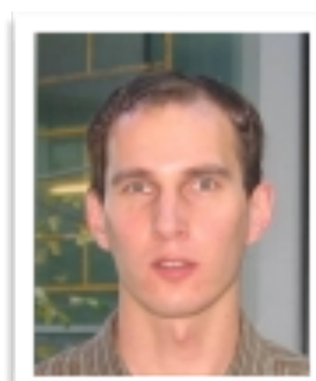
arXiv:1904.01502 (will be presented at FOCS 2019)

Quantum advantage with noisy shallow circuits in 3D

(Wollongong MACAO workshop, 26/11/2019)

Marco Tomamichel
(with Sergey Bravyi, David Gosset, Robert König)

UTS:QSI
CENTRE FOR QUANTUM SOFTWARE AND INFORMATION

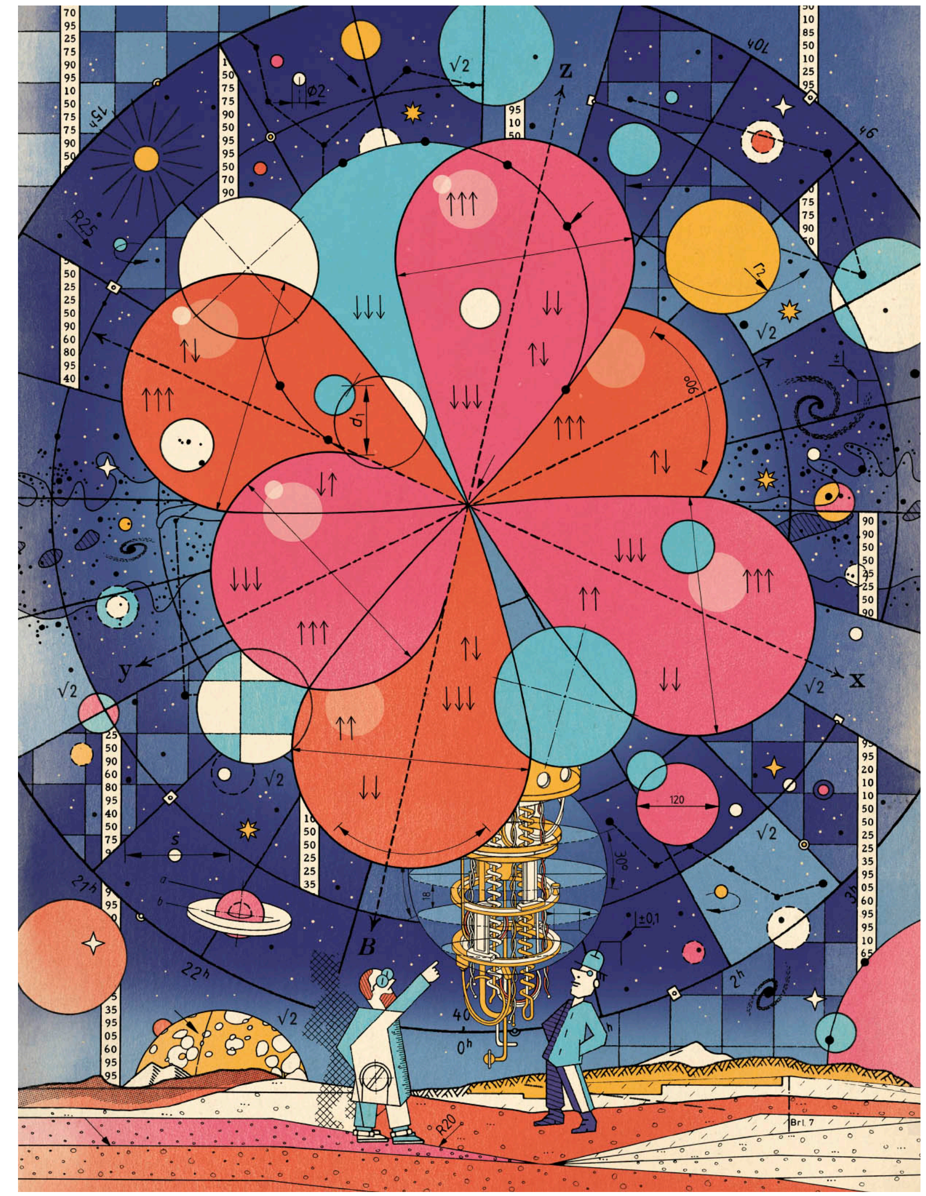


IBM

IQC/Waterloo

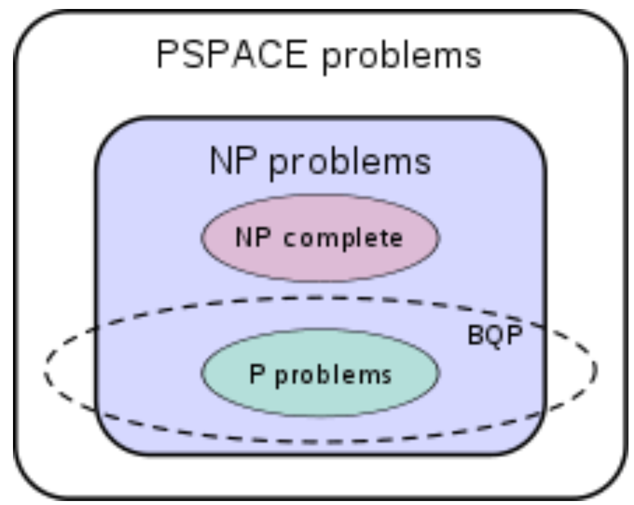
TU Munich

- How to convince the sceptics that quantum computers work?
- It is (relatively) easy to experimentally show a quantum advantage under locality constraints.
  - e.g. Bell violation, where the locality constraints are either assumed or enforced (loophole free)
- Showing a gap between classical and quantum computing is more challenging.



Source: IEEE Spectrum: *The Case Against Quantum Computing*

- We know that P ⊆ BQP ⊆ PSPACE. But we cannot exclude that they are all the same.

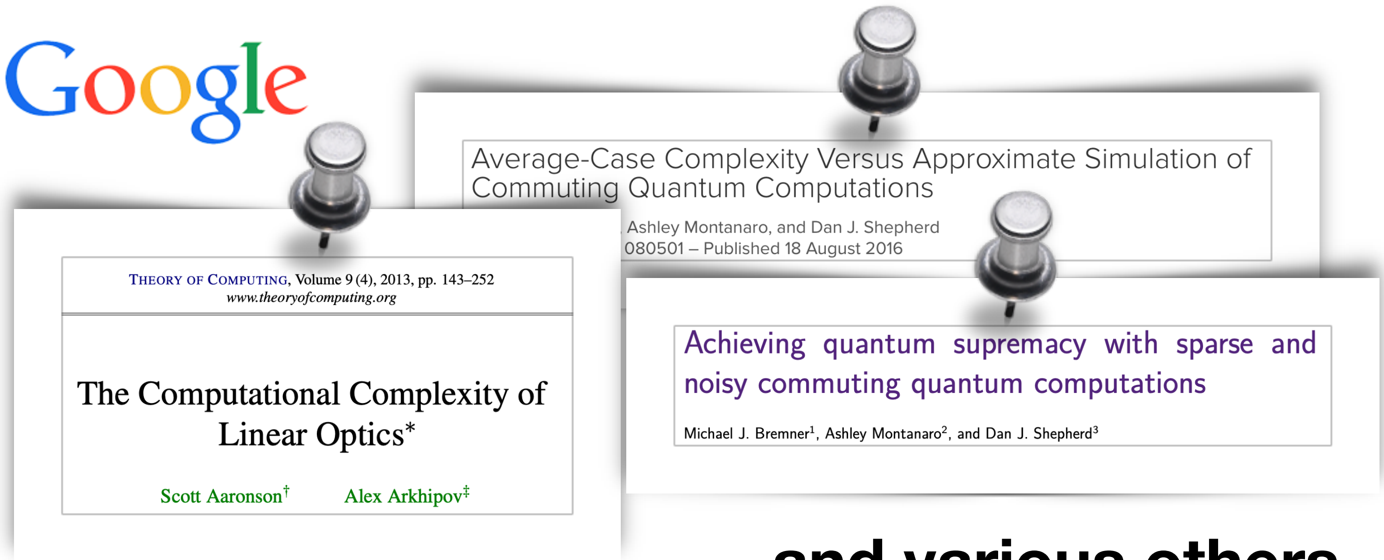


- Showing a separation P ≠ PSPACE would be a major breakthrough in complexity theory.

