[Quantum Algorithms] I [9/3]

Matt Klasen 425-895-4423

Introduction to Quantum Algorithms - Johannes Buchmann

1[What is quantum Computing?

Qbit: Complex Vector
↳ Major Consideration: reliability of qbits

Diff between Simulated & literal execution?

Current hardware → 100 qbits
ideal → 1000

11[Physical qbits
↳ Certain # of entangled physical qbits

u[Logical qbits
↳ primarily used for error correction

1[Algorithms
↳ Shor's, Grover's, ~~linear~~ linear system Solving

equivalent of Moore's law?

"Quantum Computing is multiplying very large Complex Matrices by very large Complex Vectors"

1[Complex Matrices
$\mathbb{R}$: ~~Real~~ Orthonormal
$\mathbb{C}$: Unitary

// Basis to simplify quantum operations

1[Deutsch Algorithm] - chapter 5
Classical Deutsch Problem:
given: $f:\{0,1\} \longrightarrow \{0,1\}$

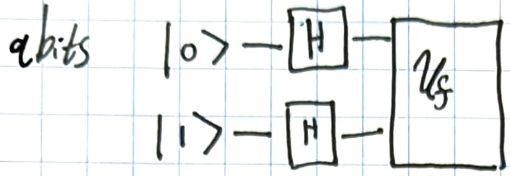
Impossible to know f w/o query f at least twice (to determine which $f_n == f$)

1[Quantum Version can determine f w/ a single query using a unitary matrix, U_f

Why unitary? Quantum Physics obeys "Unitary time evolution" which is based on the ~~pa~~ linear Partial diff Eq Schrodinger's equation. When discretized, becomes unitary

[Quantum Algs]$^{\text{II}}$

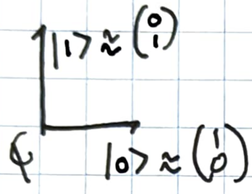
U_f embeded in a circuit (p. 207)



// unit vector basis

// unitary matrices use "adjoint", ie

$$A^* := \overline{A^T}$$ // Transposed conjugate



A is unitary iff $A^* = A^{-1}$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Complex Calculations

$$e^{i\theta} = \cos\theta + i\sin\theta$$

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i$$

$$e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$$

[Quantum Algs] II

[9/8]

[Deutsch's Algorithm] → The first Q. Alg. "mundane"

Given $f: \{0,1\} \to \{0,1\}$ determine if f is <u>constant</u> or <u>balanced</u>

// Ask for rephrase
Constant: input same as output

$f_1(0) = 0,\ f_1(1) = 0 \ \Big|\ f_2(0) = 1,\ f_2(1) = 1$ // constant

$f_3(0) = 0,\ f_3(1) = 1 \ \Big|\ f_4(0) = 1,\ f_4(1) = 0$

in classical, need to "query f" twice to determine // Clarify "query"

In Quantum, use unitary U_f & only query once // query in Q Comp, assume same calc

[Qubits] → Linear Combination of states from (0, 1)

Single Qubit space $\mathbb{H}_1 \cong \mathbb{C}^2 = \left\{ \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} : \alpha, \beta \in \mathbb{C} \right\}$

↳ isomorphic

$\mathbb{C}^2 \cong \mathbb{R}^4$ $\quad \alpha = a + bi,\ \beta = c + di$

/[$\mathbb{H}_1$ basis:

$\{ |0\rangle, |1\rangle \} \ \Big|\ \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$

$\mathbb{H}_1 = \{ \alpha |0\rangle + \beta |1\rangle : \alpha, \beta \in \mathbb{C} \}$

// $|\ \rangle$ "ket"
Pauli notation

Qubits change over time according to unitary transformations

$\alpha|0\rangle + \beta|1\rangle \xrightarrow{H} H(\alpha|0\rangle + \beta|1\rangle)$

$= \alpha H|0\rangle + \beta H|1\rangle$

// ΔH not really relevant. Number of repetitions ~~also~~ like O notation is more useful

α

$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ +1 \end{bmatrix}$

$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$

[Quantum Algs]$^{\text{IV.}}$

[Qubits] - Hadamar Gate

↳ Take 1 Qubit & spread across 2 into a superposition

$$H|0\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) := |X_+\rangle$$

$$H|1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) := |X_-\rangle$$

[Linear Algebra vs. Quantum Mechanics]

// once superposition established, must not observe / collapse

Linear Combination $\longleftrightarrow$ Superposition

Vector $\longleftrightarrow$ State

[2 Qubit Space

$\mathbb{H}_2 \cong \mathbb{H}_1 \otimes \mathbb{H}_1$ // Tensor Product

1[Tensor Product

if V, W are vector spaces with basis:

