Quantum Computation - Lecture 03 - Simple Protocols

Mateus de Oliveira Oliveira

TCS-KTH

November 19, 2012

1. Superpositions and other tricks:
2. Deutsch Problem
3. Bernstein Vazirani Problem

Garbage Elimination

- In the problem set: For any Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$ there is a quantum circuit U_f that sends $|x\rangle|0\rangle$ to $|x\rangle|f(x)\rangle$.

Superposition 1 qubit:

- Let $f : \{0, 1\} \rightarrow \{0, 1\}$

Superposition 1 qubit:

- Let $f : \{0, 1\} \to \{0, 1\}$
- Start with $|0\rangle|0\rangle$

Superposition 1 qubit:

- Let $f : \{0, 1\} \to \{0, 1\}$
- Start with $|0\rangle|0\rangle$
- Apply H to the first qubit: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$

Superposition 1 qubit:

- Let $f : \{0,1\} \to \{0,1\}$
- Start with $|0\rangle|0\rangle$
- Apply H to the first qubit: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$
- Apply U_f: $\frac{1}{\sqrt{2}}|0\rangle|f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|f(1)\rangle$

Superposition 2 qubits:

- Let $f : \{0,1\}^2 \to \{0,1\}$

Superposition 2 qubits:

- Let $f : \{0,1\}^2 \to \{0,1\}$
- Start with $|00\rangle|0\rangle$

Superposition 2 qubits:

- Let $f : \{0,1\}^2 \rightarrow \{0,1\}$
- Start with $|00\rangle|0\rangle$
- Apply $H^{\otimes 2}$ to the first two qubits: $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)|0\rangle$

Superposition 2 qubits:

- Let $f : \{0,1\}^2 \to \{0,1\}$
- Start with $|00\rangle|0\rangle$
- Apply $H^{\otimes 2}$ to the first two qubits: $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)|0\rangle$
- Apply U_f: $\frac{1}{2}|00\rangle|f(00)\rangle + \frac{1}{2}|01\rangle|f(01)\rangle + \frac{1}{2}|01\rangle|f(01)\rangle$

Superposition n qubits:

- Let $f : \{0,1\}^n \rightarrow \{0,1\}$

Superposition n qubits:

- Let $f : \{0,1\}^n \rightarrow \{0,1\}$
- Start with $|0\rangle_n|0\rangle$

Superposition n qubits:

- Let $f : \{0,1\}^n \rightarrow \{0,1\}$
- Start with $|0\rangle_n|0\rangle$
- Apply $H^{\otimes n}$ to the first n qubits: $\frac{1}{\sqrt{2^n}}(\sum_{x=0}^{2^n-1} |x\rangle_n)|0\rangle$

Superposition n qubits:

- Let $f : \{0,1\}^n \rightarrow \{0,1\}$
- Start with $|0\rangle_n|0\rangle$
- Apply $H^{\otimes n}$ to the first n qubits: $\frac{1}{\sqrt{2^n}}(\sum_{x=0}^{2^n-1}|x\rangle_n)|0\rangle$
- Apply U_f: $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle_n|f(x)\rangle$

Superposition: First register nonzero

- Let $f : \{0,1\}^n \rightarrow \{0,1\}$

Superposition: First register nonzero

- Let $f : \{0,1\}^n \to \{0,1\}$
- Start with $|y\rangle_n|0\rangle$

Superposition: First register nonzero

- Let $f : \{0,1\}^n \to \{0,1\}$
- Start with $|y\rangle_n|0\rangle$
- Apply $H^{\otimes n}$ to the first n qubits: $\frac{1}{\sqrt{2^n}}(\sum_{x=0}^{2^n-1}(-1)^{x\cdot y}|x\rangle_n)|0\rangle$

