Quantum Information Theory and Applications to Local Decoding

Sayak Chakrabarti

Topics

- Quantum Information Theory

Topics

- Quantum Information Theory
- Local Decoding

Topics

- Quantum Information Theory
- Local Decoding
- Random Access Codes

Quantum Information Theory: Mixed States

- States given by

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_n |n\rangle$$

.

Quantum Information Theory: Mixed States

- States given by

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_n |n\rangle$$

  .

- The concept of Quantum noise

Quantum Information Theory: Mixed States

- States given by

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_n |n\rangle$$

  .

- The concept of Quantum noise
- Implementing a Quantum System,

$$\text{the device outputs} \begin{cases} |\psi_1\rangle & \text{with probability } p_1 \\ |\psi_2\rangle & \text{with probability } p_2 \\ & \vdots \\ |\psi_d\rangle & \text{with probability } p_d \end{cases}$$

Mixed States

Definition

A mixed state $\{p_i \left|\psi\right\rangle_i\}$ is represented by the density matrix
$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$

Mixed States

Definition

A mixed state $\{p_i \left|\psi\right\rangle_i\}$ is represented by the density matrix $\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$

- Given basis $\left|v_0\right\rangle, \ldots \left|v_n\right\rangle$

$$Pr[\text{observe } \left|v_i\right\rangle] = \left\langle v_i\right| \left(\sum_j p_j \left|\psi_j\right\rangle \left\langle\psi_j\right|\right) \left|v_i\right\rangle = \left\langle v_i\right| \rho \left|v_i\right\rangle$$

Mixed States

Definition

A mixed state $\{p_i \left|\psi\right\rangle_i\}$ is represented by the density matrix
$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$

- Given basis $\left|v_0\right\rangle, \ldots \left|v_n\right\rangle$

$$Pr[\text{observe } \left|v_i\right\rangle] = \left\langle v_i\right| \left(\sum_j p_j \left|\psi_j\right\rangle \left\langle\psi_j\right|\right) \left|v_i\right\rangle = \left\langle v_i\right| \rho \left|v_i\right\rangle$$

- Mixed state through unitary transformation U: $U\rho U^\dagger$

Mixed States

Definition

A mixed state $\{p_i \left|\psi\right\rangle_i\}$ is represented by the density matrix $\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$

- Given basis $\left|v_0\right\rangle, \ldots \left|v_n\right\rangle$

$$Pr[\text{observe } \left|v_i\right\rangle] = \left\langle v_i\right| \left(\sum_j p_j \left|\psi_j\right\rangle \left\langle\psi_j\right|\right) \left|v_i\right\rangle = \left\langle v_i\right| \rho \left|v_i\right\rangle$$

- Mixed state through unitary transformation U: $U\rho U^\dagger$
- Can be written as probability distribution over orthogonal pure states using SVD

Properties of mixed states

Theorem

If ρ is a mixed state then $Tr(\rho) = 1$ and ρ is a positive semi-definite matrix.

Properties of mixed states

Theorem

If ρ is a mixed state then $Tr(\rho) = 1$ and ρ is a positive semi-definite matrix.

Mixed states might not always be distinguishable.

Measurements

- **Simple measurements:** Measurements in orthogonal basis

Measurements

- **Simple measurements:** Measurements in orthogonal basis
- **More general measurements:** Matrices M_i's satisfying $\sum_i M_i^\dagger M_i = I$

Measurements

- **Simple measurements:** Measurements in orthogonal basis
- **More general measurements:** Matrices M_i's satisfying $\sum_i M_i^\dagger M_i = I$
- **Projective measurements:** M_i's chosen as projector matrices

Holevo's Bound

- Encodings of bits and existence of incompressible bits.

Holevo's Bound

- Encodings of bits and existence of incompressible bits.
- How many bits does a qubit represent?