- P ≠ BQP would imply such a separation. (Thus, let us better try something else.)

Two approaches: Supremacy vs. Advantage

Quantum computational supremacy


Average-Case Complexity Versus Approximate Simulation of Commuting Quantum Computations
Ashley Montanaro, and Dan J. Shepherd
080501 – Published 18 August 2016

Theory of Computing, Volume 9 (4), 2013, pp. 143–252
www.theoryofcomputing.org

The Computational Complexity of Linear Optics*

Scott Aaronson† Alex Arkhipov‡

Achieving quantum supremacy with sparse and noisy commuting quantum computations

Michael J. Bremner[1], Ashley Montanaro[2], and Dan J. Shepherd[3]

and various others

complexity theoretic assumptions
(P ≠ PSPACE and beyond)

no classical computer can solve this problem (if assumptions hold up), but a quantum computer can

sampling problem

feasible with NISQ devices
(tolerates little noise, 2D)

Advantage for restricted circuits


Quantum advantage with shallow circuits

Sergey Bravyi[1], David Gosset[1,*], Robert König[2,†]
+ See all authors and affiliations

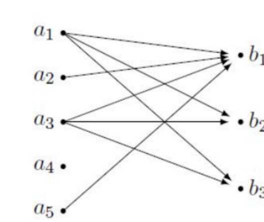
Science 19 Oct 2018:

and this work

circuit restrictions (e.g. low-depth)

no low depth classical can solve the problem, but a low-depth quantum computer can

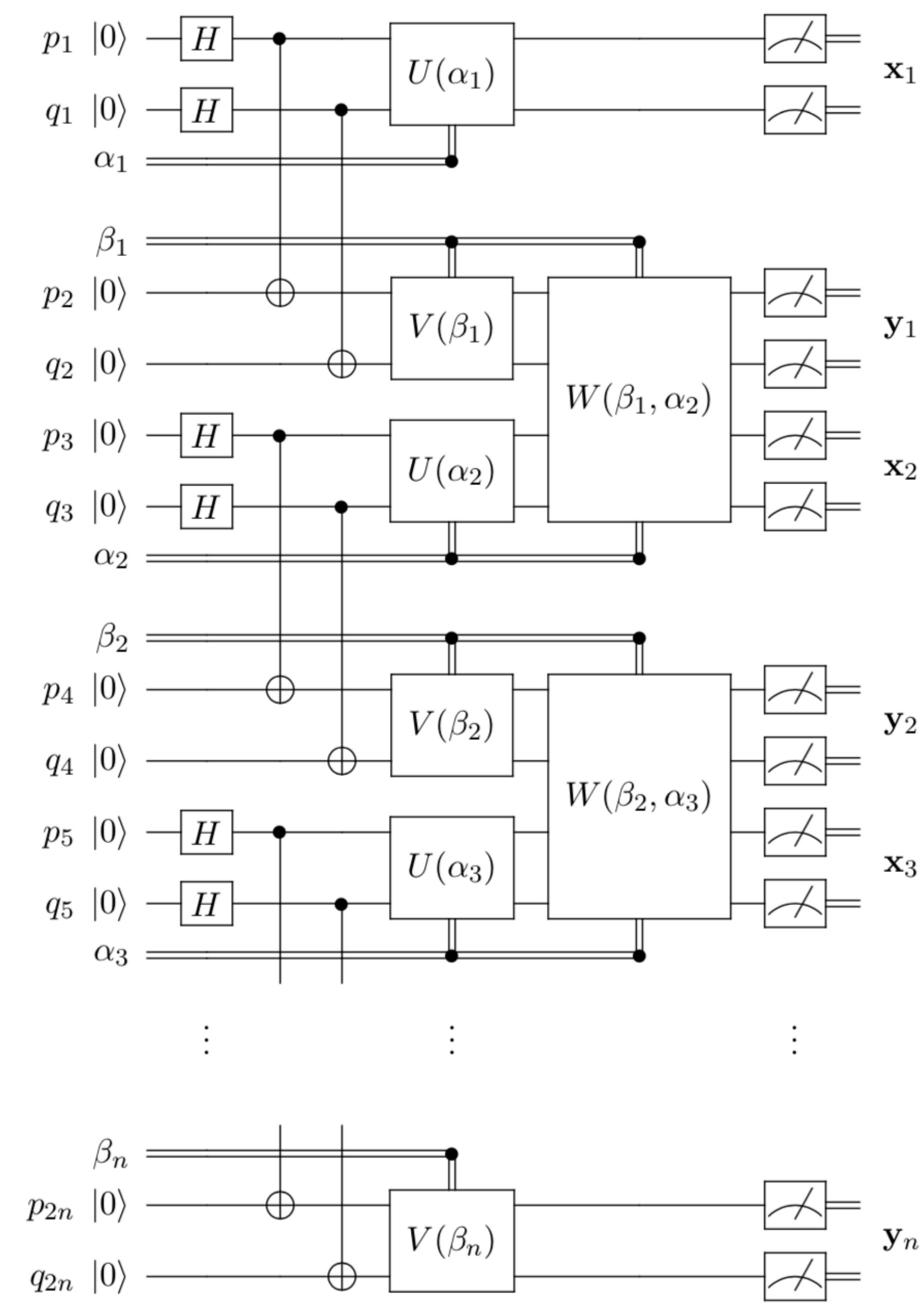
relational problem



feasible-ish with NISQ devices
(tolerates constant stochastic noise, 3D)

Outline

- The results in a nutshell
- The noiseless case: from magic squares to quantum circuits
- The noisy case: fault-tolerance in constant depth



Results - noiseless

Result 1 (Quantum advantage with 1D shallow circuits — informal). *For each n there exists a relation problem R with roughly n input-output bits and a set of inputs S of size $|S| = \mathrm{poly}(n)$ such that the following holds:*

- *The problem R can be solved with certainty for all inputs by a constant-depth quantum circuit composed of geometrically local gates on a 1D grid.*
- *Any classical probabilistic circuit composed of constant fan-in gates that solves R with probability exceeding 0.9 for a uniformly random input from S must have depth at least $\Omega(\log n)$.*

- Shows gap between constant-depth quantum circuits in 1D and log-depth classical circuits.
  - Quantum circuit wins with certainty while...
  - ...classical circuits win at most with 90% probability.

- Improves on the original result:
  - requires only 1D circuit instead of 2D
  - conceptually simple

Quantum advantage with shallow circuits

Sergey Bravyi[1], David Gosset[1,*], Robert König[2,†]

+ See all authors and affiliations

Science 19 Oct 2018:

Results - noisy

- Gap persists if we allow constant local stochastic noise (on system and ancillas, circuit and measurements).

Let $p \in [0,1]$. A random n-qubit Pauli error E is called *p-local stochastic noise* if

$$\Pr[F \subseteq \mathrm{Supp}(E)] \leq p^{|F|} \qquad \text{for all } F \subseteq [n].$$

- Constant-depth quantum circuit in 3D wins with 99% probability while...
- ...classical circuits can win at most with 90% probability, unless it is almost log-depth.

