

Q Notes

By Peter Montgomery

November 28, 2020

Contents

1	Complex Arithmetic	11
1.1	Complex Dot Product	11
1.2	Complex Conjugate	11
1.3	Roots of Unity	11
1.4	Summing Roots of Unity	11
1.5	Kronecker Delta	12
2	Real Vector Spaces	13
2.1	Linear Algebra	13
2.2	The Objects	13
2.3	The Rules	13
2.4	Positive Definite Property	14
2.5	Linear Combination	14
2.6	Bases of a Vector Space	14
2.7	Natural (Standard) Basis	14
2.8	Properties of a Basis	14
2.9	Orthonormal Bases	14
2.10	Expansion Coefficients	14
2.11	Subspace $\{a\vec{v} \mid a \in R\}$	14
3	Matrices	15
3.1	Matrices	15
3.2	Matrix Multiplication	15
3.3	Row Vector x Column Vector	15
3.4	Definition of Matrix Multiplication	15
3.5	Matrix Product of Vectors	15
3.6	Matrix Transpose	16
3.7	Matrix Addition and Scalar Multiplication	16
3.8	Zero Matrix (Additive Identity)	16
3.9	Identity Matrix (Multiplicative Identity)	16
3.10	Determinants of a 2 x 2 Matrix	16
3.11	Determinants of a 3 x 3 Matrix	16
3.12	Determinants of an n x n Matrix	16
3.13	Determinants of Products	16
3.14	Matrix Inverses	17
3.15	System of Linear Equations	17
3.16	Matrix Equations	17
3.17	Cramer's Rule	17
3.18	Complex Vector Space, \mathbb{C}^n	17
3.19	Complex Inner Product	17
3.20	Norm	18

3.21	Distance	18
3.22	Expansion Coefficients	18
4	Hilbert Space, \mathcal{H}	19
4.1	Definitions	19
4.2	Finite Dimensional Hilbert Spaces	19
4.3	Infinite Dimensional Hilbert Spaces	19
4.4	The Space L^2 [a, b]	19
4.5	Properties of Hilbert Spaces	19
4.6	Modeling Quantum Systems	20
4.7	Ray	20
4.8	0 in \mathcal{H}	20
4.9	Interacting with these Vectors	20
5	Linear Transformation	21
5.1	Linear Transformation	21
5.2	Role of Bases	21
5.3	Dependence of Matrix on Basis	21
5.4	Matrix M_T in a Non-Standard Basis	22
5.5	Transformation in an Orthonormal Basis	22
5.6	The Adjoint of a Matrix	22
5.7	Unitary Operators	22
5.8	Non-Unitary Operators	22
5.9	Hermitian Operators	22
6	The Experimental Basis of Quantum Computing	23
6.1	Spin 1/2 Quantum Mechanics	23
6.2	Naive Electron Spin Definition	23
6.3	Spherical Representation	23
6.4	Electron Spin z-Projection	23
6.5	Follow up $ +\rangle_z$ in S_x	24
6.6	Follow up $ +\rangle_x$ in S_z	24
6.7	Construction of Hilbert Space	24
6.8	Representing Spin	24
6.9	Measuring Spin θ from the Standard Axis	24
7	Time Independent Quantum Mechanics	25
7.1	Particle Energy and Position	25
7.2	Stern-Gerlach Apparatus	25
7.3	First Postulate of Quantum Mechanics	25
7.4	Trait #1: The State Space	25
7.5	Fundamental State Space for Quantum Computing	25
7.6	Orthonormality Expression	26
7.7	The x-Basis for \mathcal{H}	26
7.8	Reasoning for Complex Vector Space	26
7.9	Second Postulate of Quantum Mechanics	26
7.10	Trait #2: The Operator for an Observable	26
7.11	Completeness of the Eigenbasis	26
7.12	The Observable S_z	26
7.13	Third Postulate of Quantum Mechanics	27
7.14	Trait #3: Eigenvalues of an Observables	27

7.15	Eigenvectors and Eigenvalues	27
7.16	Trait #3': Eigenvectors and Eigenvalues of S_z	27
7.17	Computing Eigenvectors and Eigenvalues	27
7.18	Eigenvalue Theorem	27
7.19	Summary of Eigenvectors and Eigenvalues for spin 1/2 Observables .	28
7.20	Trait #4: Real Eigenvalues and Orthonormal Eigenvectors	28
7.21	General States Expressed in Alternate Bases	28
7.22	Orthonormal Basis in Higher Dimensions	28
7.23	Trait #5: Closure (Completeness) Relation	28
7.24	Fourth Postulate of Quantum Mechanics	29
7.25	Trait #6: Probability of Outcome	29
7.26	Fifth Postulate of Quantum Mechanics	29
7.27	Trait #7: Post-Measurement Collapse (complex inner product) . . .	29
7.28	Dirac's Bra-ket Notation	29
7.29	Transforming Ket to Bra	29
7.30	The Bra Space (Adjoint of a ket)	29
7.31	The Adjoint of an Operator	29
7.32	Trait #8: Adjoint Conversion Rules	30
7.33	Expectation Values	30
7.34	Trait #9: Expectation Value Theorem	30
8	Time Dependent Quantum Mechanics	31
8.1	The Hamiltonian	31
8.2	Trait #10: Constructing the Hamiltonian	31
8.3	Classical Hamiltonian (1/2 Spin)	31
8.4	Quantum Hamiltonian	31
8.5	Energy Eigenkets	32
8.6	Trait #11: Quantization of Energy	32
8.7	Sixth Postulate of Quantum Mechanics	32
8.8	Trait #12: Time-Dependent Schrodinger Equation	32
8.9	Solving the Schrodinger Equation	32
8.10	Trait #13: Stationary States	33
8.11	General Technique for Computing Time-Evolved States	33
8.12	Trait #14: Evolution of any Observable	33
8.13	Larmor Precession	33
8.14	Rewriting $ \psi\rangle$	33
8.15	Convenient Angle	34
8.16	Expectation Value at Time t	34
9	The Qubit	35
9.1	Vector Space $\mathcal{B} = \mathbb{B}^2$ ($\mathbb{B} \equiv \{0, 1\}$)	35
9.2	Definition of a Classical Bit	35
9.3	Definition of Bit Value	35
9.4	Alternate Definition of a Bit	35
9.5	Definition of a Classical Logical Operator	35
9.6	Unitary Properties	36
9.7	Definition of a Qubit	36
9.8	Alternate Definition of a Qubit	36
9.9	Definition of Qubit Value	36
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)	37
9.14	Phase Flip (Z)	37
9.15	Bit and Phase Flip (Y)	37
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	38
9.20	Combining Gates	38
9.21	The Bloch Sphere	38
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	39
10.5	Vector Addition	40
10.6	Scalar Multiplication	40
10.7	Inner Product in $V \otimes W$	40
10.8	Natural Basis for $V \otimes W$	40
10.9	Tensor Product Basis Theorem	40
10.10	Proof of Basis Theorem	40
10.11	Conventional Order of Tensor Basis	41
10.12	Tensor Coordinates from Component-Space Coordinates	41
10.13	Linear Operators on the Tensor Product Space	41
10.14	Matrix of General Operator	42
10.15	Matrix Tensor Product	42
11	Two Qubits and Binary Quantum Gates	43
11.1	Definition of Two Qubits ($\mathcal{H}_A \otimes \mathcal{H}_B$)	43
11.2	Definition of a Two-Qubit Value	43
11.3	Preferred Bipartite CBS	43
11.4	Alternate Bipartite Bases	43
11.5	Inherit Second Order Mixed CBS	43
11.6	Non-Standard Second Order CBS in Natural Basis	44
11.7	Alternate Definition of Two Qubits	44
11.8	Binary Quantum Operator Definition	44
11.9	Complete Description of Binary Quantum Operator	44
11.10	Measurement of Separable Outputs	44
11.11	Quantum Entanglement (Non-separable outputs)	44
11.12	Controlled-NOT (CNOT Gate)	45
11.13	Quantum Entanglement for CNOT	45
11.14	CNOT in Different CBS	45
11.15	Second Order Hadamard Gate	45
11.16	Condensed Form	45
11.17	Circuits in Separable Basis	45
11.18	Circuits in Non-Separable Basis	46
11.19	Controlled-U Gate	46

11.20	Separable Operators on Separable States	46
11.21	Separable Operators on Entangled States	46
11.22	Trait #15: Born Rule for Bipartite States	46
11.23	Bell States Circuit	47
11.24	Binary Operators on Bell States	47
11.25	BELL as Basis Transform Operator	47
11.26	Upside Down CNOT Circuit	47
11.27	Order-3 Tensor Product	47
11.28	Tripartite System Definition ($\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C = \mathcal{H}_{(3)}$)	48
11.29	Trait #15': Born Rule for Tripartite States	48
12	First Quantum Algorithms	49
12.1	Superdense Coding	49
12.2	Quantum Teleportation	49
12.3	Application of Born Rule	49
12.4	Expanding Initial States along $BELL_{AC}$ basis	50
12.5	B's Action from A's Message	50
12.6	Boolean Functions and Reversibility	50
12.7	Unary Gates as Boolean Function	50
12.8	Binary Gates as Boolean Functions	50
12.9	Quantum Oracle for Boolean Functions	50
12.10	Deutsch's Algorithm	51
13	Multi-Qubit Systems and Algorithms	53
13.1	Higher Order Tensor Products	53
13.2	Toffoli Gate (CCX)	53
13.3	Definition of n Qubits	53
13.4	n-qubit CBS	54
13.5	nth Order Hadamard Gate	54
13.6	Higher Order Basis conversion	54
13.7	Oracle for n-qubit Functions	54
13.8	Deutsch-Jozsa Problem	54
13.9	Quantum vs. Classical Time Complexity	55
13.10	Non-Deterministic Algorithm with small error $\epsilon \ll 1$	55
13.11	Deutsch-Jozsa Measurements	55
13.12	Bernstein-Vazirani Problem	55
13.13	Trait #15'': Generalized Born Rule	56
14	Probability Theory	57
14.1	Outcomes	57
14.2	Events	57
14.3	Sample Space (ω)	57
14.4	Null Event (\emptyset)	57
14.5	Probability $P(\mathcal{A})$	57
14.6	Set Operations	57
14.7	Linear Independence	58
14.8	Span	58
14.9	Fundamental Probability Theory	58
14.10	The Axioms	58
14.11	Definitions for Finite Equiprobable Sample Space	59
14.12	Conditional Probability	59

14.13	Bayes' Law	59
14.14	Statistical Independence	59
14.15	Two Independent Events	59
14.16	Multiple Independent Events	59
14.17	Other Formulas	60
14.18	Wedge and Vee Notations	60
14.19	Applications to Deutsch-Jozsa	60
14.20	Sampling with Replacement	60
14.21	Sampling without Replacement	60
14.22	Probability Algorithm	60
14.23	Looping Algorithm	61
14.24	Constant Time Complexity for Looping Algorithm	61
15	Computational Complexity	62
15.1	Big-O Growth	62
15.2	Ω Growth	62
15.3	Θ Growth	63
15.4	Little-o Growth	63
15.5	Easy vs. Hard	63
16	Computational Basis States and Modular Arithmetic	64
16.1	Single Qubit Hilbert Space	64
16.2	Multi Qubit Hilbert Spaces	64
16.3	\mathbb{Z}_N , or mod N Arithmetic	64
16.4	$(\mathbb{Z}_2)^n$ with \oplus Arithmetic	65
16.5	The group \mathbb{Z}_{2n} (encoded binary form)	65
16.6	Connection Between $(\mathbb{Z}_2)^n$ and (\mathbb{Z}_{2n})	65
16.7	General Notations	65
17	Quantum Oracle	66
17.1	General Oracle (maps from \mathbb{Z}_{2n} to \mathbb{Z}_{2m})	66
17.2	Complexity of Quantum Oracle	66
18	Simon's Algorithm	67
18.1	Ordinary Periodicity	67
18.2	$(\mathbb{Z}_2)^n$ Periodicity	67
18.3	Collapsing 1 bit Periodicity	67
18.4	Collapsing More Than 1 Bit \rightarrow Not Periodic	68
18.5	Simon's Problem	68
18.6	The Circuit	68
18.7	The Strategy	68
18.8	Circuit Breakdown	69
18.9	Hypothetical B-Measurement	69
18.10	Final Hadamard Gate	69
18.11	The Algorithm	70
18.12	Producing $n - 1$ Linear Independent w_k in Polynomial time	71
18.13	Gaussian Elimination (GE)	71
18.14	Back Substitution	71
18.15	GE in Determining Linear Independence	72
18.16	Completing the Basis with Non-Orthogonal nth Vector	72
18.17	Back Substitution to Solve for α	72

