**Problem 1:** The trick here is to notice that controlled phase gates are symmetric: a controlled phase from qubit $i$ to qubit $j$ is the same as a controlled phase from qubit $j$ to qubit $i$. With this fact, and the fact that all the controlled phase gates commute, you can move the gates so that as soon as you do the Hadamard on qubit $k$, you measure qubit $k$, and then you perform phase gates that are classically controlled by the results of the measurement. It’s a lot clearer with a diagram, but I don’t have time to draw it.

**Problem 2a:** This time, we only have one register, of length $n$. We start by making an equal superposition of all states:

$$
\frac{1}{2^{n/2}} \sum_{s=0}^{2^n-1} \left| s \right> .
$$

We next apply the oracle $f$:

$$
\frac{1}{2^{n/2}} \sum_{s=0}^{2^n-1} \left| s \right> (-1)^{f(s)}.
$$

We then apply a Hadamard gate to each qubit:

$$
\frac{1}{2^n} \sum_{s,t=0}^{2^n-1} \left| t \right> (-1)^{f(s)} (-1)^{s+t}.
$$

Finally, we measure the state. We obtain the value $| t \rangle$ with probability

$$
\left| \frac{1}{2^n} \sum_{s} (-1)^{f(s)+s+t} \right|^2
$$

and we want to show that this probability is zero if $c \cdot t$ is odd. Let’s group the $s$’s into pairs, $s$ and $s+c$. We know $f(s) = f(s+c)$, so when we add up the $s$’s from each pair, we find

$$
(-1)^{f(s)+s+t} + (-1)^{f(s+c)+(s+c)+t}
$$

which is 0 if $c \cdot t$ is odd. Thus, this whole sum is 0 if $c \cdot t$ is odd, meaning we only observe $| t \rangle$ such that $c \cdot t = 0(\ mod \ 2)$.

**2b:** The problem with the analysis in part 2a is that we haven’t shown that we don’t always find $t = 0$, which doesn’t help us. In fact, if we have $f(x) = 0$ for all $x$, it is easy to see that we will always observe $| 0 \rangle$. If $f(x) = 0$ except for two values, then this is nearly true. Look at the probability of success again.

$$
\left| \frac{1}{2^n} \sum_{s} (-1)^{f(s)+s+t} \right|^2
$$

1
If $t = 0$, and $f(x) = 0$ except for two values, we get that the sum is $2^n - 2$ (since one of these two values will be $-1$ instead of 1). Thus, the probability of 0 is

$$\left(\frac{2^n - 2}{2^n}\right)^2 = 1 - \frac{2^{n-1} - 1}{2^{2(n-1)}}$$

and you can check that the probability of each of the other $2^{n-1} - 1$ possible values of $|t\rangle$ is $\frac{1}{2^{n-1}}$.

2c: If $f$ is random, then Simon’s algorithm will work. For each $t$, the sum

$$\left| \sum_s (-1)^{f(s)+st} \right|^2$$

is the sum of $2^{n-1}$ random variables, each of which is $\pm 2$ with equal probability (these variables come from the pairs $f(s)$ and $f(s + c)$). We expect this to have size roughly $2\sqrt{2^{n-1}}$. So the square of this quantity is roughly $2^{n-1}$, and dividing by $2^{2n}$ gives roughly $1/2^n$.

In fact, because we are computing the square of the expected value of a sum of variables which are $\pm 2$, we can get the exact expected value of the square from the variance of the binomial distribution, and this is $\frac{1}{2^{n-1}}$. So all the values of $t$ with $ct = 0 \mod 2$ are equally likely.

To rigorously show that the algorithm works well, we need to look at the probability that any particular one of these is small, which is not hard.