COM SCI M238 (Quantum Computing)

October 6, 2022

1 9.22 0th

- first quantum computer working in 2016
- rn = 127 qubits
- google projected to have 1mil qubits by 2029
- largest simulation of a quantum computer by a classical computer: nasa, 70 (perfect) qubits, half a year
  - only need 37 for practical uses
- 1% err rate
  - current err corrections reqs ~1000 qubits to support 1 perfect qubit
- moores law of quantum computing
  - err rate improves linearly per qubit
- quantum volume for the decade: 100 qubits * 1000 ops = 100k ops
  - need to push decoherence time
- good problem: small input, lots of calculation, small output, easily verifiable
- double slit experiment
  - numbers of photons that come thru when either slit is covered are not additive
  - complex α_1 and α_2 for probability for either, can be negative, amplitude leq 1
  - eg $\alpha_1 = 1/\sqrt{2}$ and $\alpha_2 = -1/\sqrt{2}$
  - probability = $|\alpha|^2 = 1/2$
  - probability when both are uncovered = $|\alpha_1 + \alpha_2|^2 = 0$
- borns rule: when measured, a state with amplitude α is observed with probability $|\alpha|^2$

2 9.27 1t

	classical	quantum
software	boolean algebra	linear algebra
hardware	classical mechanics	quantum mechanics

2.1 4 postulates that define the interface between us and the qubits

1. state space rule

- $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
- $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- $\left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right)$

2. composition rule

- tensor product

3. step rule

- unitary matrix
- $U|\psi\rangle = |\varphi\rangle$
- $|\psi\rangle$ and $|\varphi\rangle$ are unit vectors of size 2^n
- U is $2^n \times 2^n$ but can be programmed in polynomial amount of code

4. measurement rule

- bit $\xrightarrow{\text{load}}$ quantum $\xrightarrow{\text{compute}}$ quantum $\xrightarrow{\text{measure}}$ bit

2.2 from classical computing to probabilistic computing to quantum computing

- classical
  - step: $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
    * rows: from 00, 01, 10, 11
    * cols: to 00, 01, 10, 11
- probabilistic: model of the world with uncertainties
  - state is a vector, taking a step = multiply by probability matrix
  - step: $\begin{bmatrix} 0 & 0 & 0 & 1/4 \\ 1 & 2/3 & 1/3 & 1/4 \\ 0 & 1/3 & 1/3 & 1/4 \\ 0 & 0 & 1/3 & 1/4 \end{bmatrix}$
  - tensor product: $\begin{bmatrix} p \\ 1-p \end{bmatrix} \otimes \begin{bmatrix} q \\ 1-p \end{bmatrix} \to \begin{bmatrix} pq \\ p(1-q) \\ (1-p)q \\ (1-p)(1-q) \end{bmatrix}$
  - "not gate": $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} p \\ q \end{bmatrix} = \begin{bmatrix} q \\ p \end{bmatrix}$
  - fair flip: $\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \begin{bmatrix} p \\ q \end{bmatrix} = \begin{bmatrix} \frac{1}{2}(p+q) \\ \frac{1}{2}(p+q) \end{bmatrix} = \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}$
  - $\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}$ can never equal $\begin{bmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{bmatrix}$
    * $\frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2} = (ac)(bd) \neq (ad)(bc) = 0 \cdot 0 = 0$
- comparison between probabilistic and quantum

	probabilistic	quantum
value	real	complex
state	vector of probabilities	vector of amplitudes
	$\sum p_i = 1$	$\sum \lvert a\rvert^2 = 1$
step	stochastic matrix	unitary matrix

- quantum
  - fair flip: $H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
    * $H\,|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$
    * $H\,|1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$
    * distinguishing $\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$ and $\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix}$:
      · $H \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = |0\rangle$
      · $H \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = |1\rangle$
  - $f\colon \{0,1\} \to \{0,1\}$

2.3 encoding a function to be invertible

- encoding of f: $U_f\colon \{0,1\}^2 \to \{0,1\}^2$
  - $U_f(x,b) = (x, b \oplus f(x))$ invertible
  - $(U_f \circ U_f)(x,b) = U_f(U_f(x,b)) = U_f(x, b \oplus f(x)) = (x, b \oplus f(x) \oplus f(x)) = (x,b)$

3 9.29 1th

3.1 complex numbers

- $a + ib$
- $\overline{a + ib} = a - ib$
- $e^{i\theta} = \cos\theta + i\sin\theta$
- $\overline{e^{i\theta}} = \cos\theta - i\sin\theta = e^{-i\theta}$