18.18	New Linear Independence Step	72
18.19	New w_{n-1} Step	73
18.20	Cost of the Circuit Summary	73
18.21	Classical Deterministic Cost	73
18.22	Classical Probabilistic Cost	73
19	Real & Complex Fourier Series	74
19.1	Periodic Functions over \mathbb{R}	74
19.2	Functions with Bounded Domain or Compact Support	74
19.3	Periodicity & Bounded Domain	74
19.4	Real Fourier Series (of 2π periodic function)	74
19.5	Interpretations	74
19.6	Finite Approximation	75
19.7	The Spectrum	75
19.8	Fourier Series as Function Mapping Operator	75
19.9	Computing Fourier Coefficients	75
19.10	Complex Fourier Series	76
19.11	Computing Complex Fourier Coefficients	76
19.12	Ordinary Frequency	76
19.13	Angular Frequency	77
20	Continuous Fourier Transform	78
20.1	Fourier Transform	78
20.2	Inverse Fourier Transform	78
20.3	Real vs. Complex, Even vs. Odd	78
20.4	Conditions for Fourier Transform	78
20.5	The Delta Function	79
20.6	Delta Functions as Limits of Rectangles	79
20.7	Delta Functions as Limits of Exponentials	79
20.8	The Sifting Property	79
20.9	Fourier Transform with $\delta(x)$	80
20.10	Translation Invariance	80
20.11	Plancherel's Theorem	80
20.12	Convolution	80
20.13	Convolution Theorem	80
20.14	Period and & Frequency in Fourier Transform	81
20.15	Applications for Fourier Transform	81
20.16	The Uncertainty Principle	81
21	Discrete & Fast Fourier Transforms	82
21.1	Adapting Continuous \mathcal{FT} to \mathcal{DFT}	82
21.2	Definition of \mathcal{DFT}	82
21.3	Inverse \mathcal{DFT}	82
21.4	\mathcal{DFT} as Matrix	83
21.5	Convolution of Two Vectors	83
21.6	Translation Invariance for Vectors	83
21.7	Computational Complexity of \mathcal{DFT}	83
21.8	Period & Frequency in \mathcal{DFT}	83
21.9	Cost Benefit of \mathcal{FFT}	83
21.10	Recursion Equation for \mathcal{FFT}	84
21.11	Danielson-Lanczos Recursion Relation	84

21.12	Recursive $N \log N$ Solution	84
21.13	Bit Reversal	84
21.14	Time Complexity	85
21.15	Rebuilding from the Bit-Reversed Array	85
21.16	Time Complexity	85
21.17	Normalization	85
21.18	Time Complexity	85
22	Quantum Fourier Transform	86
22.1	Approaches to Operator Definition	86
22.2	Characteristics of QFT	86
22.3	Definition 1 of QFT	87
22.4	Definition 2 of QFT	87
22.5	Translation Invariance	87
22.6	Comparing Hadamard & QFT	87
22.7	Quantum Fourier Basis	87
22.8	Applications	88
22.9	QFT Circuit	88
22.10	Factoring y-even Group	88
22.11	Factoring y-odd Group	88
22.12	Recursion Relation	88
22.13	General Circuit	89
22.14	Computational Complexity of QFT	89
23	Shor's Algorithm	90
23.1	Functions of Integers	90
23.2	Functions of the Group \mathbb{Z}_M	90
23.3	Shor's Periodicity Problem	90
23.4	Domain Size	91
23.5	Range Size	91
23.6	N & M Time Complexity Equivalence	91
23.7	$\mathbb{Z}_N - (\mathbb{Z}_2)^n$ - CBS	91
23.8	The Circuit	91
23.9	Initial State Preparation	91
23.10	The Plan	92
23.11	Hadamard Preparation of the A Register	92
23.12	Quantum Oracle	92
23.13	GCD & Coprime	92
23.14	Easy Case (αN)	92
23.15	Partitioning Domain into Cosets	92
23.16	Output of the Oracle	93
23.17	Effect of QFT on A Register	93
23.18	Easy Case Measurements Probability	93
23.19	Step 1	93
23.20	Step 2	94
23.21	Step 3	94
23.22	Step 4	94
23.23	Step 5	94
23.24	Complexity of Euclidean Algorithm	94
23.25	Full Easy Case Algorithm	95

23.26	Full Easy Case Complexity	95
23.27	General Case	95
23.28	Partitioning Domain into Cosets	95
23.29	Output of the Oracle	96
23.30	Hypothetical B-Measurement	96
23.31	Effect of the Final QFT on A-Register	96
23.32	General Case Final Measurement Probabilities	96
23.33	Step 1: Identify set of $\{y_c\}_{c=0}^{\alpha-1}$	97
23.34	Step 2: Prove that $\{y_c\}_{c=0}^{\alpha-1}$ have high likelihood	97
23.35	Estimating Bounds for $ e^{i\phi} - 1 $	97
23.36	Estimating Probability of Step 2	98
23.37	Step 3: Associate $\{y_c\}_{c=0}^{\alpha-1}$ with $\{c/\alpha\}_{c=0}^{\alpha-1}$	99
23.38	Step 4: CFA that Produces c/α from y_c	99
23.39	Step 5: Measuring $y_c \leftrightarrow c \phi \alpha$ in Constant Time	100
23.40	Full Algorithm	100
23.41	Full General Case Complexity	101
24	Euclidean Algorithm & Continued Fractions	102
24.1	Long Division	102
24.2	Euclidean Algorithm $EA(P, Q)$ $P > Q$	102
24.3	Continued Fractions Algorithm CFA	102
24.4	Convergents	102
24.5	Properties of Convergences	103
24.6	CFA Complexity	103

Chapter 1

Complex Arithmetic

1.1 Complex Dot Product

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

$$|\vec{a}| = \sqrt{\vec{a} \cdot \vec{a}} \geq 0, \in \mathbb{R}$$

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

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.

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

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

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

Now, the dot product definition changes:

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

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

$$zw = r s e^{i\theta+\phi}; \quad \frac{z}{w} = r s e^{i\theta+\phi}; \quad z^* = r e^{-i\theta} \text{ (Complex Polar Form)}$$

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

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

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 objects of a vector space and the rules.

2.2 The Objects

Scalars The scalars of the vector space are 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: $\vec{v} + 0 = 0 + \vec{v} = \vec{v}$
- Vector Opposites (additive inverses): $\vec{v} + (-\vec{v}) = 0$
- 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 norm 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 paring.

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: $\vec{u} \neq \vec{v} + \vec{w} \forall \vec{u}, \vec{v}, \vec{w} \in A$ where A is the subset of the basis of the space
- Completeness (Spanning): A is closed under linear combination

2.9 Orthonormal Bases

B is orthonormal if $\vec{b}_k \cdot \vec{b}_j = \delta_{kj}$

2.10 Expansion Coefficients

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

*Inner product is dependent on bases.

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

A subset of vectors closed under vector/ scalar operations.

Chapter 3

Matrices

3.1 Matrices

A matrix is a rectangular arrays of number.

The size is expressed as $[\# \text{ rows}] \times [\# \text{ columns}]$.

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 Vector x Column Vector

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

- $Av, v^T A$ is compatible
- Av is a linear transformation

3.6 Matrix Transpose

$$(A_{kl})^T = A_{lk}$$

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)

$$IM = MI = M$$

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

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

* Physicists conjugate the left vector of the inner product.

- Distributive: $\langle a|b + b'\rangle = \langle a|b\rangle + \langle a|b'\rangle$ and $\langle a + a'|b\rangle = \langle a|b\rangle + \langle a'|b\rangle$
- Anti-linear in the 1st position: $c\langle a|b\rangle = \langle c^*a|b\rangle$
- 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 $||b - a|| \geq 0$

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, \mathcal{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 exists only if x & y are linearly dependent.

4.6 Modeling Quantum Systems

Most quantum computations take place in \mathbb{C}^n .

4.7 Ray

A ray is a set of all scalar multiples of some non-zero vector that passes through the origin.

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

Every possible quantum state can be represented as a unit vector in \mathcal{H} .

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

4.8 0 in \mathcal{H}

- 0 (the zero vector) is not a quantum state because it's is not normalizable.
- Every other vectors 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 $\hat{v} \in \mathcal{H}$ of a quantum states
2. Apply unitary transformation
3. Renormalize vectors

*The 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

$T|_B = (T(b_0)|_B, T(b_1)|_B, \dots)$ 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 preserves 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.

In essence, unitary operators map one set of orthonormal basis to another.

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 superpositions.

6.2 Naive Electron Spin Definition

An electron has

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 % $+\frac{\hbar}{2}$ & 50% $-\frac{\hbar}{2}$ instead of a continuum between $\pm\frac{\sqrt{3}}{2}\hbar$. The post-measurement states remain for future measurements of the same orientation.

This is because of $\Delta x \Delta p \leq \frac{\hbar}{2}$ (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 post-measurement states remain for future measurements of the same orientation.

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 orientation (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 on a projective sphere.

6.8 Representing Spin

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

1. $|+\rangle$ & $|-\rangle$ are linearly independent of one another, instead of \pm (multiples) of the same basis vector.
2. The observable of one basis can be written as linear combination of the two observables of another basis, instead of being linearly independent. What this means is that for basis A and B so that if $A \neq B$, $|\pm\rangle_A = \alpha|+\rangle_B + \beta|-\rangle_B$

6.9 Measuring Spin θ from the Standard Axis

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

Non-zero azimuthal ϕ will not change the result.

* ϕ is the angle of the vector on 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

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

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

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

7.5 Fundamental State Space for Quantum Computing

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

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

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

$$\langle +|+\rangle = \langle -|-\rangle = 1$$

$$\langle +|-\rangle = \langle -|+\rangle = 0$$

7.7 The x-Basis for \mathcal{H}

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

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

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 basis, 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 \mathcal{H} . This matrix is always related to a Hermitian.

For Observable $\mathcal{A} \in \mathcal{S}$,

$$T_A: \mathcal{H} \text{ linear} \quad \& \quad T_A^\dagger = T_A \text{ (Hermitian condition)}$$

7.11 Completeness of the Eigenbasis

Eigenvectors of an observable span the state space

7.12 The Observable S_z

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

1. the observable “spin projected onto the z-axixs”
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 \mathcal{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 are the 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 \mathcal{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 observables.

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 of the unknown λ

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

To solve for the eigenvector:

1. Plug in 1 to 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:

$$\begin{aligned} S_z : \quad +\frac{\hbar}{2} &\leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad -\frac{\hbar}{2} \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ S_x : \quad +\frac{\hbar}{2} &\leftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad -\frac{\hbar}{2} \leftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \\ S_y : \quad +\frac{\hbar}{2} &\leftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \quad -\frac{\hbar}{2} \leftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \end{aligned}$$

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

$$\begin{aligned} S_z : \quad +\frac{\hbar}{2} &\leftrightarrow |+\rangle, \quad -\frac{\hbar}{2} \leftrightarrow |-\rangle \\ S_x : \quad +\frac{\hbar}{2} &\leftrightarrow |+\rangle_x = \frac{|+\rangle + |-\rangle}{\sqrt{2}}, \quad -\frac{\hbar}{2} \leftrightarrow |-\rangle_x = \frac{|+\rangle - |-\rangle}{\sqrt{2}} \\ S_y : \quad +\frac{\hbar}{2} &\leftrightarrow |+\rangle_y = \frac{|+\rangle + i|-\rangle}{\sqrt{2}}, \quad -\frac{\hbar}{2} \leftrightarrow |-\rangle_y = \frac{|+\rangle - i|-\rangle}{\sqrt{2}} \end{aligned}$$

7.20 Trait #4: Real Eigenvalues and Orthonormal Eigenvectors

An observable \mathcal{A} in \mathcal{S} will always correspond to an operator

1. with real eigenvalues
2. and with unique eigenvectors that form an orthonormal basis for \mathcal{H} .

7.21 General States Expressed in Alternate Bases

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

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 the Hilbert space \mathcal{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 will satisfy the closure relation.

7.24 Fourth Postulate of Quantum Mechanics

7.25 Trait #6: Probability of Outcome

The normalized state $|\psi\rangle$ can be expanded along the eigenbasis $\{\vec{v}_k\}$ of some observable \mathcal{A}

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

then the probability that a measurement of \mathcal{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 \mathcal{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

$|\psi\rangle = \langle\psi|^\dagger$ 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 finite dimensions.

7.31 The Adjoint of an Operator

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

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

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.

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

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

7.34 Trait #9: Expectation Value Theorem

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

where \mathcal{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 equation

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

However, H is time-independent for our purpose.

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

$$H|\vec{v}_k\rangle = a_k |\vec{v}_k\rangle \quad (2)$$

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 equation (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 $|\psi(t)\rangle = \begin{pmatrix} ce^{i\phi(t)} \\ se^{-i\phi(t)} \end{pmatrix}$,

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 $\mathcal{B} = \mathbb{B}^2$ ($\mathbb{B} \equiv \{0, 1\}$)

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

\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 \mathcal{B} .

9.3 Definition of Bit Value

A bit's value is any unit vector in \mathcal{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 \mathcal{B} .

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

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: $\langle A\vec{v} | A\vec{w} \rangle = \langle \vec{v} | \vec{w} \rangle$
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.

Any 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 $(\vec{\sigma} \cdot \hat{n})$, where

$$\begin{pmatrix} \sigma_x \\ \sigma_y \\ \sigma_z \end{pmatrix}; \quad \hat{n} = \begin{pmatrix} \hat{n}_x \\ \hat{n}_y \\ \hat{n}_z \end{pmatrix} \text{ real spin vector}$$

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)

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

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

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-identical Pauli matrices anti-commute: $\sigma_i \sigma_j = -\sigma_j \sigma_i$

*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 $\mathbb{R}^3\{|\hat{n}| = 1\}$ 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,

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

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 ($\dim=\ell$) and W ($\dim=m$) is a new vector space with $\dim=\ell m$

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 spans the full space $V \otimes W$.

