

Q7:

$$f_s: \{0,1\}^3 \rightarrow \{0,1\}^3$$

$$f_s(000) = f_s(111) = 000$$

$$f_s(001) = f_s(110) = 001$$

$$f_s(010) = f_s(101) = 010$$

$$f_s(011) = f_s(100) = 011$$

1. $f(x) = f(y)$ if $x \oplus y \in \{0^n, s\}$

$$x \oplus y = s \text{ for } x \neq y \text{ and } s \neq 0^n \text{ implies } y = s \oplus x \text{ and}$$

$$\underline{f(x) = f(y) = f(x \oplus s)}$$

$$000 \oplus 111 = \underline{111 = s} \quad f_{111} \quad \text{so} \quad f_{111}(000) = f_{111}(111) = f_{111}(000 \oplus 111)$$

$$\Leftrightarrow 001 \oplus 110 = 010 \oplus 101 = 011 \oplus 100$$

satisfies Simon's problem:

$$\rightarrow f_{111}(001) = f_{111}(110) = f_{111}(001 \oplus 111) = f_{111}(110)$$

$$\rightarrow f_{111}(010) = f_{111}(101) = f_{111}(010 \oplus 111) = f_{111}(101)$$

$$\rightarrow f_{111}(011) = f_{111}(100) = f_{111}(011 \oplus 111) = f_{111}(100)$$

2. Starting State: $|000\rangle|1\rangle$

3. Hadamard $H^{\otimes 4} \cdot \frac{1}{4} (|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) (|0\rangle - |1\rangle)$

4. Oracle: phase shift $(-1)^{f(x)}$: $(-1)^{f(000)=f(111)} = 1$, $(-1)^{f(001)=f(110)} = -1$,
 $(-1)^{f(010)=f(101)} = -1$, $(-1)^{f(011)=f(100)} = 1$

$$\frac{1}{4} (|000\rangle - |001\rangle - |010\rangle + |011\rangle + |100\rangle - |101\rangle - |110\rangle + |111\rangle) (|0\rangle - |1\rangle)$$

5. 011

6. Hadamard: $|011\rangle$

7. the measurement outcome does not conclude to s , because with j we get

$$j \oplus f_s(x) = 000, \text{ which is not unique.}$$

8. $s = j_1 \oplus j_2 = 011 \oplus 101 = 110$

9. If $s = 000$ is allowed the function f is one-to-one, so you can not use Simon's Algorithm.

The algorithm depends on $s \neq 0 \dots 0$ because if not given for $f(x) = f(y)$ y is not necessarily unique. Every input with $x \oplus s$ for $s = 0 \dots 0$ will result in itself and the definition $f(x) = f(y)$ with unique y is not given. Without two-to-one and uniqueness of y the patterns might not exist and no information over s can be gained from the entanglement and following superposition.