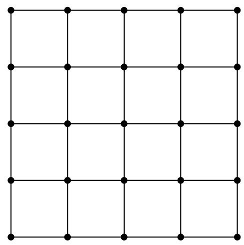
Christian B. Mendl, Irene López Gutiérrez, Keefe Huang due: 10 January 2022, 08:00 on Moodle

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 $V = \{v_1, \dots, v_n\}$ 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 $i, j \in \{1, \dots, n\}$. 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

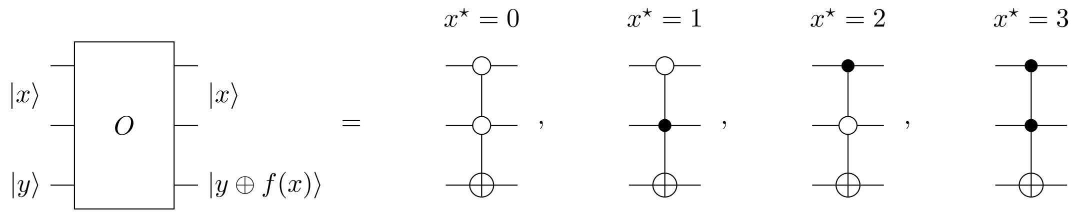
$$U_q = \prod_{(v_i, v_j) \in E} CZ_{i,j},$$

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)

Exercise 9.1 (Two-bit quantum search)
We consider the quantum search (Grover's) algorithm for the special case $n = 2$, i.e., a search space with $N = 4$ elements, and $M = 1$ (exactly one solution). The solution is denoted $x^\star$, and correspondingly $f(x^\star) = 1$, $f(x) = 0$ for all $x \neq x^\star$.

The oracle, which is able to recognize the solution, can be realized as follows (depending on $x^\star$):

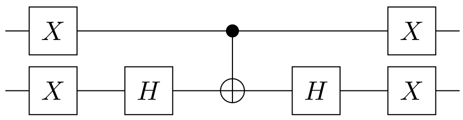


Note that the rightmost gate for $x^\star = 3$ is the Toffoli gate (cf. Exercise 5.2): the first and second qubits act as controls, and the third qubit as target, which is flipped precisely if both controls are set to 1. The empty circles in the gates for $x^\star = 0, 1, 2$ mean that the control is activated by 0 (instead of 1).

As derived in the lecture, the Grover operator G performs a rotation by angle θ in the plane spanned by the orthonormal states $|\alpha\rangle$ and $|\beta\rangle$; thus k applications to the initial equal superposition state $|\psi\rangle = \cos(\frac{\theta}{2})\,|\alpha\rangle + \sin(\frac{\theta}{2})\,|\beta\rangle$ results in

$$G^k\,|\psi\rangle = \cos\left((\tfrac{1}{2} + k)\theta\right)|\alpha\rangle + \sin\left((\tfrac{1}{2} + k)\theta\right)|\beta\rangle\,.$$

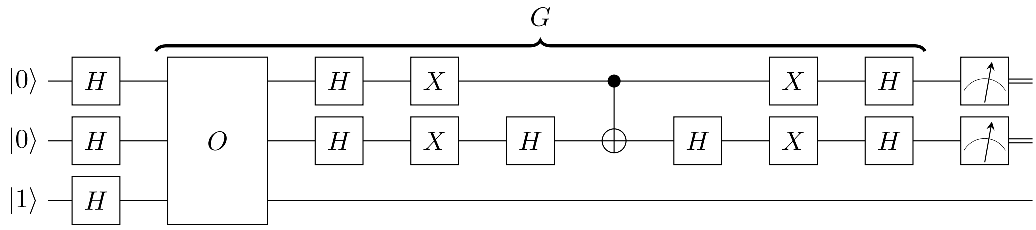
(a) Show that the following circuit implements the negated phase gate appearing in the Grover operator, that is, $-(2\,|00\rangle\langle 00| - I)$:



The global factor (-1) does not influence the final quantum measurement results and will be ignored from now on.

