# Bernstein Vazirani Algorithm

Cody M. Grant

(Dated: February 11, 2022)

## I. PROBLEM

This is an extension to the Deutsch-Jozsa alg (DJ alg). Assuming a black box function, $f$, which takes an input of a string of bits, it returns either 0 or 1:

$$f(x_0, x_1, x_2) = 0 \text{ or } 1, \text{ where } x_n \text{ is } 0 \text{ or } 1 \tag{1}$$

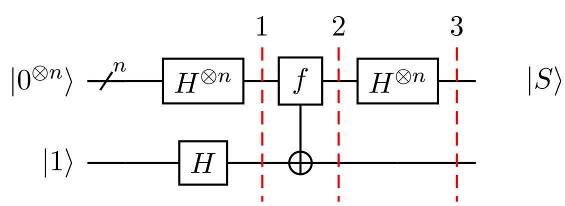
However, instead of the function as balanced or constant, the function now guarantees to return a bitwise product of the input with some string, $s$:

$$f(x) = s \cdot x (\text{mod } 2) \tag{2}$$

We are expected to find $s$.

## II. GENERIC QUANTUM SOLUTION

Similarly to the DJ alg, we have the circuit:




First, we apply the Hadamard gate to all initial qubits

$$|\psi_1\rangle = (H \otimes H)(|1\rangle \otimes \left|0^{\otimes n}\right\rangle) = \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \tag{3}$$

For the classical case, the oracle $f_s$ returns 1 for any input $x$ such that $s \cdot x$ mod $2 = 1$, and zero otherwise. Using the same phase kickback trick we did in the DJ alg and acting on the last qubit in the $|-\rangle$, we would have

$$|x\rangle \underset{f)s}{\longrightarrow} (-1)^{s \cdot x} |x\rangle \tag{4}$$

Similarly, quantum oracle would be

$$|\psi_2\rangle = \frac{|-\rangle}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{s \cdot x} |x\rangle \tag{5}$$

Like in the DJ alg, the last qubit in the $|-\rangle$ is only there to give us this extra factor of $(-1)^{s \cdot x}$. After applying this factor, a Hadamard gate to all but the last qubit, we can find the string, $s$, that was applied as it will be our final string (ignoring the last qubit). First I would like to note that

$$H^{\otimes n}\sqrt{2^n}\sum_{x=0}^{2^n-1}(-1)^{s\cdot x}\left|x\right\rangle = \frac{\left|-\right\rangle}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{s\cdot x}\left|x\right\rangle = \left|s\right\rangle \tag{6}$$

Therefore, applying the last $H$ gate means:

$$\left|\psi_3\right\rangle = (I\left|-\right\rangle)\otimes\left(H\left[\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{s\cdot x}\left|x\right\rangle\right]\right) = \left|-\right\rangle\otimes\left|S\right\rangle \tag{7}$$