

Q Notes

By Peter Montgomery

October 8, 2020

Contents

1	Complex Arithmetic	8
1.1	Complex Dot Product	8
1.2	Complex Conjugate	8
1.3	Roots of Unity	9
1.4	Summing Roots of Unity	9
1.5	Kronecker Delta	9
2	Real Vector Spaces	10
2.1	Linear Algebra	10
2.2	The Objects	10
2.3	The Rules	10
2.4	Positive Definite Property	11
2.5	Linear Combination	11
2.6	Bases of a Vector Space	11
2.7	Natural (Standard) Basis	11
2.8	Properties of a Basis	12
2.9	Orthonormal Bases	12
2.10	Expansion Coefficients	12
2.11	Subspace	12
3	Matrices	13
3.1	Matrices	13
3.2	Matrix Multiplication	13
3.3	Row x Column	13
3.4	Definition of Matrix Multiplication	13
3.5	Matrix Product of Vectors	13
3.6	Matrix Transpose	14
3.7	Matrix Addition and Scalar Multiplication	14
3.8	Zero Matrix (Additive Identity)	14
3.9	Identity Matrix (Multiplicative Identity)	14
3.10	Determinants of a 2 x 2 Matrix	14
3.11	Determinants of a 3 x 3 Matrix	14
3.12	Determinants of an n x n Matrix	14
3.13	Determinants of Products	14
3.14	Matrix Inverses	15
3.15	System of Linear Equations	15
3.16	Matrix Equations	15
3.17	Cramer's Rule	15
3.18	Complex Vector Space, \mathbb{C}^n	15
3.19	Complex Inner Product	16
3.20	Norm	16

3.21	Distance	16
3.22	Expansion Coefficients	16
4	Hilbert Space, H	17
4.1	Definitions	17
4.2	Finite Dimensional Hilbert Spaces	17
4.3	Infinite Dimensional Hilbert Spaces	17
4.4	The Space $L^2[a, b]$	17
4.5	Properties of Hilbert Spaces	17
4.6	Modeling Quantum Systems	18
4.7	Ray	18
4.8	O in H	18
4.9	Interacting with these Vectors	18
5	Linear Transformation	19
5.1	Linear Transformation	19
5.2	Role of Bases	19
5.3	Dependence of Matrix on Basis	19
5.4	Matrix M_T in a Non-Standard Basis	20
5.5	Transformation in an Orthonormal Basis	20
5.6	The Adjoint of a Matrix	20
5.7	Unitary Operators	20
5.8	Non-Unitary Operators	20
5.9	Hermitian Operators	20
6	The Experimental Basis of Quantum Computing	21
6.1	Spin 1/2 Quantum Mechanics	21
6.2	Naive Electron Spin Definition	21
6.3	Spherical Representation	21
6.4	Electron Spin z-Projection	21
6.5	Follow up $ +\rangle_z$ in S_x	22
6.6	Follow up $ +\rangle_x$ in S_z	22
6.7	Construction of Hilbert Space	22
6.8	Representing Spin	22
6.9	Measuring Spin theta from Standard Axis	22
7	Time Independent Quantum Mechanics	23
7.1	Particle Energy and Position	23
7.2	Stern-Gerlach Apparatus	23
7.3	First Postulate of Quantum Mechanics	23
7.4	Trait #1: The State Space	23
7.5	Fundamental State Space for Quantum Computing	23
7.6	Orthonormality Expression	24
7.7	The x-Basis for H	24
7.8	Reasoning for Complex Vector Space	24
7.9	Second Postulate of Quantum Mechanics	24
7.10	Trait #2: The Operator for an Observable	24
7.11	Completeness of the Eigenbasis	24
7.12	The Observable S_z	25
7.13	Third Postulate of Quantum Mechanics	25
7.14	Trait #3: Eigenvalues of an Observables	25

7.15	Eigenvectors and Eigenvalues	25
7.16	Trait #3': Eigenvectors and Eigenvalues of S_z	25
7.17	Computing Eigenvectors and Eigenvalues	26
7.18	Eigenvalue Theorem	26
7.19	Summary of Eigenvectors and Eigenvalues for spin 1/2 Observables	26
7.20	Trait #4: Real Eigenvalues and Orthonormal Eigenvectors	27
7.21	General States Expressed in Alternate Bases	27
7.22	Orthonormal Basis in Higher Dimensions	27
7.23	Trait #5: Closure (Completeness) Relation	27
7.24	Fourth Postulate of Quantum Mechanics	27
7.25	Trait #6: Probability of Outcome	27
7.26	Fifth Postulate of Quantum Mechanics	28
7.27	Trait #7: Post-Measurement Collapse (complex inner product)	28
7.28	Dirac's Bra-ket Notation	28
7.29	Transforming Ket to Bra	28
7.30	The Bra Space (Adjoint of a ket)	28
7.31	The Adjoint of an Operator	28
7.32	Trait #8: Adjoint Conversion Rules	28
7.33	Expectation Values	29
7.34	Trait #9: Expectation Value Theorem	29
8	Time Dependent Quantum Mechanics	30
8.1	The Hamiltonian	30
8.2	Trait #10: Constructing the Hamiltonian	30
8.3	Classical Hamiltonian (1/2 Spin)	30
8.4	Quantum Hamiltonian	31
8.5	Energy Eigenkets	31
8.6	Trait #11: Quantization of Energy	31
8.7	Sixth Postulate of Quantum Mechanics	31
8.8	Trait #12: Time-Dependent Schrodinger Equation	31
8.9	Solving the Schrodinger Equation	32
8.10	Trait #13: Stationary States	32
8.11	General Technique for Computing Time-Evolved States	32
8.12	Trait #14: Evolution of any Observable	32
8.13	Larmor Precession	33
8.14	Rewriting $ \psi\rangle$	33
8.15	Convenient Angle	33
8.16	Expectation Value at Time t	33
9	The Qubit	34
9.1	Vector Space $B = B^2(B \equiv \{0, 1\})$	34
9.2	Definition of a Classical Bit	34
9.3	Definition of Bit Value	34
9.4	Alternate Definition of a Bit	34
9.5	Definition of a Classical Logical Operator	35
9.6	Unitary Properties	35
9.7	Definition of a Qubit	35
9.8	Alternate Definition of a Qubit	35
9.9	Definition of Qubit Value	35
9.10	Computational Basis State (CBS)	36

9.11	Global Phase Factors	36
9.12	Definition of a Quantum Logical Operator	36
9.13	Bit Flip QNOT (X)	36
9.14	Phase Flip (Z)	36
9.15	Bit and Phase Flip (Y)	36
9.16	Hadamard Gate (H)	37
9.17	Measurement	37
9.18	Phase-Shift Gates (R_θ , S and T)	37
9.19	Basis Conversion Theorem	37
9.20	Combining Gates	37
9.21	The Bloch Sphere	37
9.22	Definition of the Bloch Sphere	38
10	Tensor Products	39
10.1	Tensor Products	39
10.2	Scalars of $V \otimes W$	39
10.3	Vectors of $V \otimes W$	39
10.4	Terms and Definition	40
10.5	Vector Addition	40
10.6	Scalar Multiplication	40
10.7	Inner Product in $V \otimes W$	40
10.8	Natural Basis for $V \otimes W$	41
10.9	Tensor Product Basis Theorem	41
10.10	Proof of Basis Theorem	41
10.11	Conventional Order of Tensor Basis	41
10.12	Linear Operators on the Tensor Product Space	41
10.13	Linear Operators on the Tensor Product Space	42
10.14	Matrix of General Operator	42
10.15	Matrix Tensor Product	43
11	Two Qubits and Binary Quantum Gates ($\mathcal{H}_A \otimes \mathcal{H}_B$)	44
11.1	Definition of Two Qubits	44
11.2	Definition of a Two-Qubit Value	44
11.3	Preferred Bipartite CBS	44
11.4	Alternate Bipartite Bases	44
11.5	Inherit Second Order Mixed CBS	44
11.6	Non-Standard Second Order CBS in Natural Basis	45
11.7	Alternate Definition of Two Qubits	45
11.8	Binary Quantum Operator Definition	45
11.9	Complete Description of Binary Quantum Operator	45
11.10	Measurement of Separable Outputs	45
11.11	Quantum Entanglement (Non-separable outputs)	46
11.12	Controlled-NOT (CNOT Gate)	46
11.13	Quantum Entanglement for CNOT	46
11.14	CNOT in Different CBS	46
11.15	Second Order Hadamard Gate	46
11.16	Condensed Form	47
11.17	Circuits in Separable Basis	47
11.18	Circuits in Non-Separable Basis	47
11.19	Controlled-U Gate	47

11.20	Separable Operators on Separable States	47
11.21	Separable Operators on Entangled States	48
11.22	Trait #15: Born Rule for Bipartite States	48
11.23	Bell States Circuit	48
11.24	Binary Operators on Bell States	48
11.25	BELL as Basis Transform Operator	48
11.26	Upside Down CNOT Circuit	49
11.27	Order-3 Tensor Product	49
11.28	Tripartite System Definition ($\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C = \mathcal{H}_{(3)}$)	49
11.29	Trait #15': Born Rule for Tripartite States	50
12	First Quantum Algorithms	51
12.1	Superdense Coding	51
12.2	Quantum Teleportation	51
12.3	Application of Born Rule	51
12.4	Expanding Initial States along $BELL_{AC}$ basis	52
12.5	B's Action from A's Message	52
12.6	Boolean Functions and Reversibility	52
12.7	Unary Gates as Boolean Function	52
12.8	Binary Gates as Boolean Functions	52
12.9	Quantum Oracle for Boolean Functions	53
12.10	Deutsch's Algorithm	54
13	Multi-Qubit Systems and Algorithms	55
13.1	Higher Order Tensor Products	55
13.2	Toffoli Gate (CCX)	55
13.3	Definition of n Qubits	56
13.4	n-qubit CBS	56
13.5	nth Order Hadamard Gate	56
13.6	Higher Order Basis conversion	56
13.7	Oracle for n-qubit Functions	56
13.8	Deutsch-Jozsa Problem	57
13.9	Quantum vs. Classical Time Complexity	57
13.10	Non-Deterministic Algorithm with small error $\epsilon \ll 1$	57
13.11	Deutsch-Jozsa Measurements	57
13.12	Bernstein-Vazirani Problem	57
13.13	Trait #15'': Generalized Born Rule	58
14	Probability Theory	59
14.1	Outcomes	59
14.2	Events	59
14.3	Sample Space ω	59
14.4	Null Event \emptyset	59
14.5	Probability $P(\mathcal{A})$	59
14.6	Set Operations	60
14.7	Linear Independence	60
14.8	Span	60
14.9	Fundamental Probability Theory	60
14.10	The Axioms	60
14.11	Definitions in Finite Equiprobable Sample Space	61
14.12	Conditional Probability	61

14.13	Bayes' Law	61
14.14	Statistical Independence	61
14.15	Two Independent Events	62
14.16	Multiple Independent Events	62
14.17	Other Formulas	62
14.18	Wedge and Vee Notations	62
14.19	Applications to Deutsch-Jozsa	62
14.20	Sampling with Replacement	62
14.21	Sampling without Replacement	63
14.22	Probability Algorithm	63
14.23	Looping Algorithm	63
14.24	Constant Time Complexity for Looping Algorithm	63
15	Computational Complexity	65
15.1	Big-O Growth	65
15.2	Ω Growth	65
15.3	Θ Growth	66
15.4	Little-o Growth	66
15.5	Easy vs. Hard	66
16	Computational Basis States and Modular Arithmetic	67
16.1	Single Qubit Hilbert Space	67
16.2	Multi Qubit Hilbert Spaces	67
16.3	\mathbb{Z}_N , or mod N Arithmetic	67
16.4	$(\mathbb{Z}_2)^n$ with \oplus Arithmetic	68
16.5	The group \mathbb{Z}_{2n}	68
16.6	Connection Between $(\mathbb{Z}_2)^n$ and (\mathbb{Z}_{2n})	68
16.7	General Notations	69
17	Quantum Oracle	70
17.1	General Oracle	70
17.2	Complexity of Quantum Oracle	71

