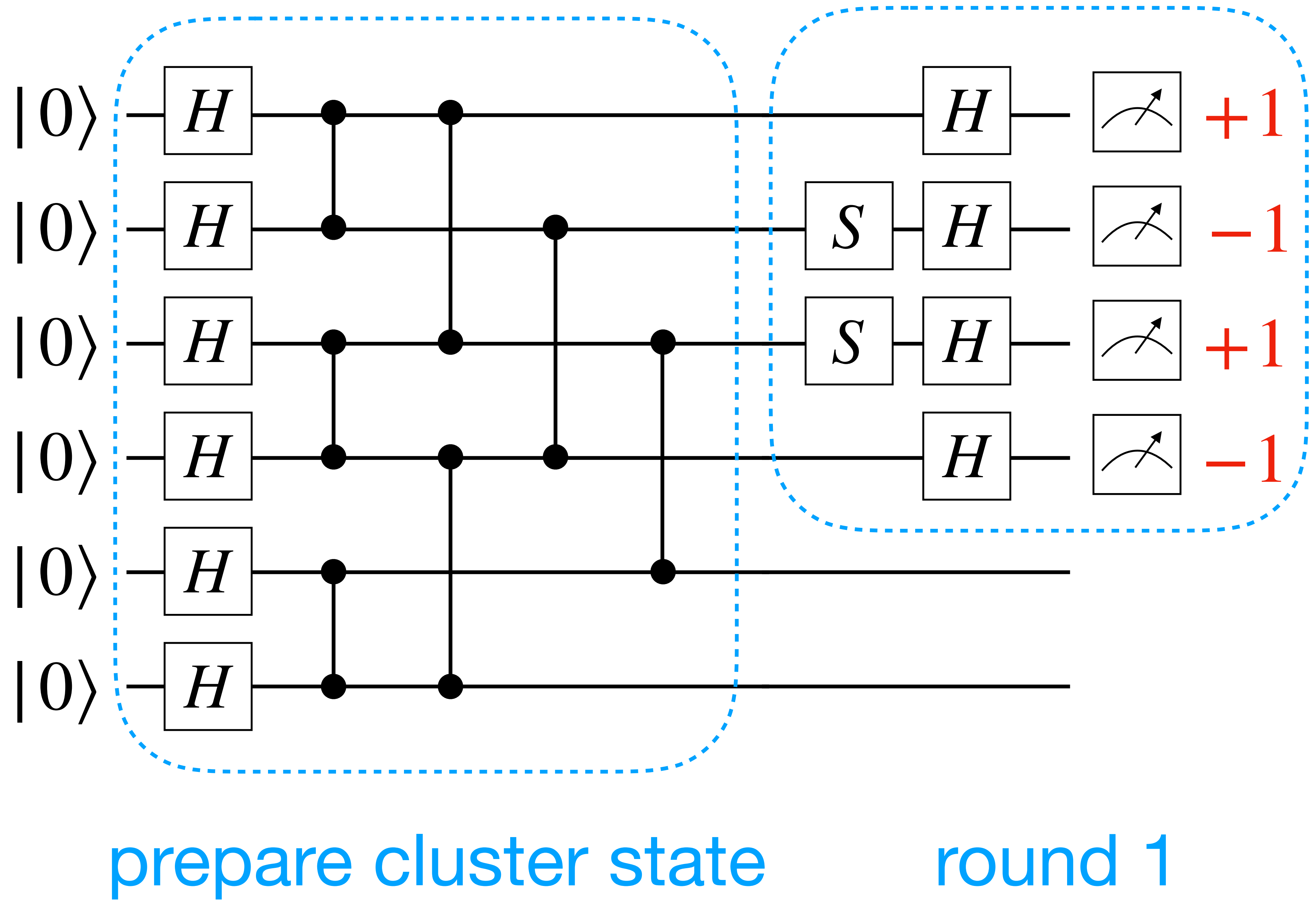




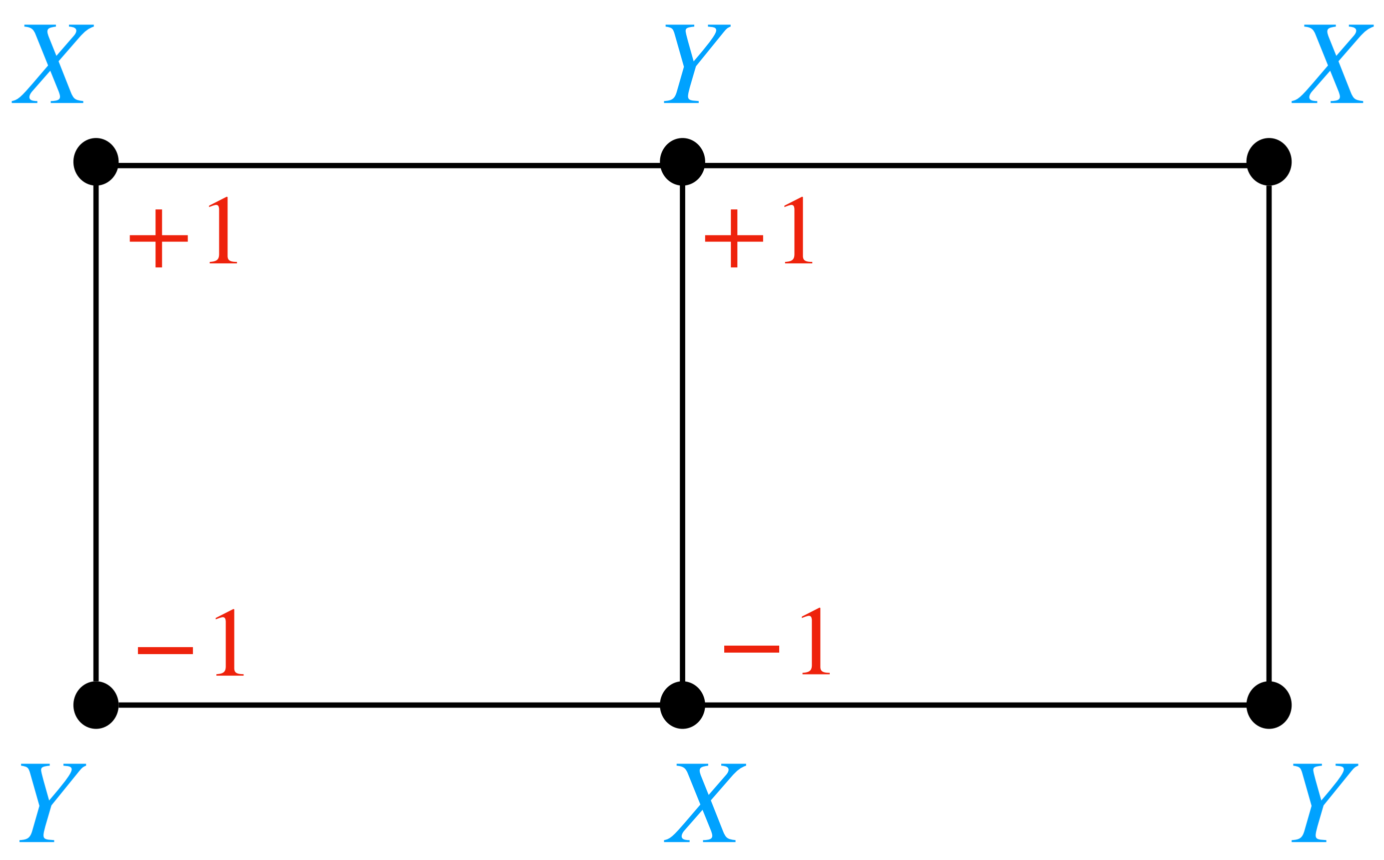
prepare cluster state

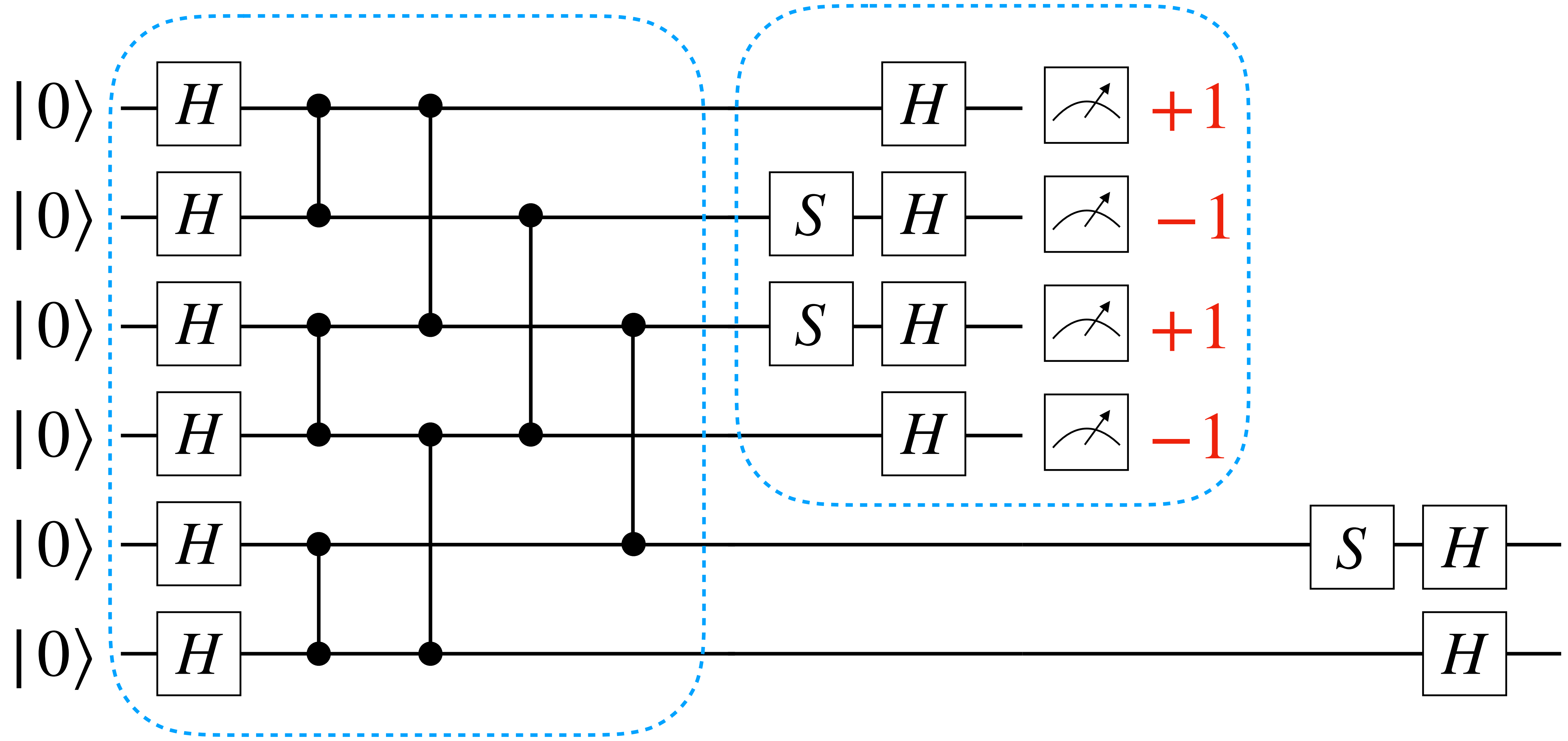
Interactive quantum task - Example





Interactive quantum task - Example

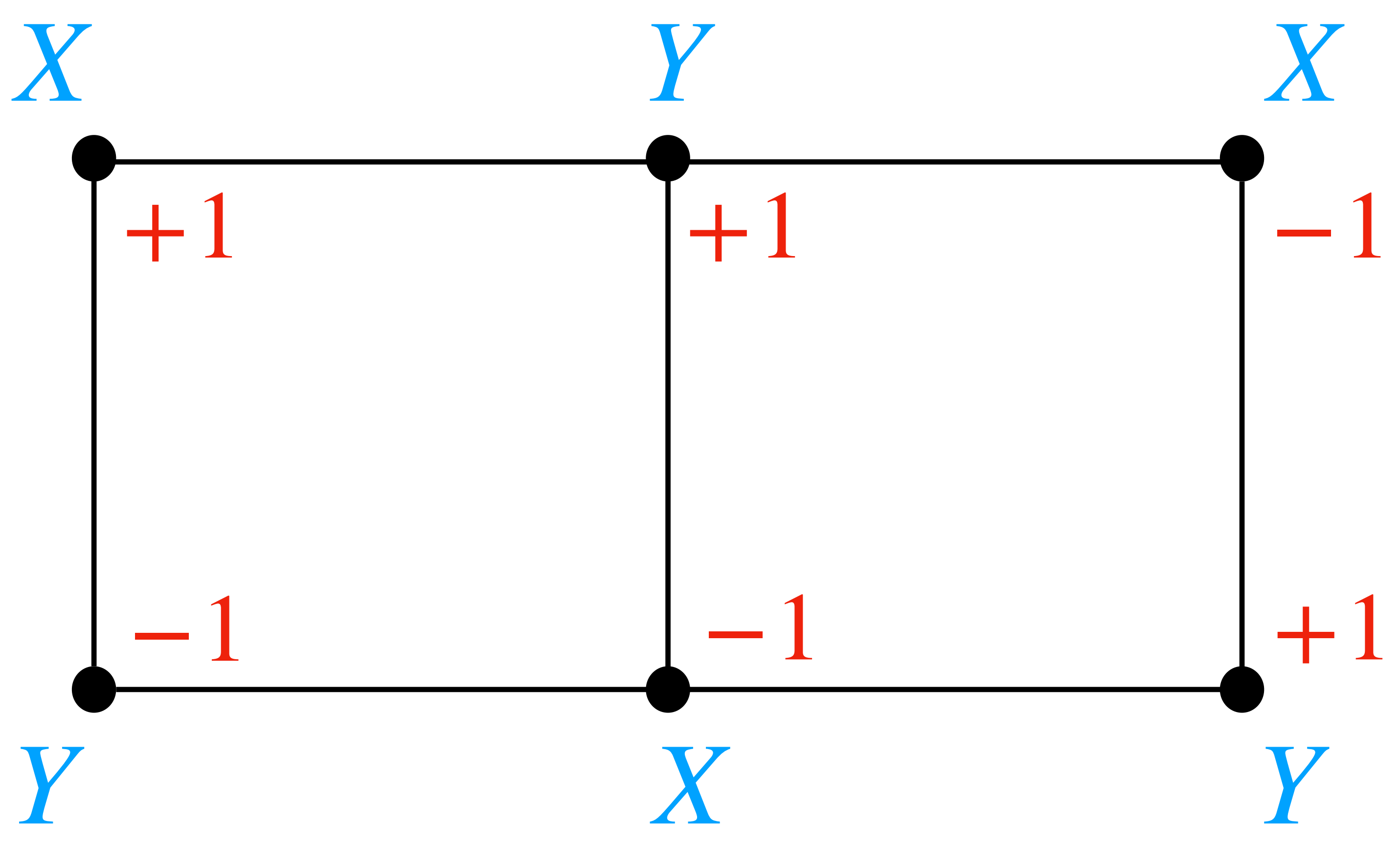


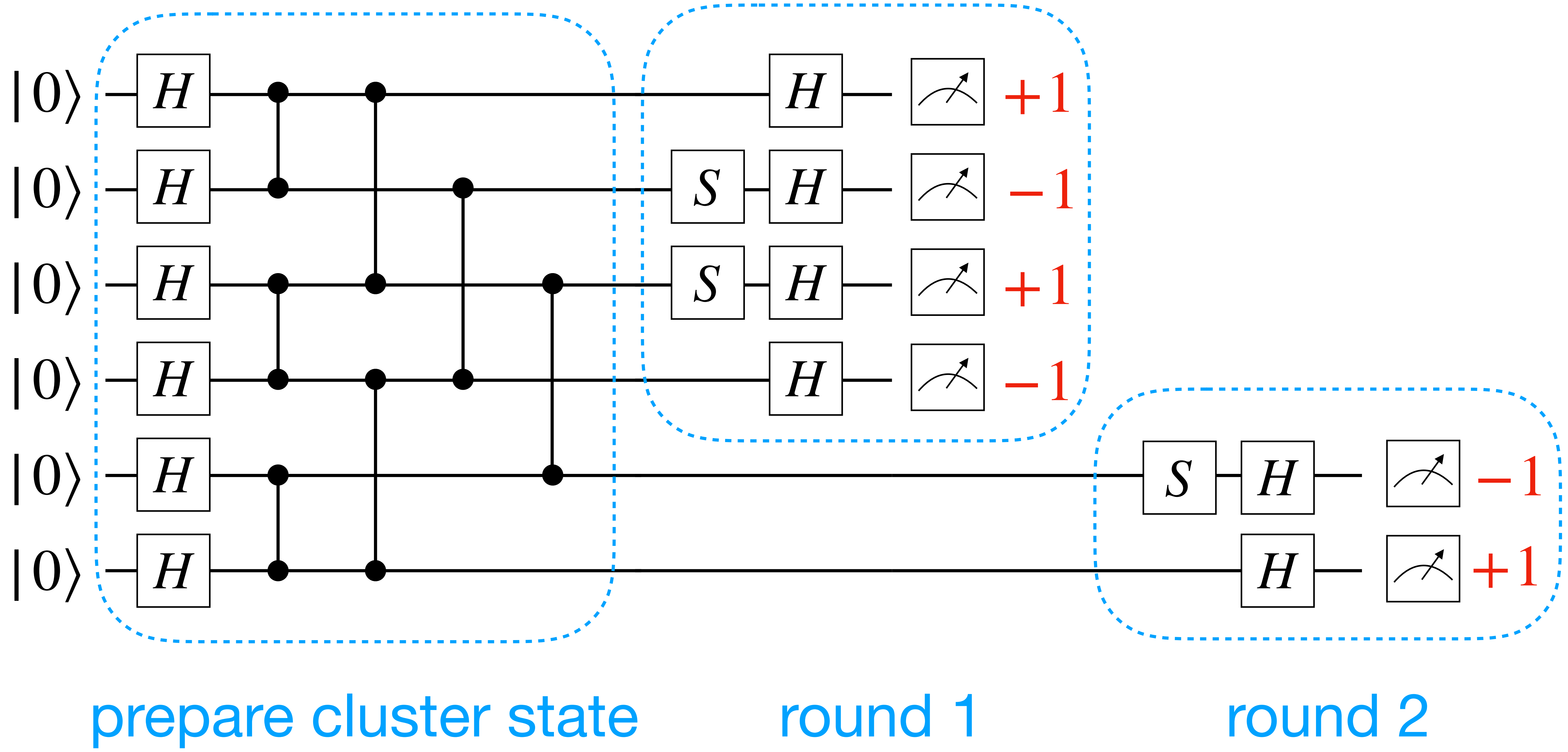


prepare cluster state

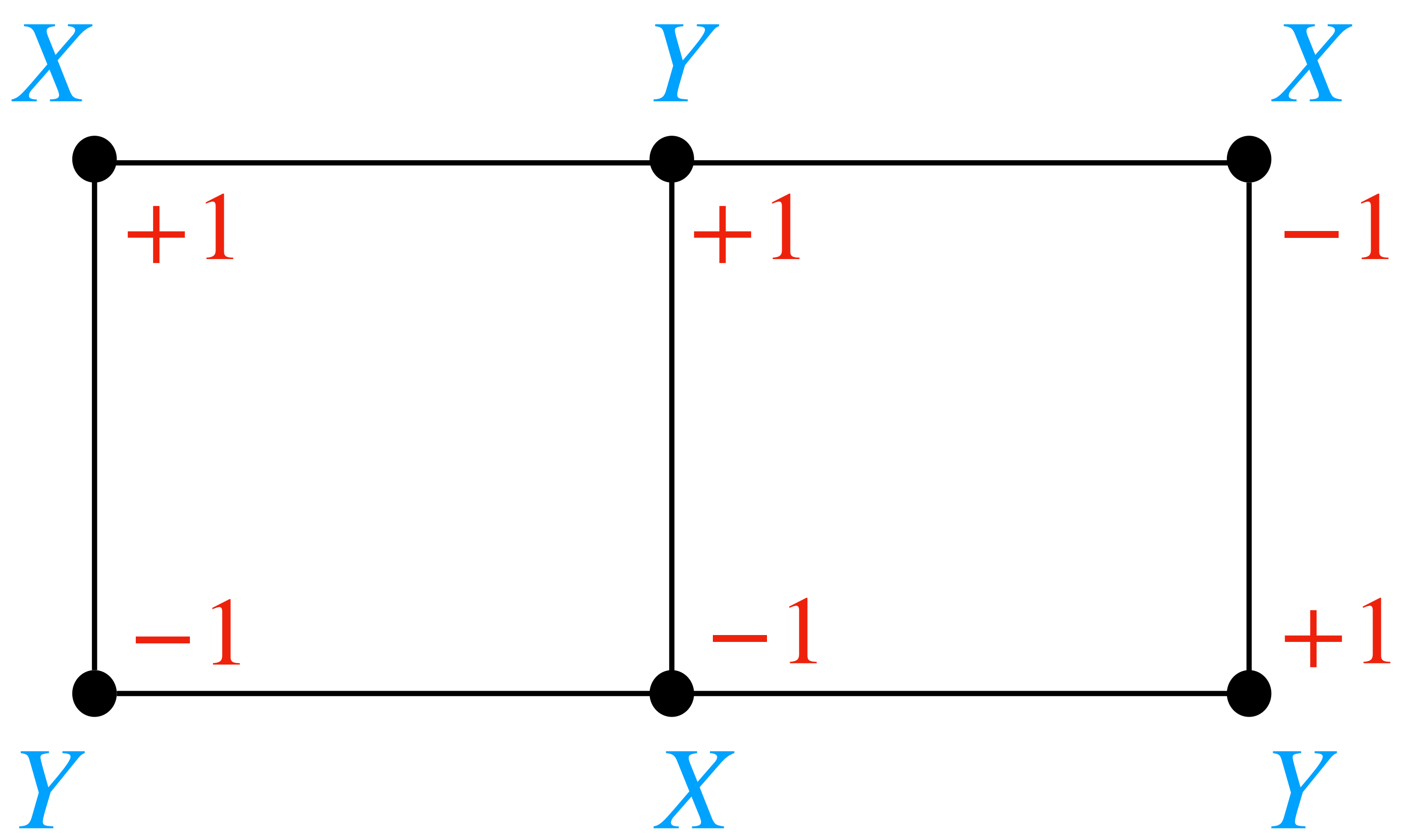
round 1