10.4 Terms and Definition

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

Tensors Vectors in the product space

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

then $V \otimes W$ ($\text{dim}=\ell m$) 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 Tensor Coordinates from Component-Space Coordinates

Natural Coordinates of Separable Tensors

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

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

Natural Coordinates of Basis Vectors

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

$\exists \ell m$ 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 ,

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

Tensor as Matrices

The basis can be put into a matrix

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

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 $\leq (\ell m)^2$ separable operators in the form P_{pq} with 1 at (p, q) and 0 everywhere, where $0 \leq p, q \leq \ell m$

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.

Using the unitary inner product, assume

$$\langle (V \otimes W)(v \otimes w) | (V \otimes W)(v \otimes w) \rangle = \langle v \otimes w | v \otimes w \rangle$$

From the above expansion, this gives $\langle Vv \otimes Ww | Vv \otimes Ww \rangle$

Using the tensor product inner product, expand with the unitary definition

$$\langle Vv | Vv \rangle \cdot \langle Ww | Ww \rangle = \langle v | v \rangle \cdot \langle w | w \rangle = \langle v \otimes w | v \otimes w \rangle$$

- 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

11.1 Definition of Two Qubits ($\mathcal{H}_A \otimes \mathcal{H}_B$)

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.

$$|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle = |0\rangle^2 \text{ (coordinate representation)}$$

\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.

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

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

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

When expanded along the z-basis, the x-basis kets have equal number of + and - terms except for the zeroth CBS ket, $|00\rangle_x$, whose coordinates are all +1.

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

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

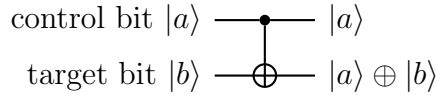
Probability of collapse is local and independent.

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, which means that it affects the state not in the local system.

11.12 Controlled-NOT (CNOT Gate)



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

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

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

Notice that γ and δ swap position.

11.13 Quantum Entanglement for CNOT

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

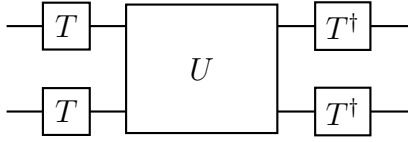
11.16 Condensed Form

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

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

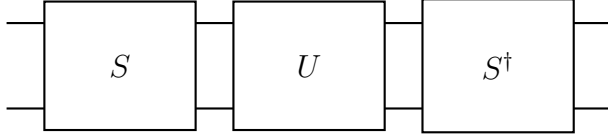
11.17 Circuits in Separable Basis

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:



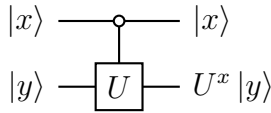
11.18 Circuits in Non-Separable Basis

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

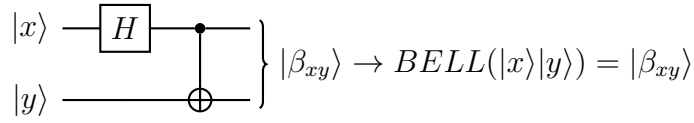
$$A \searrow 0 \Rightarrow B \searrow \frac{\alpha|0\rangle + \beta|1\rangle}{\sqrt{|\alpha|^2 + |\beta|^2}}$$

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

This solves the problem of non-normality.

11.23 Bell States Circuit

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



11.24 Binary Operators on Bell States

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

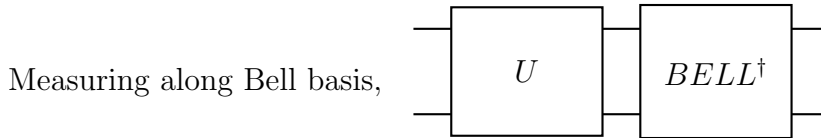
$$(I \otimes I)|\beta_{00}\rangle = |\beta_{00}\rangle$$

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

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

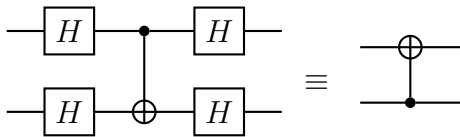
$$(iY \otimes I)|\beta_{00}\rangle = |\beta_{11}\rangle$$

11.25 BELL as Basis Transform Operator



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

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 Defintion ($\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C = \mathcal{H}_{(3)}$)

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,

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

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

Chapter 12

First Quantum Algorithms

12.1 Superdense Coding

This technique sends two classical bits through one classical bit.

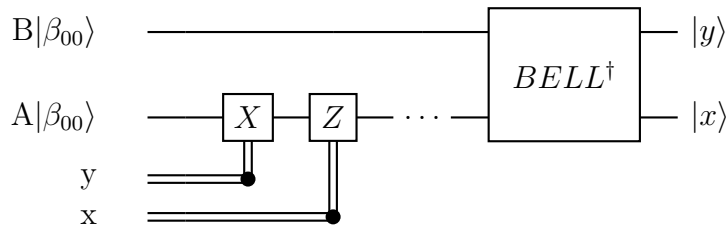
First, a Bell state (β_{00}) is prepared & separated. Then, depending on the desired number from 0-3, a unique set of gate is applied to the sender's qubit \mathcal{A} . After which, \mathcal{A} 's qubit is sent to \mathcal{B} . \mathcal{B} measures both qubit in the Bell basis with $BELL^\dagger$.

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

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

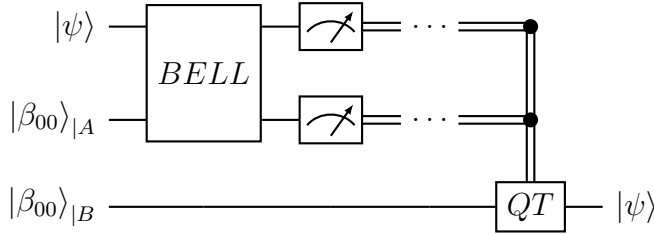
\mathcal{A} measures this state through $BELL^\dagger$, then send the result to \mathcal{B} .

12.5 B's Action from A's Message

The table shows that gate that B applies on A's message, as shown by the gate QT, to get the desired result.

\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$

Note 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

$$f : \mathbb{B}^2 \rightarrow B$$

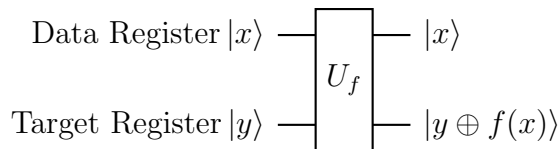
All two-bit cases are irreversible

12.9 Quantum Oracle for Boolean Functions

Oracle for Unary Functions

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

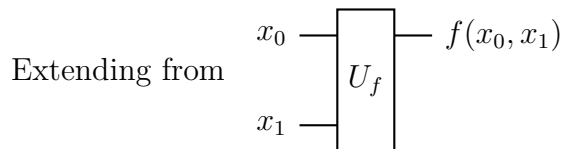
- two bits input
- two bits output
- unitary \therefore reversible
- computes f with the proper inputs
- equally efficient



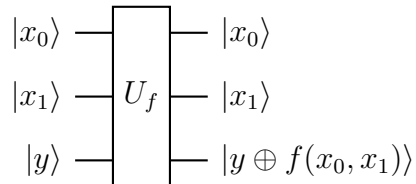
U_f for a CBS is always separable

* 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



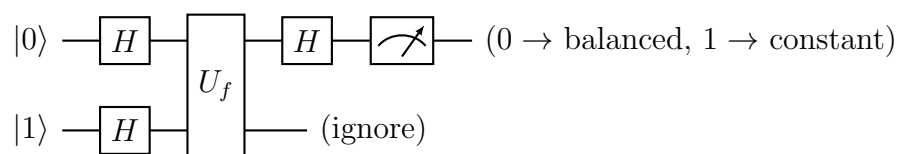
- x_0 & x_1 is usually shortened as $|x\rangle^2$
- U_f is its own inverse
- $U_f = f(x)$ with $y = 0$
- $U_f(|x\rangle |0\rangle) = |x\rangle^2 |f(x)\rangle$

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, due to loss of phase kickback

Chapter 13

Multi-Qubit Systems and Algorithms

13.1 Higher Order Tensor Products

Notation \otimes and \prod can be used to shorten expression

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

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

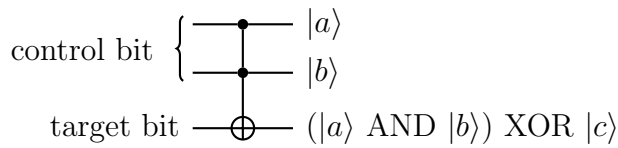
Separable Tensors $\{\prod_{j=0}^{n-1} a_j k_j\}_{k_0, \dots, k_{n-1}=0, \dots, 0}^{d_0-1, \dots, d_{n-1}-1}$

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 amplitudes.

13.3 Definition of n Qubits

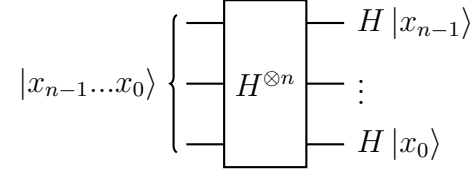
n qubits are the vector space $\mathcal{H}_{(n)}$, and the value is any unit tensors in the product space.

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

13.4 n-qubit CBS

$$|x\rangle^n = |x_{n-1}, \dots, x_0\rangle$$

13.5 nth Order Hadamard Gate



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

13.6 Higher Order Basis conversion

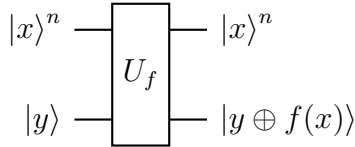
$H^{\otimes n}$ converts between x & z-basis in $\mathcal{H}_{(n)}$

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 $|0\rangle_{\pm}^n$

13.7 Oracle for n-qubit Functions

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

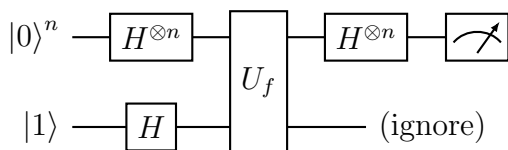


- U_f is its own inverse
- $U_f(|x\rangle|0\rangle) = |x\rangle^n|f(x)\rangle$
- Both has the same spatial circuit complexity

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

These complexity are for deterministic algorithms.

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

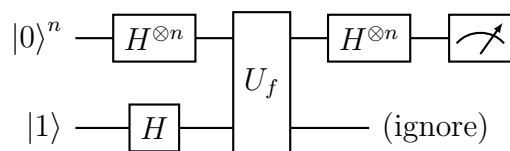
Not all balanced f has a corresponding x-CBS. However, the probability of measuring $|0\rangle_{\pm}^n$ is 0 if f is balanced

13.12 Bernstein-Vazirani Problem

For $f(x) = \alpha \odot x_n$, 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)

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

This 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 $A \otimes B = \mathcal{H}_{(n)} \otimes \mathcal{H}_{(m)}$, $|\psi^{n+m}\rangle$ 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 event is a subset of outcomes

Simple event is an event that contains exactly one outcome

Compound event is an event that contains 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 ($'$, $\bar{}$, c , \neg) All elements 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, a 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 $\{\vec{v}_{l_0} + \dots + \vec{v}_{l_s} | \vec{v}_{l_k} \in \mathcal{S}\}$

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

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

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 for 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:

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

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 #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 $P(\mathcal{S}_k) \geq p$, 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 to 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 (\oplus).

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

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

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

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 with vectors as objects

$(\mathbb{Z}_2)^n$ correspond to the CBS of $\mathcal{H}_{(n)}$

Ex: $\vec{x} = (1, 0, 0, 0)^T$

16.5 The group \mathbb{Z}_{2n} (encoded binary form)

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

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

Ex: $x = (0110)$

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

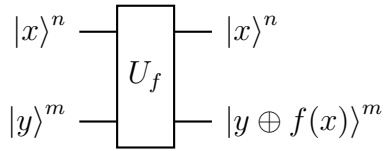
Quantum Oracle

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 (maps from \mathbb{Z}_{2n} to \mathbb{Z}_{2m})

For a general oracle,



The U_f matrix has shape $(2^{m+n})^2$ and is made up of $(2^n)^2$ 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 , where

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

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

Chapter 18

Simon's Algorithm

18.1 Ordinary Periodicity

$$f : \begin{Bmatrix} \mathbb{R} \\ \mathbb{C} \\ \mathbb{Z} \end{Bmatrix} \rightarrow S \text{ is periodic if } \exists \text{ smallest } \alpha < 0, \text{ where}$$

$$f(x + \alpha) = f(x) \forall x \in \text{dom}(f)$$

18.2 $(\mathbb{Z}_2)^n$ Periodicity

$$f : (\mathbb{Z}_2)^n \rightarrow S \text{ is periodic if } \exists \alpha \in (\mathbb{Z}_2)^n, \alpha \neq 0 \text{ s.t.}$$

$$\forall x \neq y \in (\mathbb{Z}_2)^n, f(x) = f(y) \Leftrightarrow y = x \oplus \alpha$$

This means that the cycle has two elements in the progression.

$$x \rightarrow x \oplus \alpha \rightarrow x \oplus (\alpha \oplus \alpha) = x$$

Notice that $\alpha \oplus \alpha = 0$, which means that $\alpha = x \oplus y$ (the period can be recovered from one pair of elements).