Superposition: First register nonzero

- Let $f : \{0,1\}^n \rightarrow \{0,1\}$
- Start with $|y\rangle_n|0\rangle$
- Apply $H^{\otimes n}$ to the first n qubits: $\frac{1}{\sqrt{2^n}}(\sum_{x=0}^{2^n-1}(-1)^{x \cdot y}|x\rangle_n)|0\rangle$
- Apply U_f: $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{x \cdot y}|x\rangle_n|f(x)\rangle$

Superposition: Both registers nonzero and the function is to $\{0,1\}^m$

- Let $f : \{0,1\}^n \rightarrow \{0,1\}^m$

Superposition: Both registers nonzero and the function is to $\{0,1\}^m$

- Let $f : \{0,1\}^n \to \{0,1\}^m$
- Start with $|y\rangle_n|z\rangle_m$

Superposition: Both registers nonzero and the function is to $\{0,1\}^m$

- Let $f : \{0,1\}^n \rightarrow \{0,1\}^m$
- Start with $|y\rangle_n |z\rangle_m$
- Apply $H^{\otimes n}$ to the first n qubits: $\frac{1}{\sqrt{2^n}}(\sum_{x=0}^{2^n-1}(-1)^{x \cdot y}|x\rangle_n)|z\rangle$

Superposition: Both registers nonzero and the function is to $\{0,1\}^m$

- Let $f : \{0,1\}^n \rightarrow \{0,1\}^m$
- Start with $|y\rangle_n |z\rangle_m$
- Apply $H^{\otimes n}$ to the first n qubits: $\frac{1}{\sqrt{2^n}}(\sum_{x=0}^{2^n-1}(-1)^{x \cdot y}|x\rangle_n)|z\rangle$
- Apply U_f: $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{x \cdot y}|x\rangle_n|f(x) \oplus_m z\rangle$

- Given a function $f : \{0, 1\} \rightarrow \{0, 1\}$ implemented as a black box, determine whether $f(0) = f(1)$ (Constant) or whether $f(0) \neq f(1)$ (Balanced).

- Given a function $f : \{0,1\} \to \{0,1\}$ implemented as a black box, determine whether $f(0) = f(1)$ (Constant) or whether $f(0) \neq f(1)$ (Balanced).
- Start with $|0\rangle|0\rangle$

- Given a function $f : \{0,1\} \rightarrow \{0,1\}$ implemented as a black box, determine whether $f(0) = f(1)$ (Constant) or whether $f(0) \neq f(1)$ (Balanced).
- Start with $|0\rangle|0\rangle$
- Apply X to each qubit: $|1\rangle|1\rangle$

- Given a function $f : \{0,1\} \rightarrow \{0,1\}$ implemented as a black box, determine whether $f(0) = f(1)$ (Constant) or whether $f(0) \neq f(1)$ (Balanced).
- Start with $|0\rangle|0\rangle$
- Apply X to each qubit: $|1\rangle|1\rangle$
- Apply $H \otimes H$:
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$

- Given a function $f : \{0,1\} \to \{0,1\}$ implemented as a black box, determine whether $f(0) = f(1)$ (Constant) or whether $f(0) \neq f(1)$ (Balanced).
- Start with $|0\rangle|0\rangle$
- Apply X to each qubit: $|1\rangle|1\rangle$
- Apply $H \otimes H$:
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$
  - $\frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle)$

- Given a function $f : \{0,1\} \to \{0,1\}$ implemented as a black box, determine whether $f(0) = f(1)$ (Constant) or whether $f(0) \neq f(1)$ (Balanced).
- Start with $|0\rangle|0\rangle$
- Apply X to each qubit: $|1\rangle|1\rangle$
- Apply $H \otimes H$:
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$
  - $\frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle)$

- Given a function $f : \{0,1\} \to \{0,1\}$ implemented as a black box, determine whether $f(0) = f(1)$ (Constant) or whether $f(0) \neq f(1)$ (Balanced).
- Start with $|0\rangle|0\rangle$
- Apply X to each qubit: $|1\rangle|1\rangle$
- Apply $H \otimes H$:
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$
  - $\frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle)$
- Apply U_f:

