Quantum Advantage with Shallow Circuits

… whatever that means

December 6, 2024

Rebecca Kempe

COMP/MATH 4803 Presentation

Quantum advantage with shallow circuits

Sergey Bravyi[1], David Gosset[1], Robert König[2]
[1] *IBM T.J. Watson Research Center*
[2] *Institute for Advanced Study & Zentrum Mathematik,*
Technische Universität München

(2017)

Abstract

We prove that constant-depth quantum circuits are more powerful than their classical counterparts. To this end we introduce a non-oracular version of the Bernstein-Vazirani problem which we call the 2D Hidden Linear Function problem. An instance of the problem is specified by a quadratic form q that maps n-bit strings to integers modulo four. The goal is to identify a linear boolean function which describes the action of q on a certain subset of n-bit strings. We prove that any classical probabilistic circuit composed of bounded fan-in gates that solves the 2D Hidden Linear Function problem with high probability must have depth logarithmic in n. In contrast, we show that this problem can be solved with certainty by a constant-depth quantum circuit composed of one- and two-qubit gates acting locally on a two-dimensional grid.

Questions:

- What is the scope of this claim of “quantum advantage” (in what cases does this actually apply)?
- What is a “shallow circuit” (and why do we care)?
- What does this result actually mean?
- Why is this result true? (Big ideas)

Outline

1. Quantum Computing Basics
2. Circuits
   - Gates, Size, Depth, Fan-in, Fan-out
   - Classical vs. Quantum Circuits
3. Hidden Linear Function (HLF) Problems
4. Results
5. References

Quantum computers perform computations using quantum mechanics.

- Construct a quantum system that we can control. Prepare an initial state for the system. (This is the input.)
- Make some changes to the quantum system. (These are operations.)
- Measure the state of the system at the end. (This is the output.) Outcome is probabilistic.