Chapter 1

Complex Arithmetic

1.1 Complex Dot Product

$$\vec{a} \cdot \vec{b} = \sum_i \alpha_i \beta_i = \alpha_T \beta; \alpha, \beta \in \mathbb{R}$$

$$|\vec{a}| = \sqrt{\vec{a} \cdot \vec{a}}$$

For complex vectors, $\sqrt{\vec{a} \cdot \vec{a}}$ could be negative and $|\vec{a}| \in \mathbb{C}$.

fjkjf

1.2 Complex Conjugate

$$\text{For } \vec{\gamma} = \begin{pmatrix} a + ib \\ c + id \end{pmatrix}, \vec{\gamma}^* = \begin{pmatrix} a - ib \\ c - id \end{pmatrix}$$

Conjugation is distributive across sums and products.

$$(\alpha + \beta)^* = \alpha^* + \beta^*$$

$$(\alpha \times \beta)^* = \alpha^* \times \beta^*$$

$$|z| = z^* z = z z^* = a^2 + b^2$$

Now, the dot product definition changes:

$$\vec{\alpha} \cdot \vec{\beta} = \vec{\alpha}_T \cdot \vec{\beta}, \text{ where } \vec{a} \cdot \vec{a} = \alpha_T^* \alpha \in R$$

α_T^* is also called the Hermitian conjugate $\equiv v^\dagger$ (v-dagger).

$$zw = rs e^{i\theta+\phi}; \frac{z}{w} = rs e^{i\theta+\phi}; z^* = re^{-i\theta} \text{ (Complex Polar Coordinates)}$$

1.3 Roots of Unity

$$\omega_n = \sqrt[n]{1} = \cos\left(\frac{2\pi \cdot k}{n}\right) + i \sin\left(\frac{2\pi \cdot k}{n}\right), k \in \{1, \dots, n\}$$

1.4 Summing Roots of Unity

$$\text{For } \sum_{k=0}^{n-1} \omega_n^k = A, A = 0 \text{ because } A\omega_n^k = A$$

Substitute $\omega_n = z$ and multiply by $z-1$, we get

$$\prod_{k=0}^{n-1} z - \omega_n^k = 0$$

1.5 Kronecker Delta

$$\delta_{kj} = \begin{cases} 1, & \text{if } k=j \\ 0, & \text{otherwise} \end{cases}$$

$$\sum_{k=0}^{N-1} \omega^{(j-m)k} = N\delta_{jm} \text{ for sum of roots of unity.}$$

Chapter 2

Real Vector Spaces

2.1 Linear Algebra

Axioms defines the object of a vector space and the rules.

2.2 The Objects

Scalars The scalars of the vector space is the underlying field.

Vectors The object of the vector space.

2.3 The Rules

Vector Addition: $\vec{v} + \vec{w} \Rightarrow \vec{u}$

- Zero Operator: $\mathbf{v} + 0 = 0 + \mathbf{v} = \mathbf{v}$
- Vector Opposites (additive inverses): $\mathbf{v} + (-\mathbf{v}) = 0$
- Commutativity & Associativity

Scalar Multiplication: $c\vec{v} \Rightarrow \vec{w}$

- Scalar Identity: $I\vec{v} = \vec{v}\forall\vec{v}$
- Associativity & Distributivity

Inner Product $\vec{v} \cdot \vec{w} \Rightarrow c$

- Commutativity & Distributivity
- Associativity with Scalar Multiplication

Length (Modulus or Norm): $|\vec{v}| \geq 0$

- $||\vec{v}|| = \sqrt{\vec{v} \cdot \vec{v}}$

Orthogonality

- $\vec{v} \cdot \vec{w} = 0$

A set of orthogonal vectors with norms 1 is called orthonormal.

2.4 Positive Definite Property

$$\vec{v} \cdot \vec{v} \geq 0 \text{ \& } \vec{v} \neq 0 \Rightarrow ||\vec{v}|| > 0$$

An operation that satisfies positive definiteness is an inner product, else it's a pairing.

2.5 Linear Combination

$$\vec{u} = \sum_{k=0}^{n-1} c_k \vec{v}_k$$

This is called linear combination in maths & superposition in physics.

2.6 Bases of a Vector Space

If a minimal (linear independent) subset of vectors span the vector space, they are called the basis of the space.

2.7 Natural (Standard) Basis

$$A = \{\hat{x}, \hat{y}\} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

*hat denotes unit length

2.8 Properties of a Basis

- Linear Independence: $\vec{u} \neq \vec{v} + \vec{w} \ \forall \ \vec{u}, \vec{v}, \vec{w} \in A$
- Completeness (Spanning): A closed under linear combination

2.9 Orthonormal Bases

B is orthonormal if $\vec{b}_k \cdot \vec{b}_j = \delta_{k,j}$

2.10 Expansion Coefficients

For $\vec{v} = \sum_{k=1}^n a_k \vec{b}_k$, $\vec{v} \cdot \vec{b}_j = \sum_{k=1}^n a_k \delta_{k,j} = a_j$

2.11 Subspace

A subset of vectors closed under vector/ scalar operations.

$$\{a\vec{v} \mid a \in R\}$$

Chapter 3

Matrices

3.1 Matrices

A matrix is a rectangular arrays of number. The size is expressed as (# rows) \times (# columns).

A_{kj} describes the element in the row k & column j .

3.2 Matrix Multiplication

$AB \neq BA$ where $(n \times p)(p \times q) = (n \times q)$

3.3 Row x Column

Special case where $(1 \times 1)(1 \times 1) = 1$ (scalar)

3.4 Definition of Matrix Multiplication

For A as $(n \times p)$ & B as $(p \times m)$, $C_{kl} = (AB)_{kl} \equiv \sum_{j=1}^p A_{kj}B_{jl}$

where $k = 1, \dots, n$; $l = 1, \dots, m$

Notice that $(AB)C = A(BC)$

3.5 Matrix Product of Vectors

- $A\vec{v}, \vec{v}^\dagger A$ is compatible
- $A\vec{v}$ is a linear transformation

3.6 Matrix Transpose

$$(A_k l)^\dagger = A_l k$$

3.7 Matrix Addition and Scalar Multiplication

Both are commutative, associative, and distributive.

3.8 Zero Matrix (Additive Identity)

$$(0)A = (0) \ \& \ (0)\vec{v} = 0$$

$$A + (0) = (0) + A = A$$

3.9 Identity Matrix (Multiplicative Identity)

$$IM = MI = M$$

$$I\vec{v} = \vec{v} \ \& \ v^\dagger I = v^\dagger$$

3.10 Determinants of a 2 x 2 Matrix

$$\text{For } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \det A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

3.11 Determinants of a 3 x 3 Matrix

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} \equiv a \begin{vmatrix} e & f \\ h & i \end{vmatrix} - b \begin{vmatrix} d & f \\ g & i \end{vmatrix} + c \begin{vmatrix} d & e \\ g & h \end{vmatrix}$$

$$= a(\text{minor of } a) - b(\text{minor of } b) + c(\text{minor of } c)$$

Minor is the determinant of a smaller matrix made by crossing out the element's row & column.

3.12 Determinants of an n x n Matrix

$$\det(A) = |A| = \sum_{k=1}^n (-1)^{k+j} A_{jk} (\text{minor of } A_{jk})$$

3.13 Determinants of Products

$$\det(AB) = \det(A) \det(B)$$

3.14 Matrix Inverses

$$A^{-1}A = AA^{-1} = I$$

If A has an inverse, it's invertible or non-singular.

Little Inverse Theorem M is singular if $M\vec{v} = 0$, for $\vec{v} \neq 0$

Big Inverse Theorem M is singular $\iff \det(M) = 0$

3.15 System of Linear Equations

A system of n unknowns is only solvable if there are n independent equations.

3.16 Matrix Equations

$M\vec{v} = c$, where

M is the matrix of the linear combination \vec{v} is the vectors of the unknown c is the vectors of the constants

To solve, $M^{-1}M\vec{v} = \vec{v} = M^{-1}c$

1. Determine if matrix is invertible
2. If yes, compute inverse

3.17 Cramer's Rule

For $M\vec{v} = c$, $x_k = \frac{\det M_k}{\det M}$

where M_k is the matrix M with the kth element column replace by the constant vector c,

To find inverse, split inverse into column & solve for individual variables with Cramer's Rule.

3.18 Complex Vector Space, \mathbb{C}^n

$$\mathbb{C}^n = \left\{ \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} \mid c_k \in \mathbb{C}, k = 0, \dots, n-1 \right\} \text{ (complex scalar)}$$

3.19 Complex Inner Product

$$a \cdot b = \langle a, b \rangle = \langle a|b \rangle = \sum_{k=0}^{n-1} \bar{a}_k b_k = \sum_{k=0}^{n-1} (a_k^*) b_k$$

* Non-commutative: $\langle a|b \rangle \neq \langle b|a \rangle$

However, $\langle a|b \rangle^* = \langle b|a \rangle$

* Physicist conjugate the vector of the inner product.

- Distributive: $\langle a|b + b' \rangle = \langle a|b \rangle + \langle a|b' \rangle$ or $\langle a + a'|b \rangle = \langle a|b \rangle + \langle a'|b \rangle$
- Anti-linear in the 1st position: $c\langle a|b \rangle = \langle \mathbb{C}^* a|b \rangle$
- Linear in the 2nd position: $c\langle a|b \rangle = \langle a|cb \rangle$

For both cases, $c \in \mathbb{C}$

3.20 Norm

$$||\vec{a}|| = \sqrt{\sum_{k=0}^{n-1} |\vec{a}_k|^2} = \sqrt{\sum_{k=0}^{n-1} (\vec{a}_k)^* \vec{a}_k}$$

3.21 Distance

$$\text{dist}(\vec{a}, \vec{b}) = ||b - a|| = \sqrt{\sum_{k=0}^{n-1} |\vec{b}_k - \vec{a}_k|^2}$$

These all results in $||a|| \geq 0$

3.22 Expansion Coefficients

$\langle b_k|\vec{v} \rangle = \sum_{j=0}^{n-1} \beta_j \delta_{kj}$ with \vec{v} on the right side of inner product.

This only works for orthonormal basis.

Chapter 4

Hilbert Space, H

4.1 Definitions

A Hilbert Space is a real or complex vector space that has:

1. Inner Product
2. Completeness

4.2 Finite Dimensional Hilbert Spaces

\mathbb{R}^n and \mathbb{C}^n are valid Hilbert spaces.

4.3 Infinite Dimensional Hilbert Spaces

This usually refers to function spaces. The vectors of these vector space consist of well-behaved functions.

4.4 The Space L^2 [a, b]

All complex-valued functions defined over the real interval [a, b] and which are square-integrable.

$$\int_a^b |f(x)|^2 dx < \infty$$

The inner product is defined as

$$\langle f|g \rangle = \int_a^b f(x)^* g(x) dx < \infty$$

4.5 Properties of Hilbert Spaces

- Triangle Inequality: $\forall x, y, z, \text{dist}(\vec{x}, \vec{z}) = \text{dist}(\vec{x}, \vec{y}) + \text{dist}(\vec{y}, \vec{z})$

- Cauchy-Schwartz Inequality: $|\langle x|y\rangle|^2 \leq \|x\|^2\|y\|^2$

Equality exist only if x & y are linearly dependent.

