The 2D Hidden Linear Function problem

Sriram Gopalakrishnan

- arXiv:1704.00690 (2017) : Bravyi, Gosset & Koenig : "Quantum advantage with shallow quantum circuits"

Preliminaries: Size vs Depth vs Input Size

- Circuit **Size** (called just size for simplicity) = Total # of gates

- Classical Circuit **Depth** = Max # of gates from an input bit to an output bit

- Quantum Circuit Depth = # of “layers” of gates. Each layer consists of gates acting on a disjoint sets of qubits

- For a boolean decision problem $f: \{0,1\}^n \to \{0,1\}$, **input size** = n. Circuit Size and Depth are functions of n

Preliminaries: NC vs QNC

- NC^q : Class of problems solvable with $O(n^p)$ parallel processors and $\underline{O(\log n^q)}$ depth. (Size ~ $O(n^p \log n^q)$ = $poly(n)$. So NC ⊆ P)

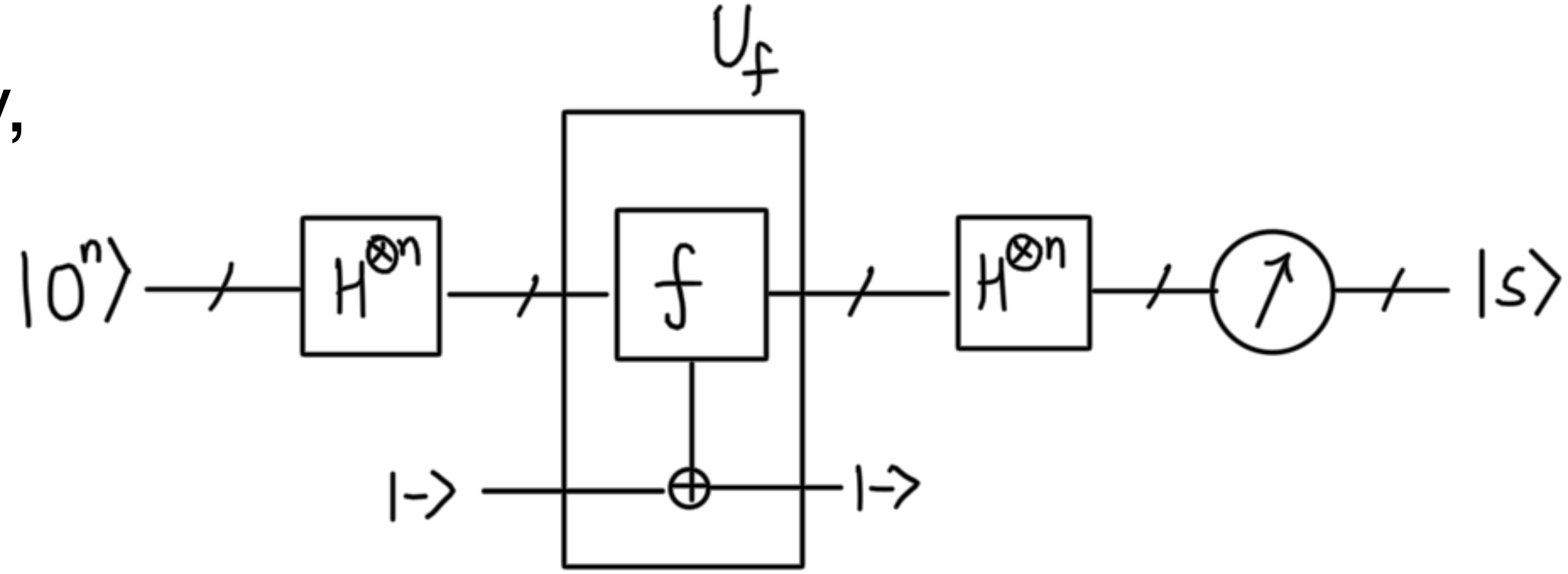
- NC^0 : $poly(n)$ size, constant depth

- QNC^0 ? Constant depth. But size? No cloning. So Circuit Size = $O(n)$, where n is the input size.