- Given a function $f : \{0,1\} \to \{0,1\}$ implemented as a black box, determine whether $f(0) = f(1)$ (Constant) or whether $f(0) \neq f(1)$ (Balanced).
- Start with $|0\rangle|0\rangle$
- Apply X to each qubit: $|1\rangle|1\rangle$
- Apply $H \otimes H$:
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$
  - $\frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle)$
- Apply U_f:
  - $\frac{1}{2}(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle - |1\rangle|0 \oplus f(1)\rangle + |1\rangle|1 \oplus f(1)\rangle)$

- Given a function $f : \{0,1\} \to \{0,1\}$ implemented as a black box, determine whether $f(0) = f(1)$ (Constant) or whether $f(0) \neq f(1)$ (Balanced).
- Start with $|0\rangle|0\rangle$
- Apply X to each qubit: $|1\rangle|1\rangle$
- Apply $H \otimes H$:
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$
  - $\frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle)$
- Apply U_f:
  - $\frac{1}{2}(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle - |1\rangle|0 \oplus f(1)\rangle + |1\rangle|1 \oplus f(1)\rangle)$
  - But $1 \oplus f(0) = \overline{f(0)}$ and $1 \oplus f(1) = \overline{f(1)}$

- Given a function $f : \{0,1\} \rightarrow \{0,1\}$ implemented as a black box, determine whether $f(0) = f(1)$ (Constant) or whether $f(0) \neq f(1)$ (Balanced).
- Start with $|0\rangle|0\rangle$
- Apply X to each qubit: $|1\rangle|1\rangle$
- Apply $H \otimes H$:
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$
  - $\frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle)$
- Apply U_f:
  - $\frac{1}{2}(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle - |1\rangle|0 \oplus f(1)\rangle + |1\rangle|1 \oplus f(1)\rangle)$
  - But $1 \oplus f(0) = \overline{f(0)}$ and $1 \oplus f(1) = \overline{f(1)}$
  - $\frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|\overline{f(0)}\rangle - |1\rangle|f(1)\rangle + |1\rangle|\overline{f(1)}\rangle)$

- Given a function $f : \{0,1\} \to \{0,1\}$ implemented as a black box, determine whether $f(0) = f(1)$ (Constant) or whether $f(0) \neq f(1)$ (Balanced).
- Start with $|0\rangle|0\rangle$
- Apply X to each qubit: $|1\rangle|1\rangle$
- Apply $H \otimes H$:
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$
  - $\frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle)$
- Apply U_f:
  - $\frac{1}{2}(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle - |1\rangle|0 \oplus f(1)\rangle + |1\rangle|1 \oplus f(1)\rangle)$
  - But $1 \oplus f(0) = \overline{f(0)}$ and $1 \oplus f(1) = \overline{f(1)}$
  - $\frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|\overline{f(0)}\rangle - |1\rangle|f(1)\rangle + |1\rangle|\overline{f(1)}\rangle)$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle))$

$$\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle))$$

- f is constant: $f(1) = f(0)$

$$\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle))$$

- f is constant: $f(1) = f(0)$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$

$$\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle))$$

- f is constant: $f(1) = f(0)$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle)$

$$\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle))$$

- f is constant: $f(1) = f(0)$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle)$
- f is balanced: $f(0) \neq f(1) \Rightarrow \overline{f(1)} = f(0)$ and $f(1) = \overline{f(0)}$:

$$\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle))$$

- f is constant: $f(1) = f(0)$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle)$
- f is balanced: $f(0) \neq f(1) \Rightarrow \overline{f(1)} = f(0)$ and $f(1) = \overline{f(0)}$:
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|\overline{f(0)}\rangle - |f(0)\rangle)) =$