$\{\vec{V}_1 \dots \vec{V}_n\}$ & $\{\vec{W}_1 \dots \vec{W}_m\}$, then:

$V \otimes W$ is the vector space w/ basis

$$\{\vec{V}_1\vec{W}_1 \dots \vec{V}_n\vec{W}_m\} = \{\vec{V}_i \vec{W}_j\} \quad \begin{matrix} 1 \le i \le n \\ 1 \le j \le m \end{matrix}$$

$$\therefore \dim(V \otimes W) = m \cdot n$$

[Quantum Algs]^{V}

[9/8]

[2 Qubit Space]

$\mathbb{H}_2$ being: $\mathbb{H}_1 \otimes \mathbb{H}_1$

basis of $\{ |0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle \}$

or $\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$ // Computational basis

// convert from binary

or $\{ |0\rangle, |1\rangle, |2\rangle, |3\rangle \}$

$|X_+\rangle|X_-\rangle$ ie $|X_+\rangle \otimes |X_-\rangle$

$\left(\frac{1}{\sqrt{2}}\right)^2 \left(|00\rangle + |01\rangle - |01\rangle - |11\rangle \right)$ // set up calculations w/ "interference"

$\mathbb{H}_n$ basis $=$ $\mathbb{R}^{2^n}$

$U_g : \mathbb{H}_2 \to \mathbb{H}_2$

[9/10]

[Review]

$\mathbb{H}_1 \rightarrow$ Single qubit space w/ basis $\{|0\rangle, |1\rangle\}$

$\mathbb{H}_1 = \{ \alpha|0\rangle + \beta|1\rangle : \alpha, \beta \in \mathbb{C} \}$

$\mathbb{H}_1 \cong \mathbb{C}^2$ // 2D Complex Vector Space

[Hadamar Matrix, H

$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ $H(|0\rangle, -2|1\rangle) = H\begin{bmatrix} 1 \\ -2 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ -2 \end{bmatrix}$

$= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -3 \end{bmatrix} = \frac{1}{\sqrt{2}}\left(-|0\rangle + 3|1\rangle\right)$

[Tensor Product - 2 qubit space

$\cancel{\mathbb{H}_2}$ $\mathbb{H}_2 = \mathbb{H}_1 \otimes \mathbb{H}_1 : \{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$

$\{ |0\rangle, |1\rangle, |2\rangle, |3\rangle \}$

[2-qubit space

n qubit space is $\mathbb{H}_1 \otimes \mathbb{H}_1 \otimes \cdots \otimes \mathbb{H}_1$ / n factors

$= \mathbb{H}_n \cong \mathbb{C}^{2^n}$ w/ computational basis:

$\{|\$\rangle : \$ \text{ is any of length } n\} \;||\; \{|0\rangle, |1\rangle, \dots, |2^n - 1\rangle\}$

[Pauli Matrices] - useful for Q gate operations

↳ equal to their adjoint, } unitary
↳ Square is identity

$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

1 [Properties

↳ Geometric Interpretation

$X \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ reflection across $y = x$

Z reflection across x axis

[Eigenvalues & Eigenvectors

$A\vec{v} = \lambda \vec{v}$ $\vec{v}$ is Eigenvector of A
λ is Eigenvalue of A

ie:

1 [$X\vec{v} = \lambda \vec{v}$

$\vec{v} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \lambda = 1 \qquad \vec{v} \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \lambda = -1$

1 [$Z\vec{v} = \lambda \vec{v}$

$\vec{v} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \lambda = 1 \qquad \vec{v} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \lambda = -1$

$H = X \cdot R_{\pi/4} \qquad \begin{bmatrix} \cos \pi/4 & -\sin \pi/4 \\ \sin \pi/2 & \cos \pi/4 \end{bmatrix}$

[Quantum Algs] VI

9/10

[Deutsch Algorithm] - Construct $\mathcal{U}_f$, unitary transform matrix

$f: \{0,1\} \to \{0,1\}$ using:

$\mathcal{U}_f: \mathbb{H}_2 \to \mathbb{H}_2$ which implements:

$$|x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$$

[$\oplus$ XOR] Exclusive OR

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

1[constant & balanced

$f(0) \oplus f(1)$

// $|x\rangle|y\rangle$ meaning:
$|x\rangle \otimes |y\rangle$ ∴
if $|x\rangle$ & $|y\rangle$ are given in & basis, multiply & collect terms

$f_1(0) = 0$, $f_1(1) = 0 \mapsto 0$ Constant
$f_2(0) = 0$, $f_2(1) = 1 \mapsto 1$ Balanced
...