Interactive quantum task - Example

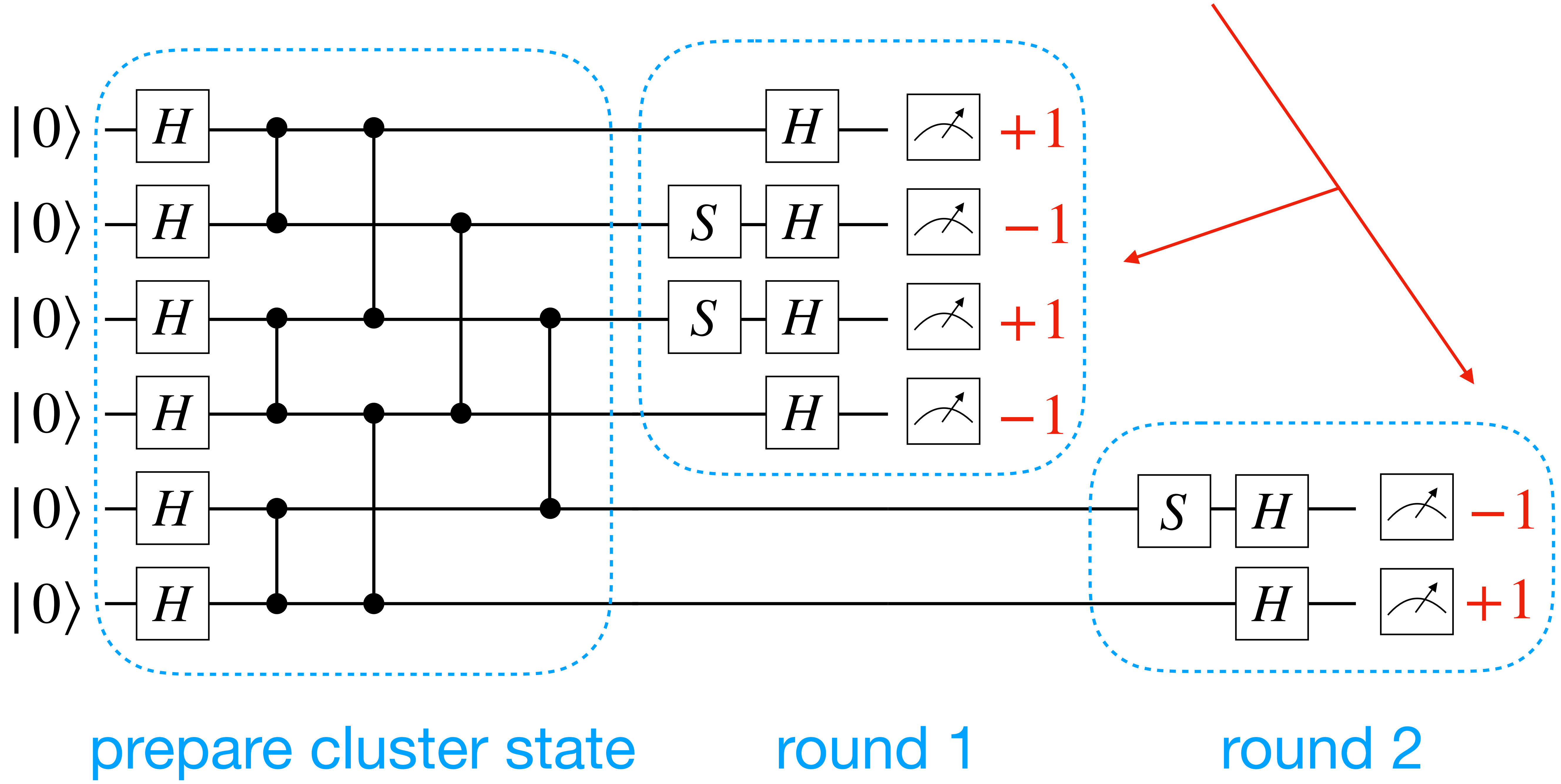




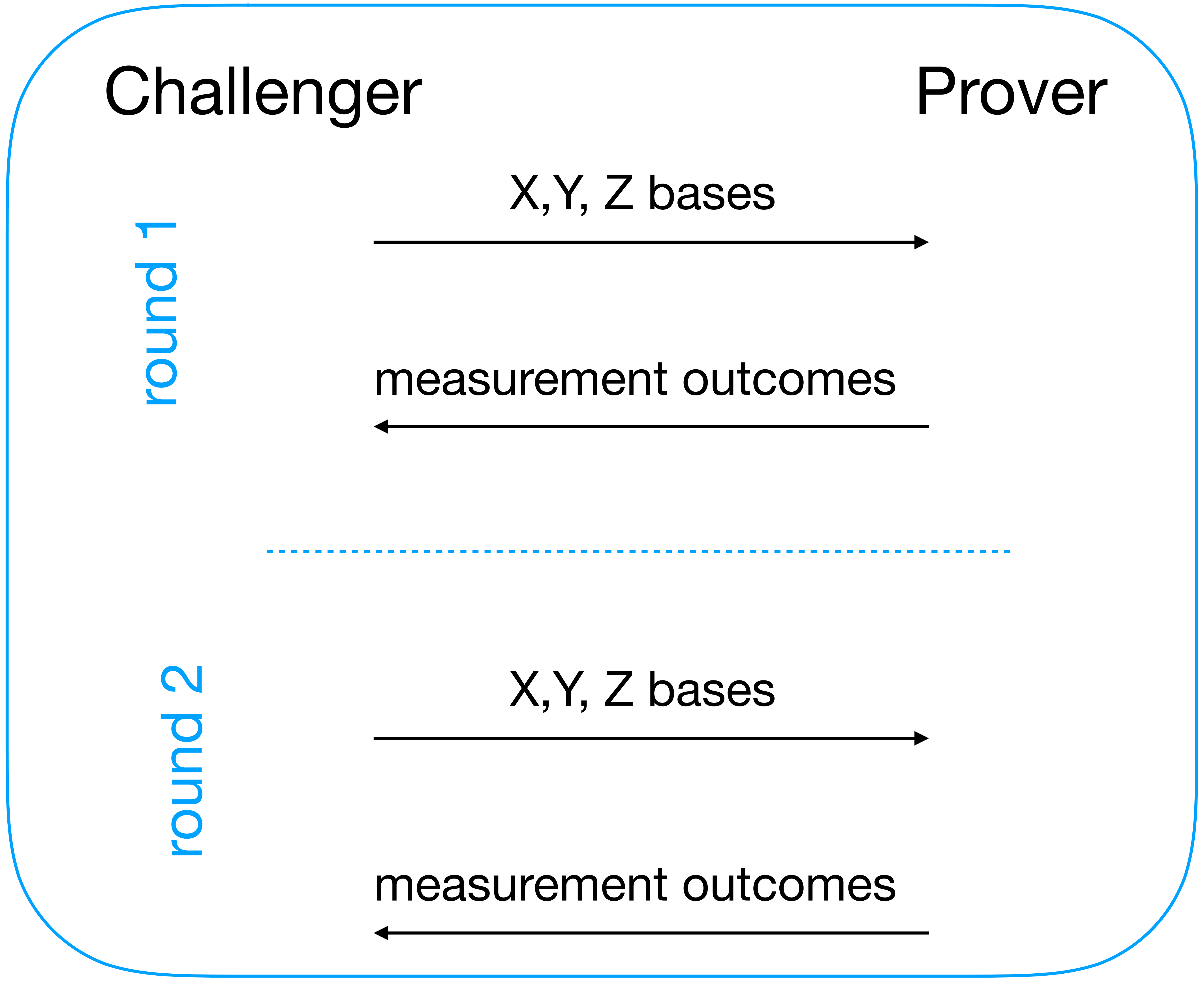
Interactive quantum task - Example



Classical simulation can return *any* valid measurement outcome



Quantum vs. classical interactive tasks



Challenger

Prover

round 1

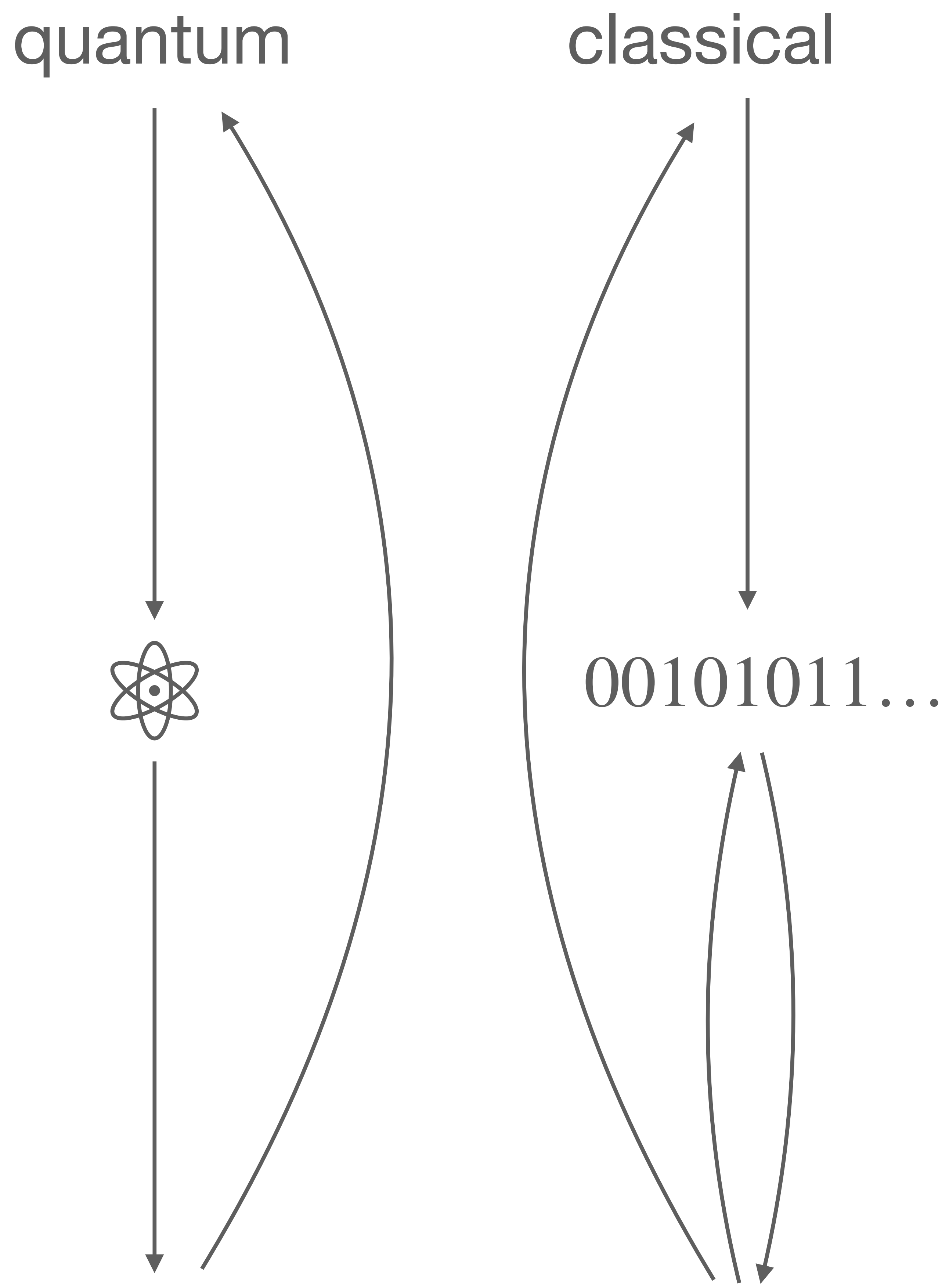
X,Y, Z bases

measurement outcomes

round 2