$$\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle))$$

- f is constant: $f(1) = f(0)$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle)$
- f is balanced: $f(0) \neq f(1) \Rightarrow \overline{f(1)} = f(0)$ and $f(1) = \overline{f(0)}$:
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(\overline{|f(0)\rangle} - |f(0)\rangle)) =$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) + |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$

$$\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle))$$

- f is constant: $f(1) = f(0)$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle)$
- f is balanced: $f(0) \neq f(1) \Rightarrow \overline{f(1)} = f(0)$ and $f(1) = \overline{f(0)}$:
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(\overline{|f(0)\rangle} - |f(0)\rangle)) =$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) + |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$
  - $\frac{1}{2}(|0\rangle + |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle)$

$$\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle))$$

- f is constant: $f(1) = f(0)$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle)$
- f is balanced: $f(0) \neq f(1) \Rightarrow \overline{f(1)} = f(0)$ and $f(1) = \overline{f(0)}$:
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|\overline{f(0)}\rangle - |f(0)\rangle)) =$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) + |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$
  - $\frac{1}{2}(|0\rangle + |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle)$
- Apply H to the first qubit:

$$\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle))$$

- f is constant: $f(1) = f(0)$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle)$
- f is balanced: $f(0) \neq f(1) \Rightarrow \overline{f(1)} = f(0)$ and $f(1) = \overline{f(0)}$:
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|\overline{f(0)}\rangle - |f(0)\rangle)) =$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) + |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$
  - $\frac{1}{2}(|0\rangle + |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle)$
- Apply H to the first qubit:
  - Constant: $\frac{1}{\sqrt{2}}|1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)$

$$\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle))$$

- f is constant: $f(1) = f(0)$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$
  - $\frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle)$
- f is balanced: $f(0) \neq f(1) \Rightarrow \overline{f(1)} = f(0)$ and $f(1) = \overline{f(0)}$:
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) - |1\rangle(|\overline{f(0)}\rangle - |f(0)\rangle)) =$
  - $\frac{1}{2}(|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) + |1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)) =$
  - $\frac{1}{2}(|0\rangle + |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle)$
- Apply H to the first qubit:
  - Constant: $\frac{1}{\sqrt{2}}|1\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)$
  - Balanced: $\frac{1}{\sqrt{2}}|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle)$

$$(H \otimes \mathbb{1})U_f(H \otimes H)(X \otimes X)(|0\rangle|0\rangle)$$

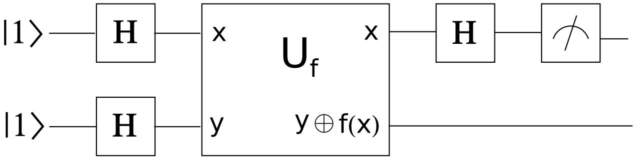

Figure: Deutsch's problem

Hadamard one more time: More concise notation

- $H|x\rangle_1 = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{xy}|y\rangle$

Hadamard one more time: More concise notation

- $H|x\rangle_1 = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{xy}|y\rangle$
- $(H \otimes H)|x_1\rangle|x_0\rangle = H|x_1\rangle \otimes H|x_0\rangle =$

Hadamard one more time: More concise notation

- $H|x\rangle_1 = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{xy}|y\rangle$
- $(H \otimes H)|x_1\rangle|x_0\rangle = H|x_1\rangle \otimes H|x_0\rangle =$
  - $\left(\frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}(-1)^{x_1 y_1}|y_1\rangle\right)\left(\frac{1}{\sqrt{2}}\sum_{y_0=0}^{1}(-1)^{x_0 y_0}|y_0\rangle\right) =$

Hadamard one more time: More concise notation

- $H|x\rangle_1 = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{xy}|y\rangle$
- $(H \otimes H)|x_1\rangle|x_0\rangle = H|x_1\rangle \otimes H|x_0\rangle =$
  - $\left(\frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}(-1)^{x_1 y_1}|y_1\rangle\right)\left(\frac{1}{\sqrt{2}}\sum_{y_0=0}^{1}(-1)^{x_0 y_0}|y_0\rangle\right) =$
  - $\frac{1}{2}((-1)^{x_1\cdot 0+x_0\cdot 0}|00\rangle + (-1)^{x_1\cdot 0+x_0\cdot 1}|01\rangle + (-1)^{x_1\cdot 1+x_0\cdot 0}|10\rangle + (-1)^{x_1\cdot 1+x_0\cdot 1}|11\rangle) =$

