Exercise sheet 2, 18 February 2021

1. The slide set for Quantum computing for cryptographers II on page 8 left open the circuit in the middle. Identify the operation that is done based on the effects you see on the amplitude vector.
   Make a circuit, i.e. a sequence of NOT_i, $\mathrm{C}_i\mathrm{NOT}_j$, $\mathrm{C}_i\mathrm{C}_j\mathrm{NOT}_k$, and H_i gates, to compute this operation.
   Hint: You will need to use the extra ancilla q_2 that is shown in the circuit.

2. Using the standard gates NOT_i, $\mathrm{C}_i\mathrm{NOT}_j$, and $\mathrm{C}_i\mathrm{C}_j\mathrm{NOT}_k$ works well for operations defined at bit level. Show how to compute integer addition with these. For concreteness, show how to obtain the $n+1$-bit sum of two n-bit integers.
   Remember the carries.

   This should give a circuit of $3n+1$ qubits (n for each of the inputs plus $n+1$ for the result) and ancillas as far as you need them.

3. Simon's algorithm for finding the "period" of a function

   $$f : \mathbb{F}_2^n \to \mathbb{F}_2^n$$

   operates on $2n$ qubits and possibly some more ancillas needed to compute f. The first n steps are H_i for $0 \le i < n$ to create a uniform superposition over the first n qubits. This is followed by the computation of $f(u)$ on the second n qubits. The last n steps are H_i for $0 \le i < n$ and then the result is measured.

   Assume that you have a function $f : \mathbb{F}_2^2 \to \mathbb{F}_2^2$ which satisfies $f(u) = f(u+01)$. Write out an example of the 4×4 matrix after computing f and trace through what H_0 and H_1 do and how the result is orthogonal to 01.

   Remember that after computing f column u has a single 1 in position $f(u)$ and that your matrix must respect $f(u) = f(u+01)$.

4. Staying with the example of $f : \mathbb{F}_2^2 \to \mathbb{F}_2^2$ from the previous exercise. Show the effect of H_0 and H_1 on the 4 unit vectors e_i, $0 \le i < 4$ where e_i has a single 1 in position i and is 0 everywhere else.

Observe that the operation of H_i is linear to show why $\mathrm{H}_1(\,\mathrm{H}_0(e_i + e_{i\oplus s}))$ gives a vector with non-zero entries only in positions j for j orthogonal to s.

5. Assume that $f(u) = 0$ for a unique n-bit string u. Assume that the amplitude vector inside Grover's algorithm has entry a at the position u where $f(u) = 0$, and has entry b at the other $2^n - 1$ positions. The amplitude vector one iteration, i.e. one pair of Step 1 and Step 2, later then has entry a' at the position u where $f(u) = 0$, and has entry b' at the other $2^n - 1$ positions.

   (a) Find a 2×2 matrix M, depending only on n (not on a and b), such that multiplying the vector $(a \quad b)$ by M gives $(a' \quad b')$.

   (b) Explain how M can be viewed as rotating a scaled version of its input, i.e., determine a scaling factor s so that $(a \quad b \cdot s)M' = (a' \quad b' \cdot s)$ and M' is a rotation matrix.