Result 2 (Quantum advantage with noisy shallow circuits — informal). *For each n there exists a relation problem R with roughly n input-output bits and a set of inputs S of size $|S| = poly(n)$ such that the following holds:*

- *The problem R can be solved with probability at least 0.99 for all inputs by a constant-depth quantum circuit composed of geometrically local gates on a 3D grid, subject to local stochastic noise. The noise rate must be below a constant threshold value independent of n.*
- *Any classical probabilistic circuit composed of constant fan-in gates that solves R with probability exceeding 0.9 for a uniformly random input from S must have depth at least*

$$\Omega\left(\frac{\log(n)}{\log(\log(n))}\right).$$

The noiseless case

classically
hard

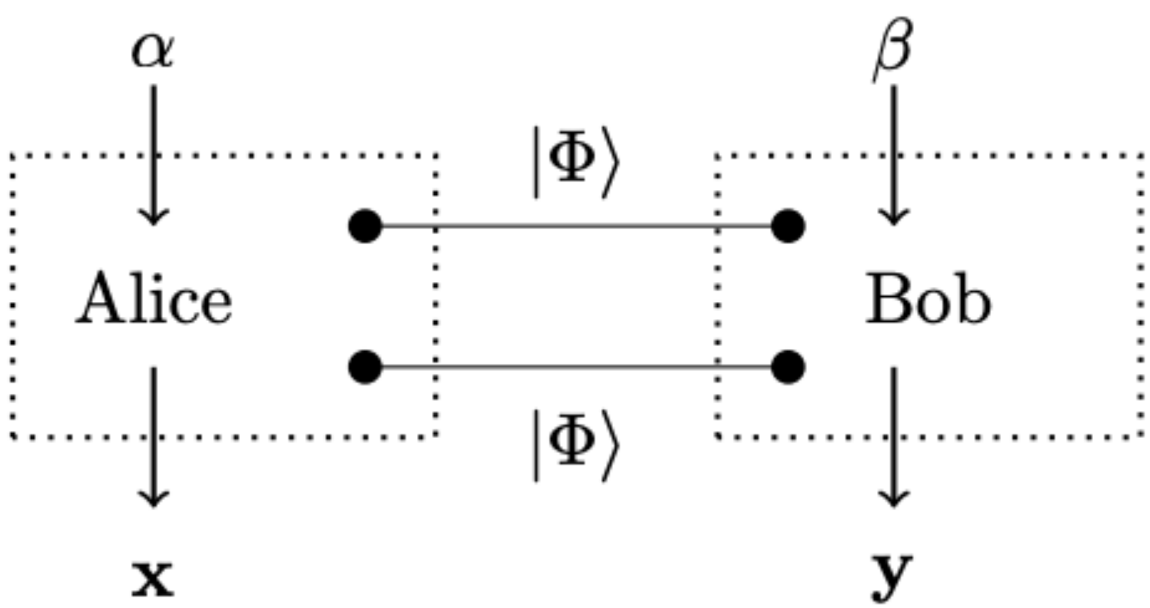
quantumly
easy

Magic squares

+1	+1	+1
+1	−1	−1
−1	+1	?

- Alice asked to fill a (random) column, Bob a (random) row.
- The columns should multiply to -1, the rows to +1.
- The element where column and row overlap needs to be consistent.
- Without communication or entanglement, this can be won with probability at most 8/9.

Magic squares



Binary α, β ∈ {01, 10, 11} are inputs for Alice and Bob.

3-bit strings x, y are outputs.

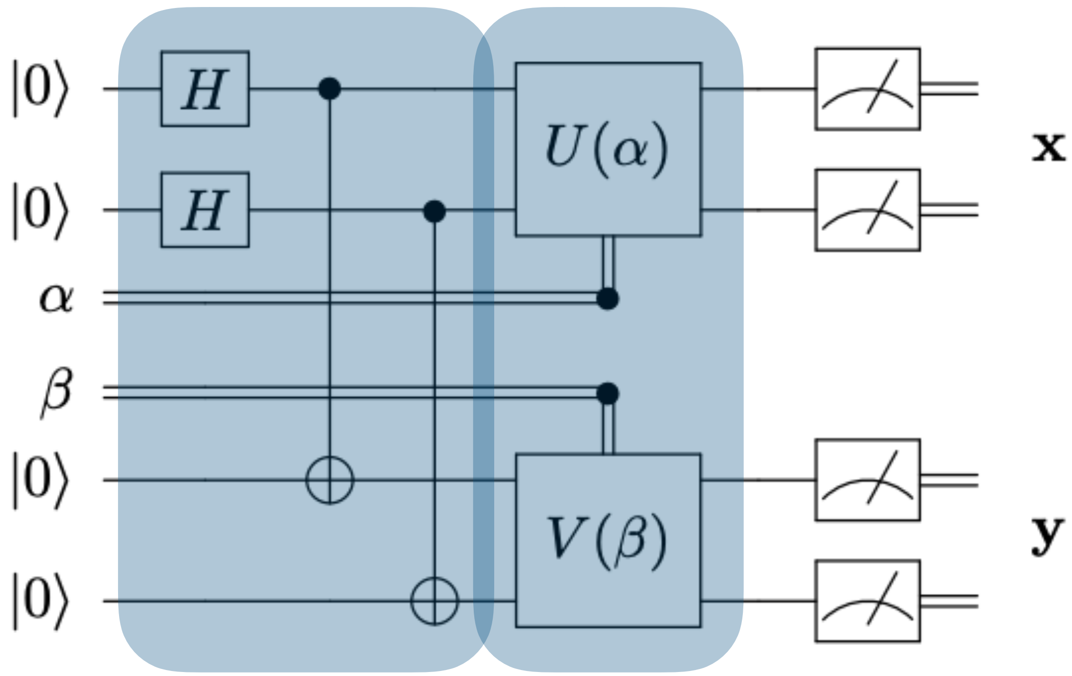
$$x_1 x_2 x_3 = -1 \qquad y_1 y_2 y_3 = 1$$
$$x_\beta = y_\alpha$$

Quantum players can win with certainty using these measurements (and their negation) on two singlets.

β \ α	01	10	11
01	$X_1 1_2$	$1_1 X_2$	$X_1 X_2$
10	$1_1 Z_2$	$Z_1 1_2$	$Z_1 Z_2$
11	$-X_1 Z_2$	$-Z_1 X_2$	$Y_1 Y_2$

Magic square circuit

too easy



	$\gamma = 00$	$\gamma = 01$	$\gamma = 10$
$U(\gamma)$	1	$H_1 1_2$	$H_1 1_2 \cdot \mathrm{SWAP}$
$V(\gamma)$	1	$H_1 H_2$	SWAP

	$\gamma = 11$
$U(\gamma)$	$H_1 1_2 \cdot \mathrm{CNOT}$
$V(\gamma)$	$(H_1 H_2) \cdot \mathrm{CZ} \cdot (Z_1 Z_2)$

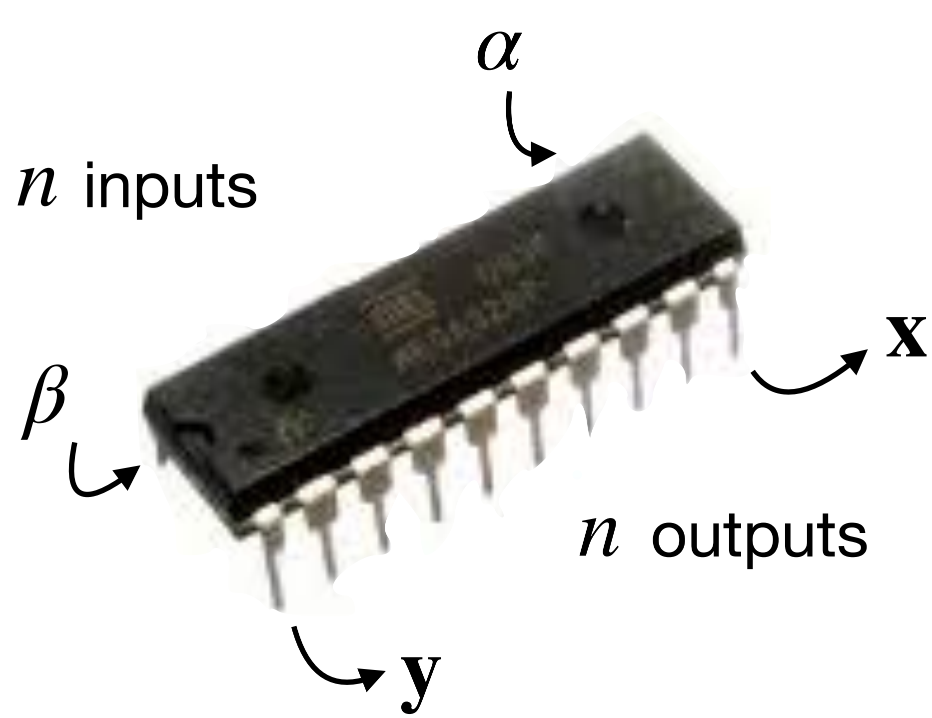
We can play this as a circuit.

