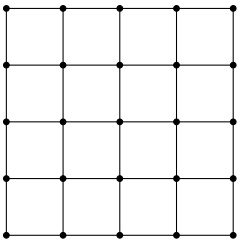
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang

Tutorial 9 (Proving quantum advantage based on a Hidden Linear Function problem)
In a recent paper[1], the authors construct a variant of the standard Bernstein-Varizani Hidden Linear Function (HLF) problem, which can be solved by a constant depth quantum circuit. The authors then prove that an analogous classical circuit with constant depth cannot solve this problem in general. This provides a working example for a provable quantum advantage over classical methods.

The problem definition uses the concept of an *adjacency matrix* of a graph $G = (V, E)$ with vertices $V = \{v_1, \ldots, v_n\}$ and edges E. The adjacency matrix $A \in \mathbb{R}^{n\times n}$ of G is defined by its entries

$$A_{i,j} = \begin{cases} 1, & \text{if } (v_i, v_j) \text{ is an edge in } E \\ 0, & \text{otherwise} \end{cases}$$

for $i, j \in \{1, \ldots, n\}$. Note that A is a binary, symmetric matrix.
In the publication, the authors choose G as square grid with $N \times N$ vertices. The edges connect the nearest neighbors on the grid. The motivation for this setup are quantum computers with the same layout, i.e., each vertex a qubit. We will see that the quantum solution will only require two-qubit gates between neighbors of the graph, which could thus be directly realized by the quantum computer.



The problem statement is based on the function

$$q(x) = \sum_{i,j=1}^{n} A_{i,j} x_i x_j \bmod 4, \quad x \in \{0,1\}^n,$$

and we will restrict x to the kernel of $A \bmod 2$: $\mathrm{Ker}(A) = \{x \in \{0,1\}^n : Ax = 0 \bmod 2\}$.

(a) Show that $q(x)$ is linear when its support is restricted to $\mathrm{Ker}(A)$.
Hint: Prove that $q(x \oplus y) = q(x) + q(y) \bmod 4$ for $x, y \in \mathrm{Ker}(A)$.

By the derivation of part (a), one concludes that $q(x)$ can be written as

$$q(x) = 2\sum_{i=1}^{n} y_i x_i \bmod 4, \quad x \in \mathrm{Ker}(A)$$

for some (non unique) binary string y, i.e., $q(x)$ effectively "hides" a binary string. The HLF problem asks to find such a y.

(b) We introduce a gate U_q that performs the following action (with i the imaginary unit):

$$U_q |s\rangle = i^{q(s)} |s\rangle, \ s \in \{0,1\}^n.$$

Derive the relation

$$H^{\otimes n} U_q H^{\otimes n} |0^{\otimes n}\rangle = \frac{1}{2^n} \sum_{x,z\in\{0,1\}^n} i^{q(x)} (-1)^{z^T x} |z\rangle .$$

One can prove (see appendix) that the coefficient of each computational basis state $|z\rangle$ in this sum is non-zero precisely if z is a solution of the HLF problem. Thus a single standard measurement will yield a solution.

(c) We now discuss how a constant depth quantum circuit can realize U_q. Show that

$$U_q = \prod_{(v_i,v_j)\in E} CZ_{i,j},$$

with $CZ_{i,j}$ the controlled-Z gate between qubits i and j, defined as $CZ_{i,j} |x\rangle = (-1)^{x_i x_j} |x\rangle$ for $x \in \{0,1\}^n$.

[1] S. Bravyi, D. Gosset, R. König: *Quantum advantage with shallow circuits.* Science 362, 308–311 (2018)

Solution

(a) We first expand the expression algebraically, for $x, y \in \mathrm{Ker}(A)$:

$$\begin{aligned} q(x \oplus y) &= \sum_{i,j=1}^{n} A_{i,j}(x_i \oplus y_i)(x_j \oplus y_j) \bmod 4 \\ &= \sum_{i,j=1}^{n} A_{i,j}(x_i x_j + y_i y_j + x_i y_j + x_j y_i) \bmod 4 \\ &= q(x) + q(y) + 2y^T Ax \bmod 4 \\ &= q(x) + q(y) \bmod 4. \end{aligned}$$

For the last step we have used that $x \in \mathrm{Ker}(A)$, such that $2Ax \bmod 4 = 0$. Using the linearity of q, we note that $0 = q(0) = q(x \oplus x) = 2q(x)$. Thus, $q(x) \in \{0, 2\}$. We now define the function l by

$$l(x) = \begin{cases} 0 & \text{if } q(x) = 0 \\ 1 & \text{if } q(x) = 2 \end{cases}$$