1[$\mathcal{U}_f$ will be one of $\mathcal{U}_{f_1}, \mathcal{U}_{f_2}, \mathcal{U}_{f_3}, \mathcal{U}_{f_4}$

$$f(x) \oplus y = X^{f(x)}|y\rangle$$

// $X^0 = I$
$X_1 = X_1$

$$X|y\rangle = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}(\alpha|0\rangle + \beta|1\rangle)$$

$$= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

ie:

$f(x) = 1$ $\quad X^{f(x)}|y\rangle = X|y\rangle \begin{cases} |1\rangle & \text{if } y = 0 \\ |0\rangle & \text{if } y = 1 \end{cases}$

$|f(x) \oplus y\rangle = |1 \oplus y\rangle \begin{cases} |1\rangle & \text{if } y = 0 \\ |0\rangle & \text{if } y = 1 \end{cases}$

$f(x) = 0$ $\quad X^{f(x)}|y\rangle = I|y\rangle$

$|0 \oplus y\rangle = |y\rangle$

// This is a reversible computation

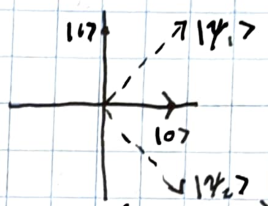
[Homework 1]
P. 209 [5.1.5]

V : Single qubit operation

$|\psi\rangle$ is eigenstate of V

$V|\psi\rangle = \lambda|\psi\rangle, \lambda \in \mathbb{C}$

$\boxed{1e}$ eigenstates for X $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$



$X = |0\rangle + |1\rangle$

$X|\psi_1\rangle = |\psi_1\rangle, \lambda = 1$
$X|\psi_2\rangle = -|\psi_2\rangle, \lambda = -1$

$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$Z: \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, |1\rangle - |0\rangle$

$Y: \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ $\quad Y|\psi\rangle = \lambda|\psi\rangle$

$Y|0\rangle = i\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = i|1\rangle$ // No $\mathbb{R}$ eigenvectors

$Y|1\rangle = i\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -i \\ 0 \end{bmatrix} = -i|0\rangle$

Find eigenvectors

$Y\vec{v} = \lambda\vec{v} \Rightarrow (Y - \lambda I)\vec{v} = \vec{0}$

$\begin{bmatrix} -\lambda & -i \\ i & -\lambda \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ $\quad -\lambda x - iy = 0$, $\quad ix - \lambda y = 0$

$ix - \lambda(i\lambda x) = 0$

$x(i - \lambda^2 i) = 0$

$\lambda = \pm 1$

|[Q Algs]| VII

[Deutsch Algorithm : $f: \{0,1\} \to \{0,1\}$

XOR: $f(0) \oplus f(1) = 0$ or 1

$f(\text{constant}) \to 0 \quad f(\text{balanced}) \to 1$

[2-Qubit

$U_f : \mathbb{H}_2 \to \mathbb{H}_2 : \; (\mathbb{H}_2 \cong \mathbb{H}_1 \otimes \mathbb{H}_1)$

$|x\rangle|y\rangle \to |x\rangle|f(x) \oplus y\rangle =$

$|x\rangle X^{f(x)} |y\rangle$

// 1 Qubit is a 2D $\mathbb{C}$ Vector 4D $\mathbb{R}$ Vector

// once measurement taken, collapses into 0 or 1

[Computational Basis of $\mathbb{H}_2$

$$\begin{aligned}
|00\rangle &\xmapsto{U_f} |0\rangle|f(0)\oplus 0\rangle \\
|01\rangle &\longmapsto |0\rangle|f(0)\oplus 1\rangle \\
|10\rangle &\longmapsto |1\rangle|f(1)\oplus 0\rangle \\
|11\rangle &\longmapsto |1\rangle|f(1)\oplus 1\rangle
\end{aligned}$$

Pauli X $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ // Reflection about y

$\mathbb{H}_2$	$f(0)=0$	$f(0)=1$
$\|00\rangle$	$\|00\rangle$	$\|01\rangle$
$\|01\rangle$	$\|01\rangle$	$\|00\rangle$
	$f(1)=0$	$f(1)=1$
$\|10\rangle$	$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|11\rangle$	$\|10\rangle$

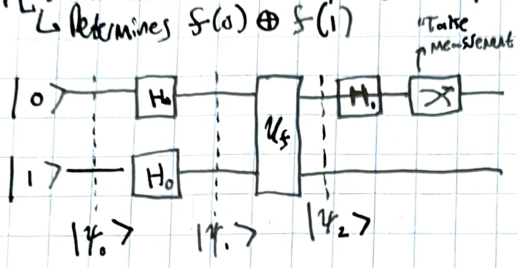
U_f as 4x4 mtx in each case

$U_{f_1} = I \quad U_{f_2} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}$