The input controls a two-qubit unitary that determines the measurement basis.

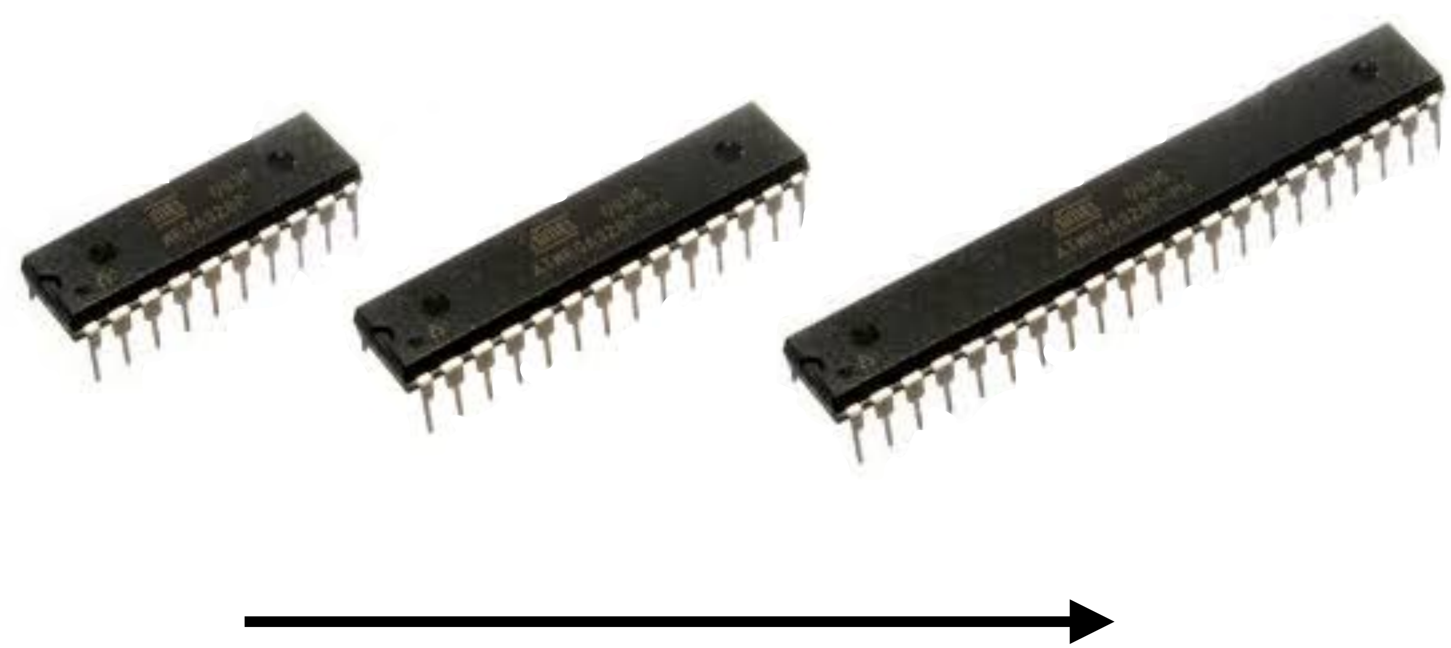
It only outputs the first two bits — fixing the third so that the parity condition holds.

α, β, x and y will satisfy the magic squares relation $x_\beta = y_\alpha$.

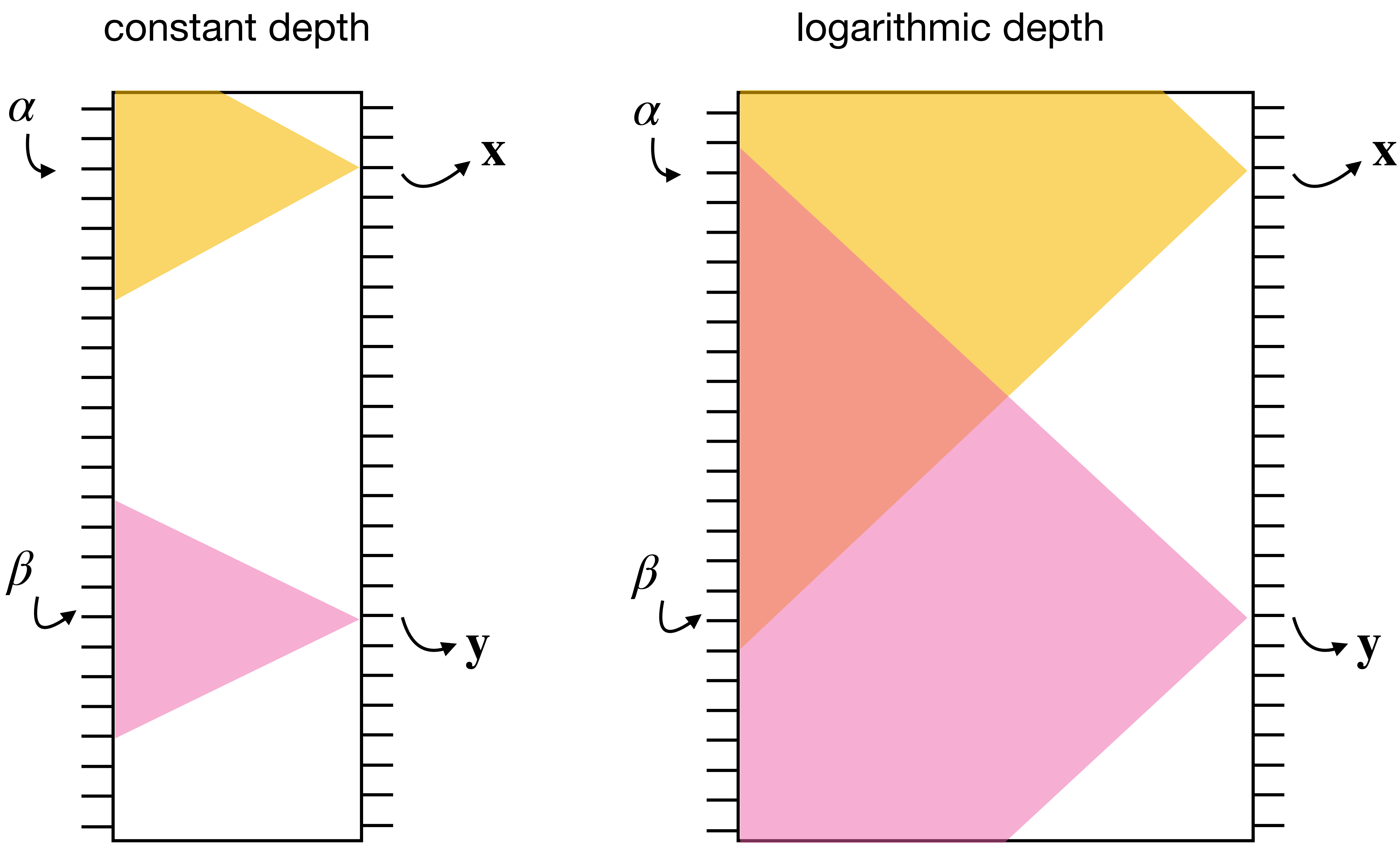
Magic squares on a (classical) chip



- What if we just put the inputs at opposite ends of the chip?
  - Idea: if the device is long enough, the depth will not suffice to communicate between the two ends due to the bounded fan-in assumption.

