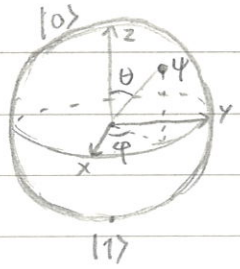
QC & QI Notes

6/23/2025 (pp. 1-32)

✳ Introduction

- Superposition: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- Rewriting & w/ Bloch Sphere:



$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$

*Restricted to 1 qubit

- Multiple qubits
  - ↳ e.g. $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$
  - ↳ After measuring 0 on 1st qubit:
    - ↳ $|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$ (post-measurement state, normalized)

⁂ Bell state / EPR Pair: $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

✳ Quantum Computation

- Qubit gates are unitary matrices ($U^\dagger U = I$)
  - ↳ Preserves norm of probability
  - ↳ $U^\dagger$ (adjoint) = complex conjugate + transpose of U
  - ↳ Only constraint on quantum gates

⁂ An arbitrary 2×2 unitary matrix can be decomposed as

$$U = e^{i\alpha}\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}\begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}\begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}$$

⁂ Some important gates

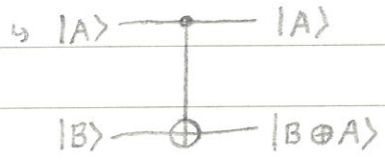
- ↳ NOT (x) gate: $\alpha|0\rangle + \beta|1\rangle$ —[X]— $\beta|0\rangle + \alpha|1\rangle$
- ↳ Z gate: $\alpha|0\rangle + \beta|1\rangle$ —[Z]— $\alpha|0\rangle - \beta|1\rangle$
- ↳ Hadamard gate: $\alpha|0\rangle + \beta|1\rangle$ —[H]— $\alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

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

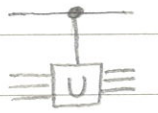
- Controlled-NOT (CNOT) gate
  - Control qubit + target qubit input
  - If control=0, no change to target, else flip.



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

%% Quantum gates are always reversible, since they're unitary.

- Controlled-U gate
  - If control=0, no change to targets, else flip

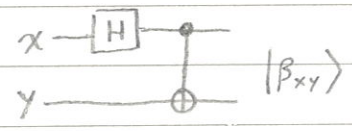


- Measurement
  - Converts qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to classical bit M

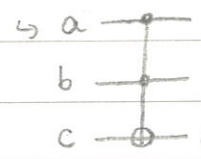
- Bell states

In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} = \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} = \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} = \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} = \|\beta_{11}\rangle$

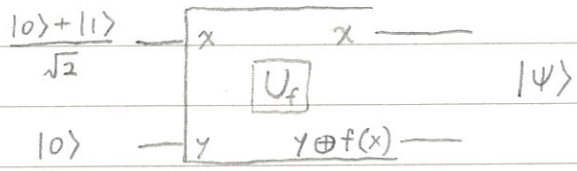
Bell states



$$|\beta_{xy}\rangle \equiv \frac{|0,y\rangle + (-1)^x |1,\bar{y}\rangle}{\sqrt{2}}, \quad \bar{y} = \text{negation of } y$$

- Toffoli gate
  - ↳ Used to simulate classical logic circuit using quantum circuit
  - ↳ 2 control bits, 1 target (flipped if both controls are 1)
  - ↳ 

- Quantum Parallelism
  - ↳ Allows quantum computers to evaluate $f(x)$ for many values of x simultaneously.
  - ↳ e.g.



"black box"

  - ↳ Results in state $\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$, contains information about both $f(0)$ and $f(1)$.
  - ↳ Note: single $f(x)$ circuit used in U_f

- Hadamard transform ($H^{\otimes n}$)
  - ↳ Performed on n qubits in $|0\rangle$ state: $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle$
  - ↳ Just H gates in parallel on n qubits

- w/ Hadamard transform:
  1. n-bit input x and 1-bit output $f(x)$
  2. Prep $n+1$ qubit state $|0\rangle^{\otimes n}|0\rangle$
  3. Apply Hadamard transform to 1st n qubits, then U_f

∴ Result: $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$

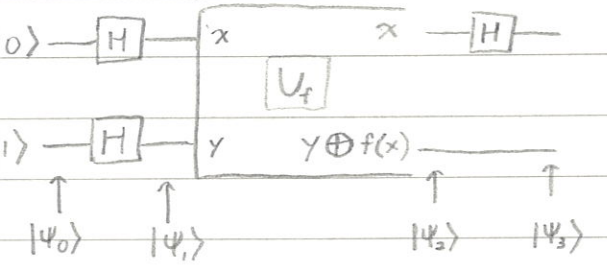
(Not too useful yet b.c. the probability in measuring result)

QC & QI

6/24/2025 (pp. 32–59)

✳ Quantum Algorithms

- Deutsch's Algorithm
  - ↳ Prepare 1st qubit as $(|0\rangle+|1\rangle)/\sqrt{2}$ and 2nd as $(|0\rangle-|1\rangle)/\sqrt{2}$.
  - ↳

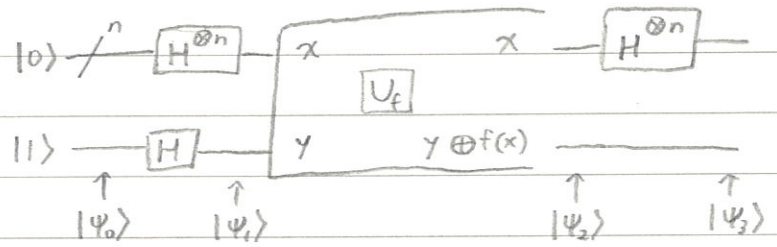


  - ↳ $|\psi_1\rangle = \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$
  - ↳ $|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)=f(1) \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)\neq f(1) \end{cases}$
  - ↳ $|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)=f(1) \\ \pm|1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)\neq f(1) \end{cases}$
  - ∴ $\boxed{|\psi_3\rangle = \pm|f(0)\oplus f(1)\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]}$ ← $f(0)\oplus f(1) = \begin{cases} 0 & \text{if } f(0)=f(1) \\ 1 & \text{otherwise} \end{cases}$
  - ↳ Ability to determine global property $f(0)\oplus f(1)$ of $f(x)$ w/ one evaluation

- Deutsch-Jozsa Algorithm
  - ↳ Deutsch's problem: Alice selects number x from 0 to 2^n-1
    Bob applies $f(x)$ and replies 0 or 1
  - ↳ How many queries to determine if $f(x)$ is constant / balanced?
  - ↳ Classically, need $2^n/2+1$ queries

↳ Prepare $|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$ of n qubits in $|0\rangle$ and one $|1\rangle$

↳



↳ $|\psi_1\rangle = \sum_{x=\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ (superpos. of all values)

↳ $|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$

Hadamard transform on state $|x\rangle$: $H^{\otimes n}|x\rangle = \frac{\sum_z (-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}}$

↳ So $\boxed{|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^n} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]}$

↳ If Alice measures all $0 \rightarrow f(x)$ is const, else balanced

- Types of quantum algorithms (broadly speaking)

1. Algorithms based on quantum Fourier transform

↳ Discrete FT: $Y_k \equiv \sum_{j=0}^{N-1} e^{2\pi i jk/N} x_j$, set $\{x_i\} \rightarrow \{y_i\}$

↳ QFT: $|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i jk/2^n} |k\rangle$, acts on $|j\rangle$ for $0 \le j \le 2^n - 1$

2. Quantum Search Algorithm

↳ Given search space of size N, how fast can we find element satisfying a property

3. Quantum Simulation

↳ Simulating natural quantum-mechanical systems

QC & QI

6/25/2025 (pp. 60 - 97)

* Introduction to QM

- Skimmed

- The Pauli Matrices

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \qquad \sigma_1 \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_3 \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Hilbert space $\leftrightarrow$ inner product space
  - ↳ In finite-dimensional complex vector spaces

- Completeness relation: $\sum_i |i\rangle\langle i| = I$
  - ↳ For orthonormal basis

- Cauchy-Schwarz inequality: $|\langle v|w\rangle|^2 \leq \langle v|v\rangle\langle w|w\rangle$
  - ↳ For any vectors $|v\rangle$ and $|w\rangle$

%% A normal matrix is Hermitian iff. it has real eigenvalues
- ↳ A is normal if $AA^\dagger = A^\dagger A$
- ↳ Spectral decomp: A is normal iff. it's diagonalizable

- A is positive if $\langle v|A|v\rangle \geq 0$
- A is positive definite if $\langle v|A|v\rangle > 0$

- Commutator: $[A, B] \equiv AB - BA$
- Anticommutator: $\{A, B\} \equiv AB + BA$
  - ↳ For Pauli matrices, $[\sigma_j, \sigma_k] = 2i \sum_{\ell=1}^{3} \epsilon_{jk\ell} \sigma_\ell$
    - ↳ $\epsilon_{jk\ell} = 0$ except $\epsilon_{123} = \epsilon_{231} = \epsilon_{312} = 1$
      and $\epsilon_{321} = \epsilon_{213} = \epsilon_{132} = -1$

✳ Postulates of Quantum Mechanics

1. Associated to any isolated physical system is a Hilbert space called the state space of system
   - ↳ Hilbert space = Complex vector space w/ inner product
   - ↳ System described completely by state vector: unit vector in that state space

2. Evolution of closed quantum system is described by unitary operator

$$|\psi'\rangle = U|\psi\rangle$$

For continuous time: the evolution is described by the Schrödinger equation:

$$i\hbar \frac{d}{dt}|\psi\rangle = H|\psi\rangle$$

- ↳ H is a Hermitian operator known as the Hamiltonian of the system.