4.6 Modeling Quantum Systems

Most quantum computation takes place in \mathbb{C}^n .

4.7 Ray

Ray is a set of all scalar multiples of some non-zero vectors that pass through the origin.

Ray of $a \neq 0 \equiv [a] = \{\alpha a \mid \alpha \in \mathbb{C}\}$ (α : global phase)

Every possible quantum state can be represented as a unit vector in H .

For each $\vec{v} \in H$, \exists infinite $e^{i\theta}\vec{v}$ rotated vectors. ($\|e^{i\theta}\vec{v}\| = 1$)

4.8 O in H

- O is not a quantum state because it's is not normalizable,
- Every other vector correspond to a quantum state.
- Scalar multiples of a vector represents the same state.
- The collection of rays $\{[a]\}$ form a complex projective sphere with one to one quantum correspondence.
- However, this complex projective sphere is not a vector space.

4.9 Interacting with these Vectors

1. Identify a unit vector $\hat{v} \in H$ of a quantum states
2. Apply unitary transformation
3. Renormalize vectors

Projective sphere collapses entire ray onto a complex point

Chapter 5

Linear Transformation

5.1 Linear Transformation

Linear Transformations map vectors from one vector space to another

Linearity $T(c\vec{v}) = cT(\vec{v})$ & $T(v_1 + v_2) = T(v_1) + T(v_2)$
where c is the domain scalar and \vec{v} is the domain vector.

Identity $I\vec{v} = \vec{v}$

Zero $0(\vec{v}) = 0$

Scale $S_c(\vec{v}) = c\vec{v}$

Projection on to \hat{x}_k $P_k(\vec{v}) = \vec{v}_k \hat{x}_k$

Projection on to \hat{n} $P_{\hat{n}}(\vec{v}) = (\vec{v} \cdot \hat{n})\hat{n}$

Differentiation $D(\psi) \equiv \psi'$

Anti-differentiation $\int^x(f) \equiv \int^x f(x')dx'$

Multiplication by matrix of constants $T_A(\vec{v}) \equiv A\vec{v}$

5.2 Role of Bases

For $\vec{v} = \sum_{k=1}^n \beta_k b_k$, $T\vec{v} = \sum_{k=1}^n \beta_k T(b_k)$

To write T as a matrix, write $T(b_k)$ in a row of vectors and expand vertically

$$T\vec{v} = (T(b_0), T(b_1) \dots) \begin{pmatrix} b_0 \\ b_1 \\ \vdots \end{pmatrix}$$

5.3 Dependence of Matrix on Basis

For $T\vec{v}$, T & \vec{v} have to be in the same basis ($w = T\vec{v}$; $w|_A = T|_A(\vec{v}|_A)$; $w|_B = T|_B(\vec{v}|_B)$)

5.4 Matrix M_T in a Non-Standard Basis

$T|_B = (T(b_0)|_B, \dots)$ with $b_{k|B} = b_k$

5.5 Transformation in an Orthonormal Basis

For an orthonormal basis B , $T_{jk|B} = \langle \hat{b}_j | T(\hat{b}_k) \rangle$

5.6 The Adjoint of a Matrix

$M^\dagger \equiv (M^T)^*$ for which $(M^T)_{jk} = M_{kj}^*$

5.7 Unitary Operators

Unitary operators are associated with quantum gates.

U is unitary if it preserve inner products for all vectors \vec{v}, \vec{w} .

This implies $\|A\vec{v}\| = \|\vec{v}\|$ and its matrix has orthonormal rows and columns.

1. For basis $B = \{b_k\}_{k=1}^n$, $\langle U(b_j) | U(b_k) \rangle = \langle b_j | b_k \rangle = \delta_{jk}$
2. $U^\dagger U = U U^\dagger = I$

Ex. $R_{\frac{\pi}{2}}$ and Phase change gates.

5.8 Non-Unitary Operators

- Scaling
- Projection Operator

5.9 Hermitian Operators

Hermitian operators are associated with measurements.

For all bases, $M^\dagger = M$

Chapter 6

The Experimental Basis of Quantum Computing

6.1 Spin 1/2 Quantum Mechanics

The vector space for spin $\frac{1}{2}$ fermions are 2-dimensional with linear combinations as sums.

Spin $\frac{1}{2}$ vectors can represent classical 0 & 1 as well as superposition.

6.2 Naive Electron Spin Definition

1. Angular Momentum, S , scalar
2. Orientation, \hat{S} , vectors with $S = (\frac{\sqrt{3}}{2}\hbar)\hat{n}_s$, where $\hat{n}_s = \frac{s}{|s|}$

6.3 Spherical Representation

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} r \\ \theta \\ \phi \end{pmatrix}; \hat{n} = (1, \theta, \phi)_{sph}$$

6.4 Electron Spin z-Projection

Measuring the z- projection of a soup of randomly oriented e^- yields 50 % $+\frac{\hbar}{2}$ & $-\frac{\hbar}{2}$ instead of a continuum between $\pm\frac{\sqrt{3}}{2}\hbar$. The states persist for future measurements.

This is because $\Delta x \Delta p \leq \frac{\hbar}{2}$ (Heisenberg's Uncertainty Principle).

Similar results are found for S_x & S_y

6.5 Follow up $|+\rangle_z$ in S_x

Measuring $|+\rangle_z$ in S_x yield the same result, 50-50. The state persists for future measurements.

6.6 Follow up $|+\rangle_x$ in S_z

Measuring this yields 50 % $|+\rangle_z$ & $|-\rangle_z$, even though $|+\rangle_z$ was selected in the above measurements.

A S_a measurement collapses into 1 of 2 allowable eigenvalues of the observable S_a .

In fact, any pairs of directions are incompatible observables.

6.7 Construction of Hilbert Space

Measurements show that $|-\rangle_x$ contains a portion of the original $|+\rangle$ & $|-\rangle$.

$$|+\rangle_x = \alpha|+\rangle + \beta|-\rangle.$$

These vectors will be normalized in a projective sphere.

6.8 Representing Spin

The (r, θ, ϕ) real vector is now represented by (α, β) complex vector space with basis $|+\rangle$ & $|-\rangle$.

1. $|+\rangle$ & $|-\rangle$ are linearly independent of one another, instead of \pm of the same basis vector.
2. \hat{a} can be written as linear combination of \hat{b} , instead of being linearly independent.

6.9 Measuring Spin theta from Standard Axis

Measuring spin θ away from S_a yields P of $\cos^2(\frac{\theta}{2})$ of getting $|+\rangle$ and P of $\sin^2(\frac{\theta}{2})$ of getting $|-\rangle$.

Non-zero azimuthal ϕ will not change the result.

* ϕ is the angle of the vector with the plane orthogonal to S_a .

*Two polar opposite direction in \mathbb{R}^3 correspond to two orthonormal vectors in \mathbb{C}^2 . This is the basis of the spin state.

Chapter 7

Time Independent Quantum Mechanics

7.1 Particle Energy and Position

E_k takes on discrete values. This helps determine the probability curve of the location of the particle.

7.2 Stern-Gerlach Apparatus

This shoots a silver atom through a magnetic field. A plate measures deflection. This is the physical system of quantum mechanics.

7.3 First Postulate of Quantum Mechanics

7.4 Trait #1: The State Space

Any system S has an associated Hilbert space H . Each physical state in S correspond to some ray in H (a point on the projective sphere of H).

physical state $\in S \leftrightarrow \vec{v} \in H$

These vectors in the space is represented as $|\psi\rangle$.

7.5 Fundamental State Space for Quantum Computing

The spin $\frac{1}{2}$ state space with $|+\rangle_z$ & $|-\rangle_z$ as natural basis ket of a 2-dimensional complex Hilbert space form a vector space of complex ordered pairs with the usual inner product.

$$H \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix} |\alpha, \beta \in \mathbb{C} \text{ with } |+\rangle \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |-\rangle \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Any physical states can be described as

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|+\rangle + \beta|-\rangle, \text{ where}$$

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

7.6 Orthonormality Expression

$$\begin{aligned} \langle +|+\rangle &= \langle -|-\rangle = 1 \\ \langle +|-\rangle &= \langle -|+\rangle = 0 \end{aligned}$$

7.7 The x-Basis for H

$$\begin{aligned} |+\rangle_x &= \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ |-\rangle_x &= \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \end{aligned}$$

7.8 Reasoning for Complex Vector Space

Measurements dictates that $|+\rangle$ electrons has 50% being up & spin down in right-angled basis. However, all 3 basis must be able to be represented as linear combination of the other. Real vector space cannot represent this, therefore complex vector space are used. if there is 1 more axis, quaternions would be used.

7.9 Second Postulate of Quantum Mechanics

7.10 Trait #2: The Operator for an Observable

An observable quantity A correspond to an operator (linear transformation) in H . This matrix is always related to a Hermitian.

For Observable $A \in S$,

$$T_A: H \text{ linear} \quad \& \quad T_A^\dagger = T_A$$

7.11 Completeness of the Eigenbasis

Eigenvectors of an observable span the state space

7.12 The Observable S_z

$S_z = \sigma_z = \frac{\hbar}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ represents

1. the observable “spin projected onto the z-axis”
2. the associate linear operator
3. the matrix of the operator

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

These are Pauli spin matrices (eigenvalues diagonal matrix).

7.13 Third Postulate of Quantum Mechanics

7.14 Trait #3: Eigenvalues of an Observables

The only possible measurements of an observable quantity A are eigenvalues of the operator's matrix.

7.15 Eigenvectors and Eigenvalues

For real or complex M , with $\vec{u} \neq 0$, $M\vec{u} = a\vec{u}$

\vec{u} is the eigenvector, a is the eigenvalues.

$$\{\vec{u}_{ak} \leftrightarrow a_k\}_{k=1}^{n \text{ or } \infty}$$

Uniqueness Degenerate eigenvalues have non-unique eigenvectors.

Diagonality The eigenvectors as basis of the space (eigenbasis) only when the matrix is diagonal.

7.16 Trait #3': Eigenvectors and Eigenvalues of S_z

The only possible outcome of A are the solutions to the eigenvector-value equation

$$T_A|\vec{v}_k\rangle = a_k|\vec{v}_k\rangle$$

Eigenvalues with non-unique eigen-kets are degenerate observable.

Eigenvectors of S_z are $(1, 0)^T$ & $(0, 1)^T$.

7.17 Computing Eigenvectors and Eigenvalues

7.18 Eigenvalue Theorem

For matrix M , the eigenvalues are solution to the system of simultaneous equations in the unknown λ

$$\det(M - \lambda I) = 0$$

To solve for eigenvector:

1. Plug in 1, solve
2. For complex vectors, split the variable into $a+bi$
3. If solution is a contradiction, plug in 0 instead

7.19 Summary of Eigenvectors and Eigenvalues for spin 1/2 Observables

The eigenvalues and eigenvectors for $S_z, S_x, \& S_y$ are:

$$S_z : +\frac{\hbar}{2} \leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad -\frac{\hbar}{2} \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$S_x : +\frac{\hbar}{2} \leftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad -\frac{\hbar}{2} \leftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$S_y : +\frac{\hbar}{2} \leftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \quad -\frac{\hbar}{2} \leftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$$

Expressed explicitly in terms of z-basis vectors, we find

$$S_z : +\frac{\hbar}{2} \leftrightarrow |+\rangle, \quad -\frac{\hbar}{2} \leftrightarrow |-\rangle$$

$$S_x : +\frac{\hbar}{2} \leftrightarrow |+\rangle_x = \frac{|+\rangle + |-\rangle}{\sqrt{2}}, \quad -\frac{\hbar}{2} \leftrightarrow |-\rangle_x = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

$$S_y : +\frac{\hbar}{2} \leftrightarrow |+\rangle_y = \frac{|+\rangle + i|-\rangle}{\sqrt{2}}, \quad -\frac{\hbar}{2} \leftrightarrow |-\rangle_y = \frac{|+\rangle - i|-\rangle}{\sqrt{2}}$$

7.20 Trait #4: Real Eigenvalues and Orthonormal Eigenvectors

An observable A in S will always correspond to an operator

1. with real eigenvalues
2. & unique eigenvectors form an orthonormal basis for H .

