# Quantum Information Processing Assignment 5

**Name:** Nate Stemen (20906566)
**Email:** nate.stemen@uwaterloo.ca
**Due:** Thur, Oct 22, 2020 11:59 PM
**Course:** QIC 710

I worked with Chelsea Komlo and Wilson Wu on this assignment.

**Problem 1**

Consider the case where $m = 35$, $r = 7$, and $s = 5$.

(a) Give an example of a function $f : \mathbb{Z}_{35} \to \mathbb{Z}_{35}$ that is strictly 7-periodic. You may give the truth table or you may give a list of 35 numbers, that we'll interpret as $f(0), f(1), f(2), \ldots, f(34)$. Although any strictly 7-periodic function will get full marks here, please try to make your function look as irregular as you can subject to the condition of being strictly 7-periodic.

(b) What are the *colliding sets* of your function in part (a)? List these sets. Also, show that they satisfy the Simon mod 35 property, namely, that they are of the form $\{a, a+7, a+2\cdot 7, \ldots, a+(s-1)\cdot 7\}$ for some $a \in \mathbb{Z}_{35}$.

(c) List all $b \in \mathbb{Z}_{35}$ such that $b \cdot 7 = 0$ (in mod 35 arithmetic).

**Solution.** (a) We will first give the values of $f$ as our strictly 7-periodic function.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| $f(x)$ | 4 | 43 | 0 | 7 | 20 | 572 | 2 |
| $x$ | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| $f(x)$ | 4 | 43 | 0 | 7 | 20 | 572 | 2 |
| $x$ | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| $f(x)$ | 4 | 43 | 0 | 7 | 20 | 572 | 2 |
| $x$ | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| $f(x)$ | 4 | 43 | 0 | 7 | 20 | 572 | 2 |
| $x$ | 28 | 29 | 30 | 31 | 32 | 33 | 34 |
| $f(x)$ | 4 | 43 | 0 | 7 | 20 | 572 | 2 |

(b) The way we've aligned the table shows clearly the colliding sets are as follows.

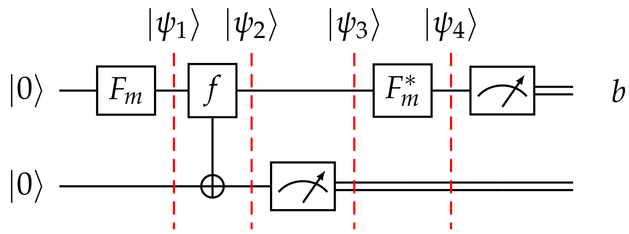
| Colliding set | Collision value |
|---|---|
| $0, 7, 14, 21, 28$ | 4 |
| $1, 8, 15, 22, 29$ | 43 |
| $2, 9, 16, 23, 30$ | 0 |
| $3, 10, 17, 24, 31$ | 7 |
| $4, 11, 18, 25, 32$ | 20 |
| $5, 12, 19, 26, 33$ | 572 |
| $6, 13, 20, 27, 34$ | 2 |

(c) Any $b \in \{0, 5, 10, 15, 20, 25, 30\}$ will satisfy $b \cdot 7 = 0$.

**Problem 2**

Simon mod $m$ algorithm in the $d = 1$ case.

**Solution.** As we did in lecture we will break this down into finding out how the state transforms at each step of the way.




With that, let's apply the first Fourier transform to $|0\rangle$.

$$|\psi_1\rangle = F_m |0\rangle |0\rangle = \frac{1}{\sqrt{m}} \sum_{b \in \mathbb{Z}_m} \omega^{0 \cdot b} |b\rangle |0\rangle = \frac{1}{\sqrt{m}} \sum_{b \in \mathbb{Z}_m} |b\rangle |0\rangle$$

And now let's apply the second gate. It's not a controlled-$f$, but that's what I want to call it. What do we call this thing?

$$|\psi_2\rangle = \frac{1}{\sqrt{m}} \sum_{b \in \mathbb{Z}_m} |b\rangle |0 + f(b)\rangle = \frac{1}{\sqrt{m}} \sum_{b \in \mathbb{Z}_m} |b\rangle |f(b)\rangle$$

That's not too bad. Now we're going to measure the second qubit. When we do this we are going to get a random $f(b)$ for $b \in \mathbb{Z}_m$. Say we get $f(\tilde{b})$. By the $r$-periodicity of $f$ we know that all of $f(\tilde{b} + kr) = f(\tilde{b})$ for $k \in \mathbb{Z}$, so the first qubit[1] collapses into a superposition of those $\tilde{b} + kr$ states.

$$|\psi_3\rangle = \frac{1}{\sqrt{m}} \sum_{k \in \mathbb{Z}_m} |\tilde{b} + kr\rangle$$

Lastly we have to apply the inverse Fourier transform.

$$\begin{aligned}
|\psi_4\rangle &= F_m^* \frac{1}{\sqrt{m}} \sum_{k \in \mathbb{Z}_m} |\tilde{b} + kr\rangle \\
&= \frac{1}{m} \sum_{b \in \mathbb{Z}_m} \sum_{k \in \mathbb{Z}_m} \omega^{-(\tilde{b}+kr)b} |b\rangle \\
&= \frac{1}{m} \sum_{b \in \mathbb{Z}_m} \sum_{k \in \mathbb{Z}_m} \omega^{-b\tilde{b}} \omega^{-krb} |b\rangle \\
&= \frac{1}{m} \sum_{b \in \mathbb{Z}_m} \omega^{-b\tilde{b}} \left[ \sum_{k \in \mathbb{Z}_m} \omega^{-krb} \right] |b\rangle
\end{aligned}$$

From here we can see if $rb \neq 0$ then using the fact that $\sum_{b \in \mathbb{Z}_m} \omega^b = 0$[2] that these terms will drop out of the expression and hence we will always measure a state with $rb = 0$. This leaves the state as $\sum_b \omega^{-b\tilde{b}} |b\rangle$ and because norm of every coefficient is the same, the probability of getting $rb = 0$ is equally distributed over the states.

[1] Well actually an $m$-dimensional qudit, right?

[2] Multiply both sides by $\frac{1}{\omega^{kr}\omega^{m-1}}$ to get the needed equation.

**Problem 3**

Deducing $r$ from $b$.

**Solution.** First let's make the following observations. $35 = m = 5 \cdot 7 = rs$. So $m$ is the product of two primes. Now assume we are given a $b$ with $br = 0$. This implies that $br$ is a multiple of $m$, and because $m = rs$ we can write $br = krs$ which implies $b = ks$ for some $k \in \mathbb{Z}$. If we take the greatest common divisor of $b$ and $m$ to $\gcd(b, m) = a$ then we will have two cases.

1. $a$ is prime because $b = ks$ and $m = rs$
2. $a$ is 0 which implies $b$ was 0

When $a$ is prime it is $s$ which we can then use to divide $m$ to get $r$.

**Problem 4**

Suppose that $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ is of the form $f(x) = ax^2 + bx + c\ldots$

**Solution.** (a) Let's first look at the three values $f$ can take.

$$\begin{aligned} f(0) &= c \\ f(1) &= a + b + c \\ f(2) &= 4a + 2b + c = a + 2b + c \end{aligned}$$

We can then solve for $a$ as

$$a = -f(0) + 2f(1) - f(2)$$

which clearly shows we need to make three queries to $f$.