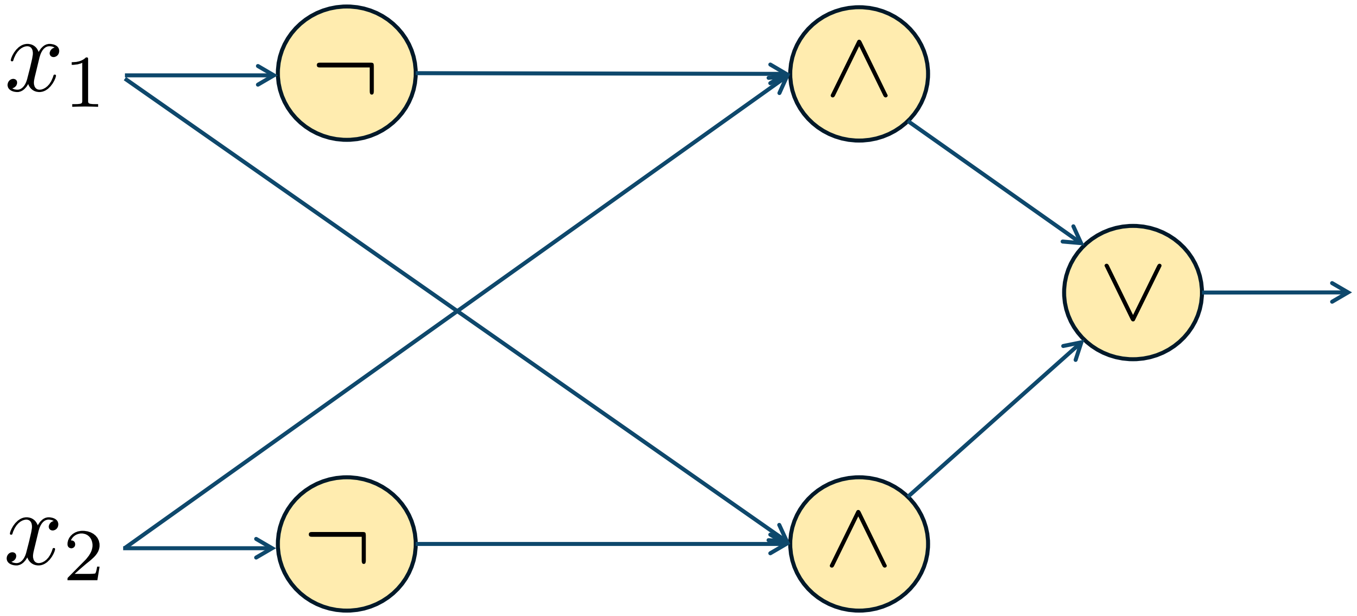
Qubits

- States are unit vectors in a 2D complex vector space
- Basis vectors: $|0\rangle, |1\rangle$ (roughly analogous to bits 0, 1 in classical computing)
- All states are of the form $\alpha|0\rangle + \beta|1\rangle, \; |\alpha|^2 + |\beta|^2 = 1$
- Probability of measuring state $|0\rangle = |\alpha|^2, |1\rangle = |\beta|^2$
- Superposition allows qubits to store “extra” (but hidden) information compared to classical bits

Circuits (introduction)

- A Boolean formula is an expression that can be written using Boolean variables $x_1, x_2, x_3, \ldots$ and the Boolean operations AND, OR, and NOT
- A Boolean circuit is a non-uniform model of computation that generalizes Boolean formulas
- Turing machines are a uniform model because we use the same TM for all input sizes; circuits require different algorithms for differently sized inputs

Circuits (introduction)



A (classical) circuit is a directed acyclic graph with n source nodes and one sink node. Each node is labelled with a gate: a logical operation AND, OR, or NOT.

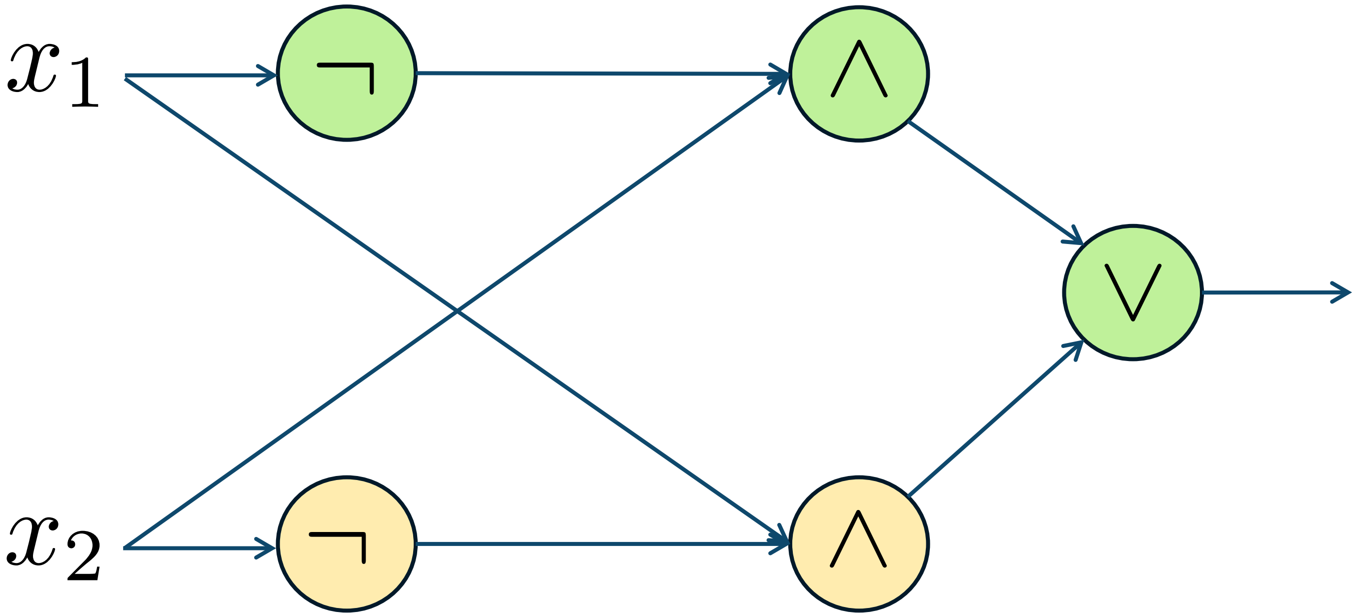
An n-input circuit computes a boolean function