7.21 General States Expressed in Alternate Bases

$$|\psi\rangle = \alpha|+\rangle + \beta|-\rangle = \alpha|+\rangle_c + \beta|-\rangle_c$$

To get $|\psi\rangle$ in c-basis,

$$|\psi\rangle = \begin{pmatrix} {}_c\langle +|\psi\rangle \\ {}_c\langle -|\psi\rangle \end{pmatrix}$$

7.22 Orthonormal Basis in Higher Dimensions

For an n -dimensional state space, the orthonormal basis is $|\vec{v}_k\rangle_{k=1}^N$

7.23 Trait #5: Closure (Completeness) Relation

Any $\{|\vec{v}_k\rangle\}$ for our Hilbert space H satisfies the relation

$$|\psi\rangle = \sum_{k=1}^n \langle \vec{v}_k | \psi \rangle |\vec{v}_k\rangle = \sum_{k=1}^n (|\vec{v}_k\rangle \langle \vec{v}_k|) |\psi\rangle = I |\psi\rangle$$

* The eigenvectors of any observable satisfies the closure relation.

7.24 Fourth Postulate of Quantum Mechanics

7.25 Trait #6: Probability of Outcome

For a system in the normalized state $|\psi\rangle$, a state is expanded along the eigenbasis $\{|\vec{v}_k\rangle\}$ of some observable A

$$|\psi\rangle = \sum_{k=1}^n c_k |\psi\rangle_k, \text{ where } c_k \text{ is the amplitude}$$

then the probability that a measurement of A yielding a non-degenerate eigenvalue and its associated eigenvectors is $|c_k|^2$.

$P(a_k)_{|\psi\rangle} = |\langle a_k | \psi \rangle|^2 = c_k^* c_k = |c_k|^2$, where a_k is the measurement, and ψ the state of the system

7.26 Fifth Postulate of Quantum Mechanics

7.27 Trait #7: Post-Measurement Collapse (complex inner product)

If the measurement of an observable of system S results in eigenvalue a_k , then the system collapse probabilistically into an eigenvectors associated with a_k . Further measurement collapses back to a_k with 100% certainty.

7.28 Dirac's Bra-ket Notation

$\langle bra | ket \rangle$, where bra is the Hermitian conjugate

$$|\psi\rangle = \langle\psi|^\dagger \text{ and } \langle\psi| = |\psi\rangle^\dagger$$

7.29 Transforming Ket to Bra

1. Turn all kets (left vectors into bras)
2. Take complex conjugate of any scalars
3. Form inner products
4. Use distributive property to combine bra & ket

7.30 The Bra Space (Adjoint of a ket)

The bra space is a different vector space from the ket space. It is an isomorphism in finit dimensions.

7.31 The Adjoint of an Operator

For A in the ket space, $\exists A^\dagger$, where

$$\langle\psi|A^\dagger \rightarrow \langle\emptyset|. \text{ Notice that, } \langle\emptyset| = |\emptyset\rangle^\dagger$$

7.32 Trait #8: Adjoint Conversion Rules

The bra space & the ket space can be mapped onto one another using the adjoint operator (\dagger).

1. $\langle\psi| \rightarrow \langle\psi|^\dagger = |\psi\rangle$

$$2. |\psi\rangle \rightarrow |\psi\rangle^\dagger = \langle\psi|$$

$$3. c \rightarrow c^\dagger = c^*$$

$$4. A \rightarrow A^\dagger$$

$$5. (AB)^\dagger \rightarrow B^\dagger A^\dagger$$

7.33 Expectation Values

The mean of multiple measurements: $\bar{m} = \frac{1}{N} \sum_{j=1} m_j$

The law of large numbers dictates that $\lim_{N \rightarrow \infty} \bar{m} = \mu$

The probability of collapse $|c_k|^2$ is seen by accumulate multiple instances.

$$\mu = \langle A \rangle_{|\psi\rangle} \equiv \sum_k |c_k|^2 a_k$$

“ The expectation value of state ψ when measured under observable A is μ . ”

7.34 Trait #9: Expectation Value Theorem

$$\langle A \rangle_{|\psi\rangle} = \langle\psi|A|\psi\rangle$$

where A is the Hermitian observable

Chapter 8

Time Dependent Quantum Mechanics

Time evolution mechanics represents noise or predictable changes in the system.

8.1 The Hamiltonian

The Hamiltonian describes the total energy of the system.

8.2 Trait #10: Constructing the Hamiltonian

1. Put \mathcal{H} (LHS), classical energy in terms of classical concepts (RHS)
2. Change \mathcal{H} to H , and classical variables to quantum operators.

For example, classical (x, y, z) \rightarrow quantum (X, Y, Z).

8.3 Classical Hamiltonian (1/2 Spin)

A stationary e^- in a constant magnetic field has

$$\mathcal{H} = -\gamma \hat{B} \cdot S = -\gamma \hat{B} \cdot S_z$$

γ is the gyromagnetic ratio

$\hat{B} = B\hat{z} = \begin{pmatrix} 0 \\ 0 \\ B \end{pmatrix}$ is the magnetic field vector in the +z direction

$S = \begin{pmatrix} S_x \\ S_y \\ S_z \end{pmatrix}$ is the intrinsic angular momentum (spin vector)

8.4 Quantum Hamiltonian

Replace classical variables with quantum operators, we get

$$H = -\gamma B S_z = -\gamma B \frac{\hbar}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

8.5 Energy Eigenkets

The eigenvectors of H is also known as energy eigenkets.

Rearrange & substitute from above the eigenvectors-eigenvalues relation

$$H|+\rangle = (-\frac{\gamma B \hbar}{2})|+\rangle; H|-\rangle = (\frac{\gamma B \hbar}{2})|-\rangle$$

\therefore When measuring the energy of the system, we get $-\frac{\gamma B \hbar}{2}$ (minimum PE) for $|+\rangle$ and $\frac{\gamma B \hbar}{2}$ (maximum energy) for $|-\rangle$.

8.6 Trait #11: Quantization of Energy

The only allowable energies of a quantum system are the eigenvalues of the Hamiltonian.

8.7 Sixth Postulate of Quantum Mechanics

Time-dependent state: $|\psi\rangle \rightarrow |\psi(t)\rangle$

For which $|\psi(t)\rangle = \sum_{k=0}^{n-1} c_k(t) |\vec{v}_k\rangle$

At fixed time, $c'_k \equiv c_k(t')$

8.8 Trait #12: Time-Dependent Schrodinger Equation

The time evolution of a state vector is governed by the Schrodinger

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = H(t) |\psi(t)\rangle \quad (1)$$

However, H is time-independent for our purpose.

The time-independent Schrodinger equation set $A = H$. This is in the eigenvectors-eigenvalues form.

$$H|\vec{v}_k\rangle = a_k |\vec{v}_k\rangle$$

(2)

Solving this gives the eigenkets and the associated eigenvalues for the time-dependent Schrodinger equation.

8.9 Solving the Schrodinger Equation

1. Solve (2) for $\{E\}_k$ and the associated $\{|E\rangle\}$.
2. Expand $|\psi\rangle$ along the energy basis.

$$|\psi\rangle = \sum_k c_k |E_k\rangle$$

3. Solve the differential (1) for time-dependent amplitude, $c_k(t)$.

$$c_k(t) = c_k e^{\frac{-itE_k}{\hbar}}$$

4. Put c_k back into the sum in the second step

$$|\psi(t)\rangle = \sum_k c_k e^{\frac{-itE_k}{\hbar}} |E_k\rangle$$

8.10 Trait #13: Stationary States

An eigenstate of the Hamiltonian operator evolves in a way that its measurement outcome does not change. It remains the same.

For spin $\frac{1}{2}$ system, the stationary states are $|+\rangle$ & $|-\rangle$.

$$|\psi(t)\rangle = e^{i\phi t} |a\rangle \cong |a\rangle = |\psi\rangle$$

8.11 General Technique for Computing Time-Evolved States

8.12 Trait #14: Evolution of any Observable

1. Solve the Schrodinger equation
2. Take the inner product with the desired eigenket $|\vec{v}_j\rangle$ of \mathcal{A}

$$\alpha_j(t) = \langle \vec{v}_j | \psi(t) \rangle$$

3. Square to get the probability of \mathcal{A} producing α_k at time t .

$$P(\alpha(t))_A = |\alpha_j(t)|^2 = \alpha_j(t)^* \alpha_j(t)$$

8.13 Larmor Precession

Combine time evolution & expectation values to relate 3-d real classical angular momentum vector to 2-d complex quantum state vector.

$$|\psi(t)\rangle = c_1 e^{it(\frac{\gamma B}{2})} |+\rangle + c_2 e^{-it(\frac{\gamma B}{2})}$$

8.14 Rewriting $|\psi\rangle$

Converting to polar form, rearranging & substituting, we get

$$|\psi(t)\rangle = \begin{pmatrix} ce^{i\phi(t)} \\ se^{-i\phi(t)} \end{pmatrix}, \text{ where } \phi(t) = \frac{1}{2}(\omega + \phi_0)$$

with $\omega = \gamma B$ and $\phi = \phi_1 - \phi_2$ (relative phase)

8.15 Convenient Angle

$$cs = \frac{\sin(\theta)}{2}$$

and

$$c^2 - s^2 = \cos(\theta)$$

8.16 Expectation Value at Time t

$$\langle S_z \rangle_{\psi(t)} = \frac{\hbar}{2} \cos(\theta)$$

$$\langle S_y \rangle_{\psi(t)} = -\frac{\hbar}{2} \sin(\theta) \sin(\omega t + \phi_0)$$

$$\langle S_x \rangle_{\psi(t)} = \frac{\hbar}{2} \sin(\theta) \cos(\omega t + \phi_0)$$

$$s(t) = \begin{pmatrix} \langle S_x \rangle_{\psi(t)} \\ \langle S_y \rangle_{\psi(t)} \\ \langle S_z \rangle_{\psi(t)} \end{pmatrix} = \begin{pmatrix} \sin\theta \cos\phi(t) \\ -\sin\theta \sin\phi(t) \\ \cos\theta \end{pmatrix}$$

- θ is the real angle between $s(t)$ & the z-axis in \mathbb{R}^3 . $\frac{\theta}{2}$ expresses $|\psi\rangle$ in \mathbb{C}^2 .
Domain: $(0 \leq \frac{\theta}{2} \leq \frac{\pi}{2})$. Range: $(0 \leq \theta \leq \pi)$
- ω (Larmor frequency) = γ (gyromagnetic ratio) B (magnetic field magnitude)
- $\phi_0 = \phi_1 - \phi_2$ (relative phase)

Chapter 9

The Qubit

9.1 Vector Space $B = B^2(B \equiv \{0, 1\})$

$$B = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

\oplus is mod-2 addition (XOR).