$U_{f_3} = \begin{bmatrix} X & 0 \\ 0 & I \end{bmatrix}$

$U_{f_4} = \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix}$

|[Deutsch Circuit : $|\psi_0\rangle = |0\rangle|1\rangle = |01\rangle$
↳ Determines $f(0) \oplus f(1)$



|[Hadamard Gate]

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H\left(|0\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) := |x_+\rangle$$

$$H\left(|1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) := |x_-\rangle$$

$$|\psi_0\rangle = |0\rangle|1\rangle$$

$$|\psi_1\rangle = |x_+\rangle|x_-\rangle$$
$$= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|x_-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle|x_-\rangle + |1\rangle|x_-\rangle)$$

|[Measurement - of a single qubit state outputs either $|0\rangle$ or $|1\rangle$ w/ probability $|\alpha|^2$ or $|\beta|^2$

$$\alpha|0\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathbb{C}$$

$$|\alpha|^2 + |\beta|^2 = 1$$

↳ Guarantees a "Reasonable" probability distribution

$$U_f|\psi_1\rangle = U_f\left(\tfrac{1}{\sqrt{2}}(|0\rangle|x_-\rangle + |1\rangle|x_-\rangle)\right)$$
$$= \tfrac{1}{\sqrt{2}}\left(|0\rangle X^{f(0)}|x_-\rangle + |1\rangle X^{f(1)}|x_-\rangle\right)$$
$$= \tfrac{1}{\sqrt{2}}\left(|0\rangle(-1)^{f(0)}|x_-\rangle + |1\rangle(-1)^{f(1)}|x_-\rangle\right)$$

// $X = (-1)$?

// factor out..?

$$= \frac{(-1)^{f(0)}}{\sqrt{2}}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right)|x_-\rangle = \begin{cases} \frac{(-1)^{f(0)}}{\sqrt{2}}|x_+\rangle|x_-\rangle, & f(0)\oplus f(1) = 0 \\ \frac{(-1)^{f(0)}}{\sqrt{2}}|x_-\rangle|x_-\rangle, & f(0)\oplus f(1) = 1 \end{cases}$$ Bal. Const.

$$H_1|x_+\rangle = H^2|0\rangle = |0\rangle$$
$$H_1|x_-\rangle = H^2|1\rangle = |1\rangle$$

if measured @ $|\psi_1|$: $H|0\rangle \otimes H|1\rangle$
$$= \tfrac{1}{2}|00\rangle - \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle - \tfrac{1}{2}|11\rangle$$
$$\alpha_0 \qquad \alpha_1 \qquad \alpha_2 \qquad \alpha_3$$

Deutsch-Jozsa

[Q Algs] VIV.

9/17

↳ Eigenstates

$\boxed{\text{ie}}$ HW 1: Eigenstates of Y

$\lambda = \pm 1$, x = any constant

$y = i\lambda x$ $\quad \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ ix \end{bmatrix} = x \underbrace{\begin{bmatrix} 1 \\ i \end{bmatrix}}_{|\psi_1\rangle}$ $\quad \lambda = 1$

// Y has 2 complex eigenvectors

$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ -ix \end{bmatrix}$ $\quad \lambda = -1$

$\lvert[|\psi_1\rangle$ & $|\psi_2\rangle$ are linearly independent:

$|\psi_1\rangle \neq c|\psi_2\rangle$
for any $c \in \mathbb{C}$:

$\begin{bmatrix} 1 \\ i \end{bmatrix} \neq c \begin{bmatrix} 1 \\ -i \end{bmatrix}$

– [Phase Estimation]

if some matrix A has a complex eigenvalue for some eigenstate $|\psi\rangle$,

$\lambda = re^{i\phi}$

// Global phase in Ch. 3

if A is unitary $\mathcal{U}$ ($\mathcal{U}^* = \mathcal{U}^{-1}$) then any such λ has length 1:

$\lambda = e^{i\phi}$, ϕ being phase.

– Phase estimation → Approximation of ϕ

$V: \mathbb{H}_1 \to \mathbb{H}_1$
$V|\psi\rangle = \lambda|\psi\rangle$ $\quad$ // only 2 real λ of a $\mathcal{U}$, ± 1

① Show Application of V to $|\psi\rangle$ applies "Global phase" to $|\psi\rangle$

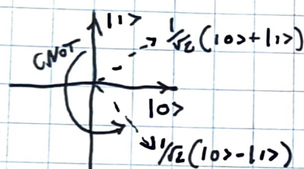
② Define C(V) – "Controlled V" operator on $\mathbb{H}_2$