3. Quantum measurement described by collection $\{M_m\}$ of measurement operators, which act on state space.
   - ↳ Probability to measure m: $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$
   - ↳ State of system after measurement: $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$
   - ↳ Satisfy Completeness relation $\sum_m M_m^\dagger M_m = I$

     Since probabilities add to 1.

4. State space of composite physical system is the tensor product of the state spaces of component physical systems

QC & QI

6/26/2025 (pp. 97-119)

✳ The Density Operator

- Let there be a quantum system in one of a number of states $|\psi_i\rangle$, w/ probabilities p_i
  - ↳ Ensemble of pure states: $\{p_i, |\psi_i\rangle\}$
  - ↳ Density operator: $\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|$

- Time evolution of closed quantum system
  - ↳ If initial state $|\psi_i\rangle$ w/ prob. $p_i \longrightarrow U|\psi_i\rangle$ w/ prob p_i

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \xrightarrow{U} \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger = \boxed{U\rho U^\dagger}$$

(evolution of density operator)

- Performing measurement M_m
  - ↳ If initial state was $|\psi_i\rangle$, prob. of getting m is

$$p(m|i) = \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = \boxed{\mathrm{tr}\left(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|\right)}$$

  - ↳ Prob. of obtaining result m: $\boxed{\mathrm{tr}(M_m^\dagger M_m \rho)}$
  - ↳ After measurement, density operator is $\boxed{\rho_m = \frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)}}$

- ✳ A quantum system whose state $|\psi\rangle$ is known exactly is a pure state, else mixed state
  - ↳ Pure state: density operator $\rho = |\psi\rangle\langle\psi|$, $\mathrm{tr}(\rho^2) = 1$
  - ↳ Mixed state: mix of pure states in ensemble for ρ, $\mathrm{tr}(\rho^2) < 1$

- ✳ An operator ρ is the density operator associated to ensemble $\{p_i, |\psi_i\rangle\}$ iff:
  1. Trace condition: ρ has trace 1
  2. Positivity condition: ρ is a positive operator

- Say that $|\tilde{\psi}_i\rangle$ generates operator $\rho \equiv \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$
  - ↳ $|\tilde{\psi}_i\rangle = \sqrt{p_i}\,|\psi_i\rangle$

- The sets $|\tilde{\psi}_i\rangle$ and $|\tilde{\varphi}_j\rangle$ generate same density matrix iff

$$\boxed{|\tilde{\psi}_i\rangle = \sum_j u_{ij} |\tilde{\varphi}_j\rangle}$$

where u_{ij} is unitary matrix of complex numbers

↳ Make $|\tilde{\psi}_i\rangle$ and $|\tilde{\varphi}_j\rangle$ have same # of elements by padding w/ 0's

- Reduced density operator
  - ↳ Describes subsystems of a composite quantum system
  - ↳ Let there be 2 systems A, B, described by ρ^{AB}
  - ↳ Reduced density operator for A is $\rho^A \equiv tr_B(\rho^{AB})$
    - ↳ $tr_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2|\, tr(|b_1\rangle\langle b_2|)$
      - ↳ Partial trace over B
      - ↳ $|a_1\rangle, |a_2\rangle$ are state vectors in A; $|b_1\rangle, |b_2\rangle$ in B
      - ↳ $tr(|b_1\rangle\langle b_2|) = \langle b_2 | b_1\rangle$

※ If ρ is dens. op. for A; σ for B → $\boxed{\rho^{AB} = \rho \otimes \sigma}$

✳ Schmidt Decomposition and Purifications

- Schmidt decomposition: suppose $|\psi\rangle$ is a pure state of a composite system AB. Then there exists orthonormal states $|i_A\rangle$ for A and $|i_B\rangle$ for B such that

$$\boxed{|\psi\rangle = \sum_i \lambda_i |i_A\rangle\langle i_B|}$$

where $\lambda_i \geq 0$, real numbers satisfying $\boxed{\sum_i \lambda_i^2 = 1}$, Schmidt coefficients

↳ Schmidt number: amount of nonzero λ_i

↳ "Amount of entanglement" between A & B (roughly)

- Purification: given state ρ^A of system A, possible to introduce another system R and define pure state $|AR\rangle$ for joint system AR, i.e. $\rho^A = tr_R(|AR\rangle\langle AR|)$
  - ↳ Pure state $|AR\rangle$ reduces to ρ^A when we look at A alone
  - ↳ R = reference system

$$|AR\rangle \equiv \sum_i \sqrt{P_i}\, |i^A\rangle |i^R\rangle$$

where $\rho^A = \sum_i P_i |i^A\rangle\langle i^A|$

QC & QI

6/28/2025 (pp. 191 – 204)

* Quantum Algorithms

- Some gates:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad T \equiv \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}$$

(Hadamard) (Phase gate) ("π/8" gate)

∴ $H = (X+Z)/\sqrt{2}$, $S = T^2$

- Rotation operators

↳ $R_x(\theta) = e^{-i\theta \hat{X}/2} = \cos\left(\frac{\theta}{2}\right)\hat{I} - i\sin\left(\frac{\theta}{2}\right)\hat{X} = \begin{bmatrix} \cos\theta/2 & -i\sin\theta/2 \\ -i\sin\theta/2 & \cos\theta/2 \end{bmatrix}$

↳ $R_y(\theta) = e^{-i\theta \hat{Y}/2} = \begin{bmatrix} \cos\theta/2 & -\sin\theta/2 \\ \sin\theta/2 & \cos\theta/2 \end{bmatrix}$

↳ $R_z(\theta) = e^{-i\theta \hat{Z}/2} = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$

- Z-Y decomposition for single qubit: if U is a unitary operator, then for some $\alpha, \beta, \gamma, \delta$, we can write

$$\boxed{U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)}$$

↳ Similarly for any 2 axes

↳ In fact, this can be done for any 2 non-parallel real unit vectors.

- Some identities:

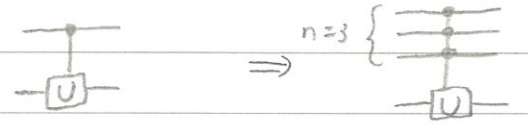
↳ $\hat{H}\hat{X}\hat{H} = \hat{Z}$

↳ $\hat{H}\hat{Y}\hat{H} = -\hat{Y}$

↳ $\hat{H}\hat{Z}\hat{H} = \hat{X}$

* Controlled operations

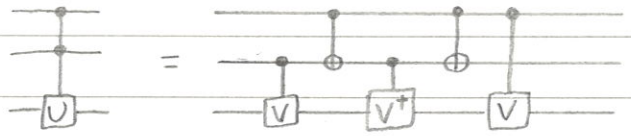
- Controlled-U operation

↳ 

↳ $C^n(U)\,|x_1x_2x_3\ldots x_n\rangle|\psi\rangle = |x_1x_2x_3\ldots x_n\rangle\, U^{x_1x_2x_3\ldots x_n}|\psi\rangle$

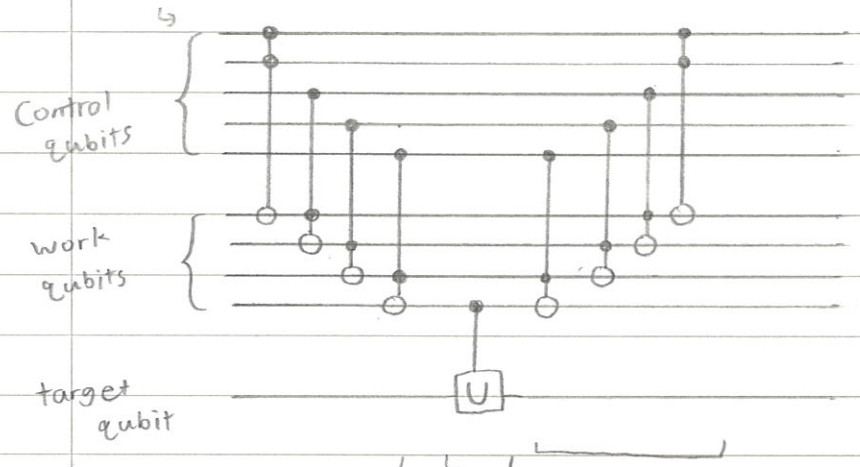
↳ $U^{x_1x_2\ldots x_n}$ means U is applied iff. $x_1=x_2\ldots=x_n=1$

↳ For an operator V satisfying $V^2=U$,



- Implementation of $C^n(U)$ w/ Toffoli gates

↳



Example w/ $n=5$ control qubits $|c_i\rangle$ and 4 work qubits

Work qubits set to $|0\rangle$

*Measurement

- Principle of deferred measurement: measurement can always be moved from intermediate stage of quantum circuit to the end
  - ↳ If measurement results are used at any stage: classically controlled operations can be replaced by conditional quantum operators

- Principle of implicit measurement: WLOG, any unterminated quantum wires (qubits not yet measured) at end of quantum circuit may be assumed to be measured.