Mod-2 Inner Product (pairing as inner product is not positive definite)

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \odot \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = x_1 \cdot x_2 \oplus y_1 \cdot y_2$$

$$\|x\| = |x| = \sqrt{x \odot x}$$

Note that $\| \begin{pmatrix} 0 \\ 1 \end{pmatrix} \| = \| \begin{pmatrix} 1 \\ 0 \end{pmatrix} \| = 1$ and $\| \begin{pmatrix} 0 \\ 0 \end{pmatrix} \| = \| \begin{pmatrix} 1 \\ 1 \end{pmatrix} \| = 0$

$(1, 0)^T$ & $(0, 1)^T$ are the orthonormal basis.

9.2 Definition of a Classical Bit

A bit is the vector space B .

9.3 Definition of Bit Value

A bit's value is any unit vector in B , which includes $(1, 0)^T$ & $(0, 1)^T$.

9.4 Alternate Definition of a Bit

A bit is a variable superposition of $[0]$ & $[1]$ of B .

$x = \alpha[0] + \beta[1]$, where $\alpha^2 \oplus \beta^2 = 1$

9.5 Definition of a Classical Logical Operator

A logical operator is a linear transformation of \mathcal{B} that maps one unit vector to another.

Unary gate with 1 input

Binary gate with 2 inputs

Constant-[0] $A(x) = [0]$

Constant-[1] $A(x) = [1]$

Negation (NOT) $A(x) = \neg x$ (reversible)

Identity $A(x) = Ix = x$ (reversible)

* An operator is reversible \iff its matrix is unitary.

9.6 Unitary Properties

1. Preserve length: $\|A\vec{v}\| = \|\vec{v}\|$
2. Preserve inner product: $\langle A\vec{v} | A\vec{w} \rangle$
3. Rows or columns are orthonormal

9.7 Definition of a Qubit

A qubit is the vector space \mathcal{H}

9.8 Alternate Definition of a Qubit

A qubit is a variable superposition of $|0\rangle$ & $|1\rangle$ in \mathcal{H} .

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$

9.9 Definition of Qubit Value

The value of a qubit is any unit vector in \mathcal{H}

9.10 Computational Basis State (CBS)

$$|+\rangle_a = |0\rangle_a; |-\rangle_a = |1\rangle_a$$

9.11 Global Phase Factors

$$e^{i\theta}|\psi\rangle = |\psi\rangle$$

9.12 Definition of a Quantum Logical Operator

A logical operator is a linear transformation of \mathcal{H} that maps one unit vector to another.

Quantum Unary Operator can be represented a 2×2 matrix.

*All quantum operators are unitary.

9.13 Bit Flip QNOT (X)

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\boxed{X}} \beta|0\rangle + \alpha|1\rangle$$

9.14 Phase Flip (Z)

$$Z|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$$

Z changes the relative phase of the two by π

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\boxed{Z}} \alpha|0\rangle - \beta|1\rangle$$

9.15 Bit and Phase Flip (Y)

$$Y|\psi\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = -i \begin{pmatrix} \beta \\ -\alpha \end{pmatrix} \cong \begin{pmatrix} \beta \\ -\alpha \end{pmatrix}$$

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\boxed{Y}} -i(\beta|0\rangle - \alpha|1\rangle)$$

* All unary operator takes the form $(\vec{\omega} \cdot \hat{n})$, where

$$\begin{pmatrix} \omega_x \\ \omega_y \\ \omega_z \end{pmatrix}; \quad \hat{n} = \begin{pmatrix} \hat{n}_x \\ \hat{n}_y \\ \hat{n}_z \end{pmatrix} \text{ real spin vector}$$

9.16 Hadamard Gate (H)

$$H|\psi\rangle = \frac{1}{\sqrt{2}}(\alpha + \beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha - \beta)|1\rangle$$

$$H|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$$

9.17 Measurement

The probability of collapse for $|\psi\rangle$ into state $|c\rangle$

$$P(|\psi\rangle) \searrow |c\rangle$$

9.18 Phase-Shift Gates (R_θ , S and T)

$$R_\theta|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ e^{i\theta}\beta \end{pmatrix}$$

$$S = R_{\frac{\pi}{2}} \text{ and } T = R_{\frac{\pi}{4}}$$

9.19 Basis Conversion Theorem

Quantum gates map one orthonormal CBS to another.

For unitary U, $\langle x|U^\dagger U|y\rangle = \langle x|y\rangle = \delta_{xy}$

9.20 Combining Gates

For $|a\rangle_x$, $HXH = Z$

$$X^2 = Y^2 = Z^2 = -iXYZ = iZYX = I$$

$$\therefore X = iYZ, Y = iZX, Z = iXY$$

Non-identitcal Pauli matrices anti-commute: $\omega_i\omega_j = -\omega_j\omega_i$

*Gates operate left to right, whereas operator algebra operates right to left.

9.21 The Bloch Sphere

$|\psi\rangle$ can be written in polar form.

$$|\psi\rangle = \begin{pmatrix} ce^{i\phi(t)} \\ se^{-i\phi(t)} \end{pmatrix}, \text{ where } c^2 + s^2 = 1$$

$$c = \cos\frac{\theta}{2}; s = \sin\frac{\theta}{2}$$

9.22 Definition of the Bloch Sphere

The sphere in $\mathbb{R}^3\{\hat{n} \mid |\hat{n}| = 1\}$ with coordinates

$$\hat{n} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \langle S_x \rangle_{\psi(t)} \\ \langle S_y \rangle_{\psi(t)} \\ \langle S_z \rangle_{\psi(t)} \end{pmatrix} = \begin{pmatrix} \sin\theta \cos\phi(t) \\ -\sin\theta \sin\phi(t) \\ \cos\theta \end{pmatrix}$$

For spherical coordinate,

$$\hat{n} = \begin{pmatrix} 1 \\ \theta \\ \phi \end{pmatrix}_{Sph} \in \text{Bloch sphere} \leftrightarrow |\psi\rangle = \begin{pmatrix} \cos\frac{\theta}{2} e^{i\phi(t)} \\ \sin\frac{\theta}{2} e^{-i\phi(t)} \end{pmatrix} \in \mathcal{H}$$

Chapter 10

Tensor Products

10.1 Tensor Products

To construct a new vector space

1. Specifying scalars & vectors
2. Defining vector addition & scalar multiplication
3. Confirming all the required properties
4. Defining inner product
5. Establishing the preferred basis

The tensor product of V ($\dim=l$) and W ($\dim=m$) is a new vector space with $\dim=lm$

10.2 Scalars of $V \otimes W$

Both V & W must have a common scalar set to form an inner product and that will be the scalar set for $V \otimes W$.

10.3 Vectors of $V \otimes W$

All of the separable tensor product of $V \otimes W$ are in the form $v \otimes w$. The general vector is the finite sum of this.

$$\sum_k \vec{v}_k \otimes \vec{w}_k, \text{ with } \vec{v}_k \in V \text{ and } \vec{w}_k \in W$$

This span the full space $V \otimes W$.

10.4 Terms and Definition

Product Space The tensor product of 2 vector space is called the tensor space

Tensors Vectors in the product state

Separable Tensors Vectors in space $V \otimes W$

Tensor Product Tensor product of spaces or separable vectors

10.5 Vector Addition

For any two tensors,

$$\zeta + \zeta' \equiv \sum_k \vec{v}_k \otimes \vec{w}_k + \sum_j \vec{v}'_j \otimes \vec{w}'_j$$

Tensor product distributes over sums in the component space.

$$(\vec{v} + \vec{v}') \otimes \vec{w} = \vec{v} \otimes \vec{w} + \vec{v}' \otimes \vec{w} \text{ and } \vec{v} \otimes (\vec{w} + \vec{w}') = \vec{v} \otimes \vec{w} + \vec{v} \otimes \vec{w}'$$

Commutativity is implied: $\zeta + \zeta' = \zeta' + \zeta$

10.6 Scalar Multiplication

Separable Tensor

$$c(\vec{v} \otimes \vec{w}) \equiv (c\vec{v}) \otimes \vec{w} \equiv \vec{v} \otimes (c\vec{w})$$

$$c(\zeta + \zeta') = c\zeta + c\zeta'$$

10.7 Inner Product in $V \otimes W$

If V & W have an inner product, the inner product of $V \otimes W$ is

$$\langle \vec{v} \otimes \vec{w} | \vec{v}' \otimes \vec{w}' \rangle \equiv \langle \vec{v} | \vec{v}' \rangle \cdot \langle \vec{w} | \vec{w}' \rangle$$

Dot product distributes as usual

10.8 Natural Basis for $V \otimes W$

10.9 Tensor Product Basis Theorem

If $V(\text{dim}=l)$ has basis $\{\vec{v}_k\}_{k=0}^{l-1}$ and $W(\text{dim}=m)$ has basis $\{\vec{w}_j\}_{j=0}^{m-1}$,

then $V \otimes W$ ($\text{dim}=lm$) inherits a natural orthonormal basis.

10.10 Proof of Basis Theorem

Spanning: any tensors can be expressed as linear combinations of $\vec{v} \otimes \vec{w}$.

For $\vec{v} \in V = \sum \alpha_k \vec{v}_k$ and $\vec{w} \in W = \sum \beta_j \vec{w}_j$,

$$\vec{v} \otimes \vec{w} = \sum \alpha_k \beta_j (\vec{v}_k \otimes \vec{w}_j)$$

Linear Independence & Orthonormality

$$\langle \vec{v}_k \otimes \vec{w}_j | \vec{v}_{k'} \otimes \vec{w}_{j'} \rangle = \langle \vec{v}_k | \vec{v}_{k'} \rangle \langle \vec{w}_j | \vec{w}_{j'} \rangle = \delta_{kk'} \& \delta_{jj'}$$

\therefore Any tensors in the product space can be expressed as

$$\vec{u} = \sum_{(k=0)(j=0)}^{(n-1)(m-1)} c_{kj} (\vec{v}_k \otimes \vec{w}_j)$$

10.11 Conventional Order of Tensor Basis

For \vec{v}_{ij} , i increments slowly & j quickly (row major).

10.12 Linear Operators on the Tensor Product Space

Natural Coordinates of Separable Tensors

For \vec{v} ($\text{dim}=l$) and \vec{w} ($\text{dim}=m$),

$$\vec{v} \otimes \vec{w} = \begin{pmatrix} \vec{v}_0 \vec{w}_0 \\ \vec{v}_0 \vec{w}_1 \\ \vdots \\ \vec{v}_{l-1} \vec{w}_{m-1} \end{pmatrix}$$

Natural Coordinates of Basis Vectors

$$\text{For } b_k \in V \otimes W, b_{k|B} = \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix}$$

\exists lm basis vectors for the product space.

Any natural basis vectors are made up of 2 separable natural bases.

Natural Coordinates of General Tensor

For tensor space with $\dim=lm$,

$$\zeta = \begin{pmatrix} \zeta_0 \\ \vdots \\ \zeta_{l-1} \end{pmatrix}$$

Tensor as Matrices

The basis can be put into a matrix

$$\begin{pmatrix} \zeta_{00} & \zeta_{01} & & \\ \vdots & \ddots & & \\ \zeta_{(l-1)0} & & a_{(l-1)(m-1)} & \end{pmatrix}$$

10.13 Linear Operators on the Tensor Product Space

Separable Operator

For $A: V \rightarrow V'$ & $B: W \rightarrow W', A \otimes B: V \otimes W \rightarrow V' \otimes W'$

On vectors, $[A \otimes B](\vec{v} \otimes \vec{w}) \equiv A\vec{v} \otimes B\vec{w}$

*Matrix tensor product follows the A-major format.