- Is there a problem in QNC^0 that is **not** in NC^0? Yes, 2D HLF, as we'll see. Classically, $O(\log n)$ depth. Quantumly, constant depth

Preliminaries: Bernstein-Vazirani

- $f: \{0,1\}^n \to \{0,1\}$ is promised to be of the form $f(x) = (s^T x) \mod 2$.
- Classically, n queries. Quantumly, 1 query due to oracle access



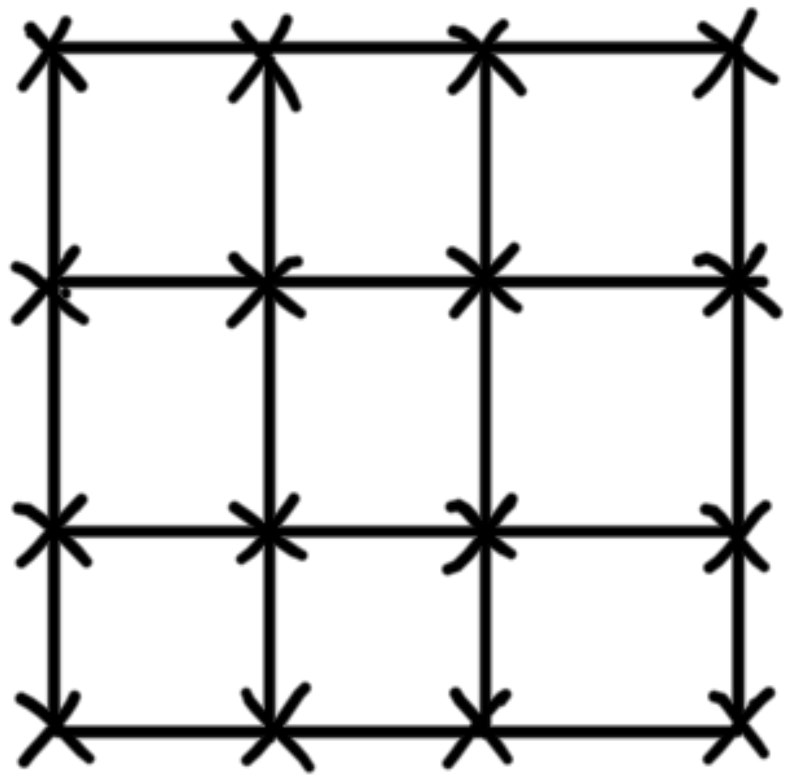
$$|0^n\rangle \xrightarrow{H^{\otimes n}} \sum_{x \in (\mathbb{F}_2)^n} |x\rangle \xrightarrow{U_f} \sum_x (-1)^{f(x)} |x\rangle \xrightarrow{H^{\otimes n}} \sum_y \left(\sum_x (-1)^{(s \oplus y) \cdot x} \right) |y\rangle = |s\rangle$$

2D HLF: Motivation

- In general, implementing a quantum oracle U_f requires **deep** quantum circuits, that are impractical in the NISQ era.
- Gate Complexity ~ (Input Size)(Depth), and Error ~ gate complexity. So for a finite error, there is a **trade-off** between input size and depth.
- We naturally prefer a larger input size for a potential quantum advantage.
- So is there a **shallow quantum circuit** with a **provable quantum advantage**? Is there a shallow, **non-oracular** generalization of Bernstein-Vazirani?

2D HLF: Problem Statement

- We are given a quadratic form $q : (\mathbb{F}_2)^n \to \mathbb{Z}_4$ defined as $q(x) = (x^T A x + b^T x) \pmod 4$



- So, <u>Inputs</u>: $b \in \{0,1\}^n$, $A \in \{0,1\}^{n \times n}$ binary symmetric. Also, A is the **adjacency matrix** of a 2D grid of n nodes.

- Define a set $\mathcal{L}_q = \left\{ x \in (\mathbb{F}_2)^n \,|\, q(x \oplus y) = q(x) + q(y) \quad \forall y \in (\mathbb{F}_2)^n \right\}$

2D HLF: Problem Statement

- **Lemma 1**: $\mathscr{L}_q$ is a linear subspace of $(\mathbb{F}_2)^n$ and $q(x) \in \{0,2\} \quad \forall x \in \mathscr{L}_q$. Additionally, $\exists z \in (\mathbb{F}_2)^n$ such that $q(x) = 2z^T x \pmod 4$ $\forall x \in \mathscr{L}_q$

- So, <u>Output</u>: Secret string $z \in \{0,1\}^n$

Proof of Lemma 1

- **Proof**: Take any $x, x' \in \mathscr{L}_q$. Does $x \oplus x' \in \mathscr{L}_q$?