3.2 hilbert space

- complex vector space w inner product
- $\left\langle \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix}, \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} \right\rangle = \overline{\alpha_1}\beta_1 + \overline{\alpha_2}\beta_2 = \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix}^* \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} = \begin{bmatrix} \overline{\alpha_1} & \overline{\alpha_2} \end{bmatrix} \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix}$
- write $\left|\psi\right\rangle = \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix}$ and $\left\langle\varphi\right| = \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix}$
- bra-ket notation: $\left\langle\psi\right| = \begin{bmatrix} \overline{\alpha_1} & \overline{\alpha_2} \end{bmatrix}$
- inner product: $\langle\psi|\varphi\rangle$
- $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

- $H|0\rangle = |+\rangle$
- $H|1\rangle = |-\rangle$
- $\langle 0|1\rangle = 1^* \cdot 0 + 0^* \cdot 1 = 0$
- $\langle +|-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{2}(1 \cdot 1 + 1 \cdot (-1)) = 0$
- outer product: $|\psi\rangle \langle\varphi| = \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} \begin{bmatrix} \overline{\beta_1} & \overline{\beta_2} \end{bmatrix} = \begin{bmatrix} \alpha_1\overline{\beta_1} & \alpha_1\overline{\beta_2} \\ \alpha_2\overline{\beta_1} & \alpha_2\overline{\beta_2} \end{bmatrix}$
- a matrix U is unitary iff $UU^* = I$ (equivalent to $U^*U = I$)

3.3 partial measurement

- start state: $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$
- measure qubit $1 \longrightarrow 0$
- new sate: $\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_0 0|^2 + |\alpha_0 1|^2}} = |0\rangle \otimes \frac{\alpha_{00}|0\rangle + \alpha_{01}|1\rangle}{\sqrt{|\alpha_0 0|^2 + |\alpha_0 1|^2}}$

3.4 generalization of tensor product

- outer product: $|\psi\rangle \langle\varphi| = \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} \otimes \begin{bmatrix} \overline{\beta_1} & \overline{\beta_2} \end{bmatrix} = \begin{bmatrix} \alpha_1\overline{\beta_1} & \alpha_1\overline{\beta_2} \\ \alpha_2\overline{\beta_1} & \alpha_2\overline{\beta_2} \end{bmatrix}$
- $\begin{bmatrix} \alpha_{00} & \alpha_{01} \\ \alpha_{10} & \alpha_{01} \end{bmatrix} \otimes B = \begin{bmatrix} \alpha_{00}B & \alpha_{01}B \\ \alpha_{10}B & \alpha_{01}B \end{bmatrix}$
- $|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$
- $\underbrace{|101\rangle}_{\text{5 in decimal}} = |1\rangle \otimes |0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$
- inner product $\rightsquigarrow$ matrix product
- outer product $\rightsquigarrow$ matrix product + tensor product
- $\otimes$ associative: $A \otimes (B + C) = A \otimes B + A \otimes C$
- $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$
- "floating scalar rule": $(\alpha A) \otimes B = A \otimes (\alpha B) = \alpha(A \otimes B)$
- $|\psi\rangle \cdot \langle\varphi| \cdot |\gamma\rangle = |\psi\rangle \cdot \langle\varphi|\gamma\rangle = \langle\varphi|\gamma\rangle \cdot |\psi\rangle$

4 10.4 2t

- todo: wire drawing

- $|0\rangle \otimes |0\rangle \otimes |0\rangle = |000\rangle$
- $(I \otimes CNOT)(I \otimes X \otimes I)(H \otimes I \otimes I)\underbrace{|000\rangle}_{\text{vector}}$
- it is more error-prone to do I than X or H
  - qiskit etc will put single operations that cancel out instead
- todo: drawing - cnot but ctrl qbit on top
- $(I \otimes S)(CNOT \otimes I)(I \otimes S)|000\rangle$
  - where S is swap
- bob creates $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends one of the qubits to alice
- alice has 2 bits ab
  - if $a = 1$, alice applies Z to A
    * $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
  - if $b = 1$, alice applies X to A
  - send A to bob
- bob
  - $CNOT(A, B)$
  - apply H to A
  - measure A, B

ab	alice 1	alice 2	bob 1	bob 2	bob measure
00	$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$	$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$	$|+0\rangle$	$|00\rangle$	00
01	$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$	$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$	$|+1\rangle$	$|01\rangle$	01
10	$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$	$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$	$|-0\rangle$	$|10\rangle$	10
11	$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$	$\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$	$-|-1\rangle$	-$|11\rangle$	11