10.14 Matrix of General Operator

Any operator on the product space can be represented as sum of $\leq (lm)^2$ separable operators in the form P_{pq} with 1 at (p, q) and 0 everywhere, where $0 \leq p, q \leq lm$

10.15 Matrix Tensor Product

$$AB \otimes CD = (A \otimes C)(B \otimes D)$$

$$(a \times b \text{ matrix}) \otimes (c \times d \text{ matrix}) = (ac \times bd \text{ matrix})$$

- The product of unitary operators is unitary in the product space.
- The product of Hermitian operators is Hermitian in the product space.
- The product of invertible operators is invertible in the product space.

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$$

Chapter 11

Two Qubits and Binary Quantum Gates ($\mathcal{H}_A \otimes \mathcal{H}_B$)

11.1 Definition of Two Qubits

A bipartite system is the product space $\mathcal{H} \otimes \mathcal{H}$. This is also referred to as an order-2 system. The need for tensor product came from entanglement.

11.2 Definition of a Two-Qubit Value

The value of a bipartite system is any unit vector in $\mathcal{H} \otimes \mathcal{H}$.

11.3 Preferred Bipartite CBS

Bipartite system inherits separable products of component space. $|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle = |0\rangle^2$ (coordinate representation)

* \exists no alternative for general separable tensors.

*When expanding along a-basis, the b-basis kets have equal numbers of + & - terms except for the 0th CBS kets, which have all +.

11.4 Alternate Bipartite Bases

CBS can inherit from other orthonormal bases.

For example, $|0\rangle_x|0\rangle_x = |+\rangle|+\rangle = |++\rangle = |0\rangle_{\pm}^2$

11.5 Inherit Second Order Mixed CBS

It is possible to create $|0\rangle_a|0\rangle_b$ orthonormal product basis as long as a & b are orthonormal bases.

11.6 Non-Standard Second Order CBS in Natural Basis

For $|0\rangle_a = \alpha_a|0\rangle + \beta_a|1\rangle$ & $|0\rangle_b = \alpha_b|0\rangle + \beta_b|1\rangle$

Using the distributive property of tensor product

$$|0\rangle_a|0\rangle_b = \alpha_a\alpha_b|00\rangle + \beta_a\alpha_b|01\rangle + \alpha_b\beta_a|10\rangle + \beta_a\beta_b|11\rangle$$

11.7 Alternate Definition of Two Qubits

Two qubits are represented by a variable superposition of the four tensors basis vectors of $\mathcal{H} \otimes \mathcal{H}$.


$|\psi\rangle^2 = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$, where

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

11.8 Binary Quantum Operator Definition

A binary quantum operator is a unitary transformation U , on the qubit system $\mathcal{H} \otimes \mathcal{H}$.

11.9 Complete Description of Binary Quantum Operator

 show symbol of the gate

$|x\rangle|y\rangle$ define gate's action on CBS

\mathbf{M} construct matrix of the gate

$|\psi\rangle^2$ gate's action on a general state

\searrow measurement probabilities of the output registers.

11.10 Measurement of Separable Outputs

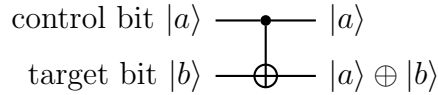
Probability of collapse is local and independent.

11.11 Quantum Entanglement (Non-separable outputs)

An entangled state in a product space is one that is not separable.

\therefore Measurements on entangled state are non-local

11.12 Controlled-NOT (CNOT Gate)



$$|y\rangle \rightarrow \begin{cases} |y\rangle, & \text{if } x=0 \\ -|y\rangle, & \text{if } x=1 \end{cases}$$

$$M_{CNOT} = (|00\rangle, |01\rangle, |10\rangle, |11\rangle)$$

$$CNOT(|\psi\rangle^2) = \alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + |10\rangle$$

Notice that γ and δ swap position.

11.13 Quantum Entanglement for CNOT

A separable bipartite state into CNOT does not usually result in a separable state out of CNOT.

*Separable operators allow separated components whereas non-separable state does not.

Control Register as CBS: separable output

Control Register as superposition: non-separable output

11.14 CNOT in Different CBS

For x-basis, B-register is the control & A is the target

11.15 Second Order Hadamard Gate

2nd-order H-gate is the tensor product of 2 Hadamard gates.

$$H^{\otimes 2} = H \otimes H$$

CBS states always map to separable states.

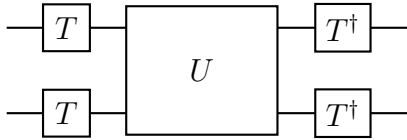
11.16 Condensed Form

$H^{\otimes 2} = \frac{1}{2} \sum_{y=0}^3 (-1)^{x \odot y} |y\rangle^2$, where \odot is mod-2 dot product.

$H^{\otimes 2}$ transform between z-CBS & x-CBS.

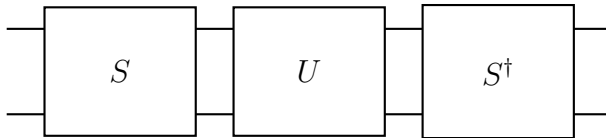
11.17 Circuits in Separable Basis

To operate circuit in alternate CBS, with operator in z-basis. First, apply T to transform from a-basis to z-basis & then T^\dagger after operator to convert back to a-basis:



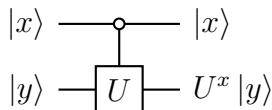
11.18 Circuits in Non-Separable Basis

To measure along a non-separable basis, define the circuit of z-basis, sandwich it between binary a-basis converter.



11.19 Controlled-U Gate

Apply U to target if CBS in control is 1.



where $U^0 = I$; $M_{CU} = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & U \end{array} \right)$

11.20 Separable Operators on Separable States

Separable operators map separable states to separable states. they preserve locality and are called local operators.

11.21 Separable Operators on Entangled States

Separable operators modify both qubits of the entangled state.

11.22 Trait #15: Born Rule for Bipartite States

If a bipartite state is factored relative to the A-register.

$$|\psi\rangle^2 = |0\rangle(\alpha|0\rangle + \beta|1\rangle) + |1\rangle(\gamma|0\rangle + \delta|1\rangle)$$

The measurement of the A-register will collapse according to

$$A \searrow 0 \Rightarrow B \searrow \frac{\alpha|0\rangle + \beta|1\rangle}{\sqrt{|\alpha|^2 + |\beta|^2}}$$

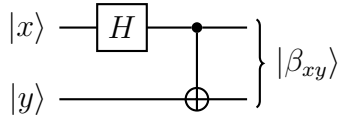
$$A \searrow 1 \Rightarrow B \searrow \frac{\gamma|0\rangle + \delta|1\rangle}{\sqrt{|\gamma|^2 + |\delta|^2}}$$

This solves the problem of non-normality.

11.23 Bell States Circuit

$$BELL = (CNOT)(H \otimes I)$$

$$|\beta_{xy}\rangle \rightarrow BELL(|x\rangle|y\rangle) = |\beta_{xy}\rangle$$



11.24 Binary Operators on Bell States

The Bell operator is unitary, \therefore Bell states form orthonormal basis

$$(I \otimes I)|\beta_{00}\rangle = |\beta_{00}\rangle$$

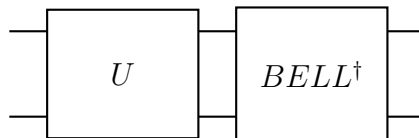
$$(X \otimes I)|\beta_{00}\rangle = |\beta_{01}\rangle$$

$$(Z \otimes I)|\beta_{00}\rangle = |\beta_{10}\rangle$$

$$(iY \otimes I)|\beta_{00}\rangle = |\beta_{11}\rangle$$

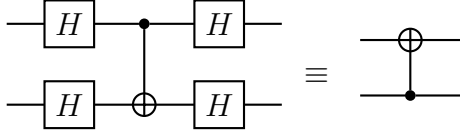
11.25 BELL as Basis Transform Operator

Measuring along Bell basis,



where $BELL^\dagger = (CNOT)^\dagger(H \otimes I)^\dagger = (H \otimes I)(CNOT)$

11.26 Upside Down CNOT Circuit



This works by transforming to x-basis, then perform CNOT (where the effect is opposite), then transform back to z-basis.

11.27 Order-3 Tensor Product

The product space can rely on second order construction.

$$W = (A \otimes B) \otimes C = A \otimes (B \otimes C),$$

where separable tensors $\vec{w} = a \otimes b \otimes c$

The dimension is the product of 3-dimensions

$$\dim(W) = \dim(A)\dim(B)\dim(C)$$

W has basis $\{\vec{w}_{jkl} \equiv a_j \otimes b_k \otimes c_l\}$,

where $\{a_j\}$, $\{b_k\}$, $\{c_l\}$ are bases of component space.

General tensors can be written in the form of linear combination.

$$\vec{w} = \sum_{j,k,l} c_{j,k,l} (a_j \otimes b_k \otimes c_l)$$

Separable operator distributes over tensors

$$[T_A \otimes T_B \otimes T_C](a \otimes b \otimes c) \equiv T_A(a) \otimes T_B(b) \otimes T_C(c)$$

11.28 Tripartite System Definition ($\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C = \mathcal{H}_{(3)}$)

Three qubits are the tensor product of $\mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H}$ and the value is any tensor with unit length in the product space

CBS in tripartite system can be represented in the same way

11.29 Trait #15': Born Rule for Tripartite States

If a tripartite system can be expressed as sum of 4 terms,

$$|\psi\rangle^3 = \sum_{k=0}^3 |k\rangle_{AB}^2 |\psi\rangle_C, \text{ C will be normalized}$$

$$A \otimes B \searrow |k\rangle^2 \Rightarrow C \searrow \frac{|\psi_k\rangle}{\sqrt{\langle\psi_k|\psi_k\rangle}}$$

Chapter 12

First Quantum Algorithms

12.1 Superdense Coding

This technique sends two classical bits through one classical bit.

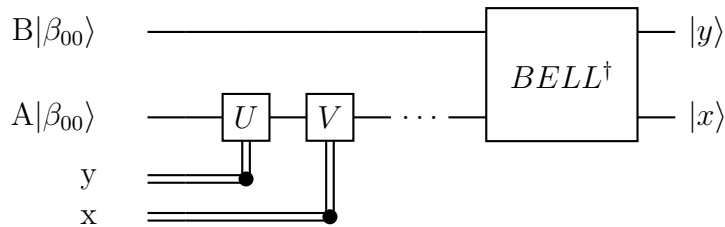
First, a Bell state (β_{00}) is prepared & separated. Then, depending on the desired number from 0-3, a unique set of gate is applied to the sender's qubit \mathcal{A} . After which, \mathcal{A} 's qubit is sent to \mathcal{B} . \mathcal{B} measures both qubit in the Bell basis with $BELL^\dagger$.

The table below refers to the gate applied.

\mathcal{A} to Send	\mathcal{A} Applies	Equivalent Binary Gate	New Bipartite State
"00"	(nothing)	$\mathbb{I} \otimes \mathbb{I}$	$ \beta_{00}\rangle$
"01"	X	$\mathbb{I} \otimes X$	$ \beta_{01}\rangle$
"10"	Z	$\mathbb{I} \otimes Z$	$ \beta_{10}\rangle$
"11"	iY	$\mathbb{I} \otimes Y$	$ \beta_{11}\rangle$

Note, iY = ZX

x, y is the encoded binary message



12.2 Quantum Teleportation

Quantum teleportation transport 1 quantum bit using 2 classical bits.

12.3 Application of Born Rule

As long as all register is in the same orthonormal basis, Born's rule will work.