X,Y, Z bases

measurement outcomes



Key Idea: Any classical simulation must have a *classical* representation of the state between round 1 and round 2.

Can rewind classical simulation to measure 2nd round state multiple times

Main theorem - classical simulation is hard

Theorem: Suppose there is a classical simulator (R) which can solve the 2-round measurement problem on grids of width m.

Then,

$m = 1:$ R solves $\mathrm{AC}^0[6]$ problems $\mathrm{AC}^0[6] \subseteq (\mathrm{AC}^0)^R$

$m = 2:$ R solves NC^1 problems $\mathrm{NC}^1 \subseteq (\mathrm{AC}^0)^R$

$m = n:$ R solves $\oplus\mathrm{L}$ problems $\oplus\mathrm{L} \subseteq (\mathrm{AC}^0)^R$

Warning: Theorem does not imply that QNC^0 circuits solve $\oplus$L-hard problems.

Corollary: There is no $\mathrm{AC}^0[2]$ circuit for the 2-round measurement problem on the $2 \times n$ grid.

proof: $\mathrm{NC}^1 \subseteq (\mathrm{AC}^0)^{\mathrm{AC}^0[2]} = \mathrm{AC}^0[2]$ False: Contradicts Razborov-Smolensky theorem

Proof goal: NC^1-hardness

Reduction: If classical device can solve the 2-round measurement problem, then it can solve the Clifford gate multiplication problem.

