Given a Boolean function $f(x) = w.x$, classical algorithm to find w.

Let f be an linear n-variable Boolean function, available in the form of an oracle. That is, for an n-bit binary input string x, the function f outputs $w.x$, where w is another n-bit binary string. More precisely —

$$w = (w_1, w_2, \dots, w_n), \quad x = (x_1, x_2, \dots, x_n)$$

$$\Rightarrow f(x) = w.x = \sum_{i=1}^{n} w_i x_i := \langle w, x \rangle \text{ inner product}$$

Classical algorithm to solve this problem of w from

~~Let us define the vectors~~

$$\cancel{x^k = (x_1^k, x_2^k, \dots, x_n^k), \text{ where, } x_j^k = \begin{cases} 1 & \text{if } k=j \\ 0 & \text{if } k \neq j \end{cases}}$$

~~and~~ ~~for all $j = 1, 2, \dots, n$~~ for $1 \leq k \leq n$.

~~Now, $f(x^k) = w.x^k$~~

Let us define the vectors —

$$e_k = (0, \dots, \underset{k\text{th position}}{1}, \dots 0)$$

Now, $f(e_k) = w.e_k = \langle w, e_k \rangle$ —

$$= \sum_{i=1}^{n} w_i e_{ki} = w_k.$$

and we can find all, $w_1, \dots, w_n$ in $O(n)$ query of the oracle access.

This problem can be solved in constant time using Deutsch-Jozsa algorithm.

We know that, for an n-bit Boolean function $f(x)$, the walsh transform of $f(x)$ at any point $a \in \{0,1\}^n$ is defined as—

$$W_f(a) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus a.x}, \text{ where}$$

$a.x$ denotes the dot product $a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n$

here $f(x) = \omega.x$

Then, $$W_f(a) = \sum_{x \in \{0,1\}^n} (-1)^{\omega.x \oplus a.x}$$

$$= \sum_{x \in \{0,1\}^n} (-1)^{(\omega \oplus a).x}$$

So, $\omega_f(\omega) = 2^n$ for $\omega \neq 0$

& $\omega_f(a) = 0$ for all $a \neq \omega$.

as, then $(\omega \oplus a).x$ is a balance function so, equal no of 1 & -1.

And, also, in Deutsch-Jozsa algorithm the observed state of n bits after Deutsch-Jozsa algorithm will output ω, with probability—

$$\frac{1}{2^{2n}}\left[\sum_x (-1)^{f(x) \oplus x.\omega}\right]^2 = \left(\frac{\omega_f(\omega)}{2^n}\right)^2$$

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

So, Deutsch-Josa algorithm solves this problem in constant time,