[Q Algs] IX

[CNOT operator] - controlled X

[only apply NOT to $|y\rangle$ only if $|x\rangle = |1\rangle$

$$
\begin{aligned}
|0\rangle|0\rangle &\xrightarrow{CNOT} |00\rangle \\
|0\rangle|1\rangle &\rightarrow |01\rangle \\
|1\rangle|0\rangle &\rightarrow |11\rangle \\
|1\rangle|1\rangle &\rightarrow |10\rangle
\end{aligned}
\qquad
CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}
$$



Quantum Computing is designed to be reversible.
└ This is because Quantum Mech. is Unitary

[Bloch Sphere] [9/22]

1[Review: 3.1, State Spaces
$H_1 \rightarrow$ Single qubit space $\{|0\rangle, |1\rangle\}$

$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

$\therefore |\alpha_0|^2 + |\alpha_1|^2 = 1$

1[3.1.14] Geometric Interpretation of Unitary operators in H_1

$S^2 \subseteq \mathbb{R}^3 : \; S^2 = \{(x, y, z \in \mathbb{R}^3 : x^2+y^2+z^2 = 1\}$

Use polar form to associate qubits $\rightarrow$ points on the Sphere.

1[3.1.18] Uniquely determined $\mathbb{R}$ numbers:

γ, θ, ϕ such that:

$|\psi\rangle = e^{i\gamma}(\cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$

This also for quaternions ($\mathbb{R}^4$)

$a^2+b^2+c^2+d^2 = 1$

$S^3 = \{(a,b,c,d) \in \mathbb{R}^4 : a^2+b^2+c^2+d^2 = 1\}$

all work

[Bloch Sphere] - AKA Unit Quaternion Sphere

[9/22]

Point on unit circle: $S^1 \subseteq \mathbb{R}^2$

$(|\alpha_0|, |\alpha_1|) = (\cos\theta/2, \sin\theta/2)$ for some angle θ

$\therefore$ $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|0\rangle$ // from 3.1.18

$= |\alpha_0| e^{i\phi_0}|0\rangle + |\alpha_1| e^{i\phi_1}|1\rangle$

* $= e^{i\phi_0}\left(\cos(\theta/2)|0\rangle + e^{i(\phi_1-\phi_0)}\sin(\theta/2)|1\rangle\right)$ // $\gamma = \phi_0$, $\phi = \phi_1 - \phi_0$

* when measuring a quantum state (like a single qubit)

$\boxed{\text{ie}}$ $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, always get $|0\rangle$ or $|1\rangle$ with probability:

$|\alpha_0|^2$ (of $|0\rangle$) and $|\alpha_1|^2$ (of $|1\rangle$)

* Quantum is constant in basis state

↳ Measurement is not affected by mult of a "Global Phase" (5.15) factor like $e^{i\gamma}$

$\boxed{\text{ie}}$ $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ has same probability as:

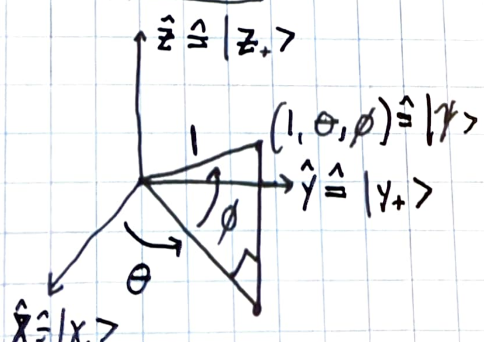
$\cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$ //Algebraic

1 [Prop 3.1.18

for $|\psi\rangle \in H_1$, choose angles γ, θ, ϕ such that:

$$|\psi\rangle = e^{i\gamma}\left(\cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle\right)$$

the qubit $|\psi\rangle$ can be represented "up to a global phase $e^{i\gamma}$" as polar coordinates $\underset{\text{azit.}}{\theta}, \underset{\text{elev.}}{\phi}$ given as <u>azimuth</u> & <u>elevation</u>



$\vec{P} = (1, \theta(\psi), \phi(\psi))$

$|\psi\vec{P}\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$

// $\hat{x}, \hat{y}, \vec{z}$ - unit vectors in $\mathbb{R}^3$

[Bloch Sphere] – "Weird Map"

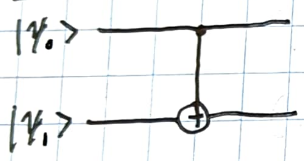
[3.1.21 p. 110] $(\vec{p}(|x_+\rangle), \vec{p}(|x_-\rangle)) = (\hat{x}, -\hat{x})$

$(\vec{p}(|y_+\rangle), \vec{p}(|y_-\rangle) = (\hat{y}, -\hat{y})$

[5.1.5 p. 208] - Amplitude of $|1\rangle$ in the first qubit:

$|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$, $\beta \in \mathbb{C}$ is the <u>amplitude</u> of $|1\rangle$

