QIC 710 / CO 681 / AMATH 871 / CS 768 / PHYS 767 Fall 2017

Homework 2

Due date: Thursday, October 25

Completed homeworks will be submitted online in Crowdmark. You will receive an email with instructions closer to the due date. A requirement for this is that each of your solutions *must begin on a new page.* Typesetting solutions in LaTeX is recommended but not required. If you do write your solutions by hand, please ensure that your scans are legible before you upload them.

1. **Modular arithmetic (20%)** For each integer $m \geq 2$, recall that we defined in class the following two groups: The additive group of integers modulo m

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$$

and the multiplicative group of integers modulo m

$$\mathbb{Z}_m^\times = \{x \in \mathbb{Z}_m : \gcd(x, m) = 1\}.$$

Note that if $m = p$ is prime, then $\mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\}$ contains all the nonzero elements of $\mathbb{Z}_p$. If g is a generator for $\mathbb{Z}_p^\times$, then the (base-g) discrete logarithm modulo p is the function $\log_g : \mathbb{Z}_p^\times \to \mathbb{Z}_{p-1}$ satisfying $a = g^{\log_g(a)}$ for each $a \in \mathbb{Z}_p^\times$.

(a) What is $19 + 20 + 21 \bmod 22$?

(b) What is $21^{10000} \bmod 22$?

(c) What is $\mathbb{Z}_{22}^\times$?

(d) What is $\mathrm{ord}_{22}(7)$?

(e) It turns out that 2 is a generator for $\mathbb{Z}_{11}^\times$. What is $\log_2(3) \bmod 11$?

2. **Mod-3 binary multiplier (20%)** Let $f : \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3$ be the multiplication function $f(x, y) = xy$ on $\mathbb{Z}_3$. In this problem, you will construct an explicit quantum circuit on 6 qubits that implements a unitary U satisfying

$$U|x_1x_2\rangle|y_1y_2\rangle|00\rangle = |x_1x_2\rangle|y_1y_2\rangle|z_1z_2\rangle$$

for all $x_1x_2, y_1y_2 \in \{00, 01, 10\}$, where $z = f(x, y)$, and where x_1x_2 is x in binary, i.e. $x = 2x_1 + x_2$. The unitary U can do anything to the remaining computational basis states.

(a) Make a table with the values of z_1z_2 for each $x_1x_2, y_1y_2 \in \{00, 01, 10\}$.

(b) Suppose that $x_1x_2 \neq 00$ and $y_1y_2 \neq 00$. Find formulas for z_1 and z_2 as (mod 2) sums of the bits x_1, x_2, y_1, y_2 and 1 that are correct under this assumption.

(c) Use your previous answer to find a quantum circuit, using only controlled-NOTs and X gates, that implements U correctly under the assumption that $x \neq 0$ and $y \neq 0$, i.e. on the 4-dimensional subspace spanned by $|x_1x_2\rangle|y_1y_2\rangle|00\rangle$ for all $x_1x_2, y_1y_2 \in \{01, 10\}$. In other words, your circuit should implement arithmetic correctly in $\mathbb{Z}_3^\times = \{1, 2\}$.

(d) Use X gates and multiply controlled-NOTs to modify your previous answer to give a quantum circuit implementing U on the full 9-dimensional subspace spanned by $|x_1x_2\rangle|y_1y_2\rangle|00\rangle$ for all $x_1x_2, y_1y_2 \in \{00, 01, 10\}$.

3. **Quantum Fourier transform (20%)**

Let

$$F_m = \frac{1}{\sqrt{m}} \sum_{i,j=0}^{m-1} \omega^{ij} |i\rangle\langle j|$$

be the quantum Fourier transform, where $\omega = e^{2\pi i/m}$.

(a) How does F_m^2 act on the computational basis?

(b) Give a complete set of eigenvectors and eigenvalues of F_m^2. There are two cases to consider: m odd and m even.

4. **Simon's algorithm mod 2^n (20%)** Let $n \geq 1$ and suppose that

$$f\colon \mathbb{Z}_{2^n} \times \mathbb{Z}_{2^n} \to \{0,1\}^n$$

is a function such that, for some (unknown) $r \in \mathbb{Z}_{2^n}$, $f(x) = f(y)$ iff $x - y \in L_0$, where

$$L_0 = \mathbb{Z}_{2^n}(r,1) = \{k(r,1) : k \in \mathbb{Z}_{2^n}\} = \{x : x \cdot (1,-r) = 0\}.$$

In other words, f is constant along the 2^n discrete lines

$$L_c = \{x \in \mathbb{Z}_{2^n} \times \mathbb{Z}_{2^n} : x \cdot (1,-r) = c\}$$

parallel to $(r,1)$ in the "discrete plane" $\mathbb{Z}_{2^n} \times \mathbb{Z}_{2^n}$. For some intuition about what such discrete lines can look like, see Problem 5 below.

Given an oracle for reversibly computing f via $|x_1\rangle|x_2\rangle|0\rangle \mapsto |x_1\rangle|x_2\rangle|f(x)\rangle$, Simon's algorithm first creates the following state by querying f on an equal superposition over its possible inputs:

$$\frac{1}{2^n} \sum_{x_1,x_2 \in \mathbb{Z}_{2^n}} |x_1\rangle|x_2\rangle|f(x)\rangle.$$

(a) Show that if we measure the third register of the above state in the computational basis, the state of the first two registers is an equal superposition

$$|L_c\rangle := \frac{1}{\sqrt{2^n}} \sum_{x \in L_c} |x_1\rangle|x_2\rangle$$

over one of the discrete lines L_c, for a uniformly random $c \in \mathbb{Z}_{2^n}$.

(b) For each $c \in \mathbb{Z}_{2^n}$, express $(F_{2^n}^{-1} \otimes F_{2^n}^{-1})|L_c\rangle$ as a superposition over basis states $|s_1\rangle|s_2\rangle$ such that $s \cdot (r,1) = 0$, i.e. such that s in on the discrete line $\mathbb{Z}_{2^n}(1,-r)$ through the origin, perpendicular to L_0.

5. **Quantum computing discrete log modulo Fermat primes (20%)**

Suppose that p is a prime of the form $2^n + 1$. Then, as we saw in class, the method of Problem 4 can be used to give a quantum algorithm for computing the discrete logarithm mod p, since $|\mathbb{Z}_p^\times| = 2^n$. Primes of this form as known as Fermat primes. To date, the only known Fermat primes are 3, 5, 17, 257 and 65537, so this is mostly of interest here for examples. In this problem, we work with the prime $p = 5$ and are concerned with discrete logarithms to base 2.

To compute $\log_2(a)$ for $a \in \mathbb{Z}_5^\times$, recall that we use the function $f_a(x) = g^{x_1} a^{-x_2}$ in place of the black-box function in Problem 4. For each of the 4 possible values of a, make a table

$$\begin{pmatrix} f(0,0) & f(0,1) & f(0,2) & f(0,3) \\ f(1,0) & f(1,1) & f(1,2) & f(1,3) \\ f(2,0) & f(2,1) & f(2,2) & f(2,3) \\ f(3,0) & f(3,1) & f(3,2) & f(3,3) \end{pmatrix}$$

of the possible values of f_a and verify that f_a is constant along the discrete lines parallel to $(r, 1)$, where $r = \log_2(a)$.