Hadamard one more time: More concise notation

- $H|x\rangle_1 = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{xy}|y\rangle$
- $(H \otimes H)|x_1\rangle|x_0\rangle = H|x_1\rangle \otimes H|x_0\rangle =$
  - $\left(\frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}(-1)^{x_1 y_1}|y_1\rangle\right)\left(\frac{1}{\sqrt{2}}\sum_{y_0=0}^{1}(-1)^{x_0 y_0}|y_0\rangle\right) =$
  - $\frac{1}{2}((-1)^{x_1\cdot 0+x_0\cdot 0}|00\rangle + (-1)^{x_1\cdot 0+x_0\cdot 1}|01\rangle + (-1)^{x_1\cdot 1+x_0\cdot 0}|10\rangle + (-1)^{x_1\cdot 1+x_0\cdot 1}|11\rangle) =$
- $H^{\otimes n}|x\rangle_n =$

Hadamard one more time: More concise notation

- $H|x\rangle_1 = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{xy}|y\rangle$
- $(H \otimes H)|x_1\rangle|x_0\rangle = H|x_1\rangle \otimes H|x_0\rangle =$
  - $\left(\frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}(-1)^{x_1 y_1}|y_1\rangle\right)\left(\frac{1}{\sqrt{2}}\sum_{y_0=0}^{1}(-1)^{x_0 y_0}|y_0\rangle\right) =$
  - $\frac{1}{2}((-1)^{x_1\cdot 0+x_0\cdot 0}|00\rangle + (-1)^{x_1\cdot 0+x_0\cdot 1}|01\rangle + (-1)^{x_1\cdot 1+x_0\cdot 0}|10\rangle + (-1)^{x_1\cdot 1+x_0\cdot 1}|11\rangle) =$
- $H^{\otimes n}|x\rangle_n =$
  - $\frac{1}{2^{n/2}}\sum_{y_{n-1}=0}^{1}\cdots\sum_{y_0=0}^{1}(-1)^{\sum_{j=0}^{n-1} x_j y_j}|y_{n-1}\rangle\cdots|y_0\rangle =$

Hadamard one more time: More concise notation

- $H|x\rangle_1 = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{xy}|y\rangle$
- $(H \otimes H)|x_1\rangle|x_0\rangle = H|x_1\rangle \otimes H|x_0\rangle =$
  - $\left(\frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}(-1)^{x_1y_1}|y_1\rangle\right)\left(\frac{1}{\sqrt{2}}\sum_{y_0=0}^{1}(-1)^{x_0y_0}|y_0\rangle\right) =$
  - $\frac{1}{2}((-1)^{x_1\cdot 0+x_0\cdot 0}|00\rangle + (-1)^{x_1\cdot 0+x_0\cdot 1}|01\rangle + (-1)^{x_1\cdot 1+x_0\cdot 0}|10\rangle + (-1)^{x_1\cdot 1+x_0\cdot 1}|11\rangle) =$
- $H^{\otimes n}|x\rangle_n =$
  - $\frac{1}{2^{n/2}}\sum_{y_{n-1}=0}^{1}\cdots\sum_{y_0=0}^{1}(-1)^{\sum_{j=0}^{n-1}x_jy_j}|y_{n-1}\rangle\cdots|y_0\rangle =$
  - $\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle_n$

Putting the Value of the Function Into the Phase.

- $U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =$

Putting the Value of the Function Into the Phase.

- $U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =$
- $\frac{1}{\sqrt{2}}|x\rangle|0 \oplus f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|1 \oplus f(x)\rangle$

Putting the Value of the Function Into the Phase.

