Christian B. Mendl, Pedro Hack, Keefe Huang, Irene López Gutiérrez

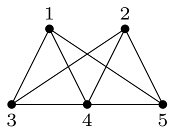
Exercise 10.1 (Hidden Linear Function problem on a specific graph)
Recall from tutorial 9 the following function q, given a square matrix A with binary entries:

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

The Hidden Linear Function (HLF) problem asks to find a binary string y such that

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

A is chosen as adjacency matrix of a graph. Instead of a general square grid, here we consider the following graph as specific realization:



(a) Write down the corresponding adjacency matrix A.

(b) Compute the kernel $\mathrm{Ker}(A) \bmod 2$. (You are allowed to use a computer algebra system for this task.)

(c) Implement the quantum algorithm from part (b) and (c) of tutorial 9 using the circuit composer of IBM Q (`https://quantum-computing.ibm.com/`). Verify that one of the computational basis states appearing in the output with non-zero probability is indeed a solution to the HLF problem. Submit a screenshot showing the circuit as well as the output amplitudes or measurement probabilities.
Hint: You can create a controlled-Z gate by adding a control modifier to the Z gate in the circuit composer.

Solution

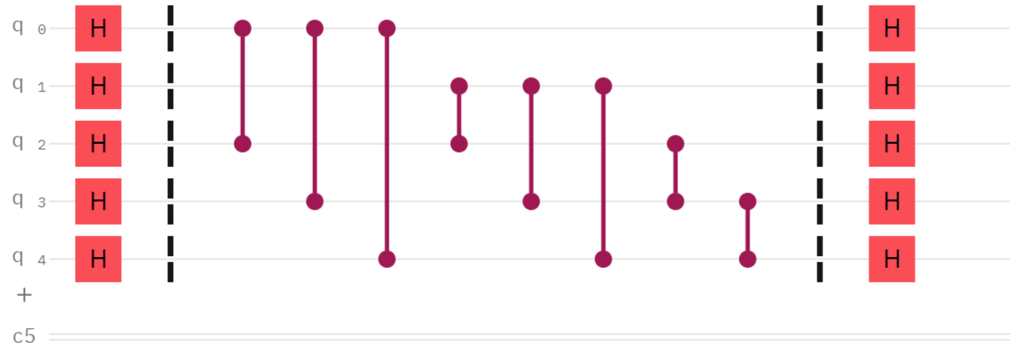
(a) The adjacency matrix of the graph is

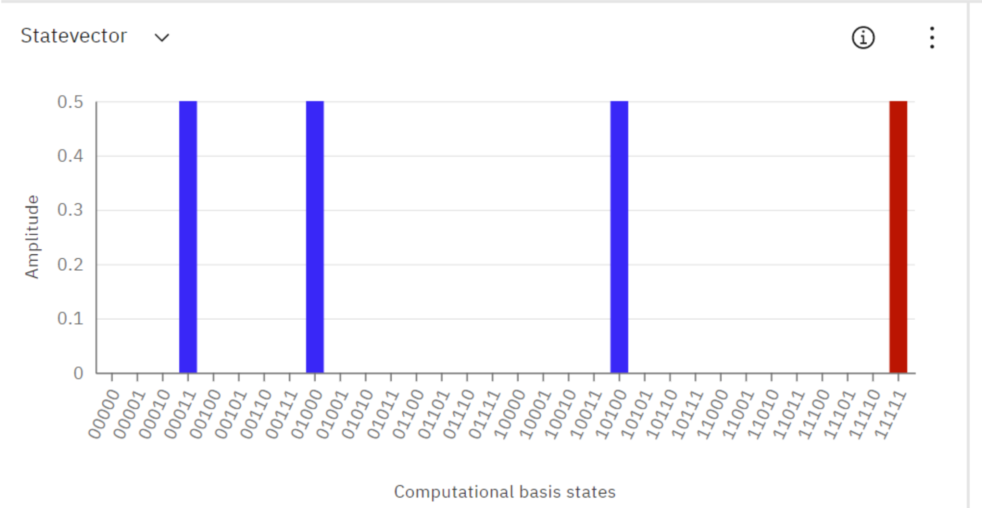
$$A = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

(b) We want to find the vectors x such that $Ax = 0 \bmod 2$. They can be computed "by hand" for example by Gaussian elimination modulo 2. The space of solutions is spanned by the following three vectors:

$$\mathrm{Ker}(A) = \mathrm{span}\left(x^1, x^2, x^3\right) \quad \text{with} \quad x^1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad x^2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad x^3 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

(c) The corresponding quantum circuit and output statevector computed by the IBM circuit composer is





The output is a superposition of four computational basis states, one of which is

$$y = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Inserting the vectors from (b) into q results in

$$q(x_1) = 0, \quad q(x_2) = 0, \quad q(x_3) = 6 \bmod 4 = 2 \bmod 4.$$

This indeed agrees with $2 \sum_{i=1}^{5} y_i x_i \bmod 4$, as required.