*Universal quantum gates

- A set of gates are universal for QC if any unitary operation may be approximated to arbitrary accuracy by a quantum circuit using only those gates

- A d-dimensional unitary matrix U can be decomposed into product of 2-level unitary matrices
  - ↳ 2-level as in they act non-trivially on 2 or less vector components.

  - ⁂ Single qubit and CNOT gates can (together) create an arbitrary 2-level unitary operator → they are universal.

- Approximations
  - ↳ Set of unitary operators is cont. → Can't implement exactly w/ discrete gates, but can approximate.

↳ U is target unitary operator, V is what we use:

$$E(U,V) \equiv \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$$

(Error when V is implemented by U)

※ $\pi/8$ and Hadamard gates can be used to approximate any single-qubit unitary operator

※ There are states of n qubits that take $\Omega\left(\frac{2^n \log(1/\epsilon)}{\log(n)}\right)$ operations to approx. within ϵ

↳ Approx'ing arbitrary unitary gates is hard

↳ Arbitrary U on n qubits can be approx'd within ϵ using $O\left(n^2 4^n \log^c(n^2 4^n/\epsilon)\right)$ gates.

✳ Quantum Circuit Model of Computation

- Features

1. Classical resources
   ↳ Ideally, not needed, but useful for things like error correction, e.g.
2. Suitable state space
   ↳ n qubits → 2^n-dimensional Hilbert space
3. Ability to prepare states in computational basis
4. Ability to perform quantum gates
5. Ability to perform measurements in computational basis

QC & QI

6/29/2025 (pp. 204-247

✳ Simulation of Quantum Systems

- Dynamical behavior of simple quantum systems governed by Schrödinger:

$$i\frac{\partial}{\partial t}\psi(x) = \left[-\frac{1}{2m}\frac{\partial^2}{\partial x^2} + V(x)\right]\psi(x)$$

↳ Position representation $\psi(x) = \langle x|\psi\rangle$

- For a time-independent H, $|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$

↳ From diff eq

↳ 1st-order solution $|\psi(t+\Delta t)\rangle \approx (I - iH\Delta t)|\psi(t)\rangle$

- Trotter formula: let A and B be Hermitian operators. Then for any real t,

$$\lim_{n\to\infty}\left(e^{iAt/n}e^{iBt/n}\right)^n = e^{i(A+B)t}$$

↳ Other results: $e^{i(A+B)\Delta t} = e^{iA\Delta t}e^{iB\Delta t} + O(\Delta t^2)$

$$e^{i(A+B)\Delta t} = e^{iA\Delta t/2}e^{iB\Delta t}e^{iA\Delta t/2} + O(\Delta t^3)$$

- Quantum simulation

↳ Input Hamiltonian $H = \sum_k H_k$ acting on N-dimensional system

Each H_k acts on small subsystem

↳ Input initial state $|\psi_0\rangle$ of system at $t=0$

↳ Desired output: $|\tilde{\psi}(t_f)\rangle$ of system at t_f

↳ For accuracy δ, we want $|\langle\tilde{\psi}(t_f)|e^{-iHt_f}|\psi_0\rangle|^2 \geq 1-\delta$

1. $|\tilde{\psi}_0\rangle \leftarrow |\psi_0\rangle$, $j=0$
2. $|\tilde{\psi}_{j+1}\rangle = U_{\Delta t}|\tilde{\psi}_j\rangle$
3. $j = j+1$, repeat 2-3 until $j\Delta t \geq t_f$
4. $|\tilde{\psi}(t_f)\rangle = |\tilde{\psi}_j\rangle$

✳ Use Trotter approximation and $H = \sum_k H_k$ in exponent $U = e^{-iHt}$

* The Quantum Fourier Transform (QFT)

- Discrete Fourier Transform
  - ↳ Takes input of complex vectors $X_0 \dots X_{N-1}$
  - ↳ Outputs transformed vectors $Y_0 \dots Y_{N-1}$

$$Y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N}$$

- QFT
  - ↳ Action on orthonormal basis $|0\rangle \dots |N-1\rangle$:

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$$

  - ↳ Product representation:

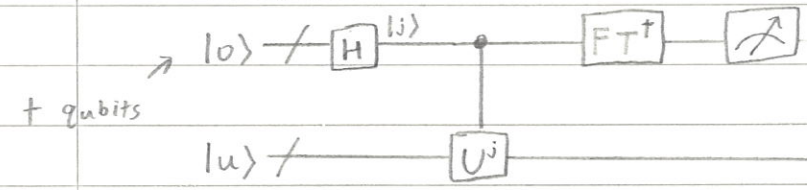
$$|j_1 \dots j_N\rangle \longrightarrow \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}}$$

  - ↳ For n qubits and basis $|0\rangle \dots |2^n - 1\rangle$
  - ↳ Write state $|j\rangle$ w/ binary $|j_1 j_2 \dots j_N\rangle$, $N = 2^n$
  - ↳ Binary fraction: $0.j_1 j_2 \dots j_N = j_1/2 + j_2/4 + \dots + j_N/2^N$

※ QFT is unitary

※ Using unitary gates, QFT can be implemented with $\Theta(n^2)$.

- Phase estimation
  - ↳ Suppose unitary U has eigenvector $|u\rangle$ w/ eigenvalue $e^{2\pi i \varphi}$
  - ↳ phase estimation algorithm can estimate φ.
  - ↳ Procedure:



  - ↳ $|u\rangle$ is eigenstate of U w/ eigenvalue $e^{2\pi i \varphi}$
  - ↳ Approx. of φ is accurate to $t - \left[\log\left(2 + \frac{1}{2\epsilon}\right)\right]$ bits, prob. of success $\geq 1 - \epsilon$

↳ 1st step: Hadamard gate + controlled U gate on t qubits initially $|0\rangle$

↳ Final state of t qubits is

$$\frac{1}{2^{t/2}}\left(|0\rangle+e^{2\pi i 2^{t-1}\varphi}|1\rangle\right)\left(|0\rangle+e^{2\pi i 2^{t-2}\varphi}|1\rangle\right)\cdots\left(|0\rangle+e^{2\pi i 2^{0}\varphi}|1\rangle\right)$$

$$=\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}e^{2\pi i\varphi k}|k\rangle$$

↳ 2nd step: apply inverse QFT to get φ

✳ Phase estimation Applications

• Order-finding

↳ For pos. int. x & N w/ $x<N$ and no common factors, the order of x mod N is least positive int. r such that

$$x^r = 1 \pmod N$$

↳ Quantum algorithm: phase estimation on unitary operator

$$U|y\rangle \equiv |xy \pmod N\rangle$$

$$y \in \{0,1\}^L$$

↳ Eigenstates of U: $|u_s\rangle \equiv \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi i s k}{r}\right]|x^k \bmod N\rangle$

for int. $0 \le s \le r-1$

↳ From eigenvalue $\exp(2\pi i s/r)$, we can obtain order r

• Factoring

↳ Given a composite N, what prime numbers equal it when multiplied?

↳ Reduce factoring to order-finding

1. Let N be a L-bit composite number, and x a non-trivial solution to $x^2 = 1 \pmod N$ in $1 \le x \le N$.
Then at least 1 of $\gcd(x-1, N)$ and $\gcd(x+1, N)$ is a non-trivial factor of N that can be computed in $O(L^3)$ operations.

2. Suppose $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ is the prime factorization for an odd composite int.

Let x be int. chosen at random so that x is co-prime to N and $1 \leq x \leq N-1$. Then

$$P\left(r \text{ is even and } x^{r/2} \neq -1 \pmod{N}\right) \geq 1 - \frac{1}{2^m}$$

↳ Steps:

1. If N is even, return 2
2. If $N = a^b$ for $a \geq 1$ and $b \geq 2$, return a
3. Randomly choose x in $1 \leq x \leq N-1$.
   ↳ If $\gcd(x, N) > 1$, return $\gcd(x, N)$
4. Use order-finding subroutine to find order r of $x \bmod N$
5. If r is even and $x^{r/2} \neq -1 \pmod{N}$, compute $\gcd(x^{r/2}-1, N)$ and $\gcd(x^{r/2}+1, N)$
   ↳ Test if one of these is non-trivial factor → if so, return
   ↳ Else, fail.