This periodicity is isomorphically equivalent in \mathbb{Z}_{2^n}

18.3 Collapsing 1 bit Periodicity

$$f = \sum_{k=0}^m \begin{Bmatrix} 0 \text{ or } 1 \text{ if } k = c \\ x_k \end{Bmatrix} 2^k$$

$f \oplus 2^k$ performs a bit flip on the k th element.

The period of f is 2^c .

18.4 Collapsing More Than 1 Bit \rightarrow Not Periodic

Domain and Range

The domain of f is $\text{dom}(f)$, the range of f is $\text{ran}(f)$.

For $\omega \in \text{ran}(f)$, the pre-image of ω is $\{x | f(x) = \omega\}$

One-to-one

$$x \neq y \Rightarrow f(x) \neq f(y) \forall x, y \in \text{dom}(f)$$

For $S \subseteq \text{dom}(f)$ if f is not 1-to-1, S can still be 1-to-1.

Two-to-one

$\omega \in \text{ran}(f)$ has two pre-images in $\text{dom}(f)$.

n-to-one

$\omega \in \text{ran}(f)$ has n pre-images in $\text{dom}(f)$.

The domain of all periodic functions in \mathbb{Z}_{2n} can be partitioned into 2 cosets

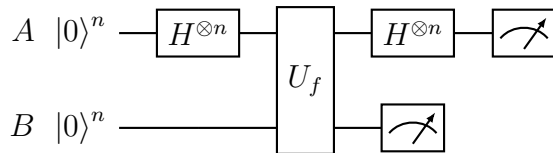
$$\begin{aligned} \mathbb{Z}_{2n} &= R \cup Q \\ &= \{\dots, x, \dots\} \cup \{\dots, x \oplus \alpha, \dots\} \end{aligned}$$

Every periodic function in \mathbb{Z}_{2n} is 2-to 1 in f and 1-to-1 in their respective coset.

18.5 Simon's Problem

Let $f: \{(\mathbb{Z}_2)^n \rightarrow (\mathbb{Z}_2)^n\}$ is periodic. Find α (the period)

18.6 The Circuit



- H-gate sets up quantum parallelism
- For B-channel, $|0\rangle$ is used for generalized Born's rule & $|1\rangle$ for phase kickback

18.7 The Strategy

Find an $n-1$ linear independent ω_k that is orthogonal to α .

Classical determine α .

18.8 Circuit Breakdown

After the oracle is applied, the state becomes

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

The superposition $|x\rangle^n \frac{1}{\sqrt{2}^n} |f(x)\rangle^n$ is separable, A-measurement will collapse B to normalized $|f(x)\rangle^n$

If B is measured, the collapsing state will be a superposition with individual probability of $\frac{1}{2^n}$

*The previous sum has 2^{2n} basis vectors but the amplitude for most is 0.

Partitioning the domain into 2 cosets, we can group the sum

$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}\right)^{n-1} \sum_{x \in \mathbb{R}} \left(\frac{|x\rangle^n + |x \oplus \alpha\rangle^n}{\sqrt{2}} \right) |f(x)\rangle^n$$

This shows that A collapses into 1 of 2 states.

18.9 Hypothetical B-Measurement

$$|\psi\rangle \searrow \left(\frac{|x\rangle^n + |x \oplus \alpha\rangle^n}{\sqrt{2}} \right) |f(x)\rangle^n$$

Which means that B measurement will collapse to

$$|\psi_{x_0}\rangle \searrow \left(\frac{|x_{x_0}\rangle^n + |x_{x_0} \oplus \alpha\rangle^n}{\sqrt{2}} \right) |f(x)\rangle^n$$

18.10 Final Hadamard Gate

The final states become

$$\left(\frac{1}{\sqrt{2}}\right)^{n+1} \sum_{y=0}^{2^n-1} (-1)^{y \cdot x_0} (1 + (-1)^{y \cdot \alpha}) |y\rangle^n$$

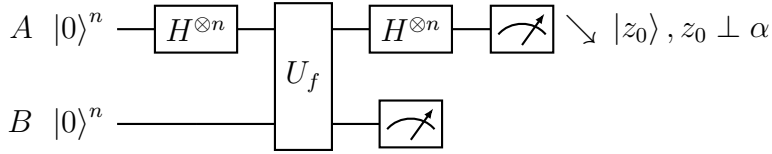
The inside expression reduces to

$$1 + (-1)^{y \cdot \alpha} = \begin{cases} 0, & \text{if } y \cdot \alpha = 1 \pmod{2}, \\ 2 & \text{if } y \cdot \alpha = 0 \pmod{2} \end{cases}$$

which leaves

$$\left(\frac{1}{\sqrt{2}}\right)^{n-1} \sum_{y \cdot \alpha = 0 \pmod{2}} (-1)^{y \cdot x_0} |y\rangle^n$$

The set of vectors in the sum is now halved (2^{n-1})



All output is orthogonal to α

$z = 0$ is orthogonal to everything and \therefore trivial

18.11 The Algorithm

1. Getting $n - 1$ linear independent vectors in polynomial time with arbitrary good confidence
2. Checking linear independence & solving n equations in polynomial time

The complexity of the algorithm is $O(n^3)$

The Steps

- Select an integer T with $P(\text{failure}) = \frac{1}{2^T}$
- Initialize an empty set W for vectors $\in (\mathbb{Z}_2)^N$
- Repeat the loop at most $n + T$ times
 1. Apply Simon's circuit
 2. Measure the A register to get z
 3. Classically determine z 's linear independence on W
 - If yes, name it ω_j & add ω_j to W
 - * If $j = n - 2$, $\exists n - 1$ vectors, break loop (success)
 - If not (including $z = 0$), start new pass
- If loop end naturally after $n + T$, failure
- Else, add non-orthogonal ω_{n-1} independent to W . The result is n independent vectors

$$\omega_k \cdot \alpha = \begin{cases} 0, & k = 0, \dots, n - 2 \\ 1, & k = n - 1 \end{cases}$$

- Classically solve for α

The first $n-1$ vectors form a basis in \mathbb{Z}_2^n . However, as the $n-1$ th vector is not orthogonal to α , this basis cannot be an orthonormal basis

$$c_k \neq v \cdot w_k$$

18.12 Producing $n - 1$ Linear Independent w_k in Polynomial time

Theorem 1 Select $m + T$ samples, $P(\mathcal{S}(m)) > 1 - (\frac{1}{2})^T$

$\mathcal{S}(m) \equiv$ event that c_0, \dots, c_{j-1} are linearly independent

$$P(\mathcal{S}(m)) = \prod_{i=1}^m P(\mathcal{S}(j) | \mathcal{S}(j-1))$$

With $P(\mathcal{S}(j) | \mathcal{S}(j-1)) = (1 - (\frac{1}{2})^{m+T-j+1})$,

$$P(\mathcal{S}(m)) = \prod_{i=1}^m (1 - (\frac{1}{2})^i) \geq \prod_{i=1}^p (1 - \alpha_i) \geq 1 - \sum_{i=1}^p \alpha_i$$

$$P(\mathcal{S}(m)) = 1 - (\frac{1}{2})^T \left[\sum_{i=1}^m 1 - (\frac{1}{2})^i \right] > 1 - (\frac{1}{2})^T$$

Theorem 2 Select mT samples, $P(\mathcal{S}(m)) > \frac{1}{4}$

$$P(\mathcal{S}(m)) \geq \sum_{i=1}^{\infty} (1 - (\frac{1}{2})^T) > \frac{1}{4}$$

This means that $P(\text{failure}) < (\frac{3}{4})^T$

Hidden Classical Algorithm

18.13 Gaussian Elimination (GE)

GE changes a matrix into row echelon form or reduced row echelon form. All-zero rows are at the bottom

RHS constant vector should also be included in the GE process

Three Operations of GE

1. Swap two rows
2. Multiply a row by a non-zero value
3. Add a multiple of one row to another

The cost for decimal-based GE is $O(n^3(\log m)^2)$, whereas for mod-2 GE is $O(n^3)$

18.14 Back Substitution

In RREF, $x_{n-1} = b_{n-1}$ can be read off. Substitute the value into the above equation to solve for unknown.

The cost for decimal-based is $O(n^2(\log m)^2)$, whereas for mod-2 back substitution is $O(n^2)$

18.15 GE in Determining Linear Independence

For $m \times n$ matrix, with $m < (n - 1)$, there will be gap in the diagonal with leading 1s. Add z to the matrix and reapply GE.

If z is linearly independent, one of the hole is filled. If not an all 0 row will appear at the bottom.

Once there are $n - 1$ vectors, $W - \alpha = 0$

The cost of this is $O(n^4)$ (n quantum, n^3 classical)

18.16 Completing the Basis with Non-Orthogonal nth Vector

1. Find ω_k where there is a gap in the all-1 diagonal
 - Place $\omega_k \equiv 2^{n-2-k}$ below ω_k
 - If diagonal is all 1s place ω_{n-1} at the bottom
2. On the RHS vectors of all 0, insert 1 in the row of ω_{n-1}

The cost of this is $O(n)$ in series.

18.17 Back Substitution to Solve for α

W is already in RREF \therefore back substitution is in series $O(n^2)$

18.18 New Linear Independence Step

The classical adding z & apply GE is replaced by

1. Loop until either z is added to W or $z = 0$ produced
 - A $m \leftarrow$ MSB position of z
 - B Search W for a ω_k row with the same MSB position
 - If not found, insert z in between. Success
 - If found, $z \leftarrow z \oplus \omega$. Continue next pass

This works because the addition process move the MSB to the right after each loop. In other words, if $z \in \text{span}(W)$.

$$z \oplus \sum_{\omega_0}^{\dots} = 0$$

The cost of this step is $O(n^2)$. This brings the overall CTC to $O(n^3)$ ($O(n)$ for quantum).

18.19 New w_{n-1} Step

Because the new linear independence step produces and $(n-1) \times n$ RREF, simply add n th linear independent vector to form $n \times n$ RREF.

$$\omega_k \cdot \alpha = \begin{cases} 0, k = 0, \dots, n-2 \\ 1, k = n-1 \end{cases}$$

18.20 Cost of the Circuit Summary

$O(n)$: Quantum with $O(n^2)$ GE nested $\rightarrow O(n^3)$

In series: $O(n)$ inserting ω_{n-1} , $O(n^2)$ back-substitution

The CTC of the circuit is therefore $O(n^3)$

18.21 Classical Deterministic Cost

$2^{n-1} + 1$ samples have to be tested in the worst case $\therefore O(2^n)$

18.22 Classical Probabilistic Cost

The upper bound of getting a repeat in m samples is

$$P(\mathcal{E}_{ij}) \leq \frac{m(m-1)}{2} \frac{1}{2^n - 1}$$

where \mathcal{E}_{ij} is the event that any $f(x_i) = f(x_j)$.

With $\lim_{n \rightarrow \infty} P = 0$, the problem is hard even probabilistically

Chapter 19

Real & Complex Fourier Series

19.1 Periodic Functions over \mathbb{R}

$f : \mathbb{R} \rightarrow \mathcal{S}$ is periodic if \exists smallest $a > 0$, where

$$f(x + a) = f(x) \forall x \in \text{dom}(f)$$

19.2 Functions with Bounded Domain or Compact Support

$f : x \in \mathbb{R}$ (defined over bounded interval)

A function has compact support when it is defined over an interval but all 0 outside the interval.

The support of a function is the closure of the domain where $f \neq 0$

19.3 Periodicity & Bounded Domain

A periodic function is a repeat of the bounded interval.

If the same action is applied to the bounded domain, we have an induced periodic function

19.4 Real Fourier Series (of 2π periodic function)

$$f(x) = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} a_n \cos nx + \sum_{n=1}^{\infty} b_n \sin nx$$

19.5 Interpretations

The amplitude determines the weighting of each term

When small- n coefficients are large, the function has low frequency characteristics.
When large- n coefficients are large, the function has high frequency characteristics.

$\{\sin nx, \cos nx\}$ are called Fourier basis functions, or normal modes, or Fourier eigenfunctions

19.6 Finite Approximation

Practical use of the series requires approximation by taking the partial sum of $n = N < \infty$ terms.

19.7 The Spectrum

The Fourier coefficients list is called the spectrum of f . They represents a new function, $F(n)$.

19.8 Fourier Series as Function Mapping Operator

$$\mathcal{FS}[f(x)] = F(n) \longleftrightarrow \{a_n, b_n\}$$

$$f : \mathbb{R} \rightarrow \mathbb{R}; F : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{R}$$

$$\mathcal{FS} : f \rightarrow F$$

19.9 Computing Fourier Coefficients

$$a_0 = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) dx, n = 0$$

$$a_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos nx \, dx, n > 0$$

$$b_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin nx \, dx, n > 0$$

This works for function with period 2π or bounded domain $[-\pi, \pi)$. For general period T , the form is as follow

$$a_0 = \frac{1}{L} \int_{-L}^L f(x) \, dx, n = 0$$

$$a_n = \frac{1}{L} \int_{-L}^L f(x) \cos nx \, dx, n > 0$$

$$b_n = \frac{1}{L} \int_{-L}^L f(x) \sin nx \, dx, n > 0$$

The domain of the series is the entire real line, so for bounded functions, only one period would be necessary.