Holevo's Bound: Preliminaries

1. **Shannon's entropy:** $H(X) = -\sum_{\omega \in X} p_\omega \log p_\omega$

Holevo's Bound: Preliminaries

1. **Shannon's entropy:** $H(X) = -\sum_{\omega \in X} p_\omega \log p_\omega$
2. Similarly $H(X, Y)$

Holevo's Bound: Preliminaries

1. **Shannon's entropy:** $H(X) = -\sum_{\omega \in X} p_\omega \log p_\omega$
2. Similarly $H(X, Y)$
3. **Mutual information:** (accessible information about X knowing outcome of Y): $I(X : Y) = H(X) + H(Y) - H(X, Y)$

Holevo's Bound: Preliminaries

1. **Shannon's entropy:** $H(X) = -\sum_{\omega \in X} p_\omega \log p_\omega$
2. Similarly $H(X, Y)$
3. **Mutual information:** (accessible information about X knowing outcome of Y): $I(X:Y) = H(X) + H(Y) - H(X, Y)$
   Classical Example: Suppose $Y \equiv U_{2n}$ and $X = (Y_1, Y_2, \ldots Y_n)$, then $I(X:Y) = H(X) + H(Y) - H(X, Y) = n + 2n - 2n = n$.

Holevo's Bound: Preliminaries

1. **Shannon's entropy:** $H(X) = -\sum_{\omega \in X} p_\omega \log p_\omega$
2. Similarly $H(X, Y)$
3. **Mutual information:** (accessible information about X knowing outcome of Y): $I(X : Y) = H(X) + H(Y) - H(X, Y)$
   Classical Example: Suppose $Y \equiv U_{2n}$ and $X = (Y_1, Y_2, \ldots Y_n)$, then
   $I(X : Y) = H(X) + H(Y) - H(X, Y) = n + 2n - 2n = n$.
   I have n bits of information

Holevo's Bound: Preliminaries

1. **Shannon's entropy:** $H(X) = -\sum_{\omega \in X} p_\omega \log p_\omega$
2. Similarly $H(X, Y)$
3. **Mutual information:** (accessible information about X knowing outcome of Y): $I(X : Y) = H(X) + H(Y) - H(X, Y)$
   Classical Example: Suppose $Y \equiv U_{2n}$ and $X = (Y_1, Y_2, \ldots Y_n)$, then $I(X : Y) = H(X) + H(Y) - H(X, Y) = n + 2n - 2n = n$.
   I have n bits of information
4. **Accessible information:** Given a density matrix $\rho = \{p_i, \rho_i\}_{i=1}^{n}$ corresponding to X, $I_{acc}(\rho, p) = \max_{All\ POVMs} I(X : Y)$

Holevo's Bound: Preliminaries

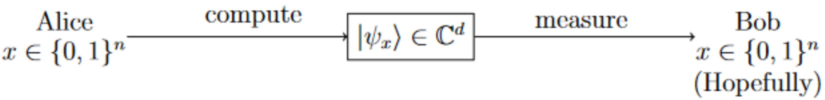
1. **Shannon's entropy:** $H(X) = -\sum_{\omega \in X} p_\omega \log p_\omega$
2. Similarly $H(X, Y)$
3. **Mutual information:** (accessible information about X knowing outcome of Y): $I(X : Y) = H(X) + H(Y) - H(X, Y)$
   Classical Example: Suppose $Y \equiv U_{2n}$ and $X = (Y_1, Y_2, \ldots Y_n)$, then $I(X : Y) = H(X) + H(Y) - H(X, Y) = n + 2n - 2n = n$.
   I have n bits of information
4. **Accessible information:** Given a density matrix $\rho = \{p_i, \rho_i\}_{i=1}^n$ corresponding to X, $I_{acc}(\rho, p) = \max_{All\ POVMs} I(X : Y)$
5. **von Neumann entropy:** Given a density matrix $\rho = \{p_i, \rho_i\}_{i=1}^n$, $S = -Tr(\rho \log \rho) = -\sum_j \lambda_j \log \lambda_j$; λ_j are the eigenvalues of ρ.

Holevo's Bound: Preliminaries

1. **Shannon's entropy:** $H(X) = -\sum_{\omega \in X} p_\omega \log p_\omega$
2. Similarly $H(X, Y)$
3. **Mutual information:** (accessible information about X knowing outcome of Y): $I(X:Y) = H(X) + H(Y) - H(X,Y)$
   Classical Example: Suppose $Y \equiv U_{2n}$ and $X = (Y_1, Y_2, \ldots Y_n)$, then $I(X:Y) = H(X) + H(Y) - H(X,Y) = n + 2n - 2n = n$.
   I have n bits of information
4. **Accessible information:** Given a density matrix $\rho = \{p_i, \rho_i\}_{i=1}^n$ corresponding to X, $I_{acc}(\rho, p) = \max_{All\ POVMs} I(X:Y)$
5. **von Neumann entropy:** Given a density matrix $\rho = \{p_i, \rho_i\}_{i=1}^n$, $S = -Tr(\rho \log \rho) = -\sum_j \lambda_j \log \lambda_j$; λ_j are the eigenvalues of ρ.

