Booleans

We represent false as 0 and we represent true as 1. Let $\oplus$ denote "exclusive or", which here is "addition modulo 2".

Question 1. Suppose $f, g : \{0,1\}^n \to \{0,1\}$. Define $h(x) = f(x) \oplus g(x)$.

Prove that h always outputs 0 if and only if f and g are the same function.

Question 2. For a Boolean string $x = x_1 \ldots x_n$, define

$$\begin{aligned} (-1)^x &= (-1)^{(x_1 + \ldots + x_n)} \\ \mathsf{XOR}(x) &= x_1 \oplus \ldots \oplus x_n \end{aligned}$$

Prove that $(-1)^x = 1$ if and only if $\mathsf{XOR}(x) = 0$.

Question 3. For a function $f : \{0,1\}^n \to \{0,1\}$, we say that f is *constant* if either f always outputs 0 or f always outputs 1.

Prove that f is constant if and only if $f(0) \oplus f(1) = 0$.

Question 1:

Question 1. Suppose $f, g : \{0,1\}^n \to \{0,1\}$. Define $h(x) = f(x) \oplus g(x)$.
Prove that h always outputs 0 if and only if f and g are the same function.

$\oplus$ exclusive or : return 1 if one of the statement is 1 and
return 0 if both statements are the same.

① Prove that h always outputs 0 if f and g are the same function.

Assume that f and g are the same function, $f(x) = g(x)$

$h(x) = f(x) \oplus g(x) = f(x) \oplus f(x)$

Since $\oplus$ always returns 0 if the values of two these functions are the same. $f(x) \oplus f(x) = 0$ $\therefore h(x) = 0$.

$\therefore$ h always outputs 0 if f and g are the same function.

② Prove that f and g are the same function if h always outputs 0

Assume that $h(x)$ always outputs 0.

$h(x) = f(x) \oplus g(x)$ $\therefore f(x) \oplus g(x) = 0$

Since $\oplus$ returns 0 only when the values of two these functions are the same, $\therefore f(x) = g(x)$ for all x.

$\therefore$ f and g are the same function.

$\therefore$ f and g are the same function if h always outputs 0

$\therefore$ h always outputs 0 if and only if f and g are the same function.

Question 2:

Question 2. For a Boolean string $x = x_1 \ldots x_n$, define

$$\begin{aligned}(-1)^x &= (-1)^{(x_1+\ldots+x_n)}\\ \mathsf{XOR}(x) &= x_1 \oplus \ldots \oplus x_n\end{aligned}$$

Prove that $(-1)^x = 1$ if and only if $\mathsf{XOR}(x) = 0$.

① Prove that $(-1)^x = 1$ if $XOR(x) = 0$.

Assume $XOR(x) = 0$. $\therefore x_1 \oplus \ldots \oplus x_n = 0$

Since $\oplus$ returns 0 only when there is an even number of 1 values in x such that every pair of 1 values would be cancelled out.

$\therefore x_1 + \ldots + x_n$ must also be an even number

$\Rightarrow (-1)^{(x_1+\ldots+x_n)} = 1$

$\because (-1)^x = (-1)^{(x_1+\ldots+x_n)}$ $\therefore (-1)^x = 1$ $\therefore (-1)^x = 1$ if $XOR(x) = 0$

②

Prove that $XOR(x) = 0$ if $(-1)^x = 1$.

Assume $(-1)^x = 1$ $\therefore (-1)^{(x_1+\ldots+x_n)} = 1$.

$\therefore x_1 + \ldots + x_n$ must be an even number

$\therefore$ There is an even number of 1 values in x

In XOR, even number of 1 values would be cancelled out, and there are only number of 0 values left.

$\therefore XOR(x) = 0$

$\therefore XOR(x) = 0$ if $(-1)^x = 1$

$\therefore (-1)^x = 1$ if and only if $XOR(x) = 0$.

Question 3:

Question 3. For a function $f : \{0,1\}^n \to \{0,1\}$, we say that f is *constant* if either f always outputs 0 or f always outputs 1.

Prove that f is constant if and only if $f(0) \oplus f(1) = 0$.

① Prove that $f(0) \oplus f(1) = 0$ if f is constant.

Assume f is constant, then f always outputs the same value (either always 0 or always 1).

$\therefore f(x) = f(0) = f(1)$.

Since $\oplus$ returns 0 if the values of two functions are the same, $\therefore f(0) \oplus f(1) = 0$.

$\therefore f(0) \oplus f(1) = 0$ if f is constant.

② Prove that f is constant if $f(0) \oplus f(1) = 0$.

$f(0) \oplus f(1) = 0$.

Since $\oplus$ returns 0 only when both of the functions return the same value, $\therefore f(0) = f(1)$

$\because f : \{0,1\}^n \to \{0,1\}$, $f(0) = f(1)$

$\therefore$ Either both of $f(0)$ and $f(1)$ return 0

or both of $f(0)$ and $f(1)$ return 1

$\therefore$ Either f always outputs 0 or f always outputs 1

$\therefore f$ is constant if $f(0) \oplus f(1) = 0$

$\therefore f$ is constant if and only if $f(0) \oplus f(1) = 0$