Quantum Error Correction and Quantum Information Theory

Vinod Sharma
Dept. of ECE
IISc Bangalore
Bangalore, India

Arun Padakandla
Dept. of EE and CS
University of Tennessee
Knoxville, USA

July 20, 2020

Classical Error Correction Codes (CECC)

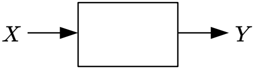
- ECC corrects errors caused by environment or noise in the system.
- In classical systems, ECC mainly used in data transmission to correct errors caused by noise in the channel and/or environmental interference.
- Finitely many errors possible.

Quantum Error Correction Codes (QECC)

- In quantum systems, since effect of environment is strong, ECC is required in any quantum information processing task.
- Error possible due to imperfect quantum gates also.
- Measurement of quantum states alters them and also due to no cloning theorem, direct application of classical ECC not possible.
- Errors are uncountably many in the quantum case.
- Nevertheless, classical techniques are basis of QECC.

Introduction : Classical ECC

- Transmit one bit $\in \{0,1\}$ on noisy channel.



$$X, Y \in \{0,1\}$$

- E.g. Transmitted $X = 0$ may become $Y = 1$.
- Channel noise causes $P(X \neq Y) > 0$.
- ECC : Three bit Repetition Code

$$0 \mapsto 000 \quad \text{and} \quad 1 \mapsto 111.$$

- At receiver, the bits received : $b_2 b_1 b_0$.
  - Channel causes error on each transmitted bit independently.

Error Detection and Correction

- After receiving $b_2 b_1 b_0$, the receiver creates two more bits called syndrome, namely $b_2 \oplus b_1$ and $b_2 \oplus b_0$.

$b_2 \oplus b_1$	$b_2 \oplus b_0$	Correction
0	0	Do Nothing
0	1	Flip b_0
1	0	Flip b_1
1	1	Flip b_2

- This procedure corrects one bit error. If two bits get flipped, it will "correct" to wrong bit.
- Works well if prob. of error for different bits are independent and small.
- Receiver needn't have computed syndromes. Could also use majority rule on b_2, b_1, b_0.
- But this does not work on general coding schemes with larger block codes. Even on quantum codes for this scheme.

Quantum ECC: Introduction

Error Models

Main Causes:

- **Coherent quantum errors:** Due to imperfect gates, applying I to $|\psi\rangle$ may not exactly give $|\psi\rangle$.
- **Decoherence of states:** Due to interaction with environment, $\rho \mapsto \sum_i E_i \rho E_i$, where E_i needn't be unitary.
- Can cause correlated errors in multiple qubits.

Quantum ECC: Introduction

- Need to transmit one qubit on a quantum channel.
- Obtain a QECC corresponding to classical 3 bit repetition code.
- Transmitted qubit can get in error by bit flip by Pauli operator.

$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, and hence

$X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$.

Quantum ECC : Introduction (Contd.)

- We use a linear code (called C_{BF} code)

$$|0\rangle \mapsto |000\rangle, \quad |1\rangle \mapsto |111\rangle,$$

$$\underbrace{a|0\rangle + b|1\rangle}_{|\psi\rangle} \mapsto a\,|000\rangle + b\,|111\rangle$$

- By no cloning theorem, we cannot prepare $|\psi\psi\psi\rangle$
- If we transmit $a|0\rangle + b|1\rangle$ by above code and first qubit is flipped by Pauli operator X, then receiver gets

$$a|100\rangle + b|011\rangle$$

Error Detection and Correction

- Suppose receiver receives qubits $x_2 x_1 x_0$.
- Receiver generates two qubit syndrome by operator U_{BF} :

$$U_{BF}|x_2 \;\; x_1 \;\; x_0 \;\; 0\; 0\rangle \mapsto |x_2 \;\; x_1 \;\; x_0 \;\; x_2 \oplus x_1 \;\; x_2 \oplus x_0\rangle$$

- Receiver makes measurements only on the first two qubits (the syndrome qubits)
  - If we get 11 then $x_2 \oplus x_1 = 1$, $x_2 \oplus x_0 = 1$, then x_2 bit has been flipped by operator $X \otimes I \otimes I$ in transmission.
  - Since $X^{-1} = X$, to correct this error use operator $X \otimes I \otimes I$ on (x_2, x_1, x_0).

Error Detection and Correction (Contd.)

Thus the error detection and correction procedure is

Bit Flipped by Channel	Syndrome	Error Correction
None	$\|00\rangle$	None
0	$\|01\rangle$	$I \otimes I \otimes X$
1	$\|10\rangle$	$I \otimes X \otimes I$
2	$\|11\rangle$	$X \otimes I \otimes I$

Error Detection and Correction (Contd.)

Comments

- We have made measurements on only the syndrome qubits.
  - Thus state $x_2x_1x_0$ remains undisturbed.
  - Also syndrome measurement tells nothing about $x_2x_1x_0$.
- Unlike in classical case, linear combination of bit flips is also corrected by above procedure.
- But it does not recover from multiple qubit bit flip errors, as in classical case.
- Also, unlike classical case, in quantum case it does not detect phase errors caused by Pauli matrix

  $$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$ and hence

  $$Z|0\rangle = |0\rangle \quad \text{and} \quad Z|1\rangle = -|1\rangle.$$

Quantum Code for Single phase-flip error (C_{PF} code)

- $X = HZH$ where $H \equiv$ Hadamard matrix $= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.
- This relation with above bit flip error correction scheme gives scheme for phase-flip error

$\|0\rangle$ $\downarrow$	Message qubit $\|\psi\rangle$ converted to three qubit code given by $\|0\rangle \mapsto \|000\rangle, \ \|1\rangle \mapsto \|111\rangle$
$\|000\rangle$ $\downarrow$	Apply $H \otimes H \otimes H$ to codeword.
$\left(\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}\right)^{\otimes 3}$ $\downarrow$	Pass through the channel $I \otimes Z \otimes I$ which can possibly cause one phase-flip error Z
$\left(\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}\right)$ $\downarrow$	Apply $H \otimes H \otimes H$ to received 3 qubits.
$\|0\rangle \otimes \|1\rangle \otimes \|0\rangle$ $\downarrow$	Apply U_{BF} to get syndrome of C_{BF}.
$\|0\rangle \otimes \|0\rangle \otimes \|0\rangle$	Detect and correct X error via syndrome.