The function l inherits linearity under addition modulo 2 from q, and can thus be represented by

$$l(x) = \sum_{i=1}^{n} y_i x_i \bmod 2$$

for some binary string $y \in \{0, 1\}^n$. Consequently, $q(x)$ can be written as

$$q(x) = 2\sum_{i=1}^{n} y_i x_i \bmod 4.$$

(b) We first note that the application of the Hadamard gate to a qubit $|x\rangle$, $x \in \{0, 1\}$, can be represented as

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{z \in \{0,1\}} (-1)^{zx} |z\rangle .$$

Thus

$$\begin{aligned} H^{\otimes n} U_q H^{\otimes n} |0^{\otimes n}\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} H^{\otimes n} U_q |x\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} i^{q(x)} H^{\otimes n} |x\rangle \\ &= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{z \in \{0,1\}^n} i^{q(x)} (-1)^{z_1 x_1} \cdots (-1)^{z_n x_n} |z\rangle \\ &= \frac{1}{2^n} \sum_{x,z \in \{0,1\}^n} i^{q(x)} (-1)^{x^T z} |z\rangle . \end{aligned}$$

(c) We can verify this via inspection of the terms $A_{i,j} x_i x_j$ defining q. The only non-trivial situation is $A_{i,j} = 1$ and $i \neq j$. The term $A_{i,j} x_i x_j$ will be non-zero precisely if both $x_i = 1$ and $x_j = 1$, and it actually appears twice in the definition of $q(x)$ ($i \leftrightarrow j$). Thus it contributes a factor of $i^2 = -1$ to $i^{q(x)}$ in this case, and $i^0 = 1$ otherwise. This matches the action of the controlled-Z gate $CZ_{i,j}$.

Thus, the circuit solely consisting of CZ gates realizes U_q. Since each vertex of the graph has at most 4 neighbors and gates on disjoint pairs of qubits can be executed in parallel, the circuit has constant depth irrespective of problem size.

Appendix (Mathematical derivations for the quantum algorithm)
This section contains parts of the proof why the quantum algorithm provides a solution for the 2D HLF problem. For the full details, refer to section B in the supplementary information of the publication.

We first read off the probability (squared coefficient) of any computational basis state $|z\rangle$ in the summation expansion shown in (b):

$$p(z) = \frac{1}{4^n} \left| \sum_{x \in \{0,1\}^n} \left| i^{q(x)} (-1)^{z^T x} \right|^2 \right| .$$

Given a linear subspace $\mathcal{L} \subseteq \{0,1\}^n$ and $z \in \{0,1\}^n$, we define the so-called *partial Fourier transform* Γ by

$$\Gamma(\mathcal{L}, z) = \sum_{x \in \mathcal{L}} (-1)^{z^T x} \cdot i^{q(x)}.$$

Thus

$$p(z) = \frac{1}{4^n} \left| \Gamma(\{0,1\}^n, z) \right|^2 .$$

Now partition $\{0,1\}^n = \mathrm{Ker}(A) + \mathcal{K}$, where $\mathcal{K} \subseteq \{0,1\}^n$ is a linear subspace and $\mathrm{Ker}(A) \cap \mathcal{K} = \{0\}$. Then, by the linearity of q,

$$\begin{aligned} \Gamma(\{0,1\}^n, z) &= \sum_{x \in \mathrm{Ker}(A), x' \in \mathcal{K}} (-1)^{z^T (x + x')} \cdot i^{q(x \oplus x')} \\ &= \sum_{x \in \mathrm{Ker}(A)} (-1)^{z^T x} \cdot i^{q(x)} \sum_{x' \in \mathcal{K}} (-1)^{z^T x'} \cdot i^{q(x')} = \Gamma(\mathrm{Ker}(A), z) \cdot \Gamma(\mathcal{K}, z). \end{aligned}$$

It can be shown that (see supplementary information of the publication) that

$$\Gamma(\mathrm{Ker}(A), z) = \begin{cases} \left|\mathrm{Ker}(A)\right| & \text{if } z \text{ is a solution to the 2D HLF problem} \\ 0 & \text{otherwise} \end{cases}$$

A required argumentation is the following: Let y be a hidden bit string such that $q(x) = 2 \sum_{i=1}^n y_i x_i$. Then $z \in \{0,1\}^n$ is another bit string with this property precisely if $z^T x = y^T x \bmod 2$ for all $x \in \mathrm{Ker}(A)$, which is equivalent to $(z \oplus y)^T x = 0 \bmod 2$ for all $x \in \mathrm{Ker}(A)$. This means that $z \oplus y \in \mathrm{Ker}(A)^\perp$ (orthogonal complement).