- $q(x \oplus x' \oplus y) = q(x) + q(x' \oplus y) = q(x \oplus x') + q(y) \quad \forall y \in (\mathbb{F}_2)^n$
  $\Rightarrow x \oplus x' \in \mathscr{L}_q$. Hence $\mathscr{L}_q \subset (\mathbb{F}_2)^n$ is a linear subspace

- Also, for $y = x$, $\quad q(x \oplus x) \; = q(0) = 0 = 2q(x) \pmod 4$
  $\Rightarrow q(x) \in \{0,2\} \quad \forall x \in \mathscr{L}_q$

Proof of Lemma 1: Hidden Linearity

- Now define a function $l : \mathscr{L}_q \to (\mathbb{F}_2)^n$ as $l(x) = \begin{cases} 1 & \text{if } q(x) = 2 \\ 0 & \text{if } q(x) = 0 \end{cases}$

- Then $q(x) = 2l(x) \quad \forall x \in \mathscr{L}_q$, so $l(x \oplus y) = l(x) \oplus l(y) \quad \forall x, y \in \mathscr{L}_q$

- Hence $l(x)$ is linear modulo 2
  $\Rightarrow l(x) = z^T x \pmod 2 \quad \forall x \in \mathscr{L}_q$, some $z \in (\mathbb{F}_2)^n$
  $\Rightarrow q(x) = 2z^T x \pmod 4 \quad \forall x \in \mathscr{L}_q$, some $z \in (\mathbb{F}_2)^n$

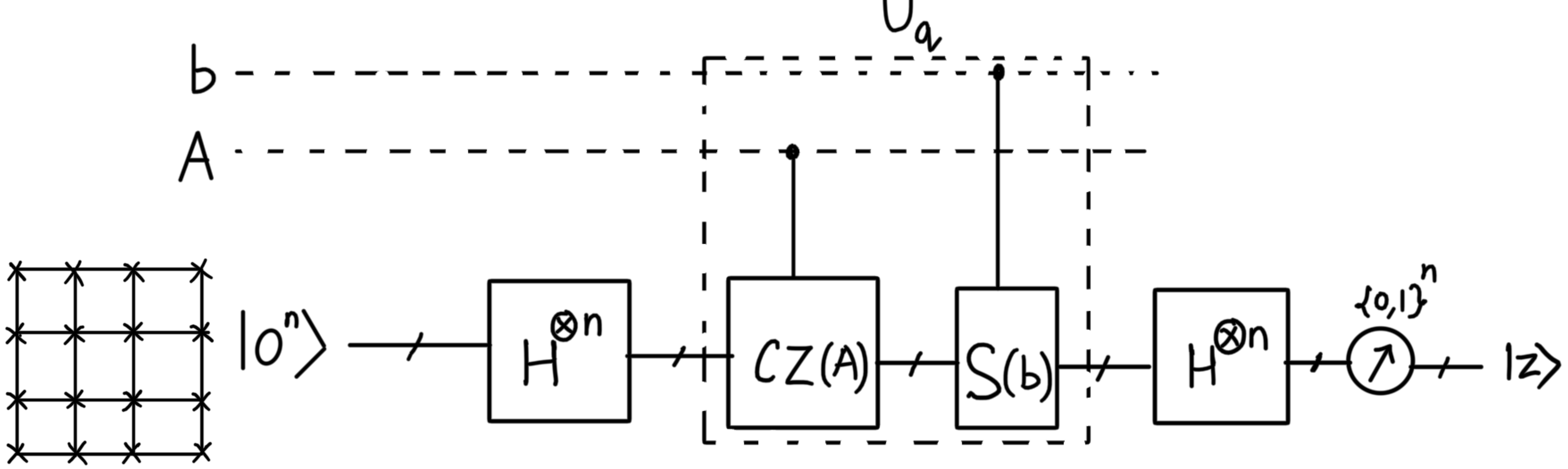
Remark

- Unlike Bernstein-Vazirani, the secret string z is not unique. This is because the linearity is restricted to a <u>*subspace*</u> $\mathscr{L}_q$ of $(\mathbb{F}_2)^n$.

- If we consider any $y \in \mathscr{L}_q^{\perp}$, the orthogonal complement of $\mathscr{L}_q$, then $z' = z \oplus y$ is also a valid secret string.

- In fact, there are $|\mathscr{L}_q^{\perp}|$ valid secret strings. The quantum algo for 2D HLF gives a uniform superposition over all valid secret strings as output.

The quantum algorithm



$$CZ(A) = \prod_{i<j} CZ_{ij}^{A_{ij}}$$ (**can be implemented with depth** ≤ 4 **for any subgraph of the 2D grid**)

$$S(b) = \bigotimes_j S_j^{b_j}$$ (**just one layer**)

$\Rightarrow$ **Total Depth** ≤ 7 $\forall$ **instances of 2D HLF**

$$U_q|x\rangle = i^{q(x)}|x\rangle \quad \forall x \in \{0,1\}^n$$

Key technique in the algo

$$S(b)CZ(A)|x\rangle = i^{(x^T Ax + b^T x)}|x\rangle \quad \forall x \in \{0,1\}^n$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