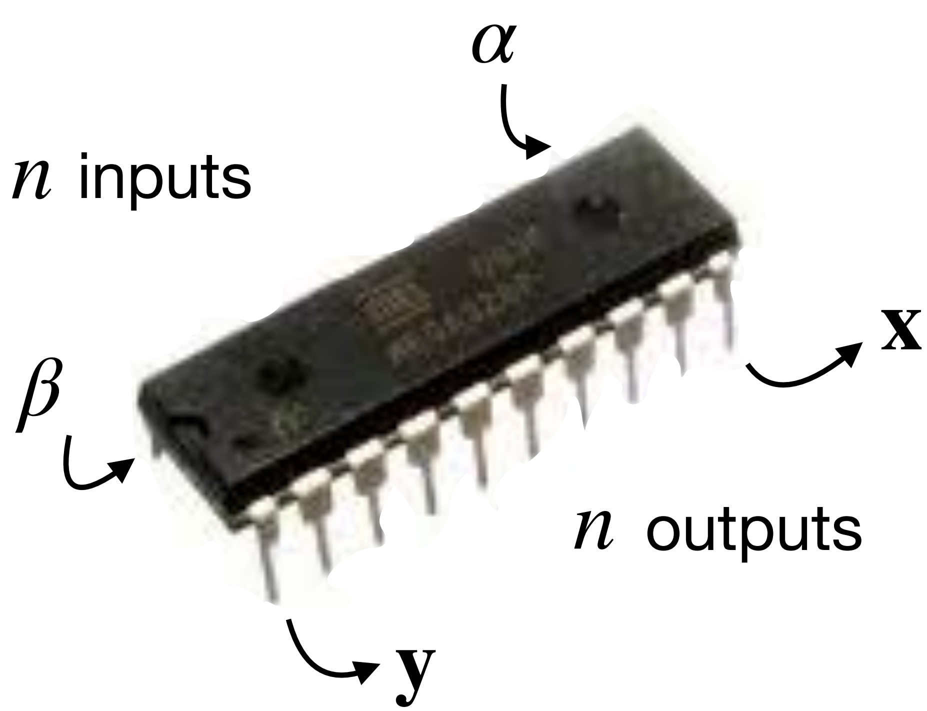


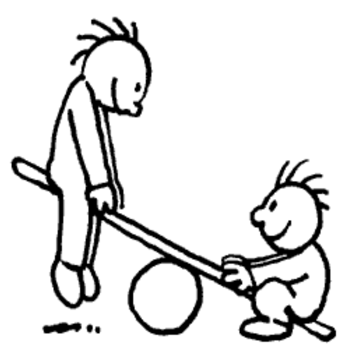
A simple idea: light cones



(Attention: this diagram wrongly suggests that the circuits are geometrically local, but we in fact don't assume that - that is in fact an important point of our proof.)

Magic squares on a (classical) chip





too hard?

- What if we just put the inputs at opposite ends of the chip?
  - Idea: if the device is long enough, the depth will not suffice to communicate between the two ends due to the bounded fan-in assumption.

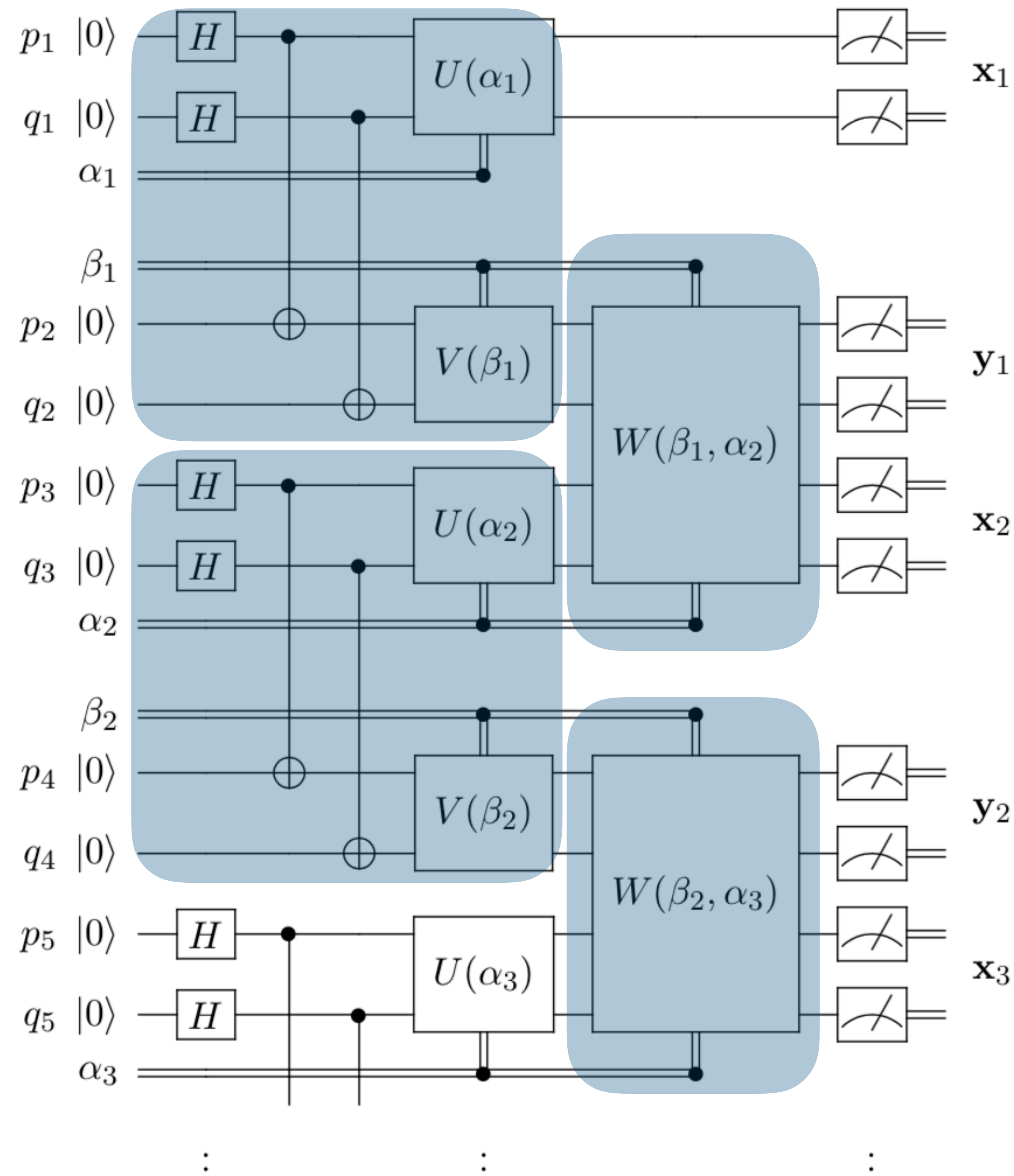
  - But wires are cheap and thus we do not want to assume locality.
- We instead put inputs at random locations, and again use the bounded fan-in assumption.

The quantum Magic squares game (I)

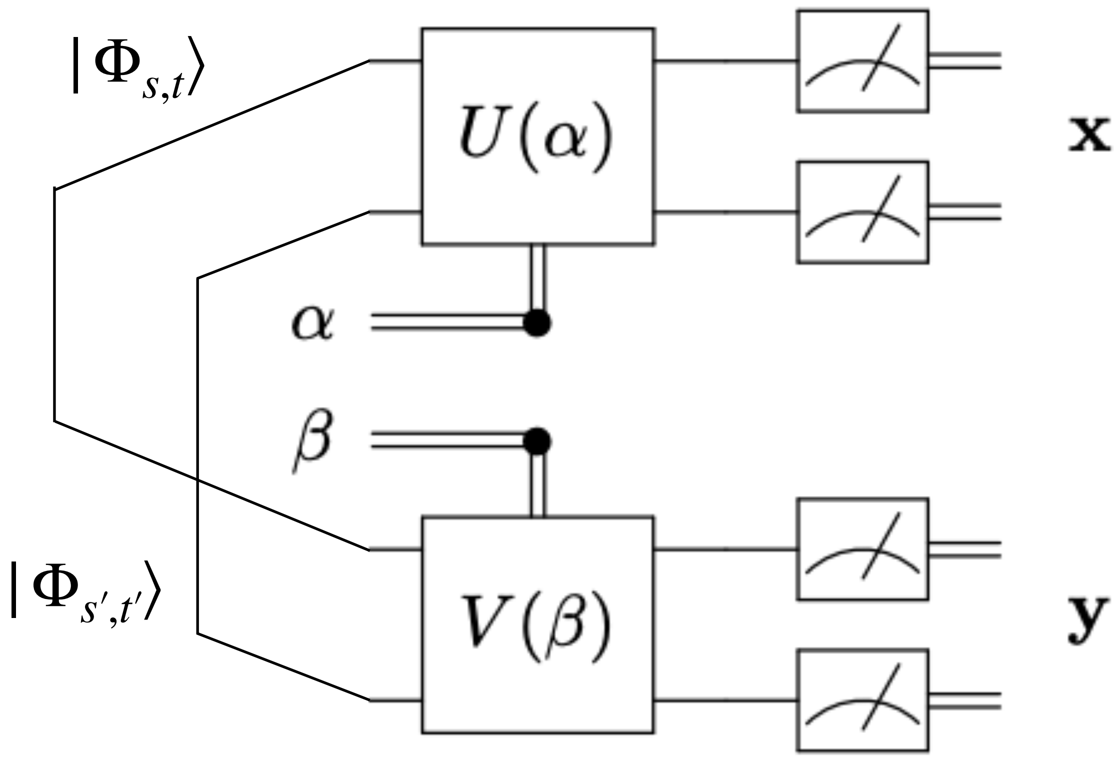
(j, k, α, β) where $1 \le j < k \le n$ and $\alpha, \beta \in \{01, 10, 11\}$