[C(v) operator



$|\psi_0\rangle|\psi_1\rangle$

$|\psi_0\rangle \oplus |\psi_1\rangle$

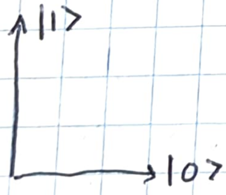
CNOT = C(x)

C(v) does similar to C(x)

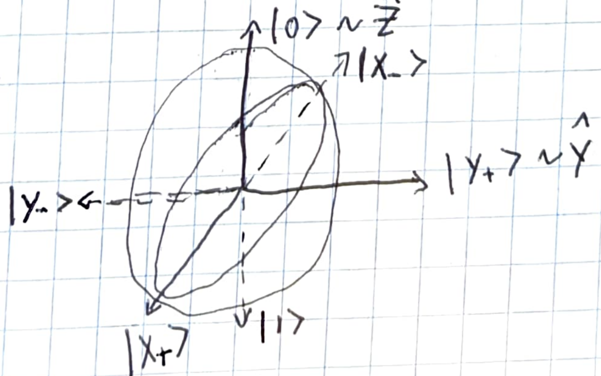
$\boxed{\text{ie}}$ applies V to $|\psi_1\rangle$ if $|\psi_0\rangle$ is $|1\rangle$ (does not if $|\psi_0\rangle$ is $|0\rangle$)

* In physics *
Qubit in non-basis state is "entangled"

$\mathbb{R}^4$
$\mathbb{C}^2$
$\mathbb{H}^1$



Bloch Sphere ($\mathbb{C}^3$)



[Deutsch-Jozsa Algorithm]

[9/22]

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

f is <u>constant</u> if $f(\vec{x}) = 0$ for all $\vec{x} \in \{0,1\}^n$
or $f(\vec{x}) = 1$ " " "

<u>balanced</u> if $f(\vec{x}) = 0$ for half of $\vec{x} \in \{0,1\}^n$
and $f(\vec{x}) = 1$ for other half

Domain of functions:

$$\binom{2^n}{2^{n-1}} = \frac{m!}{(\frac{m}{2})!\,(\frac{m}{2})!}$$

[9/21]

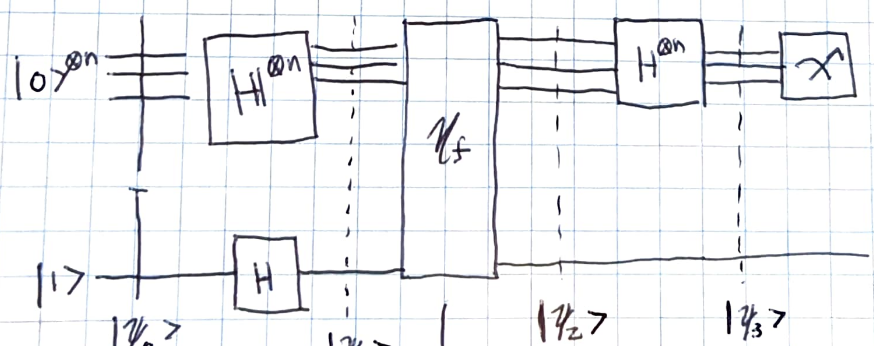
$$U_f : \mathbb{H}_n \otimes \mathbb{H}_1 \longrightarrow \mathbb{H}_n \otimes \mathbb{H}_1$$

using bit-strings of length $(\vec{x})$

$$|\vec{x}\rangle|y\rangle \longmapsto |\vec{x}\rangle|f(\vec{x}) \oplus y\rangle = |\vec{x}\rangle X^{f(\vec{x})}|y\rangle$$

U_f is unitary. $\mathbb{H}_n \otimes \mathbb{H}_1 \cong \mathbb{H}_{n+1}$

[Deutsch-Josa Circuit] - Assume f is constant or balanced



uses multilinearity of tensor products

$\llcorner$ $|\varphi\rangle \otimes c|\psi\rangle = c|\varphi\rangle \otimes c|\psi\rangle$

[Lemma 5.3.6] - "helper function" for Deutsch-Josa

for all $\vec{x} \in \{0,1\}^n$, $|\vec{x}\rangle \in H_n$

$$H^{\otimes n}|\vec{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}} (-1)^{\vec{x}\cdot\vec{z}} |\vec{z}\rangle$$ // Consider $\vec{x}, \vec{z} \in \mathbb{R}^n$, vectors of 1 & 0