4.1 quantum teleportation

- $|\underbrace{01}_{\text{Alice}}\underbrace{0}_{\text{Bob}}\rangle$, last 2 are a bell pair
- alice has $\alpha|0\rangle + \beta|1\rangle$
- start state: $(\alpha|0\rangle + \beta|1\rangle)_A \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{BC}$
- alice
  - todo: drawing
  - $CNOT(A, B)$
  - $H(A)$
  - measure
  - $\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle) \to \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)$
  - $\to \frac{1}{2}(\alpha|001\rangle + \alpha|101\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|000\rangle - \beta|100\rangle)$
  - $\to \frac{1}{2}(|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + |01\rangle \otimes (\beta|0\rangle + \alpha|1\rangle) + |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + |11\rangle \otimes (-\beta|0\rangle + \alpha|1\rangle))$
  - $\frac{1}{4}$ probability of sending any of the 4
  - $00 \to \alpha|0\rangle + \beta|1\rangle$

  - $01 \to \beta|0\rangle + \alpha|1\rangle$
  - $10 \to \alpha|0\rangle - \beta|1\rangle$
  - $11 \to -\beta|0\rangle + \alpha|1\rangle$
- bob
  - $b = 1 \Rightarrow X(C)$
    * $00 \to \alpha|0\rangle + \beta|1\rangle$
    * $01 \to \alpha|0\rangle + \beta|1\rangle$
    * $10 \to \alpha|0\rangle - \beta|1\rangle$
    * $11 \to \alpha|0\rangle - \beta|1\rangle$
  - $a = 1 \Rightarrow Z(C)$
    * $00 \to \alpha|0\rangle + \beta|1\rangle$
    * $01 \to \alpha|0\rangle + \beta|1\rangle$
    * $10 \to \alpha|0\rangle + \beta|1\rangle$
    * $11 \to \alpha|0\rangle + \beta|1\rangle$
- alice's qubit destroyed when measured

4.2 no cloning theorem

- no quantum operation maps $|\psi 0\rangle$ to $|\psi\psi\rangle$
- suppose $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$
- pick $|\psi_1\rangle, |\psi_2\rangle$ such that $\langle\psi_1|\psi_2\rangle \neq 0$ and $\langle\psi_1|\psi_2\rangle \neq 1$
- lemma: $\langle(v_1 \otimes v_2)|(w_1 \otimes w_2)\rangle = \langle v_1|w_1\rangle \cdot \langle v_2|w_2\rangle$
- $\langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle \cdot \langle 0|0\rangle = \langle\psi_1 0|\psi_2 0\rangle = \langle U(|\psi_1 0\rangle), U(|\psi_2 0\rangle)\rangle = \langle\psi_1\psi_1|\psi_2\psi_2\rangle = \langle\psi_1|\psi_2\rangle \cdot \langle\psi_1|\psi_2\rangle$

4.3 universality

- $NAND(x_1, x_2) = CCNOT(x_1, x_2, 1)$
  - $CCNOT$ can simulate all of boolean logic
- $\{CCNOT, H\}$ is universal for all real unitaries
- $\left\{CCNOT, H, S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}\right\}$ is universal for all unitaries
- quantum computers implement $\{CNOT, H, T\}$
  - $S = T^2$

5 10.6 2th

5.1 deutsch-jozsa problem

- input: a function $f\colon \{0,1\}^n \to \{0,1\}$
- assumption: either f is constant or f is balanced
- probabilistically, just guess balanced
- 2^n inputs, try one after another, know it's constant after $2^{n-1} + 1$ tries
- $n = 1$

- $f: \{0,1\} \to \{0,1\}$
- U_f : qubit$^{\otimes 2} \to$ qubit$^{\otimes 2}$
- make unitary
- $U_f(|x\rangle \otimes |b\rangle) = |x\rangle \otimes \left|b \oplus f(x)\right\rangle$