- Hidden Subgroup Problem
  ↳ Given a periodic function, we can usually use a quantum algorithm to determine the period efficiently.
  ↳ General application of QFT

  ↳ e.g. Deutsch's algorithm, Simon's algorithm, order finding

QC & QI

6/30/2025 (pp. 248-276)

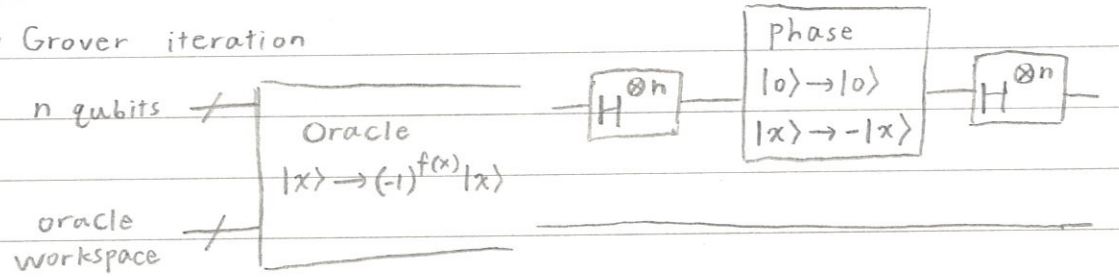
*Quantum Search Algorithm

- The Oracle: black box able to recognize solutions to problem
  - ↳ e.g. $f(x)=1$ if x is solution, else $f(x)=0$
  - ↳ Oracle qubit: $|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle$
  - ↳ If oracle qubit is initially $(|0\rangle - |1\rangle)/\sqrt{2}$:

$$|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \xrightarrow{O} (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$$

- Grover iteration



  - ↳ Initial n qubits are put into superposition

$$|\psi\rangle = \frac{1}{N^{1/2}}\sum_{x=0}^{N-1}|x\rangle$$

  - ↳ Overall effect of Grover iteration: $G = (2|\psi\rangle\langle\psi| - I)O$

- Geometric interpretation
  - ↳ Search space size N and M solutions
  - ↳ Let

$$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}}\sum_{x}{}''|x\rangle \quad \text{(sum over all non-solutions)}$$

$$|\beta\rangle \equiv \frac{1}{\sqrt{M}}\sum_{x}{}'|x\rangle \quad \text{(sum over all solutions)}$$

  - ↳ Then $|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$
  - ↳ Oracle is a reflection: $O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle$
  - ↳ So is $2|\psi\rangle\langle\psi| - I$.

↳ Combined effect is a rotation in space spanned by $|\alpha\rangle, |\beta\rangle$

↳ Let $\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$, so $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$

$$G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$$

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$

※ Repetition of G rotates $|\psi\rangle$ closer to $|\beta\rangle$.

$O(\sqrt{N/M})$ repetitions will produce a solution with high probability

✳ Quantum Counting

- Grover iteration + phase estimation
- Determines # of solutions (M) to search problem

- Rough steps
  - ↳ Let θ be the angle of rotation determined by Grover's
  - ↳ If Grover space spanned by $|\alpha\rangle, |\beta\rangle$, eigenvalues are $e^{i\theta}$ and $e^{i(2\pi-\theta)}$
  - ↳ Augment oracle (expand search space) to $2N$, so that $\sin^2(\theta/2) = M/2N$

  - ↳ Use phase estimation to estimate θ w/ prob. of success $\geq 1-\epsilon$
  - ↳ Use eq. $\sin^2(\theta/2) = M/2N$ to get estimate for M

QC & QI

7/12/2025 (pp. 277 - 297)

* Physical Realization of Quantum Computers

- well isolated to retain quantum properties
- But qubits have to be accessible

} balance

- Requirements
  1. Robustly represent quantum information
  2. Perform universal family of unitary transformations
  3. Prepare fiducial initial state
  4. Measure output result

- Harmonic Oscillator (example)
  - ↳ E.g. particle in parabolic potential well, $V(x) = m\omega^2 x^2/2$
  - ↳ Hamiltonian: $H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2$
    - ↳ $H = \hbar\omega\left(a^\dagger a + \frac{1}{2}\right)$ ← $a^\dagger$ and a are creation/annihilation operators
    - ↳ Eigenstates $|n\rangle$ of H, $n = 0, 1\ldots$ have properties

$$a^\dagger a |n\rangle = n|n\rangle$$

$$a^\dagger |n\rangle = \sqrt{n+1}\,|n+1\rangle$$

$$a|n\rangle = \sqrt{n}\,|n-1\rangle$$

  - ↳ Encode system: $|00\rangle_L = |0\rangle$

$$|01\rangle_L = |2\rangle$$

$$|10\rangle_L = (|4\rangle + |1\rangle)/\sqrt{2}$$

$$|11\rangle_L = (|4\rangle - |1\rangle)/\sqrt{2}$$

  - ↳ Let the system be spanned by above at $t = 0$ and evolve to $t = \pi/\hbar\omega$; $|n\rangle \to \exp(-i\pi a^\dagger a)|n\rangle = (-1)^n |n\rangle$
  - ↳ This is CNOT gate ($|0\rangle, |2\rangle, |4\rangle$ unchanged, $|1\rangle \to -|1\rangle$)

※ Drawback: not a digital representation

Matching eigenvalues to realize transformations

not possible for arbitrary U

- Optical Photon Computer
  - ↳ Dual-rail representation: instead of 1 electromagnetic cavity quantized in units of $\hbar\omega$, Consider 2 whose total energy is $\hbar\omega$
    - ↳ 2 states of qubit: whether photon is in 1 cavity or other

$$C_0|01\rangle + C_1|10\rangle$$

  - ↳ Generate photons by attenuating laser:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \quad \text{(coherent state)}$$

  - ↳ Computation:

1. Phase shifter
   - ↳ Light takes $\Delta \equiv (n-n_0)L/c_0$ more time to propagate dist. L in medium with high n
   - ↳ On single-photon state, $P|0\rangle = |0\rangle$, $P|1\rangle = e^{i\Delta}|1\rangle$
   - ↳ For dual-rail states: $C_0|01\rangle + C_1|10\rangle \longrightarrow C_0 e^{-i\Delta/2}|01\rangle + C_1 e^{i\Delta/2}|10\rangle$ (Like a rotation)

2. Beam Splitter
   - ↳ Acts on 2 nodes, desc. by creation/annihilation operators $a(a^\dagger)$ and $b(b^\dagger)$
   - ↳ Hamiltonian $H_{bs} = i\theta(ab^\dagger - a^\dagger b)$

     Beamsplitter performs $B = \exp[\theta(a^\dagger b - ab^\dagger)]$
   - ↳ If $|0_L\rangle = |01\rangle$ and $|1_L\rangle = |10\rangle$,

$$B = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = e^{i\theta\hat{Y}}$$

※ Phase shifter = rotation about z, beamsplitter = about y

3. Nonlinear Kerr media
   - ↳ Hamiltonian $H_{xpm} = -\chi a^\dagger a b^\dagger b$, for a and b propagating through medium
   - ↳ For crystal of length L, $K = e^{i\chi L a^\dagger a b^\dagger b}$ (unitary transform)

↳ For single-photon states, $K|00\rangle = |00\rangle$ $K|10\rangle = |10\rangle$

$K|01\rangle = |01\rangle$ $K|11\rangle = e^{i\chi L}|11\rangle$

↳ Let $\chi L = \pi$, so $K|11\rangle = -|11\rangle$

↳ For 2 dual-rail states spanned by $|e_{00}\rangle = |1001\rangle$,

$|e_{01}\rangle = |1010\rangle$, $|e_{10}\rangle = |0101\rangle$, $|e_{11}\rangle = |0110\rangle$

$$\underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}}_{U_{CN}} = \underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I \otimes H} \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}}_{K} \underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{I \otimes H}$$

↳ By factoring, CNOT (U_{CN}) can be constructed w/ K

QC & QI

9/14/2025 (pp. 297-352)

✳ Physical Realization of Quantum Computers (part 2)

- Optical Cavity QED
  - ↳ Electromagnetic cavity + atom

1. Fabry-Perot Cavity: approx. electric field to be monochromatic, occupying single spatial node

$$\vec{E}(r) = i\vec{\epsilon}E_0\left[ae^{ikr} - a^\dagger e^{-ikr}\right]$$

↳ a and $a^\dagger$ are creation/annihilation operators for photon

2. Two-Level Atoms: model atom as only having 2 states
   - ↳ Energy cons.: $\hbar\omega = E_2 - E_1$
   - ↳ $\int Y^*_{\ell m_1} Y_{1m} Y_{\ell_2 m_2}\, d\Omega = 0$
     - ↳ Parity cons. $\Delta\ell = \pm 1$
     - ↳ Angular momentum cons.: $m_2 - m_1 = \pm 1$

✳ The Jayne-Cummings Hamiltonian

↳ Interactions between 2-level atoms and EM field

$$H = H_{atom} + H_{field} + H_I$$

$$H = \frac{\hbar\omega_0}{2}Z + \hbar\omega a^\dagger a + g\left(a^\dagger\sigma_- + a\sigma_+\right) \quad \leftarrow \sigma_\pm = \frac{X \pm iY}{2}$$