Compact support has no Fourier Series unless it is broken up

19.10 Complex Fourier Series

From Euler's formula

$$\cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2}; \sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$$

Substituting into the real Fourier Series, we get

$$f(x) = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} (a_n - ib_n)e^{inx} + \sum_{n=1}^{\infty} (a_n + ib_n)e^{-inx}$$

The Complex Fourier Series of 2π period function is

$$f(x) = \sum_{n=-\infty}^{\infty} c_n e^{inx}$$

$$\text{where } c_n \equiv \begin{cases} \frac{1}{2}(a_n - ib_n), & n > 0 \\ \frac{1}{2}(a_{-n} + ib_{-n}), & n < 0 \\ \frac{1}{2}a_0, & n = 0 \end{cases}$$

The coefficient c_n is complex, but the sum is still real.

19.11 Computing Complex Fourier Coefficients

$$c_n = \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{-inx} f(x) dx$$

Note that the 2 in the denominator can be dropped depending on the format.

c_n is the weighted sum of e^{inx} in the summation, where c is a function of n and e^{-inx} is the weighted sum of $f(x)$ in the integral, with f as a function of x

The correspondence $f(x) : \mathbb{R} \rightarrow c(n) : \mathbb{Z}$ is the complex Fourier series

19.12 Ordinary Frequency

The frequency, f , is the reciprocal of the period

$$f = \frac{1}{T}$$

This is the number of period in a 1 unit interval

$$f \cdot T = 1$$

19.13 Angular Frequency

This expresses the number of period per cycle or revolution

$$\omega = \frac{2\pi}{T} ; \omega = 2\pi f ; \omega \cdot T = 2\pi$$

For frequency of arbitrary interval l ,

$$f = \frac{l}{T} ; f \cdot T = l$$

Chapter 20

Continuous Fourier Transform

To represents unbounded periodic functions as sums of exponentials,

- The integer index n becomes a real number s
- The sum becomes an integral
- The limit of integration changes from $\pm\pi$ to $\pm\infty$
- Normalization constant $\left(\frac{1}{\sqrt{2\pi}}\right)$

20.1 Fourier Transform

$$F(s) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(x) e^{-isx} dx$$

$$F = \mathcal{F}[f]; f \xrightarrow{\mathcal{F}} F$$

20.2 Inverse Fourier Transform

$$f(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} F(s) e^{isx} ds$$

20.3 Real vs. Complex, Even vs. Odd

If f is even, F is real-valued. If f is odd, F is imaginary-valued. Else, F is mixed.

20.4 Conditions for Fourier Transform

A function that can be Fourier transformed must be absolutely integrable

$$\int_{-\infty}^{\infty} |f(x)| dx < \infty$$

20.5 The Delta Function

A delta function is 0 everywhere and spike to infinity at a point

$$\delta(x) = \begin{cases} \infty, & \text{if } x = 0 \\ 0, & \text{otherwise} \end{cases} \quad \text{and} \quad \int_{-\infty}^{\infty} \delta(x) dx = 1$$

20.6 Delta Functions as Limits of Rectangles

$$\delta_n(x) = \begin{cases} \frac{1}{n}, & \text{if } x \in [-\frac{1}{2}n, \frac{1}{2}n] \\ 0, & \text{otherwise} \end{cases}$$

This is true because the area of the rectangle is 1.

$$\delta(x) = \lim_{n \rightarrow \infty} \delta_n(x)$$

20.7 Delta Functions as Limits of Exponentials

$$\delta_a(x) = \sqrt{\frac{a}{\pi}} e^{-ax^2}$$

With the area of the Gaussian function being 1, this is smoother than the rectangular approximation

$$\delta(x) = \lim_{n \rightarrow \infty} \delta_n(x)$$

20.8 The Sifting Property

Using the rectangular sum approximation, we can prove

$$f(d) = \int_{-\infty}^{\infty} f(t) \delta(t-d) dt$$

$$\text{or equivalently } = \int_{x_0-\epsilon}^{x_0+\epsilon} f(t) \delta(t-d) dt$$

The integral returns the value of f at point d

By applying Fourier transform and substituting the whole expression, we get

$$\delta(x) = \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{isx} ds$$

The delta function represent the different frequencies.

By definition of even function, $\delta(x) = \delta(-x)$, which implies

$$\delta(x-d) = \delta d - x \quad \therefore \text{ the delta function is even}$$

20.9 Fourier Transform with $\delta(x)$

Using the Delta function, the Fourier Transform of

- $f(x) = a \leftrightarrow F(s) = a\sqrt{2\pi}\delta(s)$
- $f(x) = \cos(x) \leftrightarrow F(s) = \sqrt{\frac{\pi}{2}}(\delta(s+1) + \delta(s-1))$
- $f(x) = \sin(x) \leftrightarrow F(s) = -\sqrt{\frac{\pi}{2}}(\delta(s+1) - \delta(s-1))$

20.10 Translation Invariance

$$f(x+a) \xrightarrow{\mathcal{F}} e^{ias} F(s) \text{ \& } F(s-\gamma) \xrightarrow{\mathcal{F}^{-1}} e^{i\gamma x} f(x) \quad \forall a, \gamma \in \mathbb{R}$$

A translation in the time or spatial domain causes a phase shift in the frequency domain. The multiple is a unit vector in \mathbb{C} so there is no effect on the magnitude of the output function.

Because probabilities of collapse is amplitude absolute squared,

$$|e^{ias} F(s)|^2 = |e^{ias}|^2 |F(s)|^2 = |F(s)|^2$$

translation doesn't affect collapse probabilities.

20.11 Plancherel's Theorem

For any Fourier transform pair, F and f , we have

$$\int_{-\infty}^{\infty} |f(x)|^2 dx = \int_{-\infty}^{\infty} |F(s)|^2 ds$$

If the function are amplitudes of quantum states, the squared absolute values are probabilities density of the function. This will always sum up to 1.

20.12 Convolution

Convolution is a binary operator on two functions that produces a third function

$$[f * g](x) \equiv \int_{-\infty}^{\infty} f(\xi)g(x-\xi)d\xi$$

20.13 Convolution Theorem

A convolution of two functions can be represented as point-to-point multiplication of their Fourier transforms.

$$f * g = \sqrt{2\pi} \mathcal{F}^{-1}[\mathcal{F}(f) \cdot \mathcal{F}(g)]$$

The constant $\sqrt{2\pi}$ depends on the definition of \mathcal{F}

20.14 Period and & Frequency in Fourier Transform

For the angular frequency, ω , the period is $\frac{2\pi}{\omega}$

Taking the Fourier transform of this gives, a delta function with the absolute value of its position being ω

The Fourier transform absolute value of the delta result is Ω

20.15 Applications for Fourier Transform

- Target certain frequencies of a picture, audio or signal. Perform work on \mathcal{F} then take \mathcal{F} to recover the original
- Represents quantum state wave-function. ψ is a vector in a Hilbert space with different bases.
 - Position Basis - $\Psi(x)$. This form shows the amplitude of the particle at any point in time. Integrate $|\psi(x)|^2$ over a region of position space to find out the P(particle at x).
 - Momentum Basis - $\Psi(x)$. This form shows the amplitude of the particle at any point in time. Integrate $|\psi(p)|^2$ over a region of momentum space to find out the P(particle at p).

The movement between x -space & p -space is through the Fourier transform

$$\psi(p) = \mathcal{F}(\psi(x)) ; \psi(x) = \mathcal{F}^{-1}(\psi(p))$$

20.16 The Uncertainty Principle

If a Gaussian wave packet is used to represent the position state $\psi(x)$, as $|\psi(x)|^2$ becomes narrower, $|\psi(p)|^2$ becomes more spread out.

This is the Heisenberg Uncertainty Principle

Chapter 21

Discrete & Fast Fourier Transforms

\mathcal{DFT} maps functions from \mathbb{Z}_N to \mathbb{C} . This is useful for discretely sampled functions and generated data.

Because $\text{dom}(f) = \mathbb{Z}_N$, it can be represented as a vector of operation on all values within the set or a vector in \mathbb{C}^N .

21.1 Adapting Continuous \mathcal{FT} to \mathcal{DFT}

- The integral becomes sums from 0 from $N-1$. There will be N discrete real-valued vector (f_k) and N complex spectrum vector (F_k)
- The factor $\frac{1}{\sqrt{2\pi}}$ replaces by $\frac{1}{\sqrt{N}}$
- The n th root of unity ω^{jk} replaces e^{isx} , where $\omega = e^{\frac{2\pi i}{N}} \therefore \omega^{jk} = e^{\frac{(2\pi i)}{N}j \cdot k}$ (bounded domain implies periodicity)

If $\psi_s(x) = e^{-isx}$ then $\phi_j(k) = \omega_N^{-jk} = \omega^{-jk}$

e^{-isx} becomes N vectors $v_j = (\omega^{-j0}, \dots, \omega^{-j(N-1)})^T$

$j = 0, \dots, N-1$. k is the coordinate index & j is the parameter label

21.2 Definition of \mathcal{DFT}

For $f_k : \mathbb{C}^N$ with $\text{dom}(\mathbb{Z}_N)$, $\mathcal{DFT}^{(N)}(f) = F_j : \mathbb{C}^N$, where

$$F_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} f_k \omega^{-jk}, \text{ for } j = 0, \dots, N-1$$

21.3 Inverse \mathcal{DFT}

$$f_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} F_j \omega^{kj}, \text{ for } k = 0, \dots, N-1$$

Naturally, $\mathcal{DFT}^{-1} \circ \mathcal{DFT} = \mathcal{DFT} \circ \mathcal{DFT}^{-1} = \mathbb{I}$

21.4 DFT as Matrix

DFT can be represented as matrix W with $\zeta = \omega^{-1}$

$$W = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \zeta & \ddots \\ 1 & & \zeta^{(N-1)(N-1)} \end{pmatrix}$$

$\mathcal{DFT}(f) = W \cdot (f_k) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} f_k \zeta^{jk} = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} f_k \omega^{-jk}$, where \mathcal{DFT} is unitary

21.5 Convolution of Two Vectors

$$[f * g] = \sum_{l=0}^{N-1} f_l f_{k-l}$$

The convolution theorem also hold with \mathcal{DFT}

$$f * g = \sqrt{2\pi} \mathcal{DFT}^{-1}[\mathcal{DFT}(f) \odot \mathcal{DFT}(g)]$$

21.6 Translation Invariance for Vectors

$$f_{k-l} \xrightarrow{\mathcal{DFT}} \omega^{-lk} F_k$$

21.7 Computational Complexity of DFT

The complexity of \mathcal{DFT} is $O(N^2)$ relative to arithmetic operations for matrix computation.

21.8 Period & Frequency in DFT

For $dom(f)$ bounded over \mathbb{Z}_N , if f has period T then

$$f(k+T) = f(k) \Rightarrow T \cdot = N$$

Non-zero amplitudes in the spectrum are multiples of f (frequency)

Looking at the multiples of the frequency $\Rightarrow T$

21.9 Cost Benefit of FFT

FFT relies on the symmetry of the DFT matrix to speed up computation from $O(n^2)$ to $O(n \log n)$

This is the main method for computing DFT.

FFT only operates on vectors with 2^n components. If f is not in this form, simply pad 0 to the end and perform FFT.

21.10 Recursion Equation for \mathcal{FFT}

Split the k index into odd and even, where

$$f_k^{even} = f_{2k} \text{ and } f_k^{odd} = f_{2k+1}$$

We get,

$$\begin{aligned} \mathcal{FFT}[f]_j &= \frac{1}{\sqrt{N}} \left(\sum_{k=0}^{\frac{N}{2}-1} f_k^{even} \omega^{-j(2k)} + \sum_{k=0}^{\frac{N}{2}-1} f_k^{odd} \omega^{-j(2k+1)} \right) \\ &= \frac{1}{\sqrt{N}} \left(\sum_{k=0}^{\frac{N}{2}-1} f_k^{even} (\omega^2)^{-jk} + \omega^{-j} \sum_{k=0}^{\frac{N}{2}-1} f_k^{odd} (\omega^2)^{-jk} \right) \end{aligned}$$

Notice that ω^2 is a $N/2$ root of unity, we get

$$[F^{(N)}]_j = \frac{1}{\sqrt{2}} ([F_E^{(N/2)}]_{(j \bmod N/2)} + \omega_N^{-j} [F_O^{(N/2)}]_{(j \bmod N/2)})$$

f is periodic with $\frac{N}{2}$ period, $\mathcal{FFT}[f]$ also has $\frac{N}{2}$ period.

21.11 Danielson-Lanczos Recursion Relation

With f being $\frac{N}{2}$ periodic $\Rightarrow f(\frac{N}{2} + P) = f(P)$

$$F^{(N)}[f]_j = \frac{1}{\sqrt{2}} ([F_E^{(N/2)}]_{(j \bmod N/2)} + \omega_N^{-j} [F_O^{(N/2)}]_{(j \bmod N/2)})$$

Once F is restricted for example F_{EOE} , the size of j is restricted to the number of elements in the group.