$$f : \{0,1\}^n \to \{0,1\}.$$

This circuit computes the XOR function for two vars x_1, x_2.

Note: sometimes arbitrary gates are used to define a circuit.

Circuits (definitions)

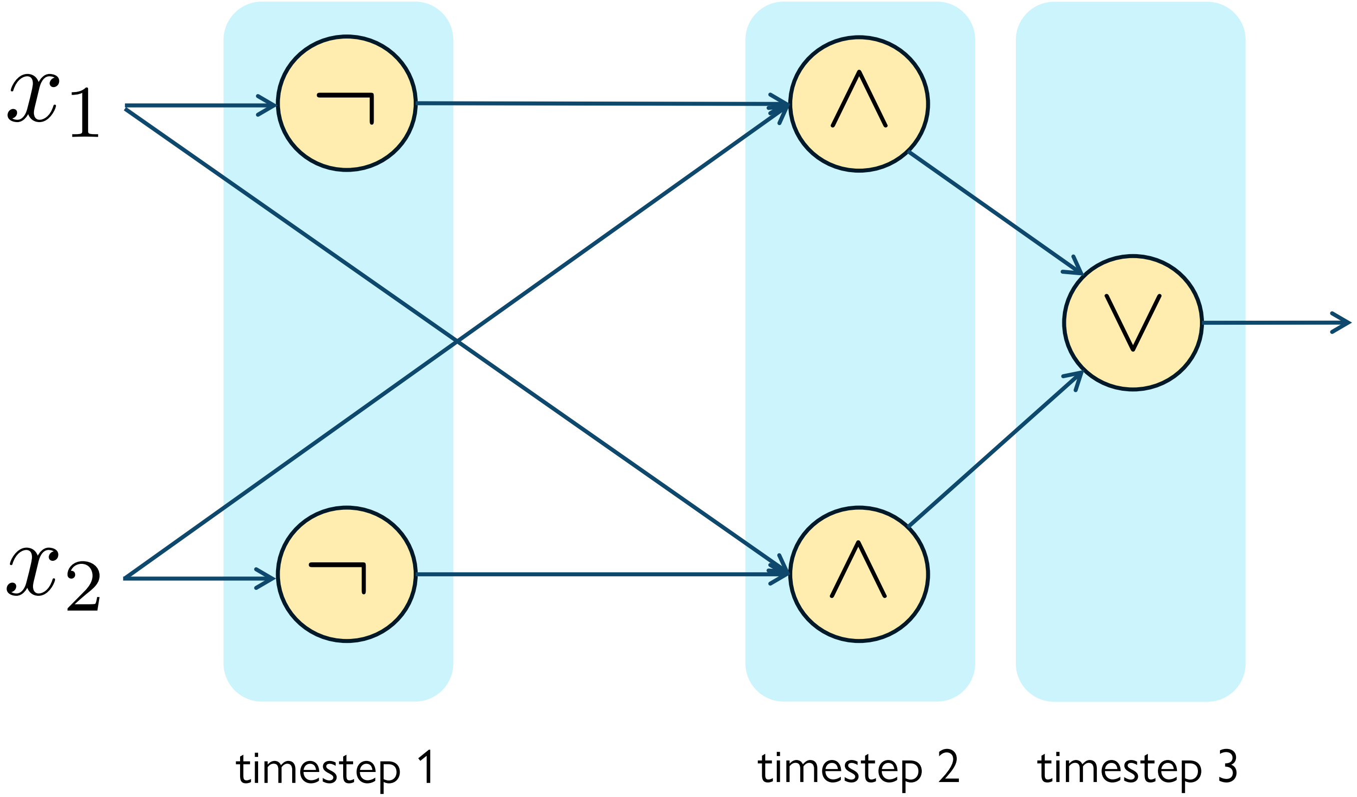


The size of a circuit is the number of vertices (gates) in its graph representation.