Quantum Code for Single phase-flip error (C_{PF} code)

Comments

- Above scheme corrects all single qubit phase errors but not single bit flip errors.
- We combine above ideas to obtain a code that converts all single qubit errors obtaining Shor's nine qubit code.

The following facts will be used

- Pauli Matrices I, X, Y, Z form a basis and hence any error is a superposition of these errors.
- If X and Z errors can be corrected then Y error can also be corrected.
- Thus a code correcting one X, Z error will correct all single qubit errors.

Code to Correct an X or Z error

- First encode a qubit using C_{PF} to a 3 qubit code.
- Encode each of the 3 qubits of above code via C_{BF} to get nine qubit code :

$$|0\rangle \to |000\rangle \mapsto \frac{1}{\sqrt{8}}\left[(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)\right]$$

$$|1\rangle \to |111\rangle \mapsto \frac{1}{\sqrt{8}}\left[(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)\right]$$

For Error Correction

- Use U_{BF} on each block of three qubits to correct for possible X errors in each block separately.
- Use expansion of U_{PF} to nine bits to correct for phase errors.

General Framework of ECC

- We now develop a general framework to obtain codes that correct multiple qubit errors.
- First we study classical codes and then extend to quantum ECC.
- We limit to linear codes due to computational complexity.

Classical Linear ECC

Notation

- $\{1, 2, \cdots, M\}$ set of messages to be transmitted on a channel with binary input, output.

- $\mathbb{F}_2 = \{0, 1\}$ vector space with field $\{0, 1\}$.

  For $x, y \in \mathbb{F}_2$, $\quad x + y \;:= x \oplus y$

  For $a, x \in \mathbb{F}_2$, $\quad ax \;:= a \wedge x$

- $\mathbb{F}_2^n = \mathbb{F}_2 \times \cdots \times \mathbb{F}_2$ n product.

  For $x, y \in \mathbb{F}_2^n$, $\quad x + y \;:= \;((x_1 \oplus y_1), \cdots, (x_n \oplus y_n))^T$

  For $a, x \in \mathbb{F}_2$, $\quad ax \;:= \;((a_1 \wedge x_1), \cdots, (a_n \wedge x_n))^T$

Linear Classical Coding

- $M = 2^k$, Elements of M denoted by $k-$length binary vectors $\in \mathbb{F}_2^k$.
- Linear code $\phi : \mathbb{F}_2^k \to \mathbb{F}_2^n$, $n \geq k$, one-one map.
- Subspace $C = \phi(\mathbb{F}_2^k) \subseteq \mathbb{F}_2^n$ called (n, k) code.
- Define generator matrix G to denote ϕ :

$$Gx = \phi(x), x \in \mathbb{F}_2^k$$

  $x \mapsto Gx$, efficient way to encode.
- Define parity check matrix H of dimension $(n-k) \times n$ s.t $Ker(H) = H^{-1}(0) = C$ and H is one-one on $C^{\perp}$. Thus $HG = 0$. This provides an efficient way of error detection and correction.

Linear Classical Coding

- Hamming Norm : $x \in \mathbb{F}_2^n$, $||x|| =$ No. of 1's in x.
- Hamming Distance : $x, y \in \mathbb{F}_2^n$

$$\|x - y\| = \sum_i |x_i \oplus y_i|$$

- $D_{\min} = \min$ Hamming distance between code words of C.

Error Detection and Correction

- $x^n \in \mathbb{F}_2^n$ transmitted on channel (n uses of binary channel) and $\hat{x}^n = x^n + y^n$ received. y^n channel error.

- If $\|y^n\| < d_{\min}$, then $y^n \notin C$ and $\hat{x}^n = x^n + y^n \notin C$.

  Thus receiver can detect there is error in transmission. An efficient detector is to declare error if $H\hat{x}^n \neq 0$.

- If $\|y^n\| < \lfloor \frac{d_{\min}-1}{2} \rfloor$ then error can be detected and by replacing $\hat{x}^n$ by the nearest codeword c it can be corrected to x^n.

- $H\hat{x}^n = Hy^n$ is the syndrome. Since H is one-one on $C^{\perp}$, we can identify y^n. Then $\hat{x}^n + y^n = x^n$ corrects the error.

Error Detection and Correction contd.

- Set of correctable errors

$$A = \left\{ y^n \in \mathbb{F}_2^n : \|y^n\| < \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor \right\}$$

can be written as: $e_1, e_2 \in A$ if for $c_1, c_2 \in C$,

$$e_1 + c_1 \neq e_2 + c_2 \text{ unless } e_1 = e_2 \text{ and } c_1 = c_2$$

This is disjointness condition.

There is another set in $\mathbb{F}_2^n$ that also satisfies disjointness condition (and hence correctable) but it is not most probable set of errors.

ECC examples

Ex. : 3 bit repetition code

$0 \mapsto 000, \qquad 1 \mapsto 111$

$c = \{(0,0,0)^T, (1,1,1)^T\}$ subspace of $\mathbb{F}_2^3$

$$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad d_{\min} = 3.$$

Therefore can detect upto 2 errors and correct upto 1.

$$A = \left\{(0,0,1)^T, (0,1,0)^T, (1,0,0)^T\right\}$$

ECC examples contd.