Clifford gate multiplication:

Input: 2-qubit Clifford gates $g_1, g_2, \ldots, g_n$

Output: $g_n \cdots g_2 g_1$

Fact: Clifford gate multiplication is NC^1-hard. → Even when product is always $I \otimes I$ or $H \otimes H$.

Proof Outline (high level):

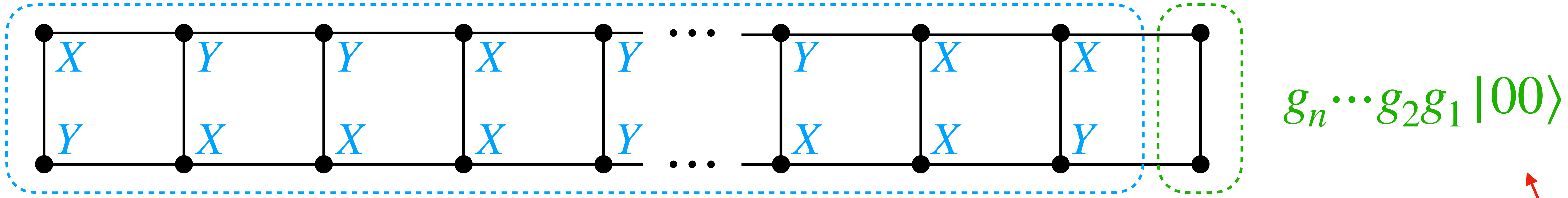
Round 1 - Use measurement-based computation to create $g_n \cdots g_2 g_1 |00\rangle$