- **Proof**: Note that we do expect $S(b)CZ(A)|x\rangle$ to differ from $|x\rangle$ only by a phase, since
  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} \xrightarrow{CZ} \{|00\rangle, |01\rangle, |10\rangle, -|11\rangle\}$
  $\{|0\rangle, |1\rangle\} \xrightarrow{S} \{|0\rangle, i|1\rangle\}$

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

- So $CZ_{ij}|x_ix_j\rangle = (-1)^{A_{ij}x_ix_j}|x_ix_j\rangle$ where $x = x_1x_2\dots\ x_n$

$$\Rightarrow CZ(A)|x\rangle = \prod_{i<j} CZ_{ij}|x\rangle = (-1)^{\sum A_{ij}x_ix_j}|x\rangle = (-1)^{\frac{1}{2}x^T Ax}|x\rangle = i^{x^T Ax}|x\rangle$$

- Similarly, $S_j|x_j\rangle = i^{b_jx_j}|x_j\rangle \Rightarrow S(b)|x\rangle = i^{b^T x}|x\rangle$

Analysis of the algo

$$|0^n\rangle \xrightarrow{H^{\otimes n}} \sum_{x\in(\mathbb{F}_2)^n} |x\rangle \xrightarrow{U_q} \sum_{x\in(\mathbb{F}_2)^n} i^{q(x)}|x\rangle \xrightarrow{H^{\otimes n}} \sum_{y\in(\mathbb{F}_2)^n} \left(\sum_{x\in(\mathbb{F}_2)^n} i^{(q(x)+2y^Tx)} \right) |y\rangle$$

$$\equiv \sum_{y\in(\mathbb{F}_2)^n} \Gamma(\mathbb{F}_2^n, y)\,|y\rangle$$

- Where we define a *Partial Fourier Transform* w.r.t any $\mathscr{L} \subseteq \mathbb{F}_2^n$ and any $y \in \{0,1\}^n$ as

$$\Gamma(\mathscr{L}, y) \equiv \sum_{x\in\mathscr{L}} i^{(q(x)+2y^Tx)}$$

- So $P(y) = \dfrac{|\Gamma(\mathbb{F}_2^n, y)|^2}{4^n} \quad \forall y \in \{0,1\}^n$

Analysis of the algo

- Note that $\mathbb{F}_2^n = \mathscr{L}_q + \mathscr{L}_q^\perp$, and $|\mathscr{L}_q||\mathscr{L}_q^\perp| = |\mathbb{F}_2^n| = 2^n$

- So it can be seen that $\Gamma(\mathbb{F}_2^n, y) = \Gamma(\mathscr{L}_q, y)\ \Gamma(\mathscr{L}_q^\perp, y)$

- But $\Gamma(\mathscr{L}_q, y) = \sum_{x \in \mathscr{L}_q} i^{2(z \oplus y)^T x} = \begin{cases} |\mathscr{L}_q| & , y \in z \oplus \mathscr{L}_q^\perp \\ 0 & \text{, otherwise} \end{cases}$

- Also, $\Gamma(\mathscr{L}_q^\perp, y) = |\mathscr{L}_q^\perp|^{1/2} \quad \forall y \in \{0,1\}^n$ [involved proof!]

Analysis of the algo

- So finally, we find that $P(y) = \begin{cases} \frac{1}{|\mathscr{L}_q^\perp|} & \text{if } \; y \in z \bigoplus \mathscr{L}_q^\perp \\ 0 & \text{otherwise} \end{cases}$

- Hence, just before measurement,

  state $= \dfrac{1}{|\mathscr{L}_q^\perp|} \displaystyle\sum_{y \in z \bigoplus \mathscr{L}_q^\perp} |y\rangle \xrightarrow{\text{measure}} |z'\rangle$

  - such that $z' \in z \bigoplus \mathscr{L}_q^\perp$, which of course includes z as well.

Classical depth lower bound

- **Lemma 2**: C_n be a classical probabilistic circuit with gate fan-in $\leq K$. If C_n solves *all* size-n instances of 2D HLF with error probability $< 1/8$, then depth$(C_n) \geq \dfrac{\log n}{16 \log K}$

- **Rough idea**: There are special instances of 2D HLF, specifically when A is the adjacency matrix of an **even length cyclic sub-graph** of the 2D grid, when the input-output correlations of 2D HLF exhibit **strong non-locality**, which cannot be reproduced by constant depth circuits.

Take aways

- 2D HLF is a specially designed problem to demonstrate a computational advantage with constant depth quantum circuits.

- Classically, the authors prove a depth lower bound of $\Omega(\log n)$ for bounded fan-in boolean circuits. Quantumly, **all** instances of 2D HLF can be solved by **depth-7** quantum circuits.

- 2D HLF is still in P, so a practical time advantage hasn't been demonstrated yet.

- However, the analysis now creates an explicit separation between QNC^0 and NC^0.