Bernstein-Vazirani Algo

- Extension to DJ Algo. Mathematical Expressions + Ckt Design similar, however, as DJ → BV

DJ: $f(x)$ → Constant, Balanced

BV: $f(x)$ → Linear Function

Input: $\{0,1\}^n \rightarrow \{0,1\}^n$

Desired: $\exists\, \underline{a} = a_{n-1} \cdots a_1 a_0$ for which

$f(x) = \underline{a} \cdot \underline{x}, \quad \forall x \in \{0,1\}^n$

Output: $\underline{a}$ $(a_{n-1} \cdots a_1 a_0)$ $(x_{n-1} \cdots x_1 x_0)$

Ex $f(x) = (\underline{a} \cdot \underline{x}) \bmod 2$

$\underline{a}$: hidden/unknown binary string; $\underline{x}$: given parameter to probe

$a = 101$ ✓

$f(x)$ = Dot product of x with a mod 2

To determine 101,

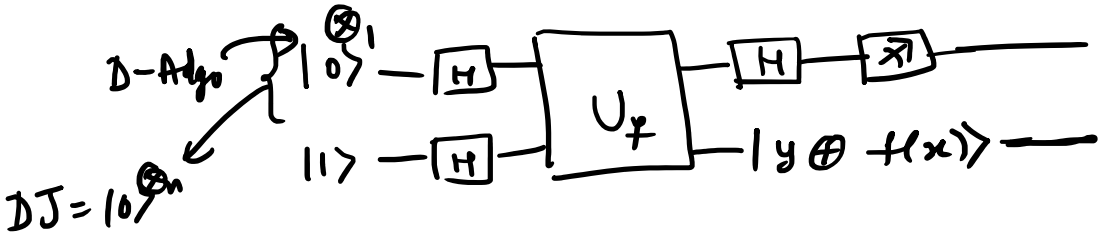
① $f(\overset{x}{001}) = 1\cdot 0 + 0\cdot 0 + 1\cdot 1 = 1 \bmod 2 = 1$

② $f(010) = 0$

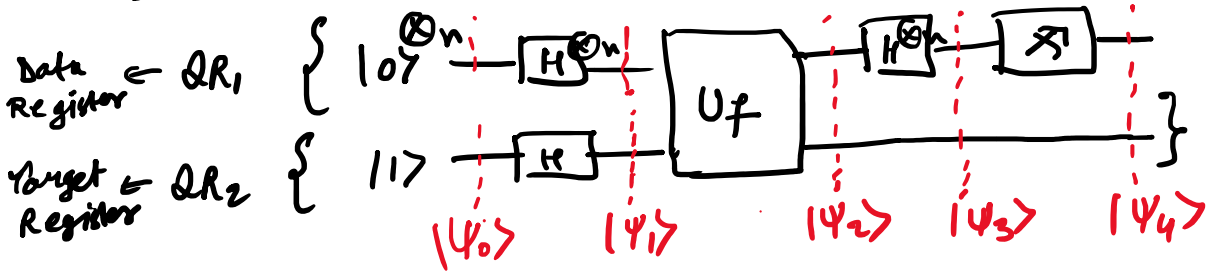
③ $f(100) = 1$

Objective: Proposed to find hidden bit string $\underline{a}$ from the function that takes binary input $\underline{x}$ and return dot product (mod 2) of the input with hidden string.

$$f(x) = \underline{a} \cdot \underline{x} = a_{n-1} x_{n-1} \oplus \cdots \oplus a_1 x_1 \oplus a_0 x_0$$



BV Circuit



$$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$$

$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$

$|\psi_1\rangle = (H^{\otimes n} \otimes H)(|\psi_0\rangle)$

$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |-\rangle \cong \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$|\psi_2\rangle =$ Apply U_f to all qubits $(U_f(|\psi_1\rangle))$

$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{a \cdot x} |x\rangle \otimes |-\rangle$

$|\psi_3\rangle =$ Apply $H^{\otimes n}$ on QR1 and $I^{\otimes 1}$ on QR2

$= \frac{1}{2^n} \sum_{z \in \{0,1\}^n} \left(\sum_{x \in \{0,1\}^n} (-1)^{a \cdot x \oplus x \cdot z} \right) |z\rangle \otimes |-\rangle$

$f(z)$

$|\psi_4\rangle =$ Apply measurement on QR1 in computational basis.