21.12 Recursive $N \log N$ Solution

- Bit Reversal
- Iterative Array Building
- Normalization

21.13 Bit Reversal

Recursion after $\log N$ calls gives order-one \mathcal{FFT}

$$\mathcal{FFT}^{(1)}(\{c\}) = \{c\}$$

For order-2 DFT, however

$$[F_{EO...OE}^{(2)}]_j = \frac{1}{\sqrt{2}} (f_p + (-1)^{-j} f_q)$$

If f_p & f_q is arranged in order, then $(-1)^{-j}$ can just be multiplied out & added up.

By dividing the sum into even and odd sections, we find that the new index of f_k is f_n where n is k with its bits reversed relative to the size of k .

For example, $10010 \rightarrow 01001$

21.14 Time Complexity

If performed independently for each input, the time complexity is $n \log n$.

However, a static array can be produced ahead of time & is independent of the input & so therefore has constant time complexity.

21.15 Rebuilding from the Bit-Reversed Array

The input array is first bit-reversed, then built up using Danielson-Lanczos recursion relation.

$$F^{(N)}[j] = \frac{1}{\sqrt{2}}([F_E^{(\frac{N}{2})}]_{(j \bmod N/2)} + \omega_N^{-j}[F_O^{(\frac{N}{2})}]_{(j \bmod N/2)})$$

Note that F_E & F_O repeats twice but j goes from 0 to $N - 1$.

Thanks to the bit reversal step, the elements are already in order of j -index

21.16 Time Complexity

There are $\log N$ outer loops until the full size N array is reached. This is because information is reduced by half as only $a + b$ is important & not what a & b are. There is a maximum of N operations in each loop \therefore the complexity is $N \log N$.

21.17 Normalization

The array is normalized by multiplying by $\frac{1}{\sqrt{N}}$

21.18 Time Complexity

The normalization step is linear & doesn't factor into the overall complexity

Chapter 22

Quantum Fourier Transform

Discrete Fourier Transform

$$\mathcal{DFT} : \mathbb{C}^N \rightarrow \mathbb{C}^N; \mathcal{DFT}(f_k) \rightarrow f_j$$

Fast Fourier Transform

$$\mathcal{FFT} : \mathbb{C}^{2n} \rightarrow \mathbb{C}^{2n}; \mathcal{FFT}(f_k) \rightarrow f_j$$

Quantum Fourier Transform

$$\mathcal{QFT} : \mathbb{C}^{2n} \rightarrow \mathbb{C}^{2n}; \mathcal{QFT} : \mathcal{H}_{(n)} \rightarrow \mathcal{H}_{(n)}$$

22.1 Approaches to Operator Definition

1. Actions on CBS kets
2. Actions on complex coefficients
3. Matrix for U, where $U |\psi\rangle^n \rightarrow |\psi\rangle^{n'}$

* Make sure U is linear & unitary

- $U(|\psi_1\rangle + |\psi_2\rangle) = U|\psi_1\rangle + U|\psi_2\rangle$
- $aU|\psi\rangle = U|a\psi\rangle$
- $UU^\dagger|\psi\rangle = U^\dagger U|\psi\rangle = |\psi\rangle$

22.2 Characteristics of \mathcal{QFT}

If $|\psi\rangle^n \leftrightarrow (c_x)_{x=0}^{N-1}$,

$$\mathcal{QFT}^{(N)} |\psi\rangle^n \leftrightarrow (\tilde{c}_y)_{y=0}^{N-1}$$

, where $N = 2^n$

\mathcal{QFT} transforms a vector of amplitudes into another vector of amplitudes. Its actions is similar to that of a logic gate.

22.3 Definition 1 of \mathcal{QFT}

$$\mathcal{QFT} |\psi\rangle^n = \sum_{y=0}^{N-1} \tilde{c} |y\rangle^n, \text{ where}$$

$$[\mathcal{QFT} |\psi\rangle^n]_y = \tilde{c}_y = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} c_x \omega^{xy} = {}^n\langle y | \mathcal{QFT} |\psi\rangle^n$$

Applying linearity to CBS to find \mathcal{QFT} of arbitrary states

$$\mathcal{QFT} |x\rangle^n = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{yx} |y\rangle^n$$

22.4 Definition 2 of \mathcal{QFT}

$$\mathcal{QFT} |\psi\rangle^n = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \left(\sum_{x=0}^{N-1} c_x \omega^{xy} \right) |y\rangle^n$$

22.5 Translation Invariance

$$\mathcal{QFT} |x - z\rangle^n = \omega^{xz} \sum_{y=0}^{N-1} \omega^{xy} |y\rangle^n = \omega^{xz} \mathcal{QFT} |x\rangle^n$$

22.6 Comparing Hadamard & \mathcal{QFT}

Hadamard Gate: $H^{\otimes n} |x\rangle^n = (\frac{1}{\sqrt{2}})^n \sum_{y=0}^{2^n-1} \omega_2^{x \cdot y} |y\rangle^n$, where $\omega_2 = -1$

\mathcal{QFT} : $\mathcal{QFT}^{(N)} |x\rangle^n = (\frac{1}{\sqrt{2}})^n \sum_{y=0}^{2^n-1} \omega^{xy} |y\rangle$, where $n = \log N$

Notice that \mathcal{QFT} equals H for $N = 2$

22.7 Quantum Fourier Basis

Basis Conversion Property

If A is an orthonormal basis & U is an unitary operator, UA = B is also an orthonormal basis.

Applying $\mathcal{QFT}^{(2^n)}$ to the preferred z -basis in $\mathcal{H}_{(n)}$ gives the Fourier basis or frequency basis

$$\mathcal{QFT}^{(2^n)} |z\rangle^n = |\tilde{x}\rangle^n$$

22.8 Applications

If $H^{\otimes n}$ is used to find $(\mathbb{Z}_2)^n$ periodicity, then \mathcal{QFT} is used to find periodicity of ordinary integer.

22.9 \mathcal{QFT} Circuit

For CBS in the form $x = \sum_{k=0}^{n-1} x_k 2^k$ (integer form),

$$\sqrt{N} \mathcal{QFT}^{(N)} |x\rangle^n = \sum_{y=0}^{N-1} \Pi_{xy} |y_{n-1}, \dots, y_0\rangle, \text{ where } \Pi_{xy} = \prod_{k=0}^{n-1} \omega^{xy_k 2^k}$$

22.10 Factoring y-even Group

With $y_0 = 0, \omega^{xy_k 2^k} = \omega^{x \cdot 0 \cdot 1} = 1, \Pi_{xy} = \prod_{k=0}^{n-1} \omega^{xy_k 2^k}$

With a few minor tweaks, y-even group \sum becomes

$$\begin{aligned} & \left(\sum_{y=0}^{\frac{N}{2}-1} \left(\prod_{k=0}^{n-1} (\omega^2)^{(x \bmod N/2) y_k 2^k} \right) |y_{n-2}, \dots, y_0\rangle \right) |0\rangle \\ &= \left(\sqrt{\frac{N}{2}} \mathcal{QFT}^{(N/2)} |\tilde{x}\rangle^{(n-1)} \right) |0\rangle; \tilde{x} = x \bmod N/2 \end{aligned}$$

22.11 Factoring y-odd Group

$$\begin{aligned} & \omega^x \left(\sum_{y=0}^{\frac{N}{2}-1} \left(\prod_{k=0}^{n-1} (\omega^2)^{(x \bmod N/2) y_k 2^k} \right) |y_{n-2}, \dots, y_0\rangle \right) |1\rangle \\ &= \omega^x \left(\sqrt{\frac{N}{2}} \mathcal{QFT}^{(N/2)} |\tilde{x}\rangle^{(n-1)} \right) |1\rangle = y\text{-odd group } \sum \end{aligned}$$

22.12 Recursion Relation

Combining the odd & even group to get

$$\mathcal{QFT}^{(2^n)} |x\rangle^n = \mathcal{QFT}^{(2^{n-1})} |\tilde{x}\rangle^{n-1} \left(\frac{|0\rangle + \omega_2 |1\rangle}{\sqrt{2}} \right)$$

Reapply the relation to get

$$\mathcal{QFT}^{(2^n)} |x\rangle^n = \prod_{k=1}^n \left(\frac{|0\rangle + \omega^{2^{n-k} x} |1\rangle}{\sqrt{2}} \right) = \sum_{y=0}^{2^n-1} \omega^{xy} |y\rangle$$

When $N=2$, $\mathcal{QFT} = H$

$$H |x_0\rangle = \frac{1}{\sqrt{2}} ((-1)^{0 \cdot x_0} |0\rangle + (-1)^{1 \cdot x_0} |1\rangle)$$

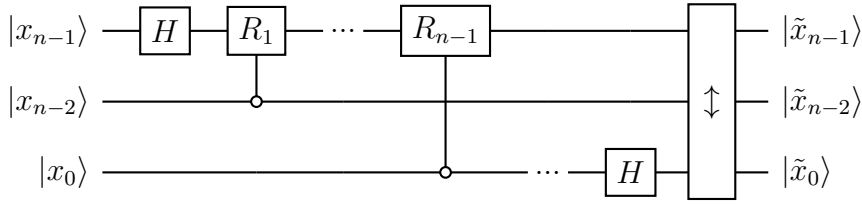
22.13 General Circuit

$$\left(\frac{|0\rangle + \omega^{2^{n-k}x} |1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}(|0\rangle + \prod_{k=0}^{k-1} \omega^{x_k} |1\rangle)$$

Notice that if y_0 to $y_{k-2} = 0$ then the state is $H |y_{k-1}\rangle$

To perform the $\omega^{2^{n-k}x}$ multiplications, simply apply R_k gates successively,

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & \omega^{2^{n-k-1}} \end{pmatrix}$$



22.14 Computational Complexity of QFT

The number of gates on each line is a triangle number is so \exists

$$\sum_{k=1}^n k = \frac{n(n+1)}{2} \text{ gates}$$

Both H & R_k is constant-time, so the complexity is $O(n^2)$

$$O(n^2) = O(\log^2 N)$$

- This circuit only computes 1 CBS state. Computing N CBS takes $O(N \log^2 N)$
- The circuit cannot be used to compute \mathcal{DFT} because we need to account for the complex part of the input

Chapter 23

Shor's Algorithm

1. Shor's algorithm for period finding is a relativized exponential speed up because it doesn't include the oracle design.
2. Shor's algorithm for factoring provides a polynomial time oracle design & therefore is an absolute exponential speed up

23.1 Functions of Integers

$$f : \mathbb{Z} \rightarrow \mathcal{S}, \mathcal{S} \subset \mathbb{Z}$$

is periodic injective, if $\exists \alpha \in \mathbb{Z} > 0$ s.t

$$\forall x \neq y \in \mathbb{Z}, f(x) = f(y) \Leftrightarrow y = x + k\alpha, k \in \mathbb{Z}$$

23.2 Functions of the Group \mathbb{Z}_M

$$f : \mathbb{Z}_M \rightarrow \mathcal{S}, \mathcal{S} \subset \mathbb{Z}_M$$

is periodic injective, if $\exists \alpha \in \mathbb{Z}_M > 0$ s.t

$$\forall x \neq y \in \mathbb{Z}_M, f(x) = f(y) \Leftrightarrow y = x + k\alpha, k \in \mathbb{Z}_M$$

Injective: 1-to-1. Shor's function is injective periodic for disjoint domain.

In Simon's algorithm getting 1 pair gives α (the period), whereas in Shor's, the output is a multiple of α

23.3 Shor's Periodicity Problem

Let $f : \mathbb{Z}_M \rightarrow \mathbb{Z}$ be injective periodic. Find α

M is a bound on α , and is used to determine complexity

Again, the algorithm is relatively easy.

Assumption: conservative $\alpha < M/2$ because the algorithm still works for 1 interval of α

23.4 Domain Size

Let $2^{n-1} < M^2 \leq 2^n$, $[0, \dots, 2^n - 1]$ be the official domain for f , or if $N = 2^n$, $N/2 < M^2 \leq N$.

$$\text{dom}(f) = \mathbb{Z}_{2^n}$$

23.5 Range Size

For sufficiently large $r > 0$

$$\text{ran}(f) \subseteq [0, 2^r - 1] \text{ or } = \mathbb{Z}_{2^r}$$

$$0 \leq f(x) < 2^r$$

All in all,

$$f : [0, N - 1] \rightarrow [0, 2^r - 1]$$

23.6 N & M Time Complexity Equivalence

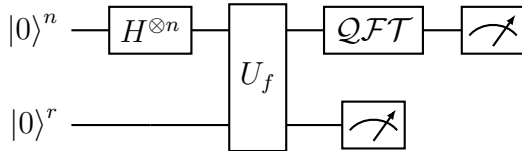
$$O(\log N) = O(\log M)$$

Bracketing M^2 allows the use of N to compute complexity and later replace with M .

23.7 \mathbb{Z}_N - $(\mathbb{Z}_2)^n$ - CBS

- $|y \oplus f(x)\rangle^r$ is mod-2 sum with r qubits B channel
- $|x + j\alpha\rangle^n$ is ordinary addition of A channel

23.8 The Circuit



- Post-oracle A-register is processed by QFT instead of $H^{\otimes n}$
- The size of the B register is significantly smaller than B

23.9 Initial State Preparation

- Prepare $|0\rangle^n \otimes |0\rangle^r$ as input
- Quantum parallelism in the data channel
- Generalized Born's rule in the target channel

23.10 The Plan

- Post-oracle state of channel A goes into QFT , which transform it from z -basis to Fourier basis. For $m = N/\alpha$, the frequency associated with period α , we will get a subset of $\{cm\}_{c=0}^{\alpha-1}$, each element with equal probability
- After a few measurements, if cm has a coprime with α , we can use that to find α . This is the easy case.
- However, the measurements will give α close to cm . This is the hard case.