$$\alpha_i = \begin{cases} \alpha, & i = j \\ 00, & i \neq j. \end{cases} \qquad \beta_i = \begin{cases} \beta, & i = k \\ 00, & i \neq k. \end{cases}$$

- The idea is to distribute entanglement using 1D local entanglement swaps.
- W rotates into the Bell basis on input 0000, inactive otherwise.
- Swap requires a Pauli rotation depending on the measured output - cannot do that here!
- Can we play magic squares with a wrong Bell state?



Magic squares and Pauli noise



$$|\Phi_{s,t}\rangle = \left(Z^{\frac{1}{2}(1+s)} X^{\frac{1}{2}(1+t)} \otimes I\right) |\Phi\rangle$$

- Since the Magic square rotations are Clifford, we can propagate any Bell rotations trough.
- This simply changes the winning condition, instead of

$$x_\beta y_\alpha = 1$$

we require

$$x_\beta y_\alpha = f_{\alpha,\beta}(s, s', t, t')$$

The quantum Magic squares game (II)

The inputs

$$(j, k, \alpha, \beta) \qquad \text{where} \quad 1 \leq j < k \leq n \quad \text{and}$$
$$\alpha, \beta \in \{01, 10, 11\}$$

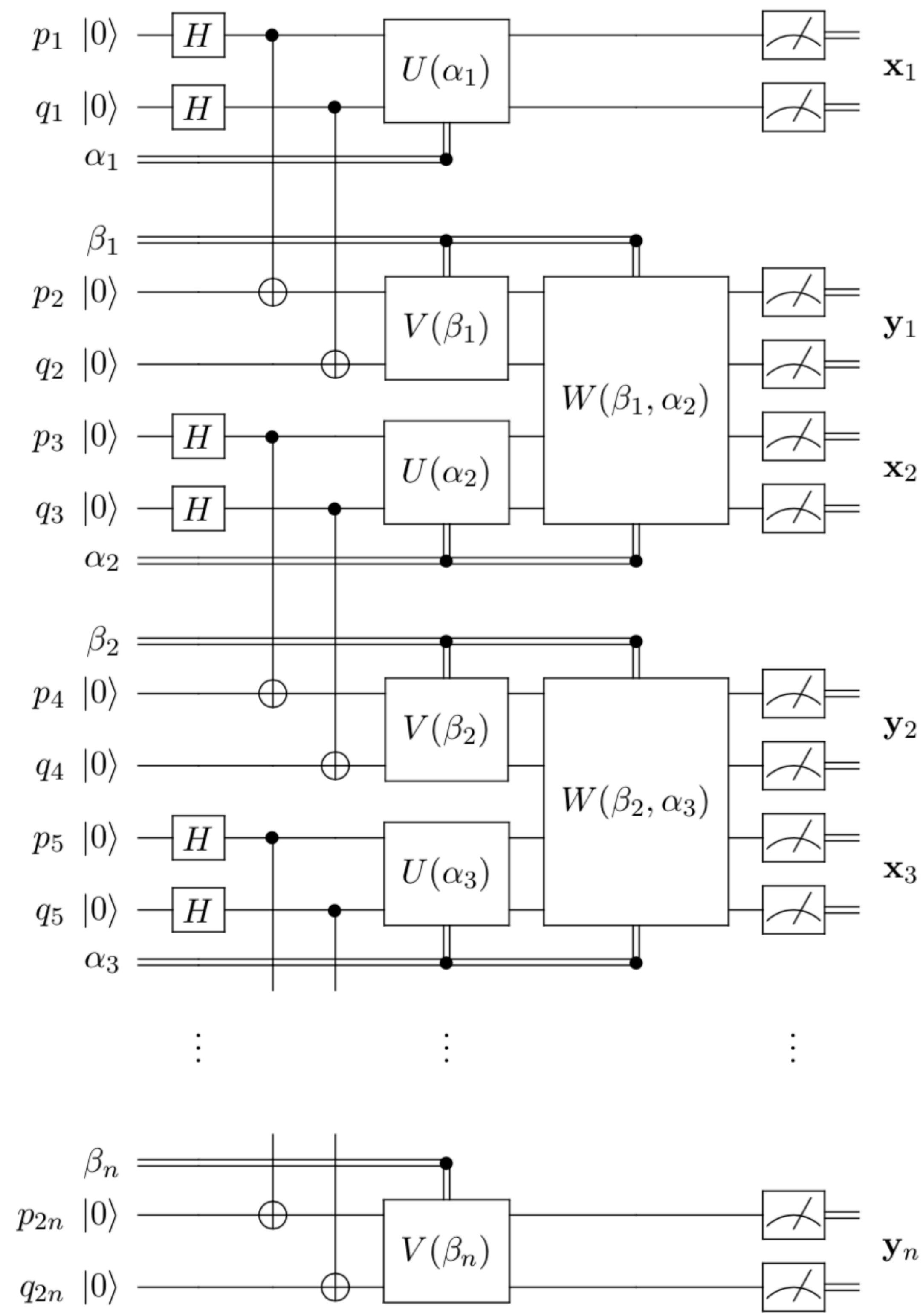
$$\alpha_i = \begin{cases} \alpha, & i = j \\ 00, & i \neq j. \end{cases} \qquad \beta_i = \begin{cases} \beta, & i = k \\ 00, & i \neq k. \end{cases}$$

and outputs must satisfy

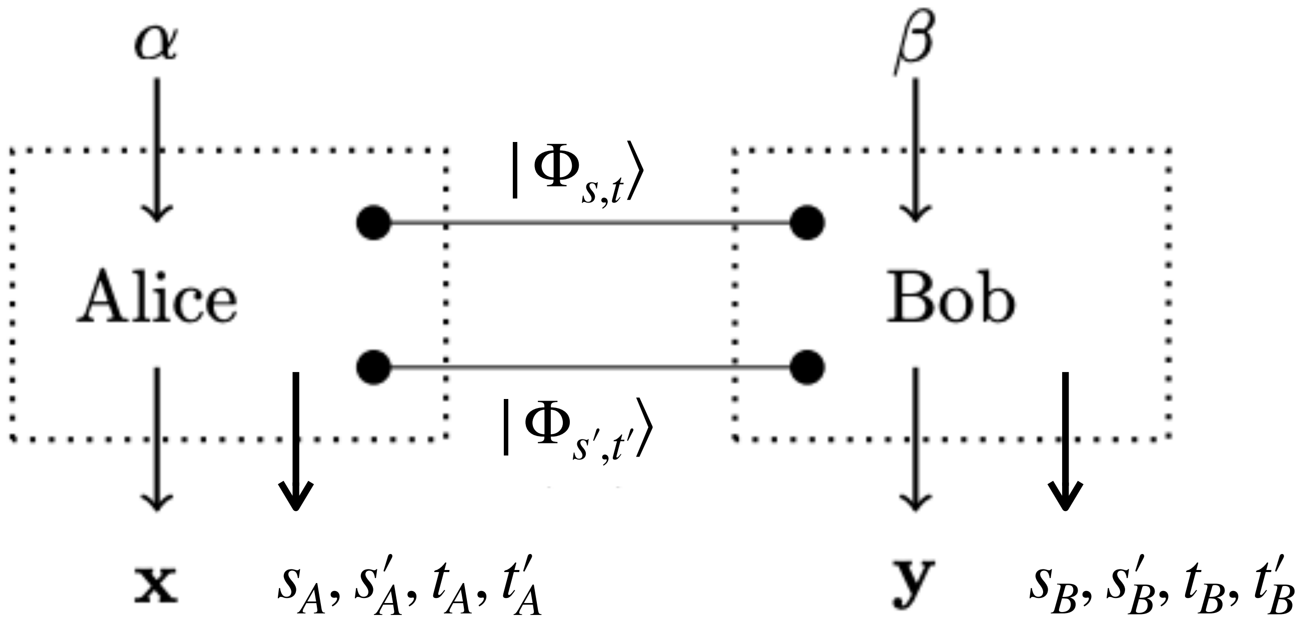
$$x_j^\beta y_k^\alpha = f_{\alpha,\beta}(s, t, s', t')$$