Round 2 - Use rewinding ability to make many measurements

- Determine if state is $|00\rangle$ or $|{+}{+}\rangle$

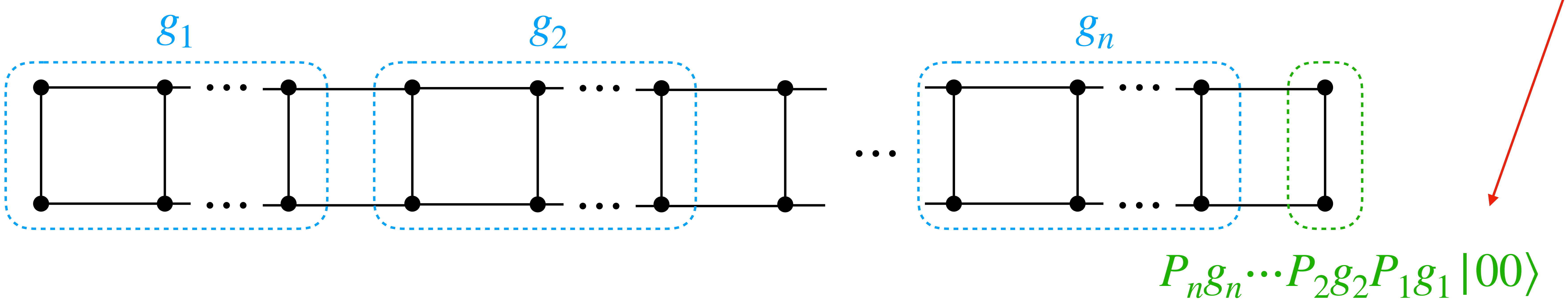
Round 1: Measurement-based computation

Ideal situation:



$g_n \cdots g_2 g_1 |00\rangle$

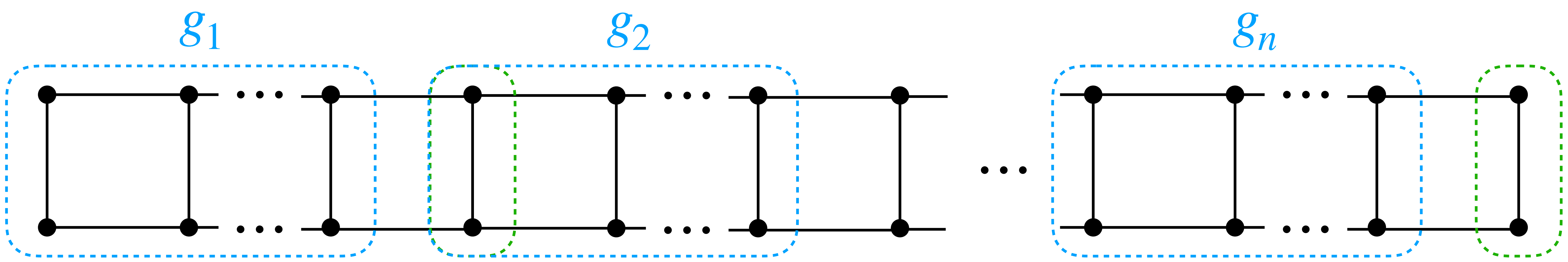
Fact (Raussendorf, Browne, Briegel 2008):
For any 2-qubit Clifford gate g, there is a set of X and Y measurements on the 2×20 grid such that the unmeasured qubits are in the state $Pg\,|00\rangle$ where the Pauli P depends on the measurement outcomes.



$P_n g_n \cdots P_2 g_2 P_1 g_1 |00\rangle$

These states are not the same

Round 1: Measurement-based computation



$P_n g_n \cdots P_2 g_2 P_1 g_1 |00\rangle$

Reason: The usual measurement-based computation technique is adaptive.

First gate (g_1): $P_1 g_1 |00\rangle$

Second gate $(g_2 P_1)$: $P_2 g_2 P_1 P_1 g_1 |00\rangle = P_2 g_2 g_1 |00\rangle$

⋮

Would require many rounds of interaction

Fact: For any Clifford g and Pauli P

$$gP = gPg^\dagger g = (gPg^\dagger)g = P'g$$

$$P_n g_n \cdots P_2 g_2 P_1 g_1 |00\rangle = P g_n \cdots g_2 g_1 |00\rangle$$

Problem:

Computing P from $P_1, P_2, \ldots, P_n$ is NC^1-hard.

Scary: The channel $\rho \mapsto P\rho P^\dagger$ for random Pauli P is the completely depolarizing channel.

Round 2: Many measurements with rewinding

Intuition: A single measurement may not reveal sufficient information to determine the state, but many "non-collapsing" measurements might suffice.

Plan: Use repeated measurements to deduce the stabilizer groups of the state.

Stabilizer group: the group of Pauli operators that fix the state. $\big(P|\psi\rangle = |\psi\rangle\big)$

$$\text{Stabilizer}(P|00\rangle) = \begin{pmatrix} II \\ a\,ZI \\ b\,IZ \\ ab\,ZZ \end{pmatrix} \qquad \text{Stabilizer}(P|{+}{+}\rangle) = \begin{pmatrix} II \\ a\,XI \\ b\,IX \\ ab\,XX \end{pmatrix} \qquad a, b \in \{\pm 1\}$$

Measurement of Pauli P on state $|\psi\rangle$:

If $aP \in$ Stabilizer($|\psi\rangle$), then outcome is $a \in \{\pm 1\}$.

If $aP \notin$ Stabilizer($|\psi\rangle$), then outcome can be either $+1$ or -1.

Round 2: Many measurements with rewinding

Plan: Make many Pauli measurements on the state and hope to receive outcomes which are both +1 and -1.

$$\begin{array}{ccc} XX & YY & ZZ \\ YZ & ZX & XY \\ ZY & XZ & YX \end{array}$$

Observations:

1) Pauli operators along any row/column commute, so we can measure them simultaneously.

Round 2: Many measurements with rewinding

Plan: Make many Pauli measurements on the state and hope to receive outcomes which are both +1 and -1.

$$XX \times YY \times ZZ = -II$$

$$YZ \times ZX \times XY = -II$$

$$ZY \times XZ \times YX = -II$$

Observations:

1) Pauli operators along any row/column commute, so we can measure them simultaneously.
2) If we measure a row, the measurement outcomes multiply to -1.