- $U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =$
- $\frac{1}{\sqrt{2}}|x\rangle|0 \oplus f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|1 \oplus f(x)\rangle$
- $\frac{1}{\sqrt{2}}|x\rangle|f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|\overline{f(x)}\rangle$

Putting the Value of the Function Into the Phase.

- $U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =$
- $\frac{1}{\sqrt{2}}|x\rangle|0 \oplus f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|1 \oplus f(x)\rangle$
- $\frac{1}{\sqrt{2}}|x\rangle|f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|\overline{f(x)}\rangle$

Putting the Value of the Function Into the Phase.

- $U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =$
- $\frac{1}{\sqrt{2}}|x\rangle|0 \oplus f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|1 \oplus f(x)\rangle$
- $\frac{1}{\sqrt{2}}|x\rangle|f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|\overline{f(x)}\rangle$
-
  - $f(x) = 0$: $\frac{1}{\sqrt{2}}|x\rangle|0\rangle - \frac{1}{\sqrt{2}}|x\rangle|1\rangle$

Putting the Value of the Function Into the Phase.

- $U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =$
- $\frac{1}{\sqrt{2}}|x\rangle|0 \oplus f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|1 \oplus f(x)\rangle$
- $\frac{1}{\sqrt{2}}|x\rangle|f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|\overline{f(x)}\rangle$
-
  - $f(x) = 0$: $\frac{1}{\sqrt{2}}|x\rangle|0\rangle - \frac{1}{\sqrt{2}}|x\rangle|1\rangle$
    $f(x) = 1$: $\frac{1}{\sqrt{2}}|x\rangle|1\rangle - \frac{1}{\sqrt{2}}|x\rangle|0\rangle = (-1)|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Putting the Value of the Function Into the Phase.

- $U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =$
- $\frac{1}{\sqrt{2}}|x\rangle|0 \oplus f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|1 \oplus f(x)\rangle$
- $\frac{1}{\sqrt{2}}|x\rangle|f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|\overline{f(x)}\rangle$
-
  - $f(x) = 0$: $\frac{1}{\sqrt{2}}|x\rangle|0\rangle - \frac{1}{\sqrt{2}}|x\rangle|1\rangle$
    $f(x) = 1$: $\frac{1}{\sqrt{2}}|x\rangle|1\rangle - \frac{1}{\sqrt{2}}|x\rangle|0\rangle = (-1)|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Then $U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = (-1)^{f(x)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$f_a : \{0,1\}^n \rightarrow \{0,1\} \qquad f_a(x) = a \cdot x = a_0 x_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n$$

- Given $f : \{0,1\}^n \rightarrow \{0,1\}$ with the promise that there exists some a for which $f = f_a$. Find a.

- Start with $|0\rangle_n |1\rangle_1$

- Start with $|0\rangle_n|1\rangle_1$
- apply H to the second qubit: $|0\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

- Start with $|0\rangle_n|1\rangle_1$
- apply H to the second qubit: $|0\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- apply $H^{\otimes n}$ to the first register: $\left(\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

- Start with $|0\rangle_n|1\rangle_1$
- apply H to the second qubit: $|0\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- apply $H^{\otimes n}$ to the first register: $\left(\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- apply U_f (trick: put the value of $f(x)$ into the phase) :

$$\left(\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- Start with $|0\rangle_n |1\rangle_1$
- apply H to the second qubit: $|0\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- apply $H^{\otimes n}$ to the first register: $\left(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle\right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- apply U_f (trick: put the value of $f(x)$ into the phase) :

$$\left(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle\right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- apply $H^{\otimes n}$ to the first register: (obs: using linearity)

$$\left(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} H^{\otimes n} |x\rangle\right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- Start with $|0\rangle_n|1\rangle_1$
- apply H to the second qubit: $|0\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- apply $H^{\otimes n}$ to the first register: $\left(\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- apply U_f (trick: put the value of $f(x)$ into the phase) :

$$\left(\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- apply $H^{\otimes n}$ to the first register: (obs: using linearity)

$$\left(\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}H^{\otimes n}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- $$\left(\frac{1}{2^{n}}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{f(x)\oplus y\cdot x}|y\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- $$\left(\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{f(x)\oplus x\cdot y}|y\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- $$\left(\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{f(x)\oplus x\cdot y}|y\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$
- $$\left(\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{a\cdot x\oplus y\cdot x}|y\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