The depth of a circuit is the number of gates in the longest path from an input to the output in its graph representation.

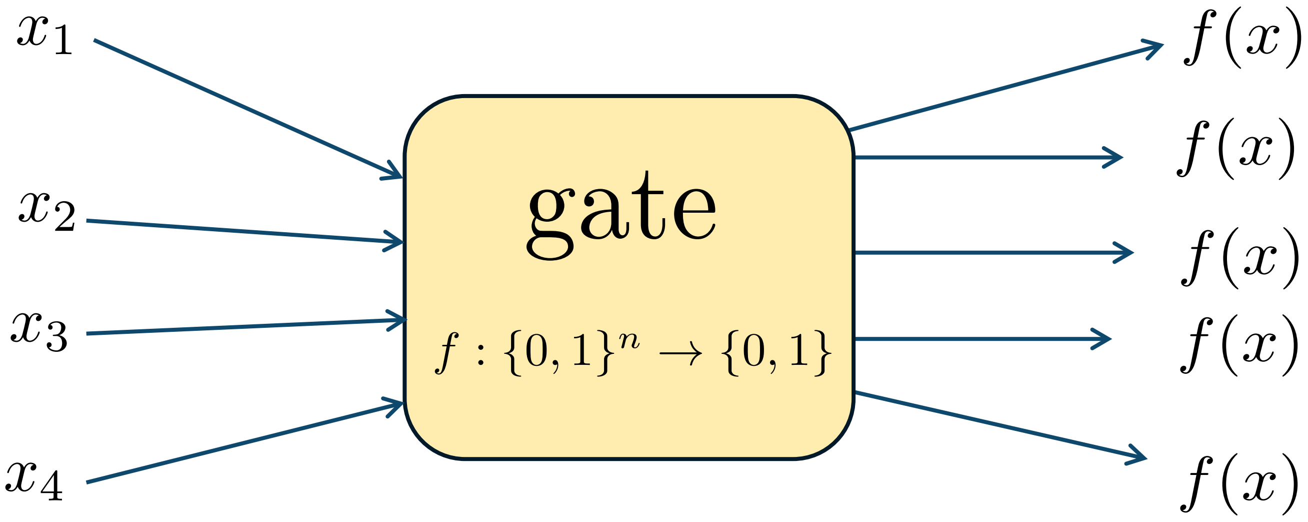
This circuit has size 5 and depth 3.

Circuits (definitions)



The depth can also be viewed as the number of timesteps of gates. (Two gates can be simultaneously evaluated if their inputs are disjoint and neither gate relies on the other already having been evaluated.)

Circuits (definitions)



This gate has fan-in 4 and fan-out 5.

