

We can now use the superposition principle. If we choose $1/\sqrt{2}(|0\rangle + |1\rangle)$ for the most significant qubit, then we obtain the result $1/\sqrt{2}(v_0 + v_1)$ since the black box B is linear. To put this in a different way, we get

$$B \left(\frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) \right) = \frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle).$$

The goal was to discriminate between functions, which satisfy $f(0) \oplus f(1) = 0$, and functions satisfying $f(0) \oplus f(1) = 1$. The previous state is equivalent to

$$\begin{cases} \pm \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) & \text{if } f(0) \oplus f(1) = 0, \\ \pm \frac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) & \text{if } f(0) \oplus f(1) = 1. \end{cases}$$