12.4 Expanding Initial States along $BELL_{AC}$ basis

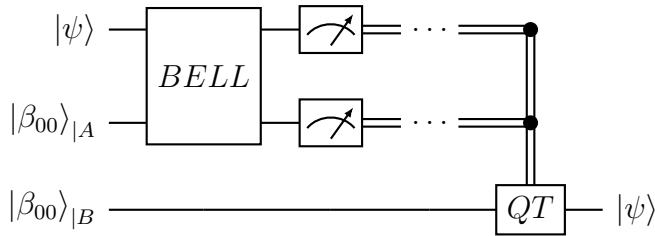
$$|\psi\rangle|\beta_{00}\rangle_{AB} = |\beta_{00}\rangle_{AC} \frac{\alpha|0\rangle_B\beta|1\rangle}{2} \dots$$

\mathcal{A} measures this state through $BELL^\dagger$, then send the result to \mathcal{B} .

12.5 B's Action from A's Message

\mathcal{B} Receives	\mathcal{B} Applies	\mathcal{B} Recovers
"00"	(nothing)	$ \psi\rangle$
"01"	X	$ \psi\rangle$
"10"	Z	$ \psi\rangle$
"11"	iY	$ \psi\rangle$

Notes that $iY = ZX$



12.6 Boolean Functions and Reversibility

Boolean function is a function with one or more binary digits as input and one or binary output.

Most boolean functions are irreversible

12.7 Unary Gates as Boolean Function

$$f : \{0, 1\} \rightarrow \{0, 1\} \text{ or } f : B \rightarrow B$$

Example of reversible unary include NOT and Identity

Example of irreversible unary include $[0]$ and $[1]$

12.8 Binary Gates as Boolean Functions

$$f : B^2 \rightarrow B$$

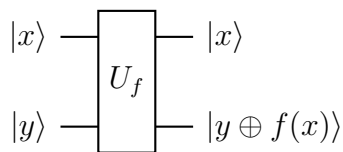
All two-bit cases are irreversible

12.9 Quantum Oracle for Boolean Functions

Oracle for Unary Functions

For $x \xrightarrow{f} f(x)$, a quantum analog must have

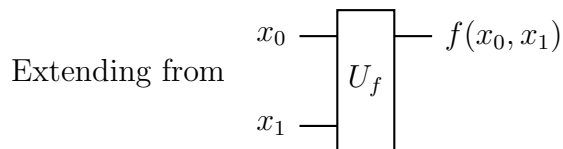
- two bits input
- two bits output
- unitary \therefore reversible
- computes f with proper inputs
- equally efficient



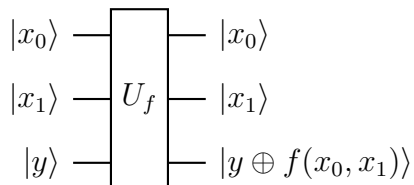
U_f for a CBS is always separable

* y is almost always set to 0 so $y \oplus f(x)$ would be always return $f(x)$

Oracle for Binary Functions



A three-in three-out oracle is defined by



- x_0 & x_1 is usually shortened as $|x\rangle^2$
- U_f is its own inverse
- $U_f = f(x)$ with $y = 0$

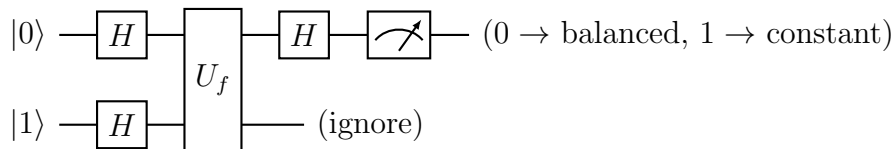
- $U_f(|x\rangle |0\rangle) = |x\rangle^2 |f(x)\rangle$

12.10 Deutsch's Algorithm

This determines whether a unary function is constant or balanced with a single query.

This takes advantage of two techniques:

1. Quantum Parallelism: Non-trivial superposition can explore both CBS at the same time. Bringing calculations out of the z-basis has this effect. Quantum entanglement also plays a big part
2. Phase Kick-back: Information of $f(x)$ from B is transferred to A. The process includes transforming both A & B to the x-basis, where phase-kickback could occur. When this is done, A will respond differently to constant v.s balanced function. This effect is visible when brought back to the z-basis.



Changing A invert the outcome

Changing B leads to inconclusive result.

Chapter 13

Multi-Qubit Systems and Algorithms

13.1 Higher Order Tensor Products

Notation \otimes and \prod

Product Space $W = \prod_{k=0}^{n-1} A_k$

Dimension $\dim(W) = \prod_{k=0}^{n-1} d_k$, where $d_k = \dim(A_k)$

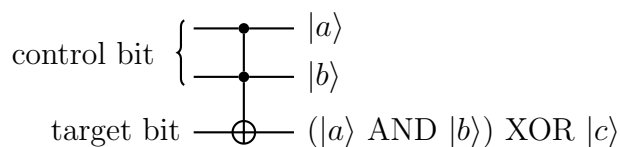
Separable Tensors $\{\prod_{j=0}^{n-1} a_j k_j\}_{k_0, \dots, k_{n-1}=0, \dots, d_0-1, \dots, d_{n-1}-1}$

Linear Combination $w = \sum c_{k_0, \dots, k_{n-1}} \{\prod_{j=0}^{n-1} a_j k_j\}$

Separable Operators $\prod_{k=0}^{n-1} T_k \prod_{k=0}^{n-1} \vec{v}_k = \prod_{k=0}^{n-1} T_k(\vec{v}_k)$

13.2 Toffoli Gate (CCX)

The CCX gate flip the last bit if both a & b = 1



For general tensors, the CCX gate flip the last two apmplitude.

n qubits are the vector space $\mathcal{H}_{(n)}$, and the value is any unit tensors in the product space.

$$\mathcal{H}_{(n)} = \prod_{k=0}^{n-1} \mathcal{H}$$

$$|x\rangle^n = |x_{n-1}, \dots, x_0\rangle$$
$$|x_{n-1} \dots x_0\rangle \left\{ \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \right\} \left[\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \right] \begin{array}{c} H |x_{n-1}\rangle \\ \vdots \\ H |x_0\rangle \end{array}$$

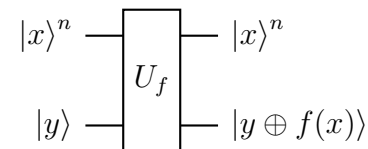
$$H^{\otimes n}|x\rangle^n = (\frac{1}{\sqrt{2}}))^n \sum_{y=0}^{2^{n-1}} (-1)^{x \odot y} |y\rangle^n, \text{ where } x \odot y = x[n-1] \cdot y_{n-1} \oplus \dots \oplus x_0 \cdot y_0$$

$H^{\otimes n}$ converts between x & z-basis in $\mathcal{H}_{(n)}$

x-basis CBS can be represented as $|x\rangle_{\pm}^n$

In z-basis, $|x\rangle_{\pm}^n$ has the same number of \pm except for $|0\rangle_{\pm}^n$

Quantum oracle for n-qubit is the quantum analog of n-bit boolean function.

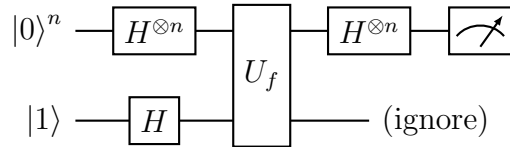


- U_f is its own inverse
- $U_f(|x\rangle|0\rangle) = |x\rangle^n|f(x)\rangle$
- Both has the same spatial circuit complexity

13.8 Deutsch-Jozsa Problem

Deutsch-Jozsa algorithm determines if an n -bit boolean function is constant or balanced. The quantum worst case n is an improvement from the 2^{n-1} classical worst case.

$$f\{0,1\}^n \rightarrow \{0,1\}$$



The algorithm uses quantum parallelism and phase kickback.

$|0\rangle$ for constant; anything else for balanced

13.9 Quantum vs. Classical Time Complexity

The classical time complexity is $2^{n-1} + 1$

The quantum time complexity is $\frac{n}{2} + 1$

With $N = 2^n$, classical is exponential to n & linear to N . Quantum is linear to n & logarithmic to N

13.10 Non-Deterministic Algorithm with small error $\epsilon \ll 1$

M-guess algorithm measures from a sample of registers. If all is 0 \rightarrow constant, else balanced. The error of predicting constant when everything else is balanced is small for constant large sample, even as n increases.

13.11 Deutsch-Jozsa Measurements

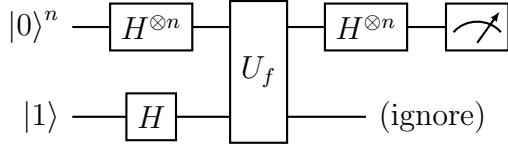
Not all balanced f has a corresponding x-CBS. However, the probability of measuring $|0\rangle_{\pm}^n$ is 0 if f is balanced

13.12 Bernstein-Vazirani Problem

For $f(x) = a \odot x_n$, this algorithm returns a in one try instead of n in classical computing.

a is an n -bit binary number & \odot is mod-2 dot product.

The circuit is the same as the Deutsch-Jozsa algorithm.



Compile the results from the $|0\rangle$ registers, we get α .

The classical complexity is linear in n and logarithmic in N . The quantum complexity is constant for both. $N = 2^n$ (encoded integer size)

The problem is non-deterministic because for $n-1$ guess, the last registers has 50% probability of being 0 or 1.

13.13 Trait #15”: Generalized Born Rule

For $(n+m)$ th order state $|\psi^{n+m}\rangle$ in the product space $A \otimes B = \mathcal{H}_{(n)} \otimes \mathcal{H}_{(m)}$, where $|\psi^{n+m}\rangle$ can be written as separable product of A CBS ket & general tensors in B.

$$|\psi\rangle^{n+m} = \sum_{k=0}^{2^n-1} |k\rangle_A^n |\psi_k\rangle_B^m$$

The probability of collapse for B given A observable is

$$A \searrow |k\rangle^n \Rightarrow B \searrow \frac{|\psi_k\rangle^m}{\sqrt{\langle \psi_k | \psi_k \rangle}} \text{ for } k = 0, \dots, 2^n-1$$

Chapter 14

Probability Theory

14.1 Outcomes

An outcome is the most basic result. A partition of legal outcomes must

1. be mutually exclusive
2. collectively represents every possible results of the experiment.

14.2 Events

An even is a subset of outcomes

Simple event is an event that contains exactly one outcome

Compound event is an event that contatins more than one outcome

14.3 Sample Space ω

The sample space is the set of all possible outcomes

14.4 Null Event \emptyset

The event consisting of no outcomes, empty set

14.5 Probability $P(\mathcal{A})$

Probability is the likelihood of certain events represented by positive numbers from 0 to 1.