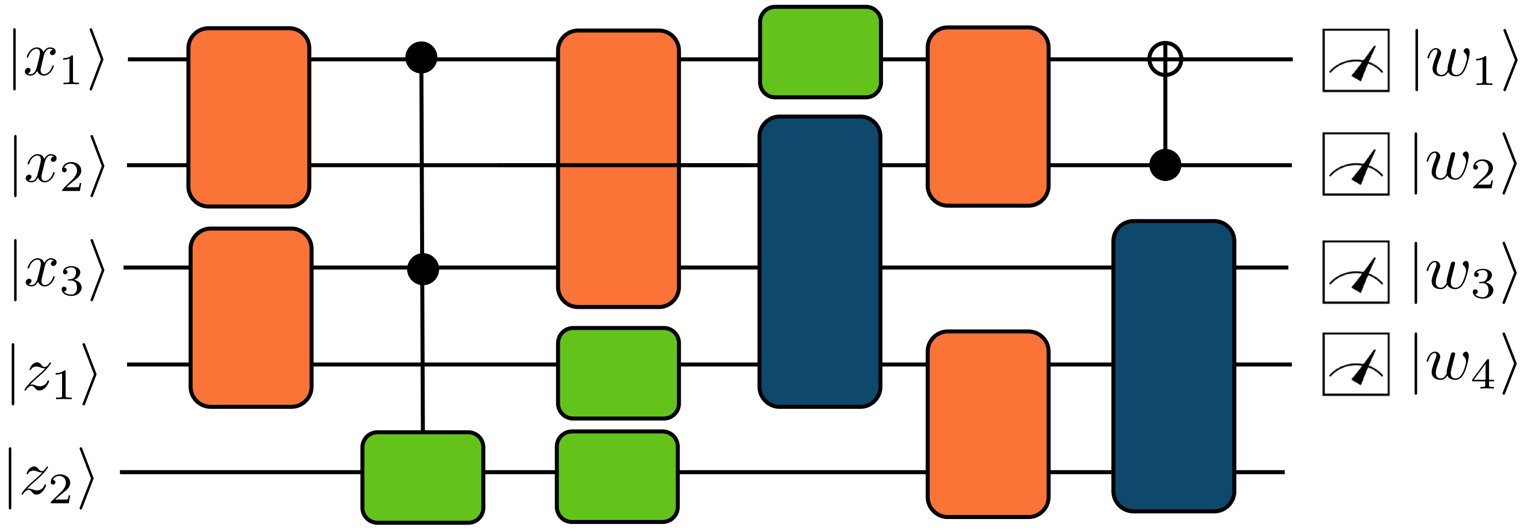
The fan-in of a gate in the number of incoming edges it has; the fan-out of a gate is the number of outgoing edges it has. These edges all carry copies of the output of the gate.

In this paper, the authors only considered circuits with constant depth (not dependent on input size) and bounded fan-in (fan-in is some constant for every gate in the circuit).

Quantum Circuits

- Quantum circuits are the default language used to describe quantum algorithms.
- Similar in spirit to classical circuits, but we do not have fan-in (gates operate on a specified number of qubits) or fan-out (qubits can’t be copied).
- Gates are unitary operators on one or more qubits, controlled by one or more qubits.