Another set that satisfies disjointness condition is

$$\{011, 101, 110\}$$

This set of errors, causing two bit errors is less likely although can also be corrected.

But a union of the two sets cannot be corrected.

Ex. Hamming Code $(n, k) = (2^m - 1, n - m)$, $m \geq 2$. For $n = 7, k = 4$ and $d_{\min} = 3$,

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

Quantum ECC

- Development parallel to classical ECC.
- Consider linear coding of states of k qubits to n qubits, $n \geq k$.
  $W =$ Hilbert space of dim 2^k, as state space of k qubits.
  $V =$ Hilbert space of dim 2^n as state space of n qubits.
  Encoder : $\phi : W \to V$ linear, one-one map
  $[n, k]$ linear quantum code.
- Considering W as subspace of V define unitary transformation
  $U_c : V \to V$ s.t.
  $U_c(W) := C$: the code space of ϕ
  and $U_c(|w\rangle) = \phi(|w\rangle)$ for $|w\rangle \in W$.

Quantum ECC (Contd.)

Ex.: Consider code

$$|0\rangle \;\mapsto\; |000\rangle, \qquad |1\rangle \;\mapsto\; |111\rangle$$

C = code space = subspace spanned by $\{|000\rangle, |111\rangle\}$ of $V = \mathbb{C}^6$.

Ex. Shor code $[9, 1]$:

$$|0\rangle \mapsto \frac{1}{\sqrt{8}} \left(|000\rangle + |111\rangle\right)^{\otimes 3}$$

$$|1\rangle \mapsto \frac{1}{\sqrt{8}} \left(|000\rangle - |111\rangle\right)^{\otimes 3}$$

$C = 2-$dim subspace spanned by
$\left\{ \frac{1}{\sqrt{8}} \left(|000\rangle + |111\rangle\right)^{\otimes 3}, \frac{1}{\sqrt{8}} \left(|000\rangle - |111\rangle\right)^{\otimes 3} \right\}$.

Correctable Set of Errors for QECC

- As in classical case we have a set of unitary transformations,

$$\mathcal{E} = \{E_1, E_2, \cdots, E_L\}, E_l : V \to V, L < \infty$$

which cause error in transmission on a quantum channel, is correctable for code C if

$$\langle c_a | E_i^\dagger E_j | c_b \rangle = m_{ij} \delta_{ab}, \forall c_a, c_b \in c, E_i, E_j \in \mathcal{E} \quad (1)$$

- As in classical case, there are many different sets of correctable errors, some more probable than others in a practical scenario.
- Any mixture or superposition of elements of $\mathcal{E}$ is also correctable by the same code.

Correctable Set of Errors for QECC (Contd.)

- A stronger condition for correctability of errors by C is

$$\langle c_a|E_i^{\dagger}E_j|c_b\rangle = 0, \forall c_a, c_b \in c, E_i, E_j \in \mathcal{E}, E_i \neq E_j \qquad (2)$$

- A code satisfying (2) is called non-degenerate. A code satisfying (1) but not (2) is degenerate for $\mathcal{E}$.
- Shor code $[9, 1]$ is degenerate. There is no analog of degenerate codes in classical case.
- For non-degenerate, since E_iC has dim 2^k and is orthogonal to E_jC, $j \neq i$, max no. in $\mathcal{E}$ is 2^{n-k}. For nondegenerate case $\mathcal{E}$ can be larger.

Correctable Set of Errors for QECC (Contd.)

Ex. : Consider again 3 bit repetition code

$$|0\rangle \quad \mapsto \quad |000\rangle, \qquad\qquad |1\rangle \quad \mapsto \quad |111\rangle$$

C = code space = subspace spanned by $\{|000\rangle, |111\rangle\}$

$$\mathcal{E} = \left\{ \underbrace{I \otimes I \otimes I}_{E_{00}}, \underbrace{X \otimes I \otimes I}_{E_{01}}, \underbrace{I \otimes X \otimes I}_{E_{10}}, \underbrace{I \otimes I \otimes X}_{E_{11}} \right\}. \qquad (3)$$

$E_{ij} \in C$ are orthogonal. Hence satisfy stronger condition (2) and C is a nondegenerate code.

Identification and correction of ERRORS

- Consider C to be nondegenerate, $[n, k]$ quantum code.
- $\mathcal{E} = \{E_1, \cdots, E_M\}$ correctable unitary errors.
- Since $E_i C$ orthogonal and E_i unitary, if $|w\rangle = E_i|v\rangle$ is received at receiver, then from $|w\rangle$, it can uniquely find E_i. Thus taking $E_i^\dagger |w\rangle = E_i^\dagger E_i|v\rangle = |v\rangle$, receiver obtains the correct code $|v\rangle$.
- Consider an $[n, k]$ nondegenerate quantum code that can correct X, Z errors. For error set with Hamming norm i, no of errors is $3^i\binom{n}{i}$ and hence

$$\sum_{i=0}^{t} 3^i \binom{n}{i} \leq 2^{n-k}. \tag{4}$$

Identification and correction of ERRORS : Comments

- If (4) is satisfied with equality, the code is called perfect code.
- Stabilizer codes are perfect codes and also efficient in implementation.
- We study CSS (Calderbank-Shor-Steane) codes which were the first stabilizer codes proposed.
- CSS codes encode only once to correct for both phase and bit flip errors and hence for any linear combinations of these.
- For 1 qubit error correction these require 7 qubits instead of 9 qubits for Shor code. The most efficient code requires 5 qubits.