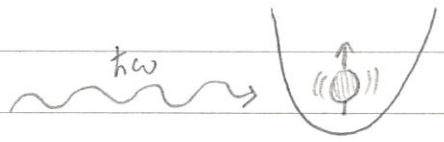
↳ Single photon & atom interactions
- ↳ Focus on single excitation in field mode, $H = -\begin{bmatrix} \delta & 0 & 0 \\ 0 & \delta & g \\ 0 & g & -\delta \end{bmatrix}$
- ↳ Basis states $|00\rangle$, $|01\rangle$, $|10\rangle$ (left = field, right = atom)
- ↳ Dropping $\hbar$'s and using time evolution $U = e^{-iHt}$,

$$U = e^{-i\delta t}|00\rangle\langle 00| +$$
$$\left(\cos\Omega t + i\frac{\delta}{\Omega}\sin\Omega t\right)|01\rangle\langle 01| +$$
$$\left(\cos\Omega t - i\frac{\delta}{\Omega}\sin\Omega t\right)|10\rangle\langle 10| -$$
$$i\frac{g}{\Omega}\sin\Omega t\left(|01\rangle\langle 10| + |10\rangle\langle 01|\right)$$

✳ Atom & field oscillate back-and-forth, exchanging quantum of energy at Rabi frequency $\Omega = \sqrt{g^2 + \delta^2}$

• Ion Traps

↳ Trap a few charged atoms in EM traps → cool until KE ≪ spin energy



Single particle in harmonic potential w/ 2 internal states
Interact w/ EM radiation

↳ Magnetic dipole interaction $H_I = -\vec{\mu} \cdot \vec{B}$, dipole moment $\vec{\mu} = \mu_m \vec{S}$

↳ $\vec{B} = B_1 \hat{x} \cos(kz - \omega t + \varphi)$, φ is phase

↳ Define Rabi freq. of spin as $\Omega = \mu_m B_1 / 2\hbar$

↳ Use $S_x = (S_+ + S_-)/2$

↳ If particle is cooled to low vibrational mode (width of oscillation small),

$$H_I = -\vec{\mu} \cdot \vec{B}$$
$$\approx \left[\frac{\hbar\Omega}{2}\left(S_+ e^{i(\varphi-\omega t)} + S_- e^{-i(\varphi-\omega t)}\right)\right]$$
$$+ \left[i\frac{\eta\hbar\Omega}{2}\left\{S_+ a + S_- a^\dagger + S_+ a^\dagger + S_- a\right\}\left(e^{i(\varphi-\omega t)} - e^{-i(\varphi-\omega t)}\right)\right]$$

↳ Quantum Computation

1. Single qubit operations: apply EM field tuned to freq ω_0
   ↳ H_I^{internal} becomes $\frac{\hbar\Omega}{2}(S_+ e^{i\varphi} + S_- e^{-i\varphi})$
   ↳ Tweak φ & interaction duration → $R_x(\theta) = \exp(-i\theta S_x)$
   $R_y(\theta) = \exp(-i\theta S_y)$

2. Controlled phase flip

↳ $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$ ← 1 qubit in atom's internal spin state other in $|0\rangle$ and $|1\rangle$ phonon states

3. Swap gate

↳ $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ ← Tune laser to $\omega_0 - \omega_z$

Arrange for phase to be such that $R_y(\pi)$ is performed on subspace spanned by $|01\rangle$ and $|10\rangle$

4. CNOT gate

↳ $CNOT_{jk} = H_k \overline{SWAP}_k C_j(z) SWAP_k H_k$

↳ Hadamard, swap gates, controlled phase flips (c)

• Nuclear Magnetic Resonance

↳ Single spin dynamics:

↳ Start w/ $H = -\vec{\mu} \cdot \vec{B}$, $\vec{\mu}$ is spin, $B = B_0 \hat{z} + B_1(\hat{x}\cos\omega t + \hat{y}\sin\omega t)$

↳ $H = \frac{\omega_0}{2}\hat{Z} + g(\hat{X}\cos\omega t + \hat{Y}\sin\omega t)$

↳ Spin-Spin Couplings:

↳ Through-space dipolar coupling: $H^D_{1,2} = \frac{\gamma_1 \gamma_2 \hbar}{4r^3}\left[\vec{\sigma}_1 \cdot \vec{\sigma}_2 - 3(\sigma_1 \cdot \hat{n})(\sigma_2 \cdot n)\right]$

↳ $\hat{n}$ = unit vec. in direction joining 2 nuclei

↳ Through-bond ("J-coupling"): $H^J_{1,2} = \frac{\hbar J}{4} Z_1 Z_2 + \frac{\hbar J}{8}\left[\sigma_+\sigma_- + \sigma_-\sigma_+\right]$

↳ Thermal equilibrium

↳ NMR uses ensemble of systems → measurement is an average

↳ Initial state is thermal eq state: $\rho = \frac{e^{-\beta H}}{Z}$

↳ $\beta = 1/k_B T$, $Z = tr(e^{-\beta H})$ ← ensures $tr(\rho) = 1$

↳ Magnetic readout

↳ Free induction decay signal $V(t) = V_0\, tr\left[e^{-iHt}\rho e^{iHt}(iX_k + Y_k)\right]$

↳ Quantum Computation:

↳ Refocusing: Consider 2-spin Hamiltonian $H = H^{SYS} + H^{RF}$

when large RF field applied at proper freq., approx.

$$e^{-iHt/\hbar} \approx e^{-iH^{RF}t/\hbar}$$

↳ Can define $R_{x_1} = e^{-i\pi X_1/4}$ and $R^2_{x_1}$ w/ high fidelity

• CNOT gate built from 1 evolution period of time $\frac{\hbar\pi}{4c}$ and several single-qubit pulses

QC & QI

9/15/2025 (pp. 353 - 373)

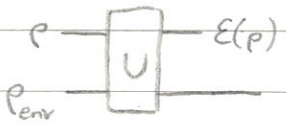
* Quantum Noise

- Classical Noise: model w/ stochastic processes
  - ↳ $\vec{q} = E\vec{p}$, $\vec{q}$ = output probabilities, $\vec{p}$ = input probabilities
    E = matrix of transition probabilities
  - ↳ E is the evolution matrix
    1) Positivity: non-negative entries
    2) Completeness: columns summing to 1

- Quantum operators: use density matrices
  - ↳ $\rho' = \mathcal{E}(\rho)$, $\mathcal{E}$ = quantum operation
    - ↳ e.g. $\mathcal{E}(\rho) = U\rho U^\dagger$ for unitary transformation

- An open quantum system: Consider as arising from interaction of principal system & environment (forms closed quantum system)

Closed system



Open system

$$\boxed{\mathcal{E}(\rho) = tr_{env}\left[U(\rho \otimes \rho_{env})U^\dagger\right]}$$

- Operator-Sum representation
  - ↳ Let $|e_k\rangle$ be orthonormal basis for state space of env
  - ↳ Let $\rho_{env} = |e_0\rangle\langle e_0|$ be initial state of env

$$\mathcal{E}(\rho) = \sum_k \langle e_k|U\left[\rho \otimes |e_0\rangle\langle e_0|\right]U^\dagger|e_k\rangle$$
$$= \boxed{\sum_k E_k \rho E_k^\dagger}, \quad E_k = \langle e_k|U|e_0\rangle$$

↑ operator-sum representation of $\mathcal{E}$

  - ↳ $\{E_k\}$ = operation elements for quantum operator $\mathcal{E}$

- ※ Completeness relation: $\boxed{\sum_k E_k^\dagger E_k = I}$ "trace-preserving"

- Physical interpretation of OSR
  - Consider measurement of env performed in $|e_k\rangle$ basis after U applies
  - This only affects state of env, not principal system

$$\rho_k = \frac{E_k \rho E_k^\dagger}{\mathrm{tr}(E_k \rho E_k^\dagger)} \leftarrow \text{state of principal system, given outcome } k \text{ occurs}$$

$$p(k) = \mathrm{tr}(E_k \rho E_k^\dagger) \leftarrow \text{Probability of outcome } k$$

$$\therefore \boxed{\mathcal{E}(\rho) = \sum_k p(k)\rho_k = \sum_k E_k \rho E_k^\dagger}$$

  - Action of quantum operation is equiv. to replacing state ρ w/ ρ_k, with prob. $p(k)$

- Measurements & OSR
  - Let principal system (Q) be in state ρ, and env. (E) in state σ.
  - Initial state: $\rho^{QE} = \rho \otimes \sigma$
  - Apply U and measure w/ projector P_m
  - Final state of QE: $\dfrac{P_m U(\rho \otimes \sigma) U^\dagger P_m}{\mathrm{tr}(P_m U(\rho \otimes \sigma) U^\dagger P_m)}$
  - Final state of Q alone (trace out E): $\dfrac{\mathrm{tr}_E(P_m U(\rho \otimes \sigma) U^\dagger P_m)}{\mathrm{tr}(P_m U(\rho \otimes \sigma) U^\dagger P_m)}$