$$s = \prod_{i=j}^{k-1} y_i^1 \qquad t = \prod_{i=j}^{k-1} x_{i+1}^1 \qquad s' = \prod_{i=j}^{k-1} y_i^2 \qquad t' = \prod_{i=j}^{k-1} x_{i+1}^2$$

too easy?



Why is this still classically hard?



$$x^\beta y^\alpha = f_{\alpha,\beta}(s, t, s', t')$$

$$s = s_A(\alpha)\, s_B(\beta)\, s_0$$
$$s' = s'_A(\alpha)\, s'_B(\beta)\, s'_0$$
$$t = t_A(\alpha)\, t_B(\beta)\, t_0$$
$$t' = t'_A(\alpha)\, t'_B(\beta)\, t'_0$$

- Influencing the winning condition depending on their respective inputs does not help the classical players.
- Proof: Reduce every strategy for this game to a strategy for the base game with the same winning probability.

Recap – noiseless case

Result 1 (Quantum advantage with 1D shallow circuits — informal). *For each n there exists a relation problem R with roughly n input-output bits and a set of inputs S of size $|S| = \mathrm{poly}(n)$ such that the following holds:*

depth 5

- *The problem R can be solved with certainty for all inputs by a constant-depth quantum circuit composed of geometrically local gates on a 1D grid.*

In fact, they are classically controlled two-qubit gates (essentially as simple as it can get).

- *Any classical probabilistic circuit composed of constant fan-in gates that solves R with probability exceeding 0.9 for a uniformly random input from S must have depth at least $\Omega(\log n)$.*

In particular, the problem is not in NC^0 but sits in the corresponding quantum class.

The noisy case

Stochastic noise in the system

Let $p \in [0,1]$. A random n-qubit Pauli error E is called *p-local stochastic noise* if

$$\Pr[F \subseteq \mathrm{Supp}(E)] \leq p^{|F|} \qquad \text{for all } F \subseteq [n].$$

Daniel Gottesman, **Fault-Tolerant Quantum Computation with Constant Overhead**, arXiv:1310.2984

Omar Fawzi, A. Grospellier, A. Leverrier, **Constant Overhead Quantum Fault-Tolerance with Quantum Expander Codes.** FOCS 2018

- We consider errors on state preparation, gates and measurements.

- They can be arbitrarily correlated…
  - …in particular there are no locality constraints…
  - …but errors affecting many qubits are exponentially suppressed.

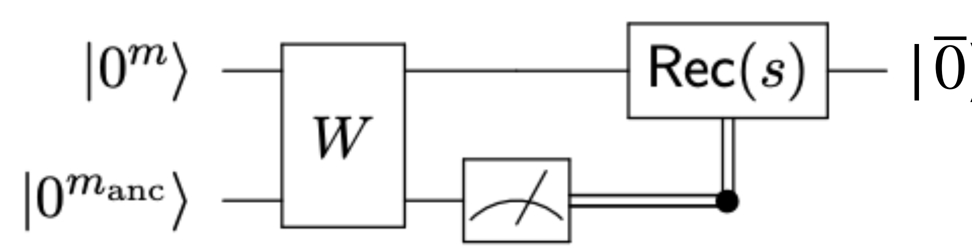
- The noise parameter p is held constant, but as things scale we need the error per logical qubit to vanish.

- Standard fault-tolerance does not apply since the circuit depth (even for preparing a logical zero) blows up with decreasing error per logical qubit.

Code properties (I)

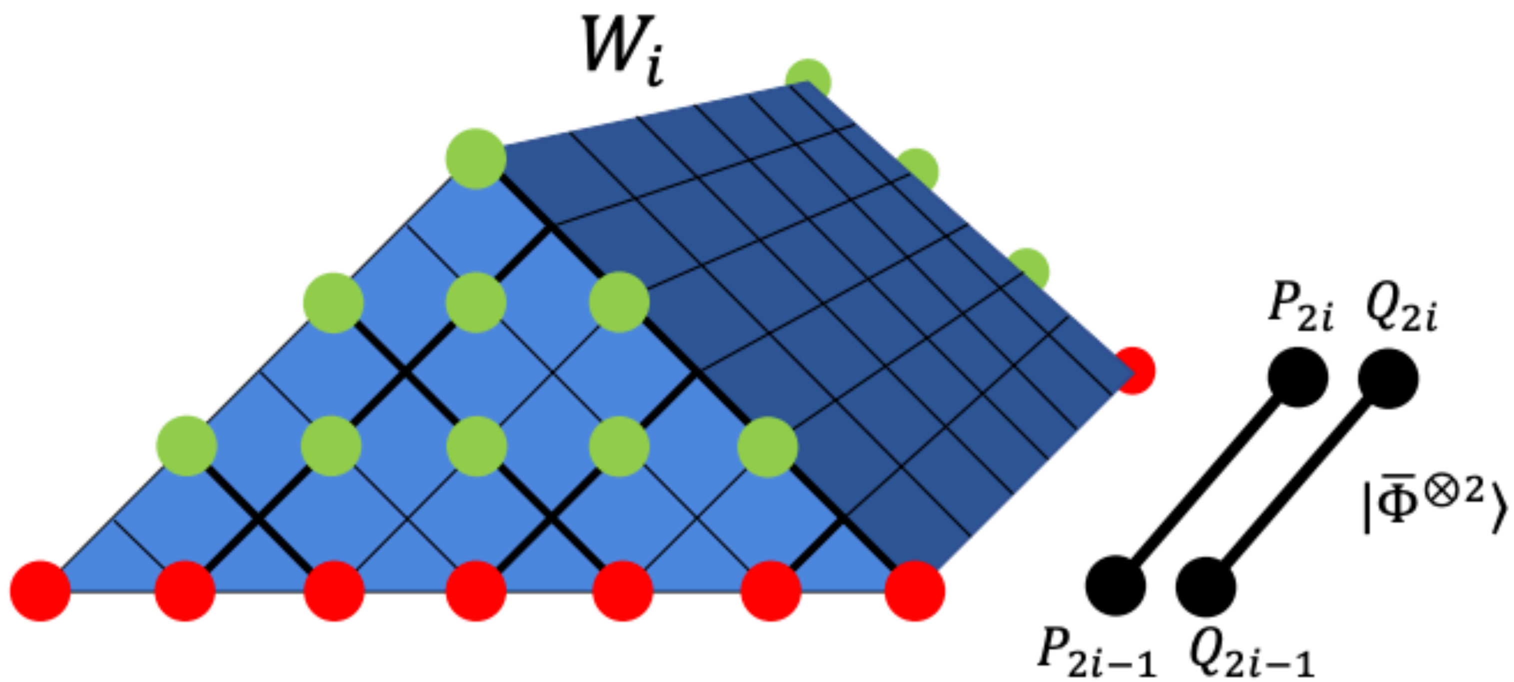
- We introduce generic way to make relational problems using Clifford circuits noise-tolerant.
- We need a CSS-type code family parametrised by *m* with the following properties:
  1. Logical H, S (and CNOT) can be implemented using depth-1 Clifford circuits composed of (at most) two-qubit gates.
  2. We have constant-depth single-shot logical basis state preparation.