CSS Codes

- Let C_1 and $C_2^\perp$ be two classical linear $[n, k_1]$, $[n, k_2]$ codes, $k_1 > k_2$. $C_2^\perp \subset C_1$.
- Both codes correct upto t errors.
- Consider C_1, C_2 as groups with binary operation as inner product. For $c \in C_1$

$$\left\{c \cdot a, a \in C_2^\perp\right\} \text{ is a coset.}$$

- There are $2^{k_1-k_2}$ distinct cosets. Denote a coset by C_g where $g \in C_1$ is in that coset.
- For each $g \in C_1$ define quantum state

$$|\phi_g\rangle = \frac{1}{\sqrt{2^{k_2}}} \sum_{c \in C_2^\perp} |c_g \oplus c\rangle \tag{5}$$

- $\{|\phi_g\rangle, g \in G\}$ where G is the set of cosets is a $[n, k_1 - k_2]$ quantum code with dim $2^{k_1-k_2}$.

Error Correction for CSS Codes

- Suppose in transmission of a quantum code $|\phi_g\rangle$ upto t qubits are in error.
- These errors are linear combinations of upto t bit flip errors and t phase flip errors.
- From (5), $|\phi_g\rangle$ is a linear combination of codes in C_1.
  - Thus above errors can be considered as linear combinations of C_1 codes with upto t bit flip and phase flip errors.
  - Correct the bit flip errors by U_{BF} for code C_1. (the phase flip error stays untouched).

Error Correction for CSS Codes (Contd)

- Now we are left with phase-flip errors. Let $e = e_{n-1} \cdots e_0$ be binary string denoting the errors : $e_i = 1$ means $i-$th qubit has phase flip, $e_i = 0$ means no error.
  - After error $|\phi_g\rangle$ becomes

$$\frac{1}{2^k} \sum_{c \in C_2^{\perp}} (-1)^{\langle e, c_g \oplus c \rangle} |c_g \oplus c\rangle$$

  - Apply Hadamard transform $H \otimes \cdots \otimes H$ on n qubits and obtain

$$\frac{1}{\sqrt{2^{n-k}}} \sum_{y \in C_2} (-1)^{\langle y, c_g \rangle} |y \oplus e\rangle$$

    This is the code word before e but with bit flip errors corresponding to $e_i = 1$ in the linear combination of codewords in C_2.

  - Apply U_{BF} for code $C_2^{\perp}$ to detect and correct the errors.

E.g. Steane code

- Take $C_1 = [7,4]$ Hamming code. Then $C_1^\perp$ is the $[7,3]$ Hamming code and so we can take $C_2 = C_1$.
- There are $2^{4-3} = 2$ cosets. Using (5), we get a $[7,1]$ CSS code called Steane code.
- $$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{8}} \sum_{c \in C_1^\perp} |c\rangle \\ |1\rangle &= \frac{1}{\sqrt{8}} \sum_{c \in C, c \notin C_1^\perp} |c\rangle \end{aligned}$$

Other QECC

- **Entangled assisted Codes**
  - Can be used for quantum communication.
  - Sender and receiver share a maximally entangled state before communication starts.
  - Entanglement can dramatically boost power of quantum codes i.e. increase rate and/or error correction ability.
- **Quantum convolutional codes**
  - Above codes were Block codes: need the whole block of prepared qubits before encoding starts.
  - In convolutional codes the qubits are encoded online as they arrive.
  - Further developed to quantum Turbo codes, providing rates close to quantum capacity.

Fault Tolerant Computing

- QECC sufficient for quantum communication: only one encoder and one decoder needed.
- For quantum computing, we store and process information repeatedly.
  - This requires repeated error correction.
  - Now, errors due to faulty gates and circuits in implementing EC accumulate.
  - Threshold theorem tells that if prob of error of physical circuits below a threshold, then can design circuits to do arbitrarily long computations with low error prob.
  - Surface codes have realistic threshold values (10^{-3}).

Quantum Cryptography: Introduction

- Alice wants to transmit a secret message to Bob such that Eve who may be eavesdropping is not able to intercept it.
- Today most important electronics comm via public key crypto systems : RSA or elliptic curve system
  - Their security depends on intractability of factoring composite integers or computing discrete log.
  - These can be broken in exp time by classical computers and in polynomial time via Quantum computers.
- One time pad is unconditionally secure
  - Distribution of private key is major issue.
  - Quantum key distribution (QKD) enables it.

Private Key Cryptography: Components

- Private Key Cryptographic
- Privacy Amplification
- Information reconciliation

In the following we explain each of above components and then explain the cryptography protocol.

Private Key Cryptography

- Alice encodes the message with an encoding key and sends to Bob.
- Bob uses a matching decoding key to decode the received message.
- A simple and effective method is vernam cipher or one time pad.
  - For n bit message, there is n bit secret key shared by Alice and Bob
  - x message $\in \mathbb{F}_2^n$, y secret key $\in \mathbb{F}_2^n$.
  - Alice XORs x and $y = x \oplus y$ and sends to Bob.
  - Bob receives $x \oplus y$ and again X-OR's with y : $(x \oplus y) \oplus y = x$.

Private Key Cryptography : Comments

- If y is truly secret (Eve has no information about y), with arbitrarily high prob (by increasing n), Eve will not get the message.
- If Eve jams the channel, Alice and Bob can detect it and declare failure.
- For any eavesdropping strategy of Eve, Alice and Bob can ensure that Eve has as small mutual information about their message as desired.
- Vernam cipher is secure only if no. of key bits is $\geq$ size of message and key bits are not reused.
- Main difficulty with this approach is secure distribution of key bits to Alice and Bob. Privacy amplification and Information reconciliation are used to ensure this.