QC & QI

7/16/2025 (pp. 373-398)

* Quantum noise & quantum operators

- Trace as a quantum operator: $\mathcal{E}(\rho) = \sum_{i=1}^{d} |0\rangle\langle i|\rho|i\rangle\langle 0| = \mathrm{tr}(\rho)|0\rangle\langle 0|$
- Partial trace is also quantum operator
  - ↳ Let $E_i : H_{QR} \to H_Q$, $E_i\left(\sum_j \lambda_j |e_j\rangle|j\rangle\right) = \lambda_i |e_i\rangle$
  - ↳ Let $\mathcal{E}$ be operator w/ operation elements $\{E_i\}$

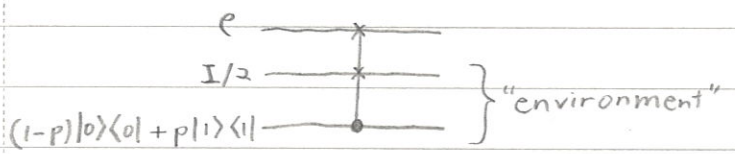
$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$$

$$\boxed{\mathcal{E}(\rho \otimes |j\rangle\langle j'|) = \mathrm{tr}_R(\rho \otimes |j\rangle\langle j'|)} \leftarrow \mathcal{E} = \mathrm{tr}_R$$

- Some examples of quantum noise

1. Depolarizing channel
   - ↳ Depolarize qubit w/ prob. p (replace w/ completely mixed state $I/2$)

$$\mathcal{E}(\rho) = \frac{pI}{2} + (1-p)\rho$$



   - ↳ Another parametrization: $\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$
     - ↳ ρ left alone w/ prob. p; X, Y, Z applied w/ prob. $\frac{p}{3}$

2. Amplitude damping
   - ↳ Description of energy dissipation
   - ↳ Consider single optical mode w/ state $a|0\rangle + b|1\rangle$
   - ↳ Scattering of photon modelled w/ beamsplitter $B = \exp[\theta(a^\dagger b - a b^\dagger)]$
     - ↳ $a, a^\dagger$ and $b, b^\dagger$ are annihilation/creation operators for photons

$$B|0\rangle(a|0\rangle + b|1\rangle) = a|00\rangle + b(\cos\theta|01\rangle + \sin\theta|10\rangle)$$

After beamsplitter $\boxed{\mathcal{E}_{AD}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger}$

   - ↳ $E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}$, $E_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}$, $\gamma = \sin^2\theta$ is prob. of losing a photon

3, Phase damping

↳ what happens as photon scatters while traveling

↳ Accumulate a phase (partial info about quantum phase lost)

↳ model: apply random $R_z(\theta)$ on qubit $|\psi\rangle = a|0\rangle + b|1\rangle$

↳ R_z = "phase kick"

↳ Assume θ has Gaussian distrib., mean 0, variance 2λ

$$\rho = \frac{1}{\sqrt{4\pi\lambda}} \int_{-\infty}^{+\infty} R_z(\theta)|\psi\rangle\langle\psi|R_z^\dagger(\theta) e^{-\theta^2/4\lambda} \, d\theta$$

$$= \begin{bmatrix} |a|^2 & ab^* e^{-\lambda} \\ a^* b e^{-\lambda} & |b|^2 \end{bmatrix}$$

↳ Expected val of off-diagonal elements decrease

✳ Applications of quantum operations

• Master equation: describe time evolution of open system w/ diff. eq suited for non-unitary behavior

↳ Lindblad Form: $\frac{d\rho}{dt} = -\frac{i}{\hbar}[H, \rho] + \sum_j \left[2L_j \rho L_j^\dagger - \{L_j^\dagger L_j, \rho\}\right]$

↳ $\{x, y\} = xy + yx$, anticommutator

↳ L_j are Lindblad operators, represent coupling of system to env

• Quantum State Tomography: process of experimentally determining an unknown quantum state

↳ If many copies of ρ exist,

$$\rho = \frac{\mathrm{tr}(\rho) I + \mathrm{tr}(X\rho) X + \mathrm{tr}(Y\rho) Y + \mathrm{tr}(Z\rho) Z}{2}$$

↳ $\mathrm{tr}(A\rho)$ = average value of observables

↳ Use central limit theorem → estimate $\mathrm{tr}(X\rho)$ and others for large number of ρ → estimate ρ

QC & QI

7/17/2025 (pp. 399-424)

* Distance Measures for Quantum Information

Classical

- Trace distance: $D(p_x, q_x) = \frac{1}{2}\sum_x |p_x - q_x|$
  - ↳ Compare 2 probability distributions $\{p_x\}$ and $\{q_x\}$
  - ↳ Symmetric: $D(x,y) = D(y,x)$
  - ↳ Triangle inequality: $D(x,z) \leq D(x,y) + D(y,z)$

- Fidelity: $F(p_x, q_x) = \sum_x \sqrt{p_x q_x}$
  - ↳ Not a metric (when distributions are identical, $F=1$)
  - ↳ Geometrically: inner product between vectors $\sqrt{p_x}$ and $\sqrt{q_x}$

- For trace dist, $D(p_x, q_x) = \max_S |p(S) - q(S)| = \max_S \left| \sum_{x \in S} p_x - \sum_{x \in S} q_x \right|$
  - ↳ Maximize over all subsets S of $\{x\}$
  - ↳ S is "optimal event" to distinguish $\{p_x\}$ and $\{q_x\}$

- Dynamic measure of distance
  - ↳ Pass random var X through noisy channel → output as Y
  - ↳ Let $\bar{x}$ be a copy of initial X

$$D((\bar{x}, x), (x, Y)) = p(x \neq Y)$$

  - ↳ Prob. of error = trace dist. between $(\bar{x}, x)$ and (x, Y)

※ Now onto QM

- Trace distance (QM): $D(\rho, \sigma) = \frac{1}{2} tr|\rho - \sigma|$
  - ↳ Note $|A| \equiv \sqrt{A^\dagger A}$
  - ↳ If ρ and σ commute (diagonal in same basis), trace dist. simplifies to classical trace dist. of eigenvalues for ρ and σ.
  - ↳ $D(\rho, \sigma) = \frac{1}{2}$ the Euclidean dist. between ρ and σ on Bloch sphere

  - ↳ Let $\{E_m\}$ be a POVM, $p_m \equiv tr(\rho E_m)$, $q_m \equiv tr(\sigma E_m)$ as prob. of obtaining measurement outcome m

$$D(\rho, \sigma) = \max_{\{E_m\}} D(p_m, q_m)$$

- Fidelity (QM): $F(\rho,\sigma) = tr\sqrt{\rho^{1/2}\sigma\rho^{1/2}}$
  - ↳ When ρ and σ commute, reduces to Classical fidelity.
  - ↳ Uhlmann's Theorem: let ρ and σ be states of quantum system Q, and R be a copy of Q

$$F(\rho,\sigma) = \max_{|\psi\rangle,|\varphi\rangle} |\langle\psi|\varphi\rangle|$$

  - ↳ Maximize over purifications $|\psi\rangle$ of ρ and $|\varphi\rangle$ of σ into RQ
  - ↳ For POVMs $\{E_m\}$, $p_m \equiv tr(\rho E_m)$, $q_m \equiv tr(\sigma E_m)$,

$$F(\rho,\sigma) = \min_{\{E_m\}} F(p_m, q_m)$$

  - ⁂ Decrease as 2 states become more distinguishable

- Relationship
  - ↳ For pure states $|a\rangle$ and $|b\rangle$,

$$\boxed{D(|a\rangle,|b\rangle) = \sqrt{1-F(|a\rangle,|b\rangle)^2}}$$

  - ↳ For mixed states, let $|\psi\rangle$ and $|\varphi\rangle$ be purifications such that $F(\rho,\sigma) = |\langle\psi|\varphi\rangle| = F(|\psi\rangle,|\varphi\rangle)$

$$\boxed{D(\rho,\sigma) \leq D(|\psi\rangle,|\varphi\rangle) = \sqrt{1-F(\rho,\sigma)^2}}$$

  - ⁂ If fidelity is close to 1, states are close in trace dist.

- Entanglement fidelity
  - ↳ Channel preserving info well ↔ channel preserving entanglement well
  - ↳ Start w/ state ρ of system Q, which is entangled w/ system R. Then apply quantum operation $\mathcal{E}$ to Q.

$$F(\rho,\mathcal{E}) \equiv F(RQ, R'Q')^2 = \langle RQ|\left[(I_R\otimes\mathcal{E})(|RQ\rangle\langle RQ|)\right]|RQ\rangle$$

  - ↳ If E_i is set of operation elements for $\mathcal{E}$,

$$\boxed{F(\rho,\mathcal{E}) = \sum_i |tr(\rho E_i)|^2}$$

QC & QI

7/21/2025 (pp. 425 - 445)

* Quantum Error Correction

- Some difficulties
  - ↳ No cloning
  - ↳ Continuous errors (several different errors on 1 qubit)
  - ↳ Measurement destroys quantum information

- 3-qubit bit flip code
  - ↳ Let X (pauli sigma x operator) be bit flip operator
  - ↳ Encode $a|0\rangle + b|1\rangle$ as $a|000\rangle + b|111\rangle$
  - ↳ Error diagnosis:

$$P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111| \qquad P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011| \qquad P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110|$$

  - ※ If measurement result $\langle\psi|P_i|\psi\rangle = 1$, error has occurred.
  - ※ Only gives information of what error has occurred — does not measure a or b directly, so state isn't perturbed.

