Exercise Set 10
Quantum Computation

Exercise 1 *Convergents in Shor's algorithm*

One runs Shor's algorithm in order to retrieve the period of the function $f(x) = 3^x \bmod N$, where $N = 35$ (yes, we all know that $N = 35 = 5\cdot 7$, but let us pretend that this factorization is not easy...). The algorithm uses $m = 11$ qubits (so that $M = 2^m = 2'048 \geq N^2 = 1'225$). Using the method of convergents seen in class, describe which of the following outcomes y of the quantum circuit lead(s) to the identification of the correct period r of f:

(a) $y = 171$ (b) $y = 512$ (c) $y = 853$

Exercise 2 *Grover's algorithm for $N = 4$*

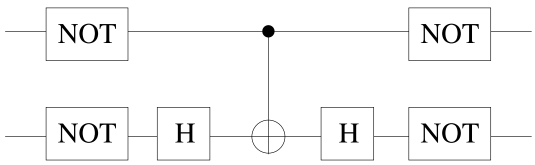
Let $x \in \{x_0, x_1, x_2, x_3\}$ and $f(x) = 1$ if and only if $x = x_0$. Otherwise $f(x) = 0$. We search x_0 thanks to an "oracle" which returns the value of f when queried with an entry.

(a) What is the theoretical prediction for the number of queries of the oracle in the quantum setting when we use Grover's algorithm ?

(b) Show that the following

$$U = \mathbb{I} - 2|\underbrace{00...0}_{n \text{ times}}\rangle\langle 00...0|$$

is unitary and show also that for $n = 2$ it can be implemented by the following circuit:



(c) Take Grover's circuit and for $N = 4$ compute the quantum state at each step of the algorithm. Draw a geometrical representation in an appropriate two dimensional space (like in class). Confirm that the measurement of the final state indeed gives x_0 and that only one query of the oracle was needed.