Secure Distribution of key between Alice and Bob

- Alice has bit string x and Bob has y, each of n bits.
- x and y are correlated and it is ensured that Eve's mutual information about x and y is upper bounded.
- Information Reconciliation is error correction conducted over a public channel to enable from x and y to create a shared bit string w between Bob and Alice, while divulging as little as possible to Eve.
- After information reconciliation, Eve has z which may be partially correlated with w. Then privacy amplification is done by Alice and Bob to distill from w a smaller set of bits s whose correlation with z is below a desired threshold.

Information Reconciliation

- Starting from bit string x, Alice performs a series of parity checks on subsets of x.
- From these subsets and parity bits, Alice makes a message u and transmits to Bob via a public channel.
  - Can be done via an ECC.
- From u, Bob corrects errors in its bit string y to obtain w.
- Since Alice used public channel, Eve gets extra information about w, (in addition to her initial information) z.

Privacy Amplification

- $\mathcal{B}$ = Set of m bit sequences s.t. if g is selected randomly uniformly from

  $\mathcal{G} := \{g : \mathbb{F}_2^n \to \mathcal{B}\}$ then prob. that for any $a_1, a_2 \in \mathbb{F}_2^n$, $a_1 \neq a_2$,

$$g(a_1) = g(a_2) \leq \frac{1}{|\mathcal{B}|}. \quad (6)$$

  (Universal hashing functions).

- Alice and Bob publicly select same $g \in \mathcal{G}$ randomly uniformly.
  - Alice and Bob compute $g(w) = s$. s is the needed secret key shared by Alice and Bob.
  - Since Eve does not have exact w, by (6), prob that it gets s is very low.

- Information reconciliation and privacy amplification can be done by ECC.

CSS code Information Reconciliation and Privacy Amplification

- This doesn't need quantum communications.
- Consider $[n, m]$ CSS code C_1, C_2, $C_2 \subseteq C_1$, both can correct upto t errors.
- Communication channel between Alice and Bob can cause mean no. of errors in a codeword $\leq t$.
- Alice chooses a random n bit string x and transmits to Bob on the channel.
- Bob receives $y = x + e$ where e is transmission error.
- Alice and Bob pick at random codes C_1, C_2 and Eve does not know about it.
- Alice and Bob both correct their states x and y to the nearest codeword $w \in C_1$ (this is information reconciliation).

CSS code Information Reconciliation and Privacy Amplification (contd.)

- Eve's mutual information about w may be unacceptably high.
- Privacy Amplification : Alice and Bob identify which of the 2^m cosets of C_2 in C_1, w belongs to : they compute $w + C_2$. This gives m bit string s.
  - Since Eve does not know C_2 and because of error correction of C_2, Eve's mutual information about s is brought below the desired threshold.

Quantum Key Distribution (QKD)

- The above procedure can be made more secure by using Quantum Channel instead of a classical channel as public channel for comm between Alice and Bob
  - Quantum channel should be able to transmit qubits with error rate lower than a threshold.
  - Due to Quantum channel Eve cannot tap the channel without disturbing quantum state transmitted. This will inform Bob.
  - By no cloning theorem, Eve cannot copy the transmitted state on channel properly.
  - Following BB84 QKD protocol was the first QKD protocol proposed.

The BB84 QKD protocol

$$\begin{aligned} Z-\text{basis} &\equiv \left\{ |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\} \\ X-\text{basis} &\equiv \{|0\rangle, |1\rangle\} \end{aligned}$$

- Alice chooses $(4+\delta)n$ random data bits.
- Alice chooses a random $(4+\delta)n$ bit string b. She encodes each data bit as $\{|0\rangle, |1\rangle\}$ if corresponding bit of b is 0 and as $\{|+\rangle, |-\rangle\}$ if b is 1.
  - Not all of of these states are orthogonal to each other. Thus Eve cannot detect them all without disturbing their states.
- Alice sends the resulting state to Bob.

The BB84 QKD protocol contd.

- Bob receives $(4+\delta)n$ qubits, announces this fact and measures each qubit in X or Z basis at random.
- Alice announces b.
- Alice and Bob discard any bits where Bob measured in a different basis than Alice prepared. With high probability, there are atleast $2n$ bits left (if not abort the protocol). They keep $2n$ bits.
  - Choose δ large enough that this probability is high.

The BB84 QKD protocol

- Alice selects a subset of n bits from $2n$ bits obtained, randomly. Then tells Bob which she selected.
- Alice and Bob announce and compare the values of n check bits. If more than an acceptable no. disagree they abort the protocol (this would have meant that Eve probably eaves dropped on the channel and hence disturbed the transmitted state).
- Alice and Bob perform reconciliation and privacy amplification on the remaining n bits to obtain m shared key bits.

BB84 protocol can be generalized to use other states and bases.
B94 is obtained this way.
QKD is easy to realize in practice.

Quantum Information Theory

$\Sigma =$ finite alphabet, $\mathbb{C} =$ complex numbers

$\mathcal{X} = \mathbb{C}^{|\Sigma|} =$ set of all functions $f : \Sigma \to \mathbb{C}$

vector space of dim $|\Sigma|$

$L(\mathcal{X}, \mathcal{Y}) =$ Set of linear maps $: \mathcal{X} \to \mathcal{Y}$

$L(\mathcal{X}) = L(\mathcal{X}, \mathcal{X}), \langle x, y \rangle$ inner product $\|x\| =$ norm $= (\langle x, x \rangle)^{\frac{1}{2}}$

$$\text{tr}(X) = \sum_{a \in \Sigma} X(a, a), \ X \in L(\mathcal{X})$$

Quantum Information Theory

$\text{Pos}(\mathcal{X}) =$ set of positive semidefinite operators on X.