- 3-qubit phase flip code
  - ↳ Phase flip operator Z applied w/ prob. p: $a|0\rangle + b|1\rangle \longrightarrow a|0\rangle - b|1\rangle$
  - ↳ Work in qubit basis $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$
  - ↳ Phase flip $\leftrightarrow$ bit flip

- Shor Code
  - ↳ Encode qubit w/ phase flip: $|0\rangle \rightarrow |+++\rangle$, $|1\rangle \rightarrow |---\rangle$
  - ↳ Then encode each w/ bit flip code: $|+\rangle \rightarrow (|000\rangle + |111\rangle)/\sqrt{2}$

$$|-\rangle \rightarrow (|000\rangle - |111\rangle)/\sqrt{2}$$

$$|0\rangle \rightarrow |0_L\rangle \equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \rightarrow |1_L\rangle \equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

※ Combined bit flip & phase flip correction

※ Also protects against arbitrary errors on 1 qubit

↳ Describe noise as trace-preserving quantum operation $\mathcal{E}$, operation elements $\{E_i\}$

↳ $|\psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle \longrightarrow$ noise $\longrightarrow \mathcal{E}(|\psi\rangle\langle\psi|) = \sum_i E_i|\psi\rangle\langle\psi|E_i^\dagger$

↳ Each operator can be expanded:

$$E_i = e_{i0} I + \underbrace{e_{i1} X_1}_{\text{bit flip}} + \underbrace{e_{i2} Z_1}_{\text{phase flip}} + \underbrace{e_{i3} X_1 Z_1}_{\text{both}}$$

↳ Measuring the error collapses this into 1 of 4 states, from which we can recover $|\psi\rangle$

↳ So a continuum of errors can be diagnosed.

✳ Theory of Quantum Error Correction

- Procedure:
  - ↳ Quantum states encoded by unitary operation → quantum error-correcting code (subspace C of larger Hilbert space)
  - ↳ P projects onto code space C, e.g. bit flip $P = |000\rangle\langle 000| + |111\rangle\langle 111|$
  - ↳ Subject to noise
  - ↳ Diagnose error type (error syndrome)
  - ↳ Recovery operation to get original state

- Assume:
  - ↳ Noise described by quantum operator $\mathcal{E}$
  - ↳ Complete error-correction procedure described by trace-preserving quantum operator R

※ For error correction to be successful,

$$(R \circ \mathcal{E})(\rho) \propto \rho$$

- Quantum error-correction conditions
  - An error-correction operation R correcting $\mathcal{E}$ on C exists iff.

$$PE_i^\dagger E_j P = \alpha_{ij} P$$

for some Hermitian matrix α of complex numbers

  - operation elements $\{E_i\}$ for noise $\mathcal{E}$ are called errors
    - If R exists, $\{E_i\}$ constitutes correctable set of errors

- Discretization of errors
  - Suppose F is quantum operation w/ operation elements $\{F_j\}$ which are linear combos of $\{E_i\}$, $F_j = \sum_i m_{ji} E_i$ for some m.
  - Then R corrects for effects of F along with C.

- Quantum Hamming Bound
  - Total # of errors that may occur in t or fewer qubits:

$$\sum_{j=0}^{t} \binom{n}{j} 3^j$$

← 3^j for 3 possible errors X, Y, Z

Encode k qubits in n qubits

  - To encode k qubits in non-degenerate way, all errors must correspond to orthogonal 2^k-dimensional subspace.
  - And all subspaces must fit in 2^n-dimensional space for n qubits

$$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n$$

← Quantum Hamming bound

QC & QI

7/23/2025 (pp. 445-499)

* Constructing Quantum Codes

- Classical linear codes:
  - ↳ Linear code C encoding k bits to n is defined by $n \times k$ generator matrix G.
  - ↳ Gx maps x to encoded version
  - ↳ G must have linearly independent columns.
  - ↳ Parity check matrix: $[n, k]$ code consists of all n-vectors x over Z_2 such that $Hx = \vec{0}$
  - ↳ H is a $(n-k) \times n$ parity check matrix.
  - ↳ "Code is the kernel of H"
  - ↳ H must have linearly independent columns

- Error recovery w/ parity check matrix
  - ↳ e.g. encode x as $y = Hx$, but due to error, encoded as $y' = y \oplus e$
  - ↳ Then $Hy = \vec{0}$, so $Hy' = He$, helps recover error (hopefully)

- Hamming distance
  - ↳ "Distance" = min. dist. between 2 codewords, $d(C) \equiv \min_{x,y \in C, x \neq y} d(x,y)$
  - ↳ $d(x,y)$ = # places where x, y differ
  - ↳ Let $wt(x) \equiv d(x,0)$, # places where x is nonzero.
  - ↳ $wt(x+y) = d(x,y)$
  - ↳ Since code is linear, $x+y$ is code if x, y are

$$d(C) = \min_{x \in C, x \neq 0} wt(x)$$

- Hamming codes: $[n, k] = [2^r - 1, 2^r - r - 1]$ for $r \geq 2$
  - ↳ Columns are all $2^r - 1$ bit strings of length r not equal to 0
  - ↳ e.g. for $r = 3$,

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

↳ If error occurs on j-th bit → He_j is binary representation for j, so we know where to correct.

↳ All Hamming codes have dist 3, can correct error on 1 bit

- Gilbert-Varshamov bound: for large n, there exists $[n, k]$ error-correcting code protecting against errors on t bits for some k, such that

$$\frac{k}{n} \geq 1 - H\left(\frac{2t}{n}\right)$$

← $H(x) \equiv -x\log(x) - (1-x)\log(1-x)$ binary Shannon entropy

* Calderbank-Shor-Steane (CSS) codes

- Suppose C_1, C_2 are $[n, k_1]$, $[n, k_2]$ classical linear codes, $C_2 \subset C_1$ and $C_1, C_2^{\perp}$ both correct t errors.

↳ The CSS code of C_1 over C_2, $CSS(C_1, C_2)$, is a $[n, k_1 - k_2]$ code capable of correcting errors on t qubits.

- Procedure

↳ Suppose $x \in C_1$, a codeword in code C_1.

↳ Then define $|x + C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$, "+" is bitwise addition mod 2

↳ Describe bit flip errors w/ n-bit e_1 (1's where bit flip)
Describe phase flip errors w/ n-bit e_2 (1's where phase flip)

↳ Corrupted state of $|x + C_2\rangle$: $\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle$

1. Correcting bit flips

↳ Introduce ancilla $|0\rangle$ to store syndrome of C_1

↳ Apply H_1: $|x+y+e_1\rangle|0\rangle \to |x+y+e_1\rangle|H_1(x+y+e_1)\rangle \to |x+y+e_1\rangle|H_1 e_1\rangle$
since $(x+y) \in C_1$ is annihilated by H_1

↳ Measure ancilla $|H_1 e_1\rangle$ to obtain e_1, then correct.

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y\rangle$$

2. Correcting phase flips

↳ Apply Hadamard to each qubit, $\frac{1}{\sqrt{|C_2|2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x+y)\cdot(e_2+z)} |z\rangle$

↳ Sum over all n-bit z

↳ Suppose $z' \equiv z + e_2$, and $z' \in C_2^\perp$. Then $\sum_{y \in C_2} (-1)^{y \cdot z'} = |C_2|$

↳ Else, if $z' \notin C_2^\perp$, $\sum_{y \in C_2} (-1)^{y \cdot z'} = 0$

↳ State becomes $\boxed{\frac{1}{\sqrt{2^n/|C_2|}} \sum_{z' \in C_2^\perp} (-1)^{x \cdot z'} |z' + e_2\rangle}$

↳ A bit flip error described by e_2, correct w/ H_2 for $C_2^\perp$

• Steane Code

↳ $H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$

↳ Construct code C w/ this parity check matrix

↳ Define $C_1 \equiv C$, $C_2 \equiv C^\perp$

↳ Parity check operator $H[C_2]$ of $C_2 = C^\perp$ is

$$H[C_2] = G[C_1]^\top = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

∴ C_1 is a $[7,4]$ code and C_2 is a $[7,3]$ code

→ $CSS(C_1, C_2)$ is a $[7,1]$ code, can correct errors on 1 qubit

* Stabilizer codes (skimmed)

• Stabilizer formalism

↳ For single qubit, Pauli group is

$$G_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

↳ Suppose S is a subgroup of G_n, define V_S to be set of n qubit states fixed by every element of S

