CPSC506 **Complexity of Computation** **Term 2, 2020**

Homework # 5

Due in class on Wednesday, April 1.

1. Consider the following pebble game, which is played on a line of nodes numbered consecutively from 0 to $T = 2^{n-1}$.

   - Initially there is a pebble on node 0; this pebble must always stay on node 0. No other node has a pebble placed on it initially.
   - For $k \geq 1$, a pebble can be placed at node k only when node $k-1$ has a pebble, and a pebble can be removed from node k only when node $k-1$ has a pebble.
   - The goal is to place a pebble at node $T = 2^n - 1$, while using as few total pebbles as possible (not counting the pebble at node 0).

   Describe a way to play the game optimally. It's fine to use a pebble multiple times—it is the total number of distinct pebbles in place at any one time that should be minimized (rather than the total number of pebble placements or removals). How many pebbles are needed? How many pebble placements does your strategy use?

   [A suggestion that might be useful:

   Let $F_1(a, a)$ denote the placement of a pebble at node a, and let $F_1(a, a)^{-1}$ denote the removal of a pebble at node a.

   For $i \geq 2$, let $F_i(a+1, a+2^{i-1})$ denote a sequence of pebble placements and removals between nodes $a+1$ and $a+2^{i-1}$ that, starting with a pebble at node a and no pebbles at nodes $a+1, \ldots a+2^{i-1}$, ends with a pebble at node $a+2^{i-1}$ (and at node a), and no pebbles at nodes $a+1, \ldots a+2^{i-1}-1$.

   Let $F_i(a+1, a+2^{i-1})^{-1}$ be the reverse of $F_i(a+1, a+2^{i-1})$. Thus, starting with a pebble at node $a+2^{i-1}$ and no pebbles at nodes $a+1, a+1, \ldots a+2^{i-1}-2$, the sequence $F_i(a+1, a+2^{i-1})^{-1}$ ends with a pebble at node a and no pebbles at nodes $a+1, \ldots a+2^{i-1}$.

   Provide an inductive definition of $F_i(a+1, a+2^{i-1})$ that uses as few pebbles as possible.]

2. Let C be a Boolean circuit and let Q_C be a reversible circuit that simulates C, as described in Lecture 7 of John Watrous' Introduction to Quantum Computing lecture notes. If C has k gates (AND, OR, NOT and Fanout), then Q_C may have $\Theta(k)$ ancilla bits.

   Can you adapt the construction to have $O(\log k)$ ancilla bits? Hint: employ the pebble game described in the previous problem.

3. A reversible k-bit gate is a 1-1 and onto function from $\{0,1\}^k$ to $\{0,1\}^k$ (or equivalently, a permutation).

   Show that there is no universal set of reversible 1- and 2-bit gates, by (i) showing an example of a 3-bit reversible gate that is not linear and (ii) showing that the composition of linear 1-bit and 2-bit gates is a linear function.

You can use without proving it the fact that each two-bit reversible gate is linear, i.e. the output bits x' and y' can be expressed in the following way as a function of the input bits x and y:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}$$

where $a, b \in \{0, 1\}$ and the binary matrix M is invertible (there are six possibilities for M).

4. Show that the following circuit (taken from Watrous' notes) simulates a Toffoli gate. Here, the second operation, indicated with an i below the black circle, corresponds to the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$