Anatomy of a quantum circuit

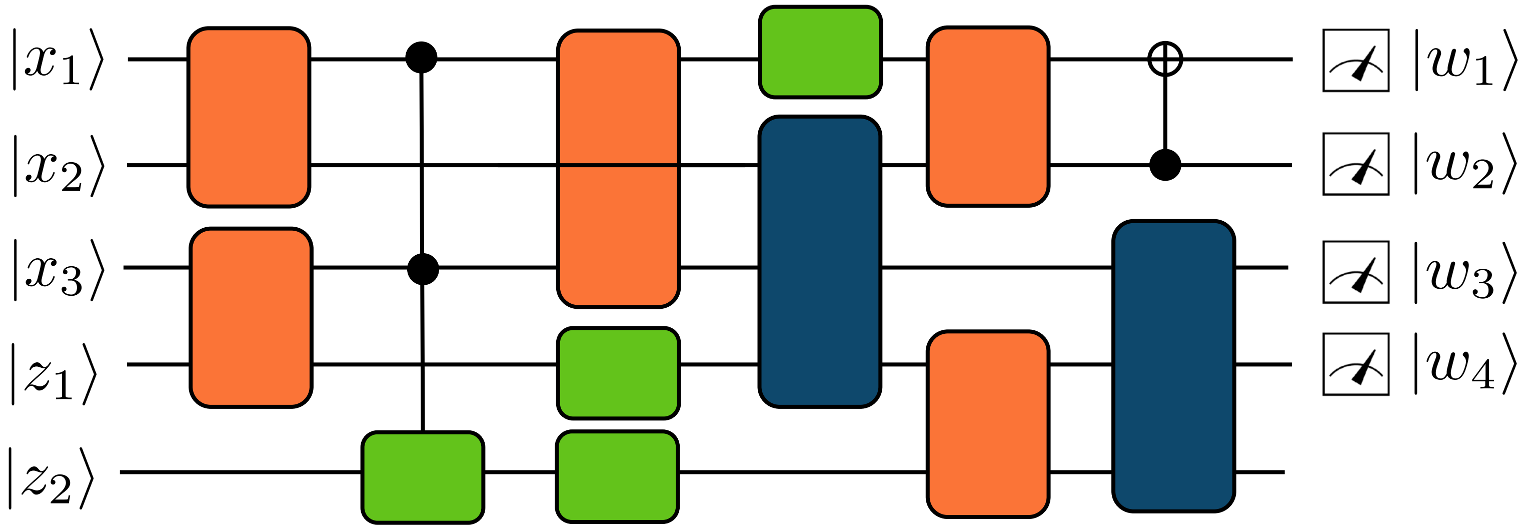


Input: a k-bit string x, plus ancillary qubits z_i

Output: Measure the first n qubits in the standard basis to get an n-bit string w.

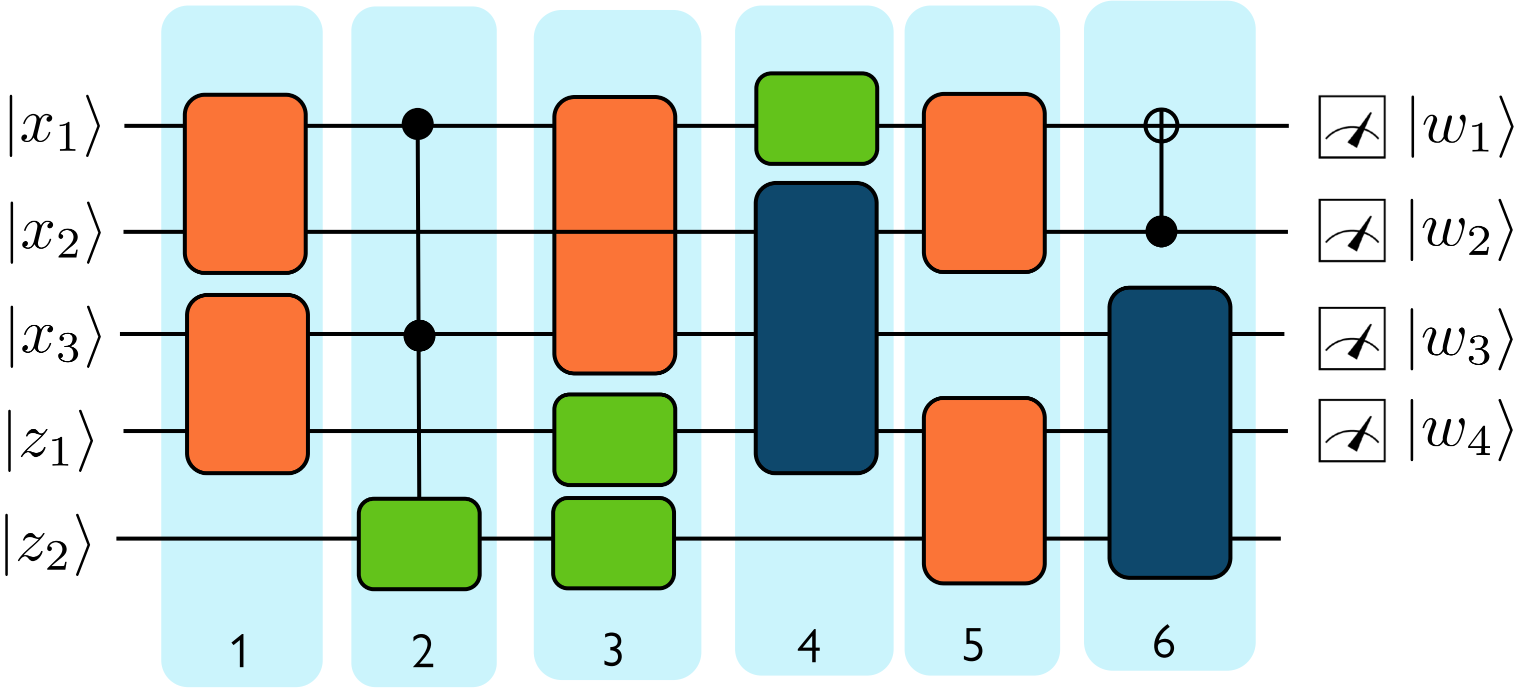
Each of these coloured rectangles represents a quantum gate on one or more qubits; each black dot represents a control bit for a controlled quantum gate.