23.11 Hadamard Preparation of the A Register

See Identical Section from Simon's algorithm

23.12 Quantum Oracle

See Identical Section from Simon's algorithm

23.13 GCD & Coprime

$gcd(a, b) =$ largest integer c , with $c \mid a$ & $c \mid b$

If $gcd(a, b) = 1 \Rightarrow a$ & b are coprime

$a \phi b : a$ & b are coprime

$\neg a \phi b : a$ & b are not coprime

23.14 Easy Case ($\alpha \mid N$)

This implies $\alpha m = N = 2^n \therefore 2^n/\alpha = m \therefore \alpha$ is in the form 2^l .

The periodicity can easily be tested by trying $\alpha = \{2^l\}_1^{n-1}$, which has $O(\log N)$ complexity. This classical approach is $O(\log N)$ relative to the oracle & $O(\log^5 N)$ absolute.

23.15 Partitioning Domain into Cosets

Injective periodicity implies disjoint cosets size α with 1-to-1 sub-domain for f . In the easy case, there are exactly m cosets in the interval $[0, N)$.

$$\begin{aligned} [0, N - 1] &= [0, \alpha - 1] \cup \dots \cup [(m - 1)\alpha, m\alpha - 1] \\ &= R \cup \dots \cup R + (m - 1)\alpha \text{ where} \end{aligned}$$

$R = \{0, \dots, \alpha - 1\}$, α : period of f , $m = N/\alpha$

$R = j\alpha$ is the j th coset of R

$$= \bigcup_{j=0}^{m-1} \{x + j\alpha\}_{x=0}^{a-1}$$

23.16 Output of the Oracle

$$\{x + j\alpha\}_{j=0}^{m-1} \rightarrow f(x) \Rightarrow \sqrt{\frac{m}{N}} \sum_{x=0}^{a-1} \left(\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |x + j\alpha\rangle^n \right) |f(x)\rangle^r$$

Collapsing the B channel produce a superposition of m x s.

$$\boxed{\text{Measurement}} \searrow \left(\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |x_0 + j\alpha\rangle^n \right) |x_0\rangle^r$$

Fed into the QFT & we get non-zero amplitudes that are multiples of the frequency m .

23.17 Effect of QFT on A Register

$$|\psi_0\rangle \xrightarrow{QFT^{(N)}} \frac{1}{\sqrt{mN}} \sum_{y=0}^{N-1} \omega^{x_0 y} \left(\sum_{j=0}^{m-1} \omega^{j\alpha y} \right) |y\rangle^n$$

The measurement of the B channel is conceptual, so it makes the expression simpler, but won't affect the probability of A.

23.18 Easy Case Measurements Probability

1. Identify the set $C = \{y_c = cm\}_{c=0}^{a-1}$
2. Observe that each $y_c = cm$ has the same P
3. Prove that $\{c\}_{c=0}^{a-1} \Phi \propto 50\%$ of the time
4. $y = cm$ with the above c value occurs 50% of the time
5. Measure the above $y = cm$ with arbitrarily high confidence in constant time

23.19 Step 1

$$|\psi_0\rangle \xrightarrow{QFT^{(N)}} \frac{1}{\sqrt{mN}} \sum_{y=0}^{N-1} \omega^{x_0 y} \left(\sum_{j=0}^{m-1} \omega^{j\alpha y} \right) |y\rangle^n$$

Because $\omega_N = 1 = \omega^{am} = (\omega^a)^m \Rightarrow \omega^a = \omega_m$

$$\sum_{j=0}^{m-1} \omega^{j\alpha y} = \sum_{j=0}^{m-1} \omega_m^{jy} = \begin{cases} m, & \text{if } y = 0 \pmod{m} \\ 0, & \text{if } y \neq 0 \pmod{m} \end{cases}$$

$$|\psi_0\rangle \xrightarrow{QFT^{(N)}} \sqrt{\frac{m}{N}} \sum_{y=0 \pmod{m}} \omega^{x_0 y} |y\rangle^n$$

, in which

$$y \equiv 0 \pmod{m} \Leftrightarrow y = \{cm\}_{c=0}^{\alpha-1}$$

23.20 Step 2

The normalization factor $\sqrt{\frac{m}{N}}$ turns into $\frac{1}{\sqrt{\alpha}}$ so each cm has probability of $1/\alpha$.

After QFT is applied, the only possible measurements are in the frequency domain.

23.21 Step 3

$N = 2^n = m\alpha \Rightarrow \alpha = 2^l \therefore c \not\equiv \alpha$ only if c is odd

$$P(c \not\equiv \alpha) = \frac{\#\text{odds} < 2^l}{2^l} = \frac{2^{l-1}}{2^l} = \frac{1}{2}$$

23.22 Step 4

For $\mathcal{B} = \{y_0 | y_b = \{bm\}_{b=0}^{\alpha-1} \text{ and } b \not\equiv \alpha\}$ & $\mathcal{C} = \{cm\}_{c=0}^{\alpha-1}$

$$P(\mathcal{B}) = P(\mathcal{B}|\mathcal{C})P(\mathcal{C}) = \frac{1}{2}$$

23.23 Step 5

Because the probability of success $P(\mathcal{B})$ is independent of N , from the CTC Theorem for Looping Algorithm, we have

$$T = \lfloor \frac{\log(\mathcal{E})}{\log(1 - \frac{1}{2})} \rfloor + 1 : \text{with arbitrary } \mathcal{E} \text{ tolerance}$$

From this, $P(\text{getting at least 1 } c \not\equiv \alpha) = 1 - (\frac{1}{2})^T$

23.24 Complexity of Euclidean Algorithm

Euclidean Algorithm takes $P > Q$ and find $\gcd(P, Q)$

Use EA to find $m' = \gcd(N, M)$ in $O(\log^3 N)$ time

$$c \not\equiv \alpha \Rightarrow m' = \gcd(N, cm) = \gcd(\alpha m, cm) = m$$

From that $\alpha = N/m$

However, it is unclear if $c \not\equiv \alpha$

23.25 Full Easy Case Algorithm

- Select T as number of loops that satisfies \mathcal{E} tolerance
- Repeat loop T times
 1. Apply Shor's circuit
 2. Measure output of \mathcal{QFT} and get cm
 3. Compute $m' = EA(N, cm)$ and set $\alpha' = N/m'$
 4. Test α' : If $f(1 + \alpha') = f(1)$ then $\alpha' = \alpha$ (success), break
 5. Else continue next pass
 6. If loop ends naturally after T passes, we fail

23.26 Full Easy Case Complexity

The full complexity will be in M since $O(\log N) = O(\log M)$

- Hadamard: $O(\log M)$
- \mathcal{QFT} : $O(\log^2 M)$
- U_f : at least $O(\log^4 M)$ for RSA factoring
- Outer loop: $O(T) = O(1)$
- Classical EA: $O(\log^3 M)$

These are done in series so they are $O(\log^3 M)$ relative to the oracle & $O(\log^4 M)$ absolute for RSA oracle.

The classical algorithm is deterministic $O(\log^5 M)$ for this easy case, whereas the quantum algorithm is probabilistic $O(\log^4 M)$

23.27 General Case

This is when $\alpha|N$ is not implied.

$N = 2^n = m\alpha + \text{excess part}$ where $m = \lfloor N/\alpha \rfloor$

23.28 Partitioning Domain into Cosets

$[0, N - 1]$ is partitioned in to m cosets plus extra

$$= [0, \alpha - 1] \cup \dots \cup [(m - 1)\alpha, m\alpha - 1] \cup [m\alpha, N - 1]$$

$$R \cup \dots \cup R + (m - 1)\alpha \cup \langle R + m\alpha \rangle \text{ where}$$

$$R = \{0, \dots, \alpha - 1\} \quad a = \text{period of } f \quad m = \lfloor M/a \rfloor$$

$R + j\alpha$ is still the j th coset of R , but now

$\langle R + m\alpha \rangle \subset [R + m\alpha](\text{partial mth coset of } R)$

$$[0, N - 1] = \cup_{j=0}^{m-1} \{x + j\alpha\}_{x=0}^{\alpha-1} \cup \{x + m\alpha\}_{x=0}^{N-m\alpha-1}$$

To deal with the partial coset, for some of the $f(x)$, there will be $x + 1$ pre-images, therefore let \tilde{m} be m or $m + 1$

$$\tilde{m} = \begin{cases} m + 1, \text{first few } x \text{ in } [0, \alpha - 1] \\ m, \text{remaining } x \text{ in } [0, \alpha - 1] \end{cases}$$

23.29 Output of the Oracle

With \tilde{m} , the output becomes

$$\approx \sqrt{\frac{\tilde{m}}{N}} \sum_{x=0}^{\alpha-1} \left(\frac{1}{\sqrt{\tilde{m}}} \sum_{j=0}^{\tilde{m}-1} |x + j\alpha\rangle^n \right) |f(x)\rangle^r$$

The inside \tilde{m} normalize each state whereas the outside is undefined between $\frac{m}{N}$ & $\frac{m+1}{N}$

23.30 Hypothetical B-Measurement

The B channel values are collapsed, giving

$$|\psi_{x_0}\rangle^n = \left(\frac{1}{\sqrt{\tilde{m}}} \sum_{j=0}^{\tilde{m}-1} |x_0 + j\alpha\rangle^n \right)$$

Although f is a pure periodic function, because of \tilde{m} , the QFT measurements no longer yields exclusively $\{cm\}_{c=0}^{\alpha-1}$

However, all values with high probability appears close to $\{cm\}_{c=0}^{\alpha-1}$ in the frequency domain

23.31 Effect of the Final QFT on A-Register

The QFT state after B-collapse is:

B-measurement picked out a x_0 so $\frac{1}{\tilde{m}N}$ is precise

23.32 General Case Final Measurement Probabilities

Because $\tilde{m} \neq m$, we can't use the fact that $\omega^\alpha = \omega_n$

To show that $y_c \neq cm$ leads to a cm , from which $c \not\equiv \alpha$ with good probability can be found, follow these steps:

1. Identify a set of $C = \{y_c\}_{c=0}^{\alpha-1}$ with high likelihood
2. Prove that $\{y_c\}_{c=0}^{\alpha-1}$ have high measurement likelihood

3. Associate $\{y_c\}_{c=0}^{\alpha-1}$ with $\{c/\alpha\}_{c=0}^{\alpha-1}$
4. Describe an $O(\log^3 N)$ algorithm that produces c/α from y_c
5. Observe that y_c associated with $c \phi \alpha$ measures in $O(1)$

23.33 Step 1: Identify set of $\{y_c\}_{c=0}^{\alpha-1}$

For $y = \{y_c\}_{c=0}^{\alpha-1}$, $y_c \cdot \alpha \in [cN - \frac{\alpha}{2}, cN + \frac{\alpha}{2}]$

With probability $P = 1 - \mathcal{E}$, one of the y_c can be measured in constant time T , independent of N .

The set of \hat{y}_c is in $[-\frac{\alpha}{2}, \frac{\alpha}{2}]$ and is associated with y_c

$$\hat{y}_c = y_c \cdot \alpha - cN \in [-\frac{\alpha}{2}, +\frac{\alpha}{2}) = y_c \cdot \alpha \pmod{N}$$

23.34 Step 2: Prove that $\{y_c\}_{c=0}^{\alpha-1}$ have high likelihood

The A channel state is: $\frac{1}{\sqrt{\tilde{m}N}} \sum_{y=0}^{N-1} \omega^{x_0 y} (\sum_{j=0}^{\tilde{m}-1} \omega^{j\alpha y} |y\rangle)^n$

$$P(\searrow |y\rangle) = \frac{1}{\tilde{m}N} |\omega^{x_0 y}|^2 \left| \sum_{j=0}^{\tilde{m}-1} \omega^{j\alpha y} \right|^2 = \frac{1}{\tilde{m}N} \left| \sum_{j=0}^{\tilde{m}-1} \omega^{j\alpha y} \right|^2$$

Let $\mu = \omega^{\alpha y}$, $\sum_{j=0}^{\tilde{m}-1} \mu^j = \frac{\mu^{\tilde{m}} - 1}{\mu - 1} = \frac{e^{i\theta_y \tilde{m}} - 1}{e^{i\theta_y} - 1}$

$$P(\searrow |y\rangle) = \frac{1}{\tilde{m}N} \left| \frac{e^{i\theta_y \tilde{m}} - 1}{e^{i\theta_y} - 1} \right|^2, \text{ where } \theta_y = \frac{2\pi\alpha y}{N}$$

23.35 Estimating Bounds for $|e^{i\phi} - 1|$

$|e^{i\phi}| \leq |\phi|$ because the chord length is always less than or equal to the arc length of a circle

$|e^{i\phi} - 1| = 2|\sin(\frac{\phi}{2})|$ using Euler's identity and double angle formula of $\phi = 2\frac{\phi}{2}$