Round 2: Many measurements with rewinding

Plan: Make many Pauli measurements on the state and hope to receive outcomes which are both +1 and -1.

$$\begin{array}{ccc} XX & YY & ZZ \\ \times & \times & \times \\ YZ & ZX & XY \\ \times & \times & \times \\ ZY & XZ & YX \\ = & = & = \\ II & II & II \end{array}$$

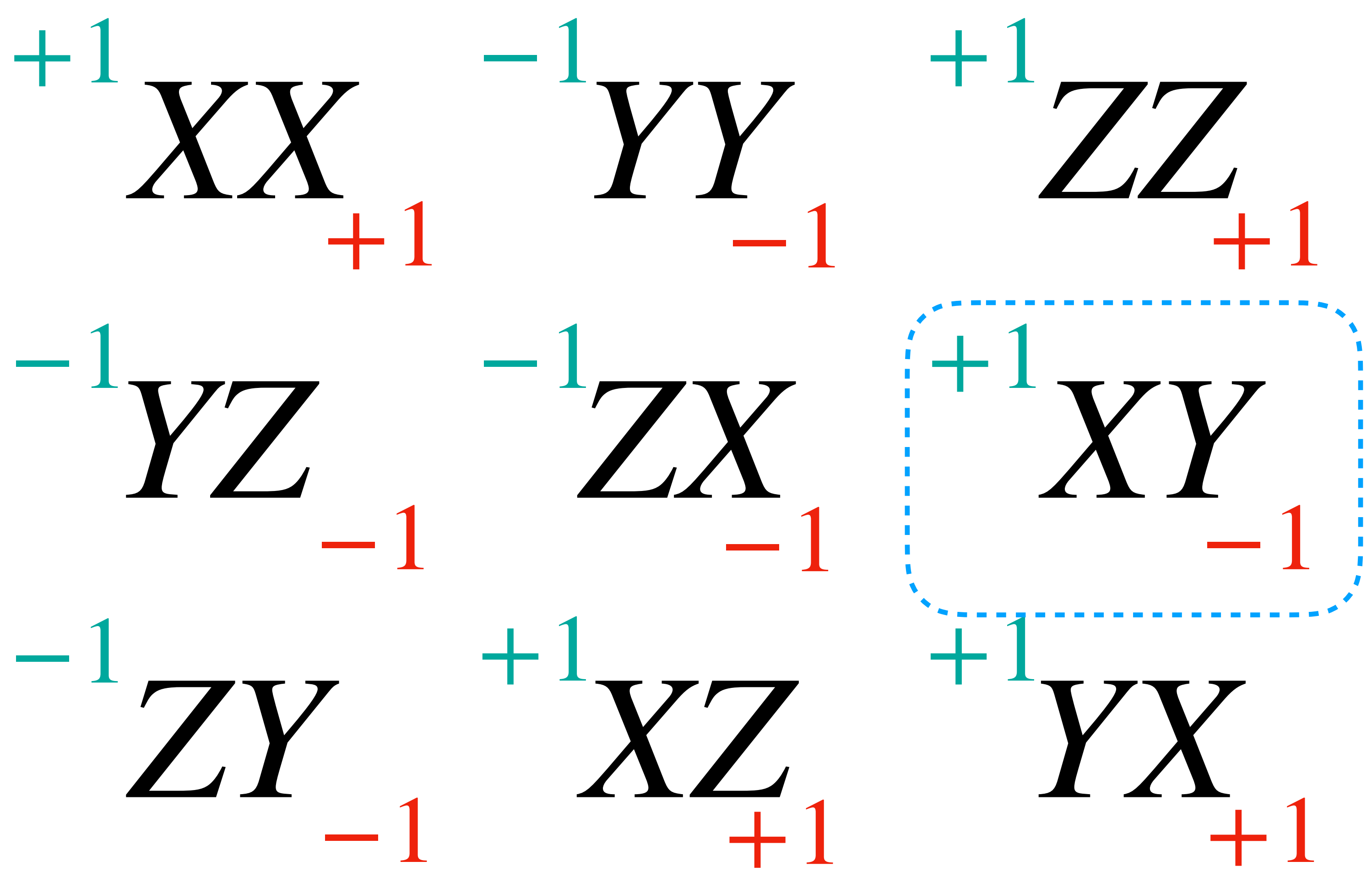
Observations:

1) Pauli operators along any row/column commute, so we can measure them simultaneously.
2) If we measure a row, the measurement outcomes multiply to -1.

   If we measure a column, the measurement outcomes multiply to +1.

Round 2: Many measurements with rewinding

Plan: Make many Pauli measurements on the state and hope to receive outcomes which are both +1 and -1.



${}^{+1}XX_{+1}$	${}^{-1}YY_{-1}$	${}^{+1}ZZ_{+1}$
${}^{-1}YZ_{-1}$	${}^{-1}ZX_{-1}$	${}^{+1}XY_{-1}$
${}^{-1}ZY_{-1}$	${}^{+1}XZ_{+1}$	${}^{+1}YX_{+1}$

Observations:

1) Pauli operators along any row/column commute, so we can measure them simultaneously.
2) If we measure a row, the measurement outcomes multiply to -1.

   If we measure a column, the measurement outcomes multiply to +1.
3) No consistent way to label the square that satisfies row/column conditions.

Round 2: Many measurements with rewinding

In previous example, we were able to deduce XY was not in the stabilizer group of our state, but…

XY does not appear in either stabilizer group

$$\text{Stabilizer}(|00\rangle) = \begin{pmatrix} II \\ ZI \\ IZ \\ ZZ \end{pmatrix} \qquad \text{Stabilizer}(|{+}{+}\rangle) = \begin{pmatrix} II \\ XI \\ IX \\ XX \end{pmatrix}$$

Solution: Randomize the input.

Instead of obtaining an arbitrary non-stabilizer of our state, we get a *random* non-stabilizer.

Open Questions

1) Hardness beyond $\oplus L$?

Theorem: 2-round measurement problem is in $\oplus L$ for Clifford circuits.

2) Allow for classical circuit simulation error?

Theorem: NC^1 reduction still holds when classical circuit errs with probability less than $2/75$.

→ Is this optimal? What about $\oplus L$?

3) Allow the quantum circuit to err?

Theorem (Bravyi, Gosset, König, Tomamichel):
Noisy QNC^0 circuits can solve a relation problem that NC^0 circuits cannot.

→ Can these techniques be ported to the interactive setting?