Anatomy of a quantum circuit



Goal: we want a circuit that manipulates the norms of the coefficients of the resulting states such that they are as skewed towards the desired outcomes as possible.

Anatomy of a quantum circuit



Goal: we want a circuit that manipulates the norms of the coefficients of the resulting states such that they are as skewed towards the desired outcomes as possible.

This circuit has size 12 and depth 6. It is comprised of one, two, and three qubit gates. If it only had one and two-qubit gates, it would be an example of a shallow circuit.

Why shallow quantum circuits?

- A shallow quantum circuit (SQC) has constant depth and is comprised of one and two-qubit gates.
- Constant-depth circuits with bounded fan-in gates model parallel algorithms that solve problems in constant time with a polynomial number of processors. (Class $\mathbf{NC^0}$)
- Shallow circuits are the quantum analogue of such classical circuits. Circuit depth and parallelism are important due to noise in quantum computations.

What problem can we solve with a SQC that can’t be solved with a constant-depth classical circuit?

- The natural place to look is at search problems
- We want something that does not rely on an oracle/black box (something that translates to real-world improvement)
- Solution: Hidden Linear Function problem

Hidden Linear Function Problem

- Suppose A is a binary symmetric matrix of size n.
- Ker(A) = set of binary vectors x such that $Ax = 0$ (mod 2).
- Quadratic form: $q(x)= x^TAx \quad$ (mod 4)
- If x was real, then x^TAx would always equal 0 when $Ax = 0$. But since x is binary, the restriction of q(x) onto Ker(A) can be non-zero. (Restriction just means take x from Ker(A).)
- Also, the restriction of q(x) onto Ker(A) is a linear boolean function (up to factor of 2).

Hidden Linear Function Problem

- Input: a binary symmetric matrix *A*.
- Output: a bit string z such that $q(x) = 2z^T x \pmod 4$ for all $x \in Ker(A)$
- Solutions to this problem are not unique.
- The authors restrict this problem to a 2D-grid and show that there is an SQC that can solve this problem.

Theorem: A classical probabilistic circuit with fan-in at most K which solves all size-N instances of the 2D Hidden Linear Function problem with probability greater than 7/8 must have depth at least (logN)/(8logK).

Results

- The 2D Hidden Linear Function problem can be solved by a shallow quantum circuit
- It cannot be solved by a constant-depth classical circuit with bounded fan-in
- This is due to something called quantum nonlocality and the locality of constant-depth classical circuits: each output bit in a circuit in $\mathbf{NC^0}$ can only be correlated with a constant number of input bits.

References

- Sanjeev Arora and Boaz Barak. Computational Complexity: A Modern Approach
- Sergey Bravyi. Quantum Advantage with Shallow Circuits (Talk). https://www.youtube.com/watch?v=xogOLp36GIA
- Sergey Bravyi, David Gosset, and Robert König. Quantum Advantage with Shallow Circuits.
- Michael A. Neilsen and Isaac L. Chuang. Quantum Computation and Quantum Information.