OUR FIRST QUANTUM ALGORITHM

Consider a black box which takes in 3 input qubits (x_1, x_2, x_3) and 5 ancilla qubits $(z_1, \ldots, z_5)$. This black box represents an operation on 256-dimensional Hilbert space! We will describe this operation using combinations of three types of feasible matrices, organized into 14 basic quantum logic gates. The three feasible matrices we will use are

$$\mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \mathrm{S} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathrm{TOF} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Together with the identity matrices of arbitrary size, I_N, these matrices will serve us as building blocks of the quantum logic gates we need, using tensor products. The sequence of 14 gates that make up our quantum algorithm is represented by the following twelve 256×256 matrices (two will be used twice):

$$G_1 = I_8 \otimes \mathrm{TOF} \otimes I_4, \quad G_2 = \mathrm{TOF} \otimes I_2 \otimes \mathrm{TOF} \otimes I_2, \quad G_3 = I_4 \otimes \mathrm{X} \otimes I_{32},$$
$$G_4 = I_4 \otimes \mathrm{TOF} \otimes I_8, \quad G_5 = I_2 \otimes \mathrm{TOF} \otimes I_{16}, \quad G_6 = I_{32} \otimes \mathrm{S} \otimes I_2,$$
$$G_7 = I_{16} \otimes \mathrm{S} \otimes \mathrm{S}, \quad G_8 = I_4 \otimes \mathrm{S} \otimes I_2 \otimes \mathrm{S} \otimes I_2, \quad G_9 = I_2 \otimes \mathrm{S} \otimes I_{32},$$
$$G_{10} = \mathrm{S} \otimes \mathrm{S} \otimes \mathrm{X} \otimes I_8, \quad G_{11} = I_{16} \otimes \mathrm{S} \otimes I_4, \quad G_{12} = I_8 \otimes \mathrm{S} \otimes I_8$$

1) To begin with, check that all these matrices are indeed 256×256!

2) Check that all of them have only eigenvalues $+1$ and -1, with different multiplicities.

We are now in a position to state our first quantum algorithm. Consider the matrix

$$M = G_1 G_6 G_7 G_8 G_3 G_2 G_9 G_{10} G_4 G_{11} G_{12} G_3 G_5 G_{12}$$

applied to the eight qubits in the sequence $z_3, x_1, x_2, x_3, z_1, z_2, z_4, z_5$, and consider the 6^{th} output qubit to represent the output of our algorithm.

3) What is this algorithm computing, if we set all ancilla qubits to 0 and let $x_1, x_2, x_3 \in \mathbb{Z}_2$?