14.6 Set Operations

Union \cup $\omega \equiv U_{x_k \in \{0,1\}} \{(x_0, \dots, x_{n-1})\}$

Intersections \cap Overlapping of two subset

Differences (- or /) $A - B = A \cap B^c$

Complement ($'$, c , \neg) Any element not in subset

*Outcomes can also be represented as vectors on the $(Z_k)^n$ vector space or integers from 0 to $k^n - 1$

14.7 Linear Independence

In a vector space, as set of vectors \vec{v} is linearly independent

$$c_0 \vec{v}_0 + \dots + c_{n-1} \vec{v}_{n-1} \Rightarrow c_k = 0$$

14.8 Span

The span of $\vec{v} = \{c_0 \vec{v}_0 + \dots + c_{m-1} \vec{v}_{m-1} | c_k \text{ are scalars}\}$

For mod-2 vectors $\{\vec{v}_{l0} + \dots + \vec{v}_{ls} | \vec{v}_{lk} \in \mathcal{S}\}$

14.9 Fundamental Probability Theory

14.10 The Axioms

For $\{\mathcal{E}\}$, the probability measure, $P()$, satisfies

1. All $P()$ values are non-negative

$$P(\mathcal{E}) \geq 0$$

2. The probability of something happening is certain

$$P(\omega) = 1$$

3. The probability of mutually exclusive events can be added

$$P\left(\bigcup_{k=0}^{n-1} \mathcal{E}\right) = \sum_{k=0}^{n-1} P(\mathcal{E}_k)$$

However, for mutually non-exclusive events

$$P(U_{k=0}^{n-1} \mathcal{E}) \leq \sum_{k=0}^{n-1} P(\mathcal{E}_k) \text{ (accounting for intersections)}$$

These axioms naturally leads to

- For any events, $P(\mathcal{E}) \leq 1$
- $P(\emptyset) = 0$
- If $\mathcal{E} \subseteq \mathcal{F}$, $P(\mathcal{E}) \leq P(\mathcal{F})$

14.11 Definitions in Finite Equiprobable Sample Space

Size of an Event

$$|\mathcal{E}| \equiv \# \text{ outcomes } \in \mathcal{E}$$

Probability of an Event

$$P(\mathcal{E}) = \frac{|\mathcal{E}|}{|\omega|}$$

14.12 Conditional Probability

For $\mathcal{E}|\mathcal{F}$, \mathcal{E} given \mathcal{F} is true,

$$P(\mathcal{E}|\mathcal{F}) = \frac{|\mathcal{E} \cap \mathcal{F}|}{|\mathcal{F}|}, \text{ whenever } \mathcal{F} \neq \emptyset$$

14.13 Bayes' Law

Dividing top & bottom by $|\omega|$

$$P(\mathcal{E}|\mathcal{F}) = \frac{P(\mathcal{E} \cap \mathcal{F})}{P(\mathcal{F})}, \text{ whenever } P(\mathcal{F}) \neq 0$$

14.14 Statistical Independence

Mutually exclusive means that two events cannot happen at the same time:

$$P(A \cap B) = 0$$

Independence means that the probability of seeing one won't affect the probability of seeing others: $P(A|B) = P(A)$

14.15 Two Independent Events

Substituting: $P(\mathcal{E}|\mathcal{F}) = P(\mathcal{E})$ into Bayes' Law

$$P(\mathcal{E} \cap \mathcal{F}) = P(\mathcal{E}) P(\mathcal{F})$$

*Note \cap here has different meaning than mutually exclusive

14.16 Multiple Independent Events

n events are independent if:

$$P\left(\bigcap_{1 \leq \dots \leq n} \mathcal{E}_{ki}\right) = \prod_{1 \leq \dots \leq n} P(\mathcal{E}_{ki})$$

14.17 Other Formulas

Events follows identity of Boolean Algebra

Probabilities:

$$P(\mathcal{E}) = P(\mathcal{E} \cap \mathcal{F}) + P(\mathcal{E} \cap \mathcal{F}')$$

$$P(\mathcal{E} \cap \mathcal{F}) = P(\mathcal{E}|\mathcal{F}) P(\mathcal{F})$$

14.18 Wedge and Vee Notations

$\wedge \rightarrow \cap$; $\vee \rightarrow \cup$; $\neg \rightarrow \text{c}$

Sets notations used for non-events sets

14.19 Applications to Deutsch-Jozsa

M and Guess sample M ; 2^n random events and test if $f(x') \neq f(x'') \Rightarrow$ balanced, else constant

14.20 Sampling with Replacement

$$P(\mathcal{S} \wedge \mathcal{B}) = P(\mathcal{S}|\mathcal{B}) P(\mathcal{B}) = \frac{1}{2^{M-1}} P(\mathcal{B})$$

where $P(\mathcal{S} \wedge \mathcal{B})$ is the probability of errors (f is balanced yet all guesses yields constant and $P(\mathcal{B})$ is the probability of f balanced

14.21 Sampling without Replacement

$$P(\theta) = P(\theta_{M-1} \wedge \dots \wedge \theta_0) = \prod_{k=0}^{M-1} \frac{2^{n-1} - k}{2^n - k}$$

where M is independent of n, number of inputs.

The numerator represents the #outcomes of 0 and the denominator represents the #outcomes in the sample space.

$$P(W \text{ without replacement}) = P(\mathcal{B}) \times 2 \prod_{k=0}^{M-1} \frac{2^{n-1} - k}{2^n - k}$$

This error rate of this is smaller than with replacement

14.22 Probability Algorithm

\mathcal{A} is probabilistic with error tolerance ϵ

14.23 Looping Algorithm

For looping algorithm, failure only occurs if all loop fails

14.24 Constant Time Complexity for Looping Algorithm

Assume \mathcal{A} is a probabilistic, looping algorithm with size N. If $P(\text{success})$ in a single loop is bounded away from 0.

$$P(\mathcal{S}) \geq p > 0$$

with p independent of the size N, then \mathcal{A} is a constant-time algorithm.

For $\mathcal{S}) \geq p$, for all $k \geq 1$,

$$P(\mathcal{S}_{tot}) = P(\neg \mathcal{S}_1) \dots P(\neg \mathcal{S}_T) = (1 - p)^T < \epsilon$$

where $P(\mathcal{S}_{tot})$ is the probability of a total failure

Because p & T is independent of size N, algorithm is constant time complexity (CTC)

To solve for integer T from $(1 - p)^T = \epsilon$,

$$T = \lfloor \log(\epsilon) / \log(1 - p) \rfloor + 1$$

Chapter 15

Computational Complexity

Computational complexity refers to the growth rate of an algorithm with respect to the size of the input.

Time complexity refers to the growth rate of running time of an algorithm whereas space complexity refers to the growth rate of hardware.

Space & time complexity together are referred to as computational complexity.

15.1 Big-O Growth

$$T_Q(N) = O(f(N))$$

$$\iff$$

$$\exists n_0, c \text{ s.t } T_Q(N) \leq c|f(N)|, \forall N \geq n_0$$

where $T_Q(N) \equiv$ time required by the algorithm Q to process N elements

This means that above a certain point, T_Q grows no faster than $c|f(N)|$. This is the upper bound of the growth rate for algorithm Q.

- Constant factor K can be ignored
- For polynomial time complexity, ignore all but the highest degree term

15.2 Ω Growth

$$T_Q(N) = \Omega(f(N))$$

$$\iff$$

$$\exists n_0, c \text{ s.t } T_Q(N) \geq c|f(N)|, \forall N \geq n_0$$

This means that above a certain point, T_Q grows no slower than $c|f(N)|$. This is the lower bound of the growth rate for algorithm Q.

15.3 Θ Growth

$$T_Q(N) = \Theta(f(N))$$

$$\iff$$

both

$$T_Q(N) = O(f(N)) \text{ and } T_Q(N) = \Omega(f(N))$$

15.4 Little-o Growth

$$T_Q(N) = o(f(N))$$

$$\iff$$

both

$$T_Q(N) = O(f(N)), \text{ but } T_Q(N) \neq \Omega(f(N))$$

15.5 Easy vs. Hard

Easy problems are those whose algorithms is polynomial time complexity.

Hard problems are those whose algorithms is exponential time complexity.

Quantum parallelism & entanglement offer exponential speed up to hard problems.

Two examples are Simon's algorithm and Shor's algorithm.

Chapter 16

Computational Basis States and Modular Arithmetic

16.1 Single Qubit Hilbert Space

One -qubit Hilbert Space, \mathcal{H} consists of the 2-D complex vector space. The typical states is a superposition of the two CBS.

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

16.2 Multi Qubit Hilbert Spaces

Multi qubit states operate in 2^n -dimensional Hilbert space $\mathcal{H}_{(n)}$

$$|x\rangle^n = \bigotimes_{k=0}^{n-1} |x_k\rangle$$

where $|x_k\rangle$ is either $|0\rangle$ or $|1\rangle$.

The index is in decreasing order because the right-most bit correspond ot the least significant bit of the binary number $x_{n-1}...x_0$

16.3 \mathbb{Z}_N , or mod N Arithmetic

\mathbb{Z}_N is the finite group consisting of N integers from 0 to N-1.

$$\mathbb{Z}_N \equiv \{0, 1, 2, \dots, N-1\}$$

The addition modulo N is the remainder after dividing by N

- $x + y \pmod{N} \equiv (x + y) \% N$
- $-x \pmod{N} \equiv (N - x)$
- $x - y \pmod{N} \equiv (x + -y) \% N$

For mod-2, the addition operator is the XOR operation.

\mathbb{Z}_2 correspond to the CBS of \mathcal{H}_1

16.4 $(\mathbb{Z}_2)^n$ with \oplus Arithmetic

The set $(\mathbb{Z}_2)^n$ is the n-tuples that have 0 or 1 as their coordinates.

$(\mathbb{Z}_2)^n$ is a vector space because it satisfies all the conditions of a vector space.

16.5 The group \mathbb{Z}_{2n}

\mathbb{Z}_{2n} has 2^N elements

Each x in (\mathbb{Z}_{2n}) can be represented as n binary digits

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

The addition operation is the bitwise \oplus operator.

$$x \oplus y \equiv \sum_{k=0}^{n-1} (x_k \oplus y_k) 2^k$$

For any $x \in (\mathbb{Z}_{2n}, \oplus)$

$$x \oplus x = 0 \quad \therefore \quad x = -x$$

16.6 Connection Between $(\mathbb{Z}_2)^n$ and (\mathbb{Z}_{2n})

$(\mathbb{Z}_2)^n$ and (\mathbb{Z}_{2n}) is the same group. They are isomorphic

$$(\mathbb{Z}_2)^n \cong (\mathbb{Z}_{2n})$$

16.7 General Notations

For $|x\rangle^n$, n represents the number of registers in the state, not the dimension of the space. The dimension would actually be 2^n . This means that $|x\rangle^n \otimes |y\rangle^m$ will result in $|xy\rangle^{n+m}$

For x, y in \mathbb{Z}_{2n} , the mod-2 sum can be taken inside a ket $(x \oplus y)$

Chapter 17

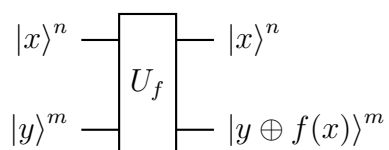
Quantum Oracle

Oracles are called black boxes, and they have to meet certain requirements:

- U_f 's actions on CBS is unitary
- multi-qubit registers takes in CBS in of the form $|x\rangle^n$ & $|y\rangle^m$
- f have domain and range $\in \mathbb{Z}_{2n}$
- f is an easy function, which means that it can be computed in polynomial time

17.1 General Oracle

For a general oracle,



The U_f matrix has shape $(2^{m+n})^2$ and is made up of 2^n sub-matrices of shape $(2^m)^2$.

The submatrices is x-major, so columns represent the output of one x and all y.

The submatrix for a particular x is the tensor product of the corresponding output in binary form, replace 0 with \mathbb{I} and 1 with σ_x .

The submatrix M_x is expanded by $|x\rangle \otimes M_x$.

$f(x)$ maps from \mathbb{Z}_{2n} of x to \mathbb{Z}_{2m} of y.

17.2 Complexity of Quantum Oracle

Relativized Time Complexity This is the time complexity without the knowledge of the oracle's design (circuit + algorithm)

Absolute Time Complexity This includes knowledge of the oracle's design

$$\sum_{k=0}^{n=10}$$