1. Prepare $m + m_{\mathrm{anc}}$ qubits in the state $|0^m\rangle \otimes |0^{m_{\mathrm{anc}}}\rangle$.
2. Apply a constant-depth Clifford circuit W.
3. Measure each ancilla qubit in the Z-basis, giving an outcome $s \in \{0,1\}^{m_{\mathrm{anc}}}$.
4. Depending on the outcome s, apply a suitable Pauli recovery $\mathsf{Rec}(s)$ to the state of the m unmeasured qubits.



Code properties (II)

- We need a CSS-type code family parametrised by *m* with the following properties:
  1. Logical H, S (and CNOT) can be implemented using depth-1 Clifford circuits composed of (at most) two-qubit gates.
  2. We have constant-depth single-shot logical basis state preparation.
  3. Error threshold akin to fault-tolerance threshold theorem, with error vanishing (almost exponentially) as *m* increases.
- These are satisfied by a folded 2D surface code (but this is not trivial to show)
- 2D surface code per logical qubit + 1D logical circuit = 3D physical circuit.



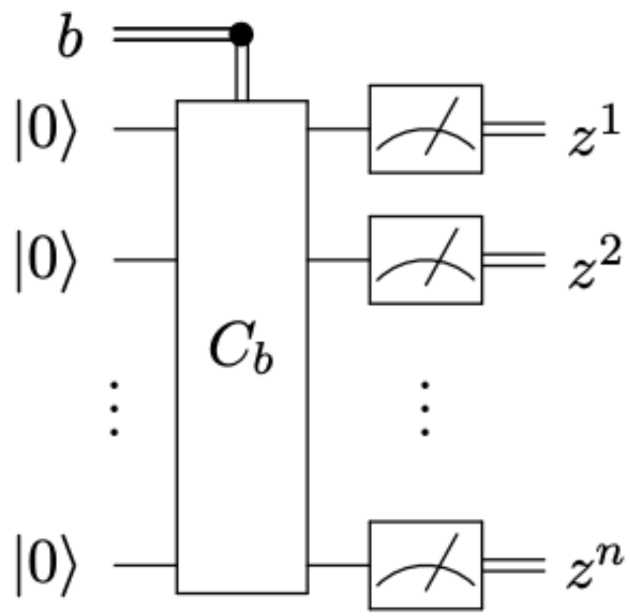
Long-range quantum entanglement in noisy cluster states

Robert Raussendorf, Sergey Bravyi, and Jim Harrington
Phys. Rev. A **71**, 062313 – Published 14 June 2005

1. Prepare 3D cluster state.
2. Measure bulk (the right way).
3. Results in surface-code encoded maximally entangled qubits at the boundaries.

The construction

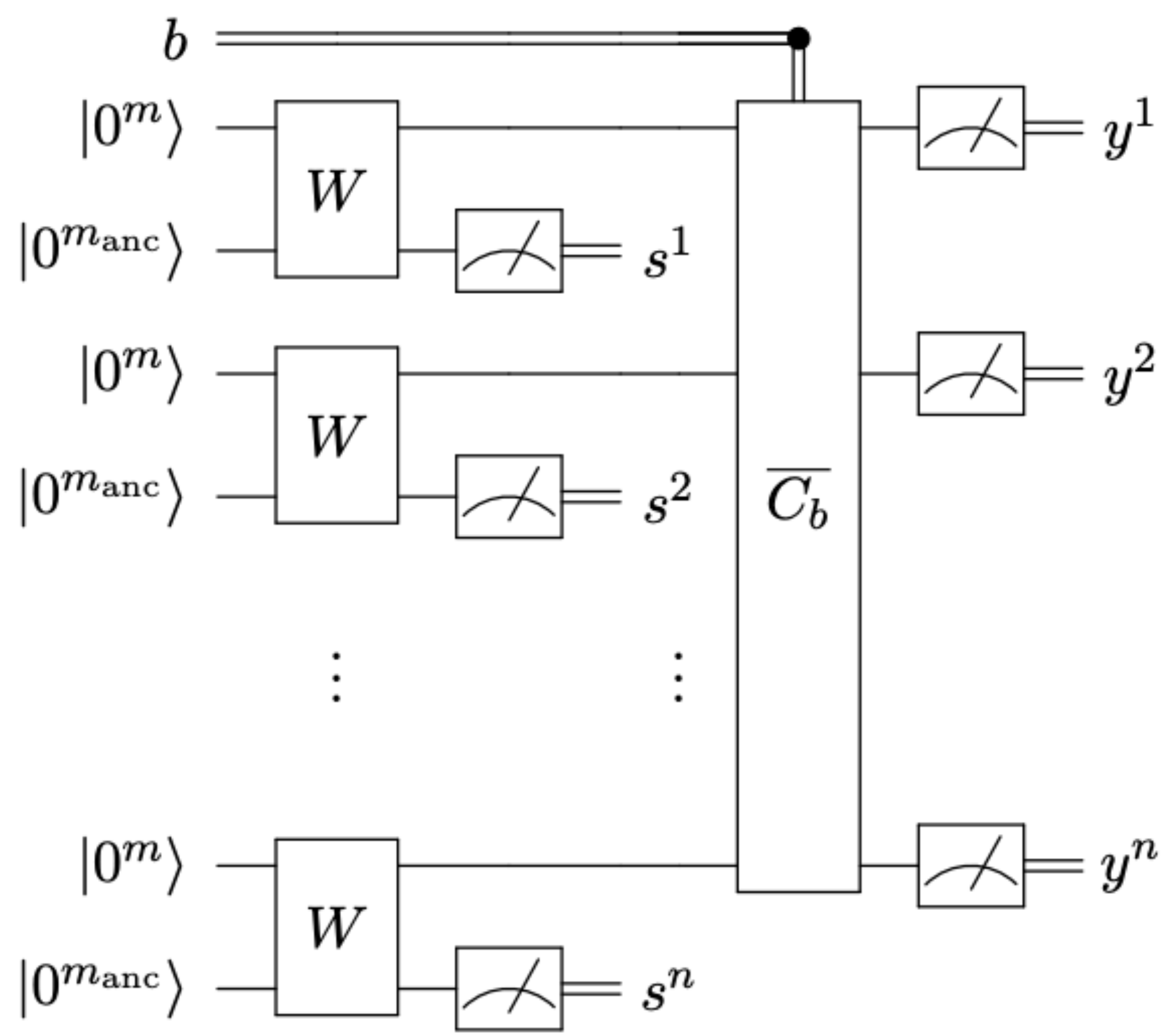
this controlled (constant depth) Clifford circuit



defines a relational problem

$$R_U(b, z) = \begin{cases} 1, & p_b(z) > 0 \\ 0, & \text{otherwise.} \end{cases}.$$

and induces a fault-tolerant relational problem



The reduction

$\Longrightarrow$ If the quantum circuit solves a relational problem perfectly in the noiseless case, its fault-tolerant version can solve it up to constant error if we choose

$$m, m_{\text{anc}} \in O(\text{polylog}\, n)$$

$\Longleftarrow$ If a $f(n)$ depth classical circuit with constant fan-in solves the fault-tolerant problem, then there exists a $f(n) + O(1)$ depth circuit with fan-in $O(\text{polylog}\, n)$ solving the original problem.

Since the latter cannot exist for $f(n) = \log n / \log(\log n)$ (according to Result 1), the former cannot either.

Recap – noisy case

Result 2 (**Quantum advantage with noisy shallow circuits — informal**). *For each n there exists a relation problem R with roughly n input-output bits and a set of inputs S of size $|S| = poly(n)$ such that the following holds:*

can it ever be 2D?

- *The problem R can be solved with probability at least 0.99 for all inputs by a constant-depth quantum circuit composed of geometrically local gates on a 3D grid, subject to local stochastic noise. The noise rate must be below a constant threshold value independent of n.*

- *Any classical probabilistic circuit composed of constant fan-in gates that solves R with probability exceeding 0.9 for a uniformly random input from S must have depth at least*

$$\Omega\left(\frac{\log(n)}{\log(\log(n))}\right).$$