↑ Sum over all basis elements of H_n

for $n=1$ $x \in \{0,1\}$ & $H|x\rangle = \frac{1}{\sqrt{2}} = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$

$$= \frac{1}{\sqrt{2}} \sum_{z \in \{0,1\}} (-1)^{x \cdot z} |z\rangle$$

$\therefore$ $\vec{x} \in \{0,1\}^n$, $\vec{x} = (x_0, \dots, x_{n-1})$

$$H^{\otimes n}|\vec{x}\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{z_0 \in \{0,1\}} (-1)^{x_0 z_0} |z_0\rangle\right) \otimes \dots \otimes \left(\sum_{z_{n-1} \in \{0,1\}} (-1)^{x_{n-1} z_{n-1}} |z_{n-1}\rangle\right)$$

$|\vec{x}\rangle = (|x_0\rangle \otimes |x_1\rangle, \otimes \dots \otimes |x_{n-1}\rangle)$

$$= \frac{1}{\sqrt{2^n}} \sum_{\vec{z} \in \{0,1\}^n} (-1)^{x_0 z_0 + \dots + x_{n-1} z_{n-1}} |z\rangle$$

$$= H^{\otimes n}|\vec{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{z} \in \{0,1\}} (-1)^{\vec{x}\cdot\vec{z}} |\vec{z}\rangle$$

[Deutsch-Josa] $\boxed{p.\ 211}$ – Deutsch on Series of inputs | input → $f: \{0,1\}^n \to \{0,1\}^n$ | Output → Constant or Balanced

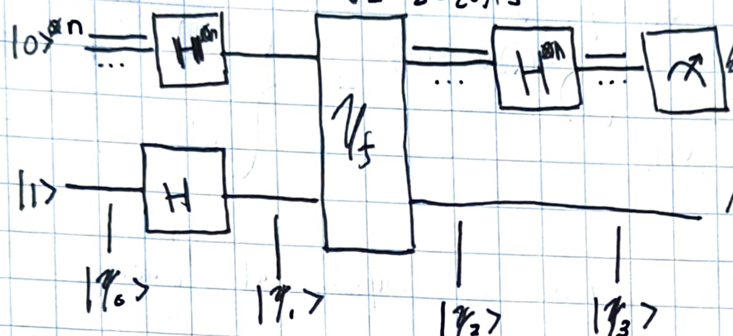
9/29

[Lemma: for all $x \in \{0,1\}^n$

$$H^{\otimes n}|\vec{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{z} \in \{0,1\}^n} (-1)^{\vec{x}\cdot\vec{z}} |\vec{z}\rangle$$

// $H^2 = I$

$$|\vec{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{z} \in \{0,1\}^n} (-1)^{\vec{x}\cdot\vec{z}} H^{\otimes n} |\vec{z}\rangle$$



// Measurement gives a discrete basis state
↳ H^n

// Measurement @ any point collapses to basis state

[$U_f(|\vec{x}\rangle|y\rangle) = |\vec{x}\rangle X^{f(\vec{x})} |y\rangle$

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

[$|\psi_1\rangle = H^{\otimes n} |0\rangle^{\otimes n} H |1\rangle$

↳ $= \left(\frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} |\vec{x}\rangle\right) \underbrace{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)}_{|x_-\rangle}$

[$|\psi_2\rangle = U_f |\psi_1\rangle$

$= U_f(|\vec{x}\rangle|x_-\rangle)$

$= \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} U_f(|\vec{x}\rangle|x_-\rangle)$

$= \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{x})} |\vec{x}\rangle |x_-\rangle$

$= \frac{(-1)^{f(\vec{0})}}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{0}) \oplus f(\vec{x})} |\vec{x}\rangle |x_-\rangle$

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

$=$

For a basis state $H^{\otimes n}|\vec{z}\rangle$, probability of that state is amplitude of its coefficient → $\frac{(-1)^{f(\vec{0})}}{2^n} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{x}) \oplus f(\vec{0})}$

[Deutsch-Josa] II

$$|\psi_2\rangle = \left(\frac{(-1)^{f(\vec{0})}}{2^n} \sum_{\vec{z} \in \{0,1\}^n} \left(\sum_{\vec{x} \in \{0,1\}^n} (-1)^{\vec{x}\cdot\vec{z} + f(\vec{x}) \oplus f(\vec{0})} \right) H^{\otimes n} |\vec{z}\rangle \right) |x_-\rangle$$

1[Amplitude at $|\psi_2\rangle$, with basis $[H^{\otimes n}|0\rangle_n]$ to get
Probability at $|\psi_2\rangle$

$$\frac{(-1)^{f(\vec{0})}}{2^n} \sum_{\vec{x} \in \{0,1\}} (-1)^{f(\vec{x}) \oplus f(\vec{0})} = \begin{cases} (-1)^{f(\vec{0})} & \text{, if } f \text{ constant} \\ 0 & \text{, if } f \text{ balanced} \end{cases}$$