(b) Compute the angle θ defined via $\sin(\frac{\theta}{2}) = \sqrt{M/N}$. Why is a single application of G sufficient to reach the desired solution state $|\beta\rangle$ exactly, that is, $G\,|\psi\rangle = |\beta\rangle$?

In summary, the quantum search circuit with one use of G and the above realization of the phase gate is:



(c) Assemble this circuit in the IBM Q Circuit Composer for one of the four possible oracles of your choice, and verify that the final measurement indeed yields the solution $x^\star$.

Hint: You can use the Pauli-X gate to initialize the oracle qubit to $|1\rangle$. The Toffoli gate is available in the Circuit Composer.

Exercise 9.2 (Quantum search as quantum simulation, part 1)
Interestingly, the quantum search algorithm can be derived from a Schrödinger time evolution governed by a certain Hamiltonian H (cf. Tutorial 3). For simplicity, we assume that there is a single solution $x \in \{0, \dots, N-1\}$ to the search problem with N elements, and we start from an arbitrary initial state $|\psi\rangle$. It turns out that the Hamiltonian

$$H = |x\rangle\langle x| + |\psi\rangle\langle\psi|$$

achieves a transition from $|\psi\rangle$ to $|x\rangle$, that is, $\mathrm{e}^{-iHt^*}\,|\psi\rangle = |x\rangle$ for a certain time t^* (up to a phase factor, which is not relevant here). In part 1 we analyze the time evolution theoretically, and part 2 (next exercise sheet) discusses the simulation of the Hamiltonian.

To understand the transition from $|\psi\rangle$ to $|x\rangle$, first note that the time dynamics under H never leaves the two-dimensional space spanned by $|x\rangle$ and $|\psi\rangle$. Let the vector $|y\rangle$ be chosen such that $\{|x\rangle, |y\rangle\}$ forms an orthonormal basis of this subspace, and represent $|\psi\rangle = \alpha\,|x\rangle + \beta\,|y\rangle$ for some coefficients $\alpha, \beta \in \mathbb{C}$ with $|\alpha|^2 + |\beta|^2 = 1$. For simplicity, we can assume that the phases of $|x\rangle$, $|y\rangle$ and $|\psi\rangle$ are such that α and β are real.

(a) Show that the matrix representation of H within this subspace is given by

$$H = I + \alpha(\beta X + \alpha Z).$$

Hint: The matrix entries of H restricted to a subspace with orthonormal basis $\{|u_j\rangle\}_{j=1,\dots,n}$ are $(\langle u_j| H |u_k\rangle)_{j,k}$.

(b) From the representation in (a), we thus obtain $\mathrm{e}^{-iHt} = \mathrm{e}^{-it}\,\mathrm{e}^{-i\alpha t(\beta X+\alpha Z)}$, where the phase factor e^{-it} stems from the identity matrix in the representation. Use the definition of the single-qubit rotation operators (see lecture) to verify that

$$\mathrm{e}^{-iHt} = \mathrm{e}^{-it}\left(\cos(\alpha t) I - i\sin(\alpha t)(\beta X + \alpha Z)\right).$$

(c) Show that $(\beta X + \alpha Z)\,|\psi\rangle = |x\rangle$. Together with (b), we thus arrive at

$$\mathrm{e}^{-iHt}\,|\psi\rangle = \mathrm{e}^{-it}\left(\cos(\alpha t)\,|\psi\rangle - i\sin(\alpha t)\,|x\rangle\right).$$

(d) Specify a time t^* such that $\mathrm{e}^{-iHt^*}\,|\psi\rangle = |x\rangle$ up to a phase factor.

(e) Since the required time t^* depends on $\alpha = \langle x|\psi\rangle$ and thus seemingly on the (a priori unknown) solution x, a natural question is how to determine t^*. To resolve this question, one can choose $|\psi\rangle$ to be the equal superposition state. Compute α in this case, assuming that $|\psi\rangle$ is normalized.