input	f_0	f_1	f_2	f_3
0	0	0	1	1
1	0	1	0	1

- $U_{f_0}(|0\rangle \otimes |b\rangle) = |0\rangle \otimes \left|b \oplus f(0)\right\rangle = |0b\rangle$
- $U_{f_0}(|1\rangle \otimes |b\rangle) = |1\rangle \otimes \left|b \oplus f(1)\right\rangle = |1b\rangle$
- U_{f_0} is the 4×4 identity matrix
- f is constant
  * $f(0) = 0 \wedge f(1) = 0 \vee f(0) = 1 \wedge f(1) = 1$
  * $f(0) \oplus f(1) = 0$
- f is balanced
  * $f(0) \oplus f(1) = 1$
- idea 1: use superposition of $|0\rangle, |1\rangle$
- observation: U_f moves $f(0), f(1)$ to the exponent so we can do addition
- idea 2: H will move $f(0) \oplus f(1)$ "back down"
- deutsch algorithm
- todo: drawing
- measure$_0$ $\left((H \otimes I)U_f(H \otimes H)|01\rangle\right) = \begin{cases} 0 & f \text{ constant} \\ 1 & f \text{ balanced} \end{cases}$
- lemma 1: $\forall a \in \{0,1\} : |0 \oplus a\rangle - |1 \oplus a\rangle = (-1)^a(|0\rangle - |1\rangle)$
- lemma 2: $\forall x \in \{0,1\}^n : U_f(|x-\rangle) = (-1)^{f(x)}|x-\rangle$
  * $U_f(|x-\rangle) = \frac{1}{\sqrt{2}}\left(U_f(|x0\rangle) - U_f(|x1\rangle)\right) = \frac{1}{\sqrt{2}}\left(|x\rangle \otimes \left|0 \oplus f(x)\right\rangle - |x\rangle \otimes \left|1 \oplus f(x)\right\rangle\right)$
  * $= |x\rangle \otimes \frac{1}{\sqrt{2}}\left(\left|0 \oplus f(x) - \left|1 \oplus f(x)\right\rangle\right\rangle\right) = |x\rangle \otimes \frac{1}{\sqrt{2}}(-1)^{f(x)}(|0\rangle - |1\rangle) = (-1)^{f(x)}|x-\rangle$
- lemma 3: $\forall a \in \{0,1\} : H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}(-1)^a|1\rangle\right) = |a\rangle$
- $(H \otimes I)U_f(H \otimes H)|01\rangle = (H \otimes I)U_f(|+-\rangle) = (H \otimes I)U_f\frac{1}{\sqrt{2}}((|0\rangle + |1\rangle) \otimes |-\rangle)$
- $= (H \otimes I)\frac{1}{\sqrt{2}}U_f\left(\sum_{x \in \{0,1\}}|x-\rangle\right) = (H \otimes I)\frac{1}{\sqrt{2}}\sum_{x \in \{0,1\}}(-1)^{f(x)}|x-\rangle$
- $= (H \otimes I)\frac{1}{\sqrt{2}}\left((-1)^f(0)|0\rangle + (-1)^{f(1)}|1\rangle\right) \otimes |-\rangle = (H \otimes I)\frac{1}{\sqrt{2}}(-1)^{f(0)}\left(|0\rangle + (-1)^{f(0) \oplus f(1)}|1\rangle\right) \otimes |-\rangle$
- $= (-1)^{f(0)}\left|f(0) \oplus f(1)\right\rangle \otimes |-\rangle$
- norm: $\left|(-1)^{f(0)}\right|^2 = 1$

5.2 deutsch-jozsa algorithm

- $n > 1$
- todo: drawing
- measure$_{0:n}$ $\left((H^{\otimes n} \otimes I)U_f H^{\otimes(n+1)}\left(|0\rangle^{\otimes n} \otimes |1\rangle\right)\right)$ gives an n-bit bitstring
- lemma 4 (todo: 5???): $\forall x \in \{0,1\} : H(|x\rangle) = \frac{1}{\sqrt{2}}\sum_{y \in \{0,1\}}(-1)^{xy}\left|y\right\rangle$
  - RHS $= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$, then see lemma 3

- lemma 5: $H^{\otimes n}(|x\rangle) = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle$
  - $H^{\otimes n}(|0\rangle) = H(|x_1\rangle) \otimes \cdots \otimes H(|x_n\rangle) = \frac{1}{\sqrt{2}} \sum_{y_1\in\{0,1\}} |y_1\rangle \otimes \cdots \otimes \frac{1}{\sqrt{2}} \sum_{y_n\in\{0,1\}} |y_n\rangle$
  - $= \frac{1}{\sqrt{2^n}} \sum_{y_1\in\{0,1\}} \cdots \sum_{y_n\in\{0,1\}} (-1)^{x_1 y_1} \cdots (-1)^{x_n y_n} |y_1 \dots y_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle$
- $(H^{\otimes n} \otimes I) U_f H^{\otimes(n+1)} \left(|0\rangle^{\otimes n} \otimes |1\rangle\right) = (H^{\otimes n} \otimes I) U_f \left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle\right) \otimes |-\rangle$
- $= (H^{\otimes n} \otimes I) \frac{1}{\sqrt{2^n}} \left(\sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle\right) \otimes |-\rangle$
- $= \frac{1}{\sqrt{2^n}} \left(\sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle\right) \otimes |-\rangle$
- $= \frac{1}{2^n} \left(\sum_x \sum_y (-1)^{f(x)\oplus x\cdot y} |y\rangle\right) \otimes |-\rangle$
- for $|y\rangle = |0\rangle^{\otimes n} |-\rangle$, only final state $= \frac{1}{2^n} \left(\sum_x (-1)^{f(x)} |0\rangle^{\otimes n}\right) \otimes |-\rangle$