$|\psi_3\rangle = H^{\otimes n}|\psi_2\rangle$ // return to computational basis

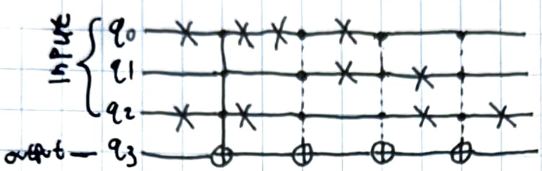
$H^{\otimes n}|\vec{0}\rangle \mapsto H^{\otimes n} H^{\otimes n} |\vec{0}\rangle_n$

$\therefore$ $|\psi_3\rangle$ produces $|\vec{0}\rangle_n$ iff f is constant
if $|\psi_3\rangle \neq |\vec{0}\rangle_n$, f is balanced.

[Qiskit]

Oracle Function → determines constant or balanced

[Oracle(f) of D-J on U_f] $f: \{0,1\}^3 \mapsto \{0,1\}$ [10/1]



X → Pauli X gates

in	out
000	0
001	0
010	1
011	1
100	0
101	1
110	1
111	0

Balanced

?

P.213

[Simon's Algorithm] - bit string to bit string. Classical Version.

$f: \{0,1\}^n \mapsto \{0,1\}^n$ $[\vec{s} \neq \vec{0}]$ ↗ "not interesting"

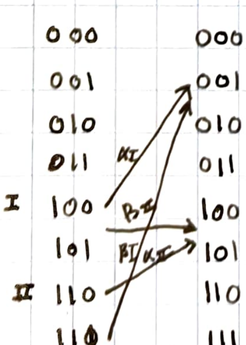
there exists $\vec{s} \in \{0,1\}^n$ such that:

for all $\vec{x}, \vec{y} \in \{0,1\}^n$ there is

$f(\vec{x}) = f(\vec{y})$ iff $\vec{x} = \vec{y}$ or $\vec{x} = \vec{y} \oplus \vec{s}$

$\boxed{\text{ie}}$ $n=3$, $\vec{s} = 011$

$\vec{y}$ $\vec{s}$ $\vec{x}$ = $\vec{x} = \vec{y} \oplus \vec{s}$ ~



I: $100 \oplus 011 = 111$
$f(\vec{y}) = 001 \Rightarrow f(\vec{y} \oplus \vec{s})$

II: $110 \oplus 011 = 101$
$f(\vec{y} \oplus \vec{s}) = \vec{x}$

Domain & Range are "equivalence classes"
↳ marked with tilde (~)

to find $\vec{s}$: check f $\frac{2^n}{2} + 1$ times
(classically)

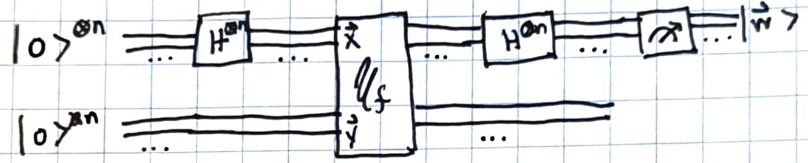
$2^{n-1} + 1$

[Simon's Algorithm] - Quantum Version
↳ uses only 1 check of U_f

let $U_f : \mathbb{H}_n \otimes \mathbb{H}_n \longmapsto \mathbb{H}_n \otimes \mathbb{H}_n$

$|\vec{x}\rangle|\vec{y}\rangle \longmapsto |\vec{x}\rangle|f(\vec{x}) \oplus \vec{y}\rangle$

Use $Q_{simon}(n, U_f)$ to produce outputs $|\vec{w}\rangle$



run Q_{simon} $n-1$ times to form Matrix W

$|\vec{w}\rangle$ is ket or vector w/ bitstring $\vec{w}$?
so that $|\vec{w}\rangle$ is a computational basis element

[Vector Space W]

$|\vec{w}_1\rangle, \cdots, |\vec{w}_{n-1}\rangle$ with $Q_{simon}(n, U_f)$

$W = [\vec{w}_1, \cdots, \vec{w}_n]$ bit strings $\vec{w}_j$ to form column vectors of 0's & 1's

W is $n \times (n-1)$
W^T is $(n-1) \times n$

To do linear algebra operations, need scalar fields
↳ such as $\mathbb{C}$, $\mathbb{R}$, & $\mathbb{F}_p$ where p is a prime number

$\boxed{\text{ie}}$ $\mathbb{F}_2 = \{0, 1\}$ $\qquad$ $= \{0, 1, \cdots, p-1\}$

x	0	1
0	0	0
1	0	1

+	0	1
0	0	1
1	1	0

Every field has:
- Multiplication, addition
- Associative
- Distributive
- Commutative

Every Field has "special" elements 0 (identity for add) & 1 (identity for mult)

fields always have inverses for both mult & add.