Density Operator : $X \in \text{Pos}(\mathcal{X})$ and $\text{tr}(X) = 1$

Projection Operator : $\Pi \in \text{Pos}(\mathcal{X})$, with $\Pi^2 = \Pi$

For $A \in L(\mathcal{X}), A^\dagger$ is its **adjoint** operator if $\langle v, Au \rangle = \langle A^\dagger v, u \rangle$.

Hermitian operator : $A \in L(\mathcal{X})$ s.t. $A = A^\dagger$

Unitary Operator : $A \in L(\mathcal{X})$ s.t. $\|Au\| = \|u\|$ for all $|u\rangle \in \mathcal{X}$.

Completely Positive Operator : $\Phi \otimes 1_{L(\mathcal{Z})}$ is a positive map for every Euclidean space $\mathcal{Z}$

Quantum Information Theory

$\mathcal{X}, \mathcal{Y}$ Finite Dim. Vector spaces over $\mathbb{C}$.

Quantum Channel $\Phi : \mathcal{X} \to \mathcal{Y}$ Linear Completely positive trace preserving operator.

E.g. : U unitary operator $\in L(\mathcal{X})$. $\Phi(X) = UXU^{\dagger}$.

$C(\mathcal{X}, \mathcal{Y})$: The set of quantum channels from $\mathcal{X}$ to $\mathcal{Y}$.

Measurement : $\mu : \Sigma \to \text{Pos}(\mathcal{X})$

where Σ a set, $\sum_{a \in \Sigma} \mu(a) = 1_{\mathcal{X}}$.

$p(a) =$ prob. of meas. outcome $a \in \Sigma$ in state $e = \langle e, \mu(a) e \rangle$.

Classical and Quantum Entropy

$u : \Sigma \to [0, \infty)$	P : Positive semidefinite operator on $\mathcal{X}$ λ_i : eigenvalues of P
Shannon entropy (log base 2) $H(u) = -\sum_{u(a)>0} u(a) \log u(a)$	Von Neumann Entropy $H(P) = -\sum_{\lambda_i>0} \lambda_i \log \lambda_i$ $= -\text{tr}(P \log P)$
Relative entropy: $D(u\|\|v) = \sum_{\substack{a\in\Sigma \\ v(a)>0}} u(a) \log \frac{u(a)}{v(a)}$	Relative entropy: $P, Q \in \text{Pos}(\mathcal{X})$ $D(P\|\|Q) = \text{tr}(P \log P) - \text{tr}(P \log Q)$
X, Y: random variables $H(X\|Y) = H(X,Y) - H(Y)$	X: Quantum system with state P $H(X) = H(P)$ $H(X\|Y) := H(X,Y) - H(Y)$ Unlike classical case, $H(X\|Y)$ can be negative!!
Mutual Information $I(X;Y) = H(X) + H(Y) - H(X,Y)$ $H(X) \leq H(X,Y)$	Quantum Mutual Information $I(X;Y) = H(X) + H(Y) - H(X,Y)$ $\|H(X) - H(Y)\| \leq H(X,Y) \leq H(X) + H(Y)$

Shannon's Classical Source Coding Theorem

Σ Alphabet, p prob. dist on Σ, $\Gamma = \{0, 1\}$.

$X_1, \cdots, X_n$ IID sequence generated by a source with dist p, $(X_1, \cdots, X_n) \in \Sigma^n$

$f : \Sigma^n \to \Gamma^m$ Encoder $m < n$, $g : \Gamma^m \to \Sigma^n$ Decoder

$\alpha > 0$, $0 < \delta < 1$, $m = \lfloor \alpha n \rfloor$

$G = \{(a_1, \cdots, a_n) \in \Sigma^n : g(f(a_1, \cdots, a_n)) = (a_1, \cdots, a_n)\}$

(f, g) is a (n, α, δ) coding scheme for p if $P(G) > 1 - \delta$.

Shannon's Classical Source Coding Theorem

Theorem (Shannon) :

(i) If $\alpha > H(p)$ then for any $0 < \delta < 1$, $\exists$ a (n, α, δ) coding scheme for p for all large n.

(ii) If $\alpha < H(p)$ then $\exists$ a (n, α, δ) scheme for p only for a finite no. of n. ■

Comment : Above theorem states that on average a source symbol X with dist p can be compressed with little error to α binary sequence iff $\alpha < H(p)$.

Proof of this theorem uses concept of typical sequences.

Quantum Source Coding Theorem

A Quantum Source produces iid quantum states $X_1, \cdots, X_n \in L(\mathcal{X})$.

$\Gamma = \{0, 1\}$, $\mathcal{Y} = \mathbb{C}^{\Gamma}$, $\alpha > 0$, $0 < \delta < 0$, $m = \lfloor \alpha n \rfloor$

$\Phi \in C(\mathcal{X}^{\otimes n}, \mathcal{Y}^{\otimes m})$ Encoder channel, $\Psi \in (\mathcal{Y}^{\otimes m}, \mathcal{X}^{\otimes n})$ Decoder channel

In Classical case for a (countable) finite alphabet Σ, we want to recover the original sequence after decoding.

In Quantum case the corresponding task is to recover the original state sequence $\rho^{\otimes n}$ as much as possible, similarity measured by Fidelity function.

Quantum Source Coding contd.

Defn : $P, Q \in \text{Pos}(\mathcal{X})$. Fidelity between P and Q is $F(P,Q) = \text{tr}(\sqrt{\sqrt{Q}P\sqrt{Q}})$.