↳ V_S = vector states stabilized by S

S = Stabilizer of state V_S

QC & QI

7/24/2025 (pp. 500-527)

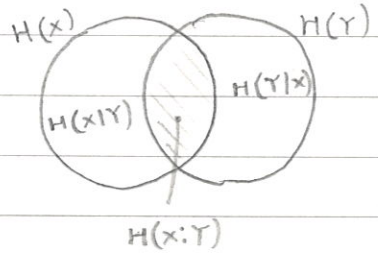
* Entropy & Information

- Shannon entropy
  - ↳ Shannon entropy of X quantifies how much info is gained by learning value of X
  - ↳ Or: entropy measures uncertainty of X before measuring

$$H(X) = H(p_1, \dots, p_n) = -\sum_x p_x \log(p_x)$$ ← Assume that $0 \log(0) \equiv 0$

  - ↳ Here, entropy quantifies the resources needed to store info

- Properties of entropy
  - ↳ Binary entropy: $H_{bin}(p) \equiv -p \log(p) - (1-p) \log(1-p)$
    - ↳ p and $1-p$ are probabilities of outcomes
  - ↳ Relative entropy: $H(p(x) \| q(x)) \equiv \sum_x p(x) \log \frac{p(x)}{q(x)} \equiv -H(x) - \sum_x p(x) \log q(x)$
    - ↳ Measures closeness of 2 probability distributions
    - ↳ Define $-0 \log(0) \equiv 0$, $-p(x) \log 0 \equiv +\infty$ if $p(x) > 0$
  - ↳ Joint entropy of pair: $H(X,Y) \equiv -\sum_{x,y} p(x,y) \log p(x,y)$
  - ↳ Entropy of X conditional on knowing Y: $H(X|Y) \equiv H(X,Y) - H(Y)$
  - ↳ Mutual info content of X, Y: $H(X:Y) \equiv H(X) + H(Y) - H(X,Y)$



- Data processing inequality: Suppose $X \to Y \to Z$ is Markov chain. Then

$$H(x) \geq H(x:Y) \geq H(x:z)$$

  - ↳ Info about output of source can only decrease with time.

- Von Neumann entropy (QM)
  - ↳ of a QM state ρ: $S(\rho) \equiv -tr(\rho \log \rho)$
  - ↳ If λ_x are eigenvalues of ρ, $S(\rho) = -\sum_x \lambda_x \log \lambda_x$

- Quantum relative entropy: $S(\rho \| \sigma) \equiv tr(\rho \log \rho) - tr(\rho \log \sigma)$
  - ↳ Klein's inequality: $S(\rho \| \sigma) \geq 0$

- Basic properties of Von Neumann entropy
  - ↳ Non-negative, 0 iff. state is pure
  - ↳ In d-dimensional Hilbert space, entropy is at most $\log(d)$
  - ↳ If composite system AB is pure, $S(A) = S(B)$
  - ↳ Joint entropy theorem: if P_i are probabilities, $|i\rangle$ are orthogonal states of A, and ρ_i is set of density operators for B,

$$\boxed{S\left(\sum_i P_i |i\rangle\langle i| \otimes \rho_i\right) = H(P_i) + \sum_i P_i S(\rho_i)}$$

- Projective measurements increase entropy
  - ↳ Suppose P_i is complete set of orthogonal projectors and ρ is density operator $\longrightarrow$ $\rho' \equiv \sum_i P_i \rho P_i$

$$\boxed{S(\rho') \geq S(\rho)}$$

- Subadditivity: Suppose systems A, B have joint state ρ^{AB}
  - ↳ $S(A,B) \leq S(A) + S(B)$
  - ↳ $S(A,B) \geq |S(A) - S(B)|$.

- Strong subadditivity: for quantum systems A, B, C

$$\boxed{S(A,B,C) + S(B) \leq S(A,B) + S(B,C)}$$

$$\boxed{S(A) + S(B) \leq S(A,C) + S(B,C)}$$

QC & QI

7/25/2025 (pp. 528 - 571)

*Quantum information theory

- Holveo Bound: Suppose Alice prepares state ρ_x, $x = 0 \dots n$ w/ probabilities $p_0 \dots p_n$. Bob performs measurement w/ POVM elements $\{E_Y\} = \{E_0 \dots E_m\}$, measurement outcome Y

$$\boxed{H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x)}, \quad \rho = \sum_x p_x \rho_x$$

↳ Upper bound on accessible information

- Data Compression

↳ Shannon's noiseless channel coding theorem

↳ Suppose independent & identically distributed source is producing $X_1, X_2, \dots$, zero w/ prob 0, one w/ prob 1-p

↳ Divide sequences $x_1, \dots x_n$ for $X_1 \dots X_n$ into typical / atypical

$$p(x_1 \dots x_n) = p(x_1)\,p(x_2) \dots p(x_n) \approx p^{np}(1-p)^{(1-p)n}$$
$$\approx 2^{-nH(x)}, \quad H(x) = -p \log p - (1-p)\log(1-p)$$

"Entropy rate" of source

↳ At most $2^{nH(x)}$ typical sequences, $nH(x)$ bits to identify

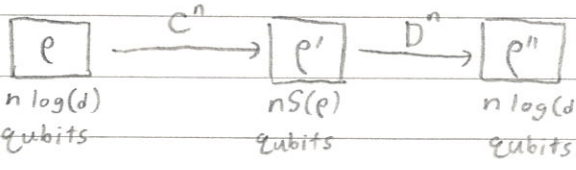
↳ Theorem: suppose $\{X_i\}$ is i.i.d. source w/ entropy rate $H(x)$. Suppose $R > H(x)$. Then there exists a reliable compression scheme of rate R for the source.

↳ Converse: if $R < H(x)$, any compression scheme isn't reliable.

↳ Schumacher's quantum noiseless channel coding theorem

↳ Info we're trying to compress: quantum states

↳ i.i.d. quantum source described by Hilbert space H



↳ Theorem: Let $\{H, \rho\}$ be an i.i.d. quantum source. If $R > S(\rho)$, there exists a reliable compression scheme of rate R for source $\{H, \rho\}$.

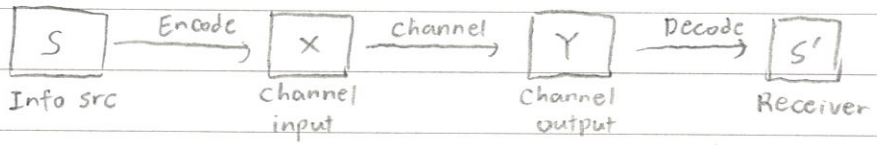
↳ Converse: if $R < S(\rho)$, any compression scheme of rate R isn't reliable.

- Communication over noisy channels

↳ Shannon's noisy channel coding theorem: for noisy channel $\mathcal{N}$, the capacity is

$$C(\mathcal{N}) = \max_{p(x)} H(X:Y)$$

↳ Over all input distributions $p(x)$ for X; Y is corresponding random variable induced at output of channel.



※ HSW theorem: let $\mathcal{E}$ be a trace-preserving quantum operation.

$$\chi(\mathcal{E}) \equiv \max_{\{p_j, \rho_j\}} \left[S\left(\mathcal{E}\left(\sum_j p_j \rho_j \right) \right) - \sum_j p_j S(\mathcal{E}(\rho_j)) \right]$$

↳ $\chi(\mathcal{E})$ takes max over all ensembles $\{p_j, \rho_j\}$ of possible input states ρ_j of channel

↳ Then $\chi(\mathcal{E})$ is Product State Capacity for channel $\mathcal{E}$: $\chi(\mathcal{E}) = C^{(1)}(\mathcal{E})$

※ Any quantum channel $\mathcal{E}$ can transmit classical info, given the channel isn't just a constant.

- Quantum information over noisy quantum channels
  - ↳ Entropy exchange of operation $\mathcal{E}$ upon input ρ:

$$S(\rho, \mathcal{E}) \equiv S(R', Q')$$

  - ↳ "How much noise $\mathcal{E}$ causes when applied to state ρ of Q"
  - ↳ Measure how much initially pure state RQ becomes mixed

  - ↳ Quantum data processing inequality
    - ↳ Classically, for Markov process $X \to Y \to Z$, $H(x) \geq H(x:Y) \geq H(x:z)$
    - ↳ Quantum: $\rho \xrightarrow{\mathcal{E}_1} \rho' \xrightarrow{\mathcal{E}_2} \rho''$
    - ↳ Quantum coherent information: $I(\rho, \mathcal{E}) \equiv S(\mathcal{E}(\rho)) - S(\rho, \mathcal{E})$

$$\boxed{S(\rho) \geq I(\rho, \mathcal{E}_1) \geq I(\rho, \mathcal{E}_2 \circ \mathcal{E}_1)}$$

  - ↳ Quantum Singleton bound: $n - k \geq 2(d-1)$
    - ↳ An $[n,k,d]$ code using n qubits to encode k qubits, able to locate errors on up to $d-1$ qubits.
    - ↳ C.f. Classical Singleton bound: $n - k \geq d - 1$