- $$\left(\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{f(x)\oplus x\cdot y}|y\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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

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

- $$\left(\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{f(x)\oplus x\cdot y}|y\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

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

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

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

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

- $$\sum_{x=0}^{2^n-1} (-1)^{(a \oplus_n y) \cdot x}$$
- $$\sum_{x=0}^{2^n-1} \prod_{j=0}^{n} (-1)^{(a_j \oplus y_j) \cdot x_j}$$

- $$\sum_{x=0}^{2^n-1} (-1)^{(a \oplus_n y) \cdot x}$$
- $$\sum_{x=0}^{2^n-1} \prod_{j=0}^{n} (-1)^{(a_j \oplus y_j) \cdot x_j}$$
- $$\prod_{j=0}^{n-1} \sum_{x_j=0}^{1} (-1)^{(a_j \oplus y_j) \cdot x_j} = \prod_{j=0}^{n-1} [1 + (-1)^{a_j \oplus y_j}]$$

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

- $$\sum_{x=0}^{2^n-1} \prod_{j=0}^{n} (-1)^{(a_j \oplus y_j)\cdot x_j}$$

- $$\prod_{j=0}^{n-1} \sum_{x_j=0}^{1} (-1)^{(a_j \oplus y_j)\cdot x_j} = \prod_{j=0}^{n-1} [1 + (-1)^{a_j \oplus y_j}]$$

-
  - $a = y \Rightarrow \forall j, a_j = y_j \Rightarrow 1 + (-1)^{a_j \oplus y_j} = 2 \Rightarrow Total = 2^n$
    $a \neq y \Rightarrow \exists j, a_j \neq y_j \Rightarrow 1 + (-1)^{a_j \oplus y_j} = 0 \Rightarrow Total = 0$

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

- $$\left(\frac{1}{2^n}\sum_{y=0}^{2^n-1}\left(\sum_{x=0}^{2^n-1}(-1)^{(a\oplus_n y)\cdot x}\right)|y\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$
- The expression in the internal bracket is 2^n if $y = a$ and 0 if $y \neq a$.

- $$\left(\frac{1}{2^n}\sum_{y=0}^{2^n-1}\left(\sum_{x=0}^{2^n-1}(-1)^{(a\oplus_n y)\cdot x}\right)|y\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
- The expression in the internal bracket is 2^n if $y = a$ and 0 if $y \neq a$.
- Thus the final state is $|a\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

- $$\left(\frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(\sum_{x=0}^{2^n-1} (-1)^{(a \oplus_n y) \cdot x} \right) |y\rangle \right) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$
- The expression in the internal bracket is 2^n if $y = a$ and 0 if $y \neq a$.
- Thus the final state is $|a\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$
- Finally, apply an aesthetical H to the second qubit: $|a\rangle|1\rangle$

Final circuit:

$$(H^{\otimes n} \otimes H)U_f(H^{\otimes n} \otimes H)|0\rangle_n|1\rangle_1$$

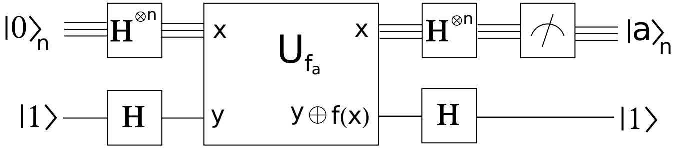

Figure: Bernstein-Vazirani