Bounding this, we get $\frac{2|\phi|}{\pi} \leq |e^{i\phi} - 1|$

Combining both sides, $\frac{2|\phi|}{\pi} \leq |e^{i\phi} - 1| \leq |\phi| \forall \phi \in [-\pi, \pi]$

$$P(\searrow |y_c\rangle) = \left| \frac{e^{i\theta_{\hat{y}_c} \tilde{m} \alpha} - 1}{e^{i\theta_{\hat{y}_c} \alpha} - 1} \right|^2, \hat{y}_c = y_c \alpha - cN \in [-\frac{\alpha}{2}, \frac{\alpha}{2})$$

To find the lower bound of this probability, find the lower bound of the numerator & upper bound of the denominator

23.36 Estimating Probability of Step 2

The upper bound of the denominator comes from previous derivations

$$|e^{i\theta\hat{y}_c/\alpha} - 1| \leq \frac{\theta\hat{y}_c}{\alpha}$$

The lower bound of the numerator when $\tilde{m} = m$

With $2\pi m\hat{y}_c/N \in (-\pi, \pi)$, previous derivations give

$$\frac{2|\frac{m}{\alpha}\theta\hat{y}_c|}{\pi} \leq |e^{i\theta\hat{y}_c\tilde{m}/\alpha}| \therefore P(\searrow |y_c\rangle) = \frac{2m}{\pi}$$

Follow this assumption for $\tilde{m} = m + 1$

$$P(\searrow \text{one } y_c) > \frac{2}{\pi^2} \text{ or } \frac{4}{\pi^2} - \mathcal{E} \text{ as } m \rightarrow \infty$$

This satisfies CTC looping theorem. However, the assumption is invalid

So for $\tilde{m} = m + 1$, $-\frac{3\pi}{2} < \frac{2\pi(m+1)}{N}\hat{y}_c < \frac{3\pi}{2}$

Using the same technique as before,

$$K \frac{2|\phi|}{\pi} \leq 2|\sin(\frac{\phi}{2})|, \forall \phi \in [-\frac{3\pi}{2}, \frac{3\pi}{2}]$$

where $K = \frac{2}{3}\sin\frac{\pi}{4} = \frac{\sqrt{2}}{3}$

Substituting in $\phi = \frac{2\pi(m+1)\hat{y}_c}{N}$, & $\theta_y = \frac{2\pi\alpha y}{N}$,

The amplitude becomes $\frac{2K\tilde{m}}{\pi}$, $\tilde{m} = m + 1$

Combining for both $\tilde{m} = m$ & $\tilde{m} = m + 1$, $\frac{2K\tilde{m}}{\pi}$ is the stronger bound

$$P(\searrow y_c) \geq \frac{1}{\tilde{m}N} \frac{4K^2\tilde{m}^2}{\pi^2} \geq \frac{m}{N} \frac{4K^2}{\pi^2}$$

$$P(\searrow y_c) \geq \frac{\alpha m}{N} \frac{4K^2}{\pi^2} > \frac{1}{2} \frac{4K^2}{\pi^2} = \frac{2k^2}{\pi^2} \approx 4.5\%$$

This is the conservative estimate

However, usually, when $\alpha \ll M < N$, $\frac{m+1}{N} \approx \frac{m}{N}$

$$P(\searrow 1y_c) > \frac{4}{\pi^2} - \mathcal{E}, \text{ where } \mathcal{E} \rightarrow 0, m \rightarrow \infty$$

In general, $P(\searrow 1y_c) > \begin{cases} 4.5\%, 3\alpha > M \text{ worst case} \\ 40.5\%, \text{ usually} \end{cases}$

Because P is independent of M, CTC theorem can be applied to get y_c within T loops (\mathcal{E} -tolerance)

23.37 Step 3: Associate $\{y_c\}_{c=0}^{\alpha-1}$ with $\{c/\alpha\}_{c=0}^{\alpha-1}$

Each $\frac{y_c}{N}$ is uniquely close to $\frac{c}{\alpha}$. If c is coprime to α , we can compute m & find α .

For each $[cN \pm \frac{\alpha}{2})$ around $y_c\alpha$, we have $|\frac{c}{\alpha} - \frac{y_c}{N}| \leq \frac{1}{2M^2}$

If $p, q \in \mathbb{R}$ s.t $0 < p, q \leq M, \forall \frac{l}{p} \& \frac{k}{q}, |\frac{l}{p} - \frac{k}{q}| \geq \frac{1}{M^2}$

$\therefore c/\alpha$ is closer to y_c/N than any n/d for $d \leq M$

y_c/N is uniquely close to $c/\alpha \Rightarrow y_c$ is uniquely close to $c\frac{N}{\alpha}$

where N/α is the frequency of f between m & $m+1$

Here, $\{y_c\}$ is uniquely associated with $\{c \cdot \text{freq}\}$

23.38 Step 4: CFA that Produces c/α from y_c

Continued fraction algorithm takes $x \in \mathbb{R}$ and produce a sequence of $\{n_k/d_k\}$ that approaches x .

The $c \leftrightarrow y_c$ may not satisfies $c \nmid \alpha$. $\frac{c}{\alpha} = \frac{n}{d}$ but $\frac{c}{\alpha}$ may not be in the most reduced form \therefore we can't imply $c = n$ & $\alpha = d$

CFA can be used to produce a unique $\frac{c}{\alpha}$ closest to $\frac{y_c}{N}$

Properties of CFA

1. CFA produces a reduced fraction $\frac{n_k}{d_k}$ at the end of k th iteration. $\frac{n_k}{d_k}$ is the k th convergent of x .

$$\text{Let } x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots + \frac{1}{a_n}}}}$$

Each k th convergent expand up to $a_{n=k}$

2. $\forall x \in \mathbb{R}, \lim_{k \rightarrow \infty} (\frac{n_k}{d_k}) = x$
3. For rational x , k is finite
4. Shor's CFA generated $\frac{n}{d}$ within \mathcal{E} of x . In some case, n/d converges exactly
5. Denominators $\{d_k\}$ is strictly increasing $\forall x \in \mathbb{R}$ and \leq denominator of x regardless of form
6. If $|\frac{n}{d} - x| < \frac{1}{d^2}$, then $\frac{n}{d} \in (\frac{n_k}{d_k})_{k=0}^k$
 $\frac{n}{d}$ appears in the convergents
7. When $x = \frac{p}{q}$, CFA completes in $O(\log^3 q)$

Using CFA to Produce c/α

Apply CFA to $x = y_c/N$ & $\mathcal{E} = \frac{1}{(2M^2)}$

$$\alpha < M \therefore |\frac{c}{\alpha} - \frac{y_c}{N}| < \frac{1}{2\alpha^2}$$

Since $\frac{c}{\alpha}$ is closest to $\frac{y_c}{N}$ & $\frac{c}{\alpha}$ is in the convergent, CFA terminates in c/α for $d_k \leq M$.

23.39 Step 5: Measuring $y_c \leftrightarrow c \phi \alpha$ in Constant Time

To show this:

- Find the ratio between the least likely & most likely y_c

To do this, bound the amplitude for the most likely y_c

Numerator upper bound: $|e^{i\theta\hat{y}_c\tilde{m}/a} - 1| \leq \left|\frac{\theta\hat{y}_c\tilde{m}}{a}\right|$

Denominator lower bound: $|e^{i\theta\hat{y}_c\tilde{m}/a} - 1| \leq L \frac{2|\theta\hat{y}_c\tilde{m}/a|}{\pi}$

Combine top & bottom, $P(\searrow y_c) \leq \frac{1}{\tilde{m}N} \frac{4L^2\tilde{m}^2}{\pi^2} \leq \frac{m+1}{N} \frac{4L^2}{\pi^2}$

With least likely probability $P(\searrow y_c) \geq \frac{m}{N} \frac{4K^2}{\pi^2}$,

$$\frac{P(\text{least likely } y_c)}{P(\text{most likely } y_c)} \geq \frac{mK^2}{(m+1)L^2} \geq \frac{2K^2}{3L^2} \approx 7.2\%$$

If $a \ll M < N, K, L \rightarrow 1$ & $\frac{m}{m+1} \rightarrow 1 \therefore P \geq 1 - \mathcal{E}$ usually

- Show that $P(c \phi \alpha)$ is constant (c, α random)

$P(c \phi \alpha) = P(\neg(2|c \wedge 2|\alpha) \wedge \dots \wedge \neg(p_k|c \wedge p_k|\alpha))$,

where $p_k = k$ th prime, $= \prod_{p \in \text{prime}}^{\text{finite}} P(\neg(p|c \wedge p|\alpha))$

With $P(p|c) = \frac{1}{p} \therefore P(\neg(p|c \wedge p|\alpha)) = 1 - \frac{1}{p^2}$

$$P(c \phi \alpha) \geq \prod_{p \in \text{prime}}^{\infty} \left(1 - \frac{1}{p^2}\right) = \zeta(2) \approx 60.7\%$$

Finally, to prove that $y_c \leftrightarrow c \phi \alpha$ in constant time, find lower bound of $P(\mathcal{B})$, where $\mathcal{B} = \{y_b | y_b \in \mathcal{C} \text{ \& } b \phi \alpha\}$

$$P(\mathcal{B}) = P(\mathcal{B}|\mathcal{C})P(\mathcal{C}) = \sum_{b \in \mathcal{B}} P(y_b) / \sum_{c \in \mathcal{C}} P(y_c) \geq \frac{|\mathcal{B}|P(y_c \text{ min})}{|\mathcal{C}|P(y_c \text{ max})} \geq q \times .072$$

The conservative lower bound gives $P(\mathcal{B}) \approx 2\%$

Normally, $P(\mathcal{B}) \approx 26.6\%$

Because P is independent of N , we can invoke CTC theorem

In some instances, it is possible to get $d = a$ when $y_c \notin \mathcal{B}$, fix this by testing for $f(1) = f(1 + d)$ everytime

23.40 Full Algorithm

- Select T based on \mathcal{E} according to number of α in $[0, N-1]$
- Repeat loop at most T times

1. Apply Shor's circuit
 2. Measure \mathcal{QFT} to get y
 3. Apply CFA to y/N with $\mathcal{E} = \frac{1}{2M^2}$ to get $\frac{n}{d}$
 4. Test $f(1) = f(1 + d)$, if true $d = a$ (success) break loop
 5. Otherwise next pass
- If loop end after T passes, failed. Else, α is found

23.41 Full General Case Complexity

- Hadamard: $O(\log M)$
- \mathcal{QFT} : $O(\log^2 M)$
- U_f : at least $O(\log^4 M)$ for RSA factoring
- Outer loop: $O(T) = O(1)$
- Classical CFA: $O(\log^3 M)$

These are done in series so they are $O(\log^3 M)$ relative to the oracle & $O(\log^4 M)$ absolute for RSA oracle.

Chapter 24

Euclidean Algorithm & Continued Fractions

24.1 Long Division

LDA does $A = qB + r$ in $O(\log^2 X)$, where $X = \max\{A, B\}$

24.2 Euclidean Algorithm EA(P, Q) $P > Q$

To compute $EA(P, Q)$, set $P, Q = r_0, r_1$

$$r_k = q_k \cdot r_{k+1} + r_{k+2}$$

When $r_{k+2} = 0$, $gcd = r_{k+1}$

EA has $\log X$ loops with $\log^2 X$ LDA within each loop making it $\log^3 X$

24.3 Continued Fractions Algorithm CFA

The numerator of x as a continued fraction is $\{a_k\}$

$\forall x = P/Q, \{a_k\} = \{q_k\}$ (From EA)

Alternatively, $x = a_0; a_n = (\lfloor a_n - 1 \rfloor - a_{n-1})^{-1}$

If the fraction = 0, break

24.4 Convergents

The k th convergent of x is the continued fraction up to a_k

The convergences zigzag from x . and can be written as $a_k = n_k/d_k$. To compute the k th convergence,

Set $n_0, n_1 = a_0, a_1 a_0 + 1$ & $d_0, d_1 = 1, a_1$

Then, repeat for both n & k : $n = a_k n_{k-1} + n_{k+2}$

24.5 Properties of Convergences

1. $\forall x \in \mathbb{R}, \lim_{x \rightarrow \infty} \frac{n_k}{d_k} = x$
2. For rational x , k is finite
3. Assuming $\frac{n_k}{d_k} \neq x, \frac{n_k}{d_k} = \begin{cases} > x, \text{ odd } k \\ < x, \text{ even } k \end{cases}$
4. $|x - \frac{n_k}{d_k}| \leq \frac{1}{d_k d_{k+1}}$ (error bound)
5. $|x - \frac{n_k}{d_k}| \leq |x - \frac{n}{d}| \forall d \leq d_k$ (best estimate)
6. $|\frac{n_{k-1}}{d_{k-1}} - \frac{n_k}{d_k}| = \frac{1}{d_k d_{k+1}}$ (bounds between convergents)
7. $d_{k+1} > d_k$ & rational $x \leq \{d_k\}$
8. If $|\frac{n}{d} - x| < \frac{1}{2d^2}, \frac{n}{d} = \frac{n_{k_0}}{d_{k_0}} \in \{\frac{n_k}{d_k}\}_{k=0}^k$

24.6 CFA Complexity

Shor's CFA uses property 4 with $\mathcal{E} = \frac{1}{d^2}$

Because CFA is based on EA, the time complexity is $O(\log^3 X)$