If $F(P,Q)$ is large then $||P-Q||_1$ is small and vice versa where $||\cdot||_1$, is trace norm :

$$||A||_1 := \text{tr}(\sqrt{A^\dagger A})$$

Def: (Φ, Ψ) is a (n, α, δ) quantum coding scheme for ρ if $F(\Psi(\Phi(\rho^{\otimes n})), \rho^{\otimes n}) \geq 1 - \delta$.

Theorem : (Schumacher)

(i) If $\alpha > H(\rho)$, then $\exists$ a (n, α, δ) quantum code for ρ for all large n.
(ii) If $\alpha < H(\rho)$ then $\exists$ a (n, α, δ) quantum code for ρ at most for finitely many n. ■

Proof of this theorem uses concept of typical subspace, corresponding to typical sequences in classical case. Historically, this correspondence was the key step in transferring classical IT results to quantum IT.

Teleportation Protocol

- Allows transmission of quantum information via a classical channel and entanglement.
- Alice has a quantum register X and Bob Y both with classical alphabet Σ.
- Alice gets a new quantum register Z whose state she wants to communicate to Bob via a classical channel.
- To send quantum state over a classical channel exactly, Alice needs to send the two complex amplitudes of the state with infinite precision.

Teleportation Protocol contd.

Following shows, using entanglement, quantum state can be transmitted by sending only two classical bits!

- Alice and Bob initially prepare (X, Y) in a maximally entangled state.

$$\tau = \frac{1}{|\Sigma|} \sum_{b,c \in \Sigma} E_{bc} \otimes E_{bc}$$

- Alice performs measurement $M : \Gamma \rightarrow \mathrm{Pos}(\mathcal{Z} \otimes \mathcal{X})$ on (Z, X) and gets measurement $a \in \Gamma$.
- Alice sends classical information a to Bob through a classical channel.
- Bob applies quantum channel $\Psi_a \in C(\mathcal{Y}, \mathcal{Z})$ to Y and the output of it is transferred to a register $Z^{'}$.

Teleportation Protocol: Comments

- Overall, the protocol provides $Z \mapsto Z'$ which is equivalent to channel.

$$\Phi(Z) = \frac{1}{|\Sigma|} \sum_{a \in \Gamma} \sum_{b,c \in \Sigma} \langle M(a), Z \otimes E_{bc} \rangle \Psi_a(E_{bc}).$$

- There exist M and $\{\Psi_a, a \in \Sigma\}$ which provides state of Z' equal to Z.
- Alice and Bob need not know the quantum state communicated. Provides long distance quantum cryptography. Using classical techniques, Alice cannot transmit state without knowing it.
- Transmission of quantum information via classical channel happened due to initial entangled state of (X, Y). Otherwise not.
- To transmit state of one qubit, it takes two classical bits to transmit; the least number of bits possible.

Teleportation Example

$\Sigma = \{0,1\}$, $\Gamma = \{0,1\}$.

- Initial state of $(X,Y) = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$.
- State of Z, $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, to be sent to Bob. α_0, α_1 unknown.
- The state of (Z,X,Y) is $|\psi\rangle\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)$.

Bell basis of $\mathbb{C}^2$ is

$$
\begin{aligned}
|\beta_{00}\rangle &= \frac{|00\rangle+|11\rangle}{\sqrt{2}},\ |\beta_{01}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}, \\
|\beta_{10}\rangle &= \frac{|00\rangle-|11\rangle}{\sqrt{2}},\ |\beta_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}.
\end{aligned}
$$

Teleportation Example contd.

In the Bell basis, state of (Z, X, Y) is

$$\frac{1}{2}|\beta_{00}\rangle(|\psi\rangle) + \frac{1}{2}|\beta_{10}\rangle(\mathsf{Z}|\psi\rangle) + \frac{1}{2}|\beta_{11}\rangle(\mathsf{XZ}|\psi\rangle) + \frac{1}{2}|\beta_{01}\rangle(\mathsf{X}|\psi\rangle).$$

- Alice performs measurement in this basis on her qubits (Z, X) and sends the result to Bob. Any of the four states occur with equal probability.
- E.g. if 10 occurs, then Y is left with state $Z|\psi\rangle$. Bob performs $I \otimes I \otimes Z$ on the system to obtain $|\psi\rangle$.

Dense Coding

- Allows transmission of classical information via a quantum channel and entanglement, optimally.
- Alice has quantum register X, Bob Y, both with alphabet Σ.
- Alice obtains classical register Z with alphabet Γ whose classical state she wants to transmit to Bob
  - Initially (X, Y) is prepared in maximally entangled state.
  - If Z has state a, Alice applies channel $\Phi_a \in C(\mathcal{X})$ to register X.
  - Alice sends state $\Phi_a(X)$ to Bob via a quantum channel.
  - Bob performs meas. $M : \Gamma \rightarrow$ Pos$(\mathcal{X} \otimes \mathcal{Y})$ on the received state $\Phi_a(X)$ and Y.
  - Outcome of meas is taken by Bob as the state of Z.
- By appropriately choosing Φ_a and Γ, if $|\Gamma| \leq |\Sigma|^2$ then Bob can exactly recover state of Z.

Dense Coding Example

$\Sigma = \{0,1\}$, $\Gamma = \{(0,0),(0,1),(1,0),(1,1)\}$.
Initial state of $(X,Y) = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, prepared by Alice.