$\Rightarrow f(z) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{a \cdot x \oplus x \cdot z} |z\rangle$

$\Rightarrow$ Based on z-value, we have two possibility

$z = a$

$f(a) = \sum_{x=0}^{2^n-1} (-1)^{a \cdot x \oplus x \cdot a}$

$= \sum_{x=0}^{2^n-1} 1 = 2^n$

then $\frac{f(a)}{2^n} = \frac{2^n}{2^n} = 1$

$z \neq a$ $(a = 01 \quad z = 00)$

there will be some no. x such that

$a \cdot x = 0$

$a \cdot x = 1$ in summation.

Prob. Amplitude Vanishes

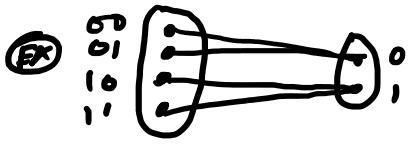
Simon's Algorithm

- Given unknown function $f: \{0,1\}^n \to \{0,1\}^n$ that can be –

  (i) One to One (Exactly one unique output for each input)

(Ex) 

(ii) Two to One (Maps two inputs to every unique output)
↳ Algo output = hidden Bitstring. (S)

(Ex) 

∴ Defining problem statement.

Input = $f: \{0,1\}^n \to \{0,1\}^n$

Promise = $\exists_{s \in \{0,1\}^n}$ such that $[f(x) = f(y)] \Leftrightarrow [(x=y) \oplus (x \oplus s = y)]$ $\forall_{x,y \in \{0,1\}^n}$

Output = hidden string s

(Ex) for x, y : $f(x) = f(y) \rightarrow$ if $(x = y)$ as it guarantees $x \oplus y = s$ (or) $y = x \oplus s$

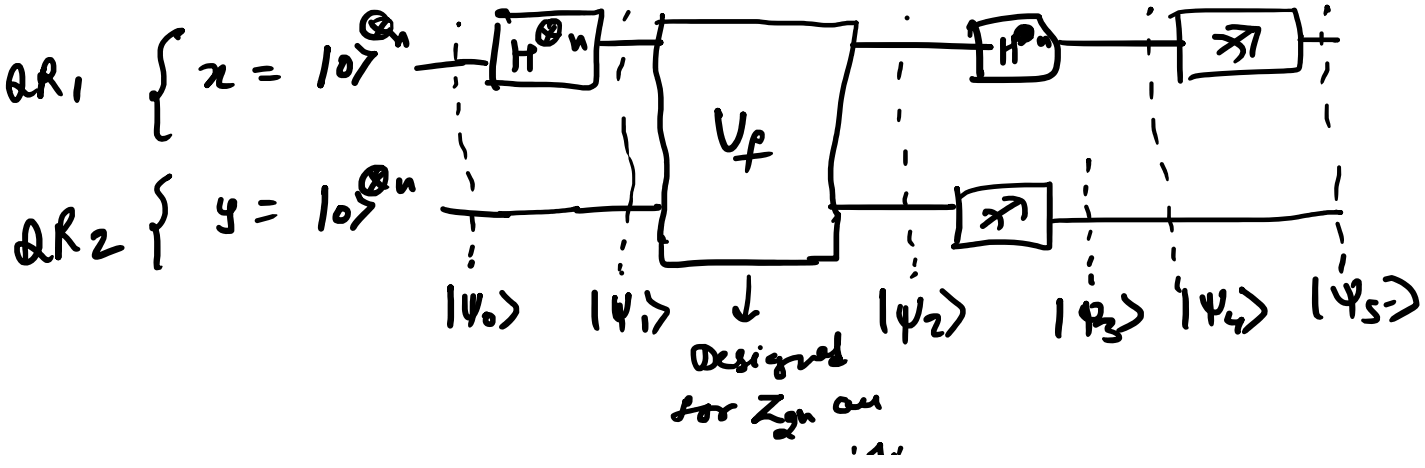
in any case if $s = \{0\}^n$ then the function is 1-1.

- Classically it takes $2^{n/2}$ queries using oracle. However, simon's quantum algo solved this problem in $O(n)$ queries
- Simon's achieved exponential speed up over classical algorithm.
- Applications — Period of function (Shor's also does same)
  — Finding Hidden Bit string
- Simon Oracle implements $U_f |x\rangle|y\rangle = |x, y \oplus f(x)\rangle$

if $y = 0$ then

$U_f |x\rangle|0\rangle = |x, f(x)\rangle$

The quantum circuit for simon's algorithm —



for Z_{2^n} an
integer periodic
function

NOTE: Quantum circuit is somehow similar to BV-Algo Circuit, so the mathematical operations can be trivially understood here. Only change is $|\psi_3\rangle$ i.e measurement of QR_2. prior to $|\psi_4\rangle$. Please find the implementation code during hackathon to understand the concept.