State of Register Z a	Φ_a channel used by Alice	State of $(\Phi_a(X),Y)$ at Bob
00	$I \otimes I$	$\lvert\beta_{00}\rangle = \frac{\lvert 00\rangle+\lvert 11\rangle}{\sqrt{2}}$
01	$\mathsf{X} \otimes I$	$\lvert\beta_{01}\rangle = \frac{\lvert 01\rangle+\lvert 10\rangle}{\sqrt{2}}$
10	$\mathsf{Z} \otimes I$	$\lvert\beta_{10}\rangle = \frac{\lvert 00\rangle-\lvert 11\rangle}{\sqrt{2}}$
11	$\mathsf{ZX} \otimes I$	$\lvert\beta_{11}\rangle = \frac{\lvert 01\rangle-\lvert 10\rangle}{\sqrt{2}}$

The state of $(\Phi_a(X),Y)$ at Bob is one of the four orthogonal Bell states.
It uses $\mu((i,j)) = \beta_{ij}$ as measurement to get back the original state (i,j) of register Z at Alice.

Classical Information on a Quantum Channel

$$\Phi \in C(\mathcal{X}, \mathcal{Y})$$

Defn. : Rate α is achievable on Φ if for any $\epsilon > 0$, for all large n, $\exists$ an encoder channel and a decoder channel for $\Phi^{\otimes n}$ s.t. a unif distributed binary string of length $m = \lfloor \alpha n \rfloor$ can be transmitted over it with Prob. of error $< \epsilon$.
The $\sup$ over such α is called classical capacity of quantum channel $\Phi := C(\Phi)$

$$\chi(\Phi) = \sup_p H\left(\Phi\left(\sum_{a\in\Sigma} p(a)\rho_a\right)\right) - \sum_{a\in\Sigma} p(a)H(\Phi(\rho_a))$$

where Σ is the alphabet of a classical input source X and

$$p(a) = P(X = a), \qquad a \mapsto \rho_a \in D(\mathcal{X})$$

Theorem: [Holevo-Schumacher-Westmoreland]

$$C(\Phi) = \lim_{n\to\infty} \frac{\chi(\Phi^{\otimes n})}{n}$$

Classical Information on a Quantum Channel : Comments

1. Computing $\chi(\Phi^{\otimes n})$ for large n is intractable because of optimization over p.

2. If $\chi(\Phi^{\otimes n}) = n\chi(\Phi)$ then $C(\Phi) = \chi(\Phi)$. This is true for many channels, not all.

Defn. : A channel Φ is entanglement breaking if $\exists$ alphabet Σ, a measurement $M : \Sigma \to \text{Pos}(\mathcal{X})$, $\sigma_a \in D(\mathcal{Y})$, $a \in \Sigma$, s.t.

$$\Phi(X) = \sum_{a \in \Sigma} \langle M(A), X \rangle \sigma_a, \qquad \forall X \in L(\mathcal{X})$$

The output state of this channel is always unentangled.
Theorem: For an entanglement breaking channel Φ,

$$\chi(\Phi^{\otimes n}) = n\chi(\Phi).$$

Classical Information on a Quantum Channel : Example

Erasure Channel : $\Phi(\rho) = (1-\epsilon)\rho + \epsilon e e^{\dagger}$,
where $0 < \epsilon < 1$, e is an erasure symbol, orthogonal to input space $\{\rho_a : a \in \Sigma\}$ of the channel.
The classical capacity of this channel is

$$C(\Phi) = (1-\epsilon)\log d$$

where $d =$ dim of $\mathcal{X}$.

Entanglement Assisted Classical Capacity

- If before transmission, sender and receiver can have entanglement of their quantum states, then classical capacity of channel can be increased.
- Super dense coding can often provide the capacity now.
- For erasure channel, entanglement doubles classical capacity.

Further Reading

Quantum Mechanics

- B. Schumaker and M. Westmoreland, *Quantum Processes, Systems and Information*, Cambridge 2010.
- L.E. Ballentine, *Quantum Mechanics, a Modern Development*, 2nd ed. World Scientific, 1998.
- J. J. Sakurai and J. Napolitano, *Modern Quantum Mechanics*, 2nd ed. Pearson, 2011.

Quantum Computation and Information

- M. Nielsen and I. Chuang (Mike and Ike), *Quantum Computation and Quantum Information*, Cambridge 2000.
- Hayashi, Ishizaka, Kawachi, Kimura, Ogawa, *Introduction to Quantum Information Science*, Springer 2015.
- Kaye, Laflamme, Mosca, *An introduction to Quantum Computing*, Oxford 2007.
- Rieffel and Polak, *Quantum Computing, a gentle introduction*, MIT Press, 2011.

Further Reading contd.

Advanced Reading

- A. M. Childs, *Lecture Notes on Quantum Algorithms*, 2017.
- Lidar and Brun (ed.), *Quantum Error Correction*, Cambridge 2013.
- M. M. Wilde, *Quantum Information Theory*, Cambridge 2013.

Concluding Remarks

- Capabilities of computers are constrained by laws of physics and not by pure math.
- Superposition, interference, non-determinism and entanglement make quantum computing different from classical computing.
- There is no function computable by quantum computers but not by classical.
  - However, computational tasks are there:
    - Generating true random numbers.
    - Teleportation of information.
- In quantum computing, two kinds of algorithms found:
  - Shor's algorithm on factoring composite integers that provide exponential speedup over classical computations.
  - Grover's algorithm for unstructured search which show only polynomial speedup.

Concluding Remarks contd.

- So far no exponential speedup found for NP-complete problems. Unlikely to be found in the future.
  - Good candidates for exp. speedup are NP intermediate problems, e.g., factoring composite integers.
- QECC and fault tolerant computing essential for quantum computing and communication.
- Public key cryptography threatened by quantum computing but QKD strengthens private key cryptography.
- Entanglement can speedup computations, strengthen QECC and enhance communication capacity.
- Classical techniques are key to develop quantum algorithms, QECC and Quantum IT results.
  - But new techniques and insights are also needed.
- Currently main challenge is in building quantum computers.