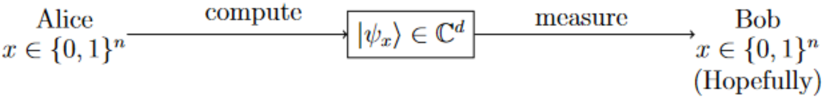
Holevo's Bound

1. **Alice:** Classical random variable X taking values $\{1, 2, \ldots n\}$ with probability $\{p_1, p_2, \ldots p_n\}$

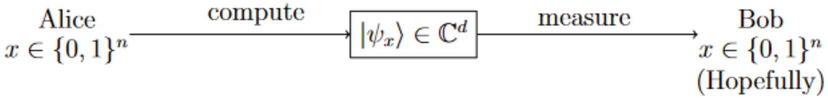


Holevo's Bound

1. **Alice:** Classical random variable X taking values $\{1, 2, \ldots n\}$ with probability $\{p_1, p_2, \ldots p_n\}$
2. Alice creates a quantum state with the density matrix ρ_X from $\{\rho_1, \rho_2, \ldots \rho_n\}$ and sends it to Bob.

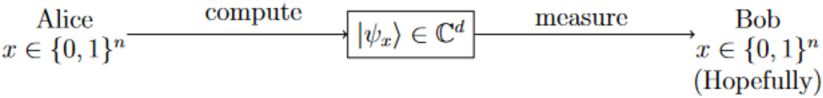


1. **Alice:** Classical random variable X taking values $\{1, 2, \ldots n\}$ with probability $\{p_1, p_2, \ldots p_n\}$
2. Alice creates a quantum state with the density matrix ρ_X from $\{\rho_1, \rho_2, \ldots \rho_n\}$ and sends it to Bob.
3. **Bob:** Tries to obtain X. Does measurements on ρ_X, outcome denoted by random variable Y.



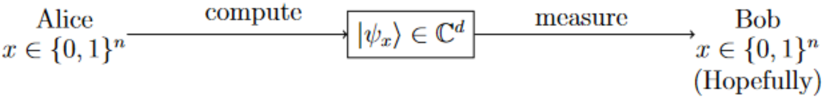
Holevo's Bound

1. **Alice:** Classical random variable X taking values $\{1, 2, \dots n\}$ with probability $\{p_1, p_2, \dots p_n\}$
2. Alice creates a quantum state with the density matrix ρ_X from $\{\rho_1, \rho_2, \dots \rho_n\}$ and sends it to Bob.
3. **Bob:** Tries to obtain X. Does measurements on ρ_X, outcome denoted by random variable Y.
4. Amount of information possible for Bob to get: $I_{acc}(\rho, p)$



Holevo's Bound

1. **Alice:** Classical random variable X taking values $\{1, 2, \dots n\}$ with probability $\{p_1, p_2, \dots p_n\}$
2. Alice creates a quantum state with the density matrix ρ_X from $\{\rho_1, \rho_2, \dots \rho_n\}$ and sends it to Bob.
3. **Bob:** Tries to obtain X. Does measurements on ρ_X, outcome denoted by random variable Y.
4. Amount of information possible for Bob to get: $I_{acc}(\rho, p)$



Holevo's bound

Theorem ([Hol73])

For measurement given by POVM $E_Y = \{E_1, E_2, \dots E_n\}$ performed on ρ with measurement outcome Y, the amount of information about X possible to find from this measurement is given by

$$I_{acc}(\rho, p) \leq S(\rho) - \sum_{i=1}^{n} p_i S(\rho_i) = \chi \tag{1}$$

Holevo's bound

Theorem ([Hol73])

For measurement given by POVM $E_Y = \{E_1, E_2, \ldots E_n\}$ performed on ρ with measurement outcome Y, the amount of information about X possible to find from this measurement is given by

$$I_{acc}(\rho, p) \leq S(\rho) - \sum_{i=1}^{n} p_i S(\rho_i) = \chi \tag{1}$$

χ : Holevo's information

Holevo's bound

[CvDNT98] gave the following interpretation of Holevo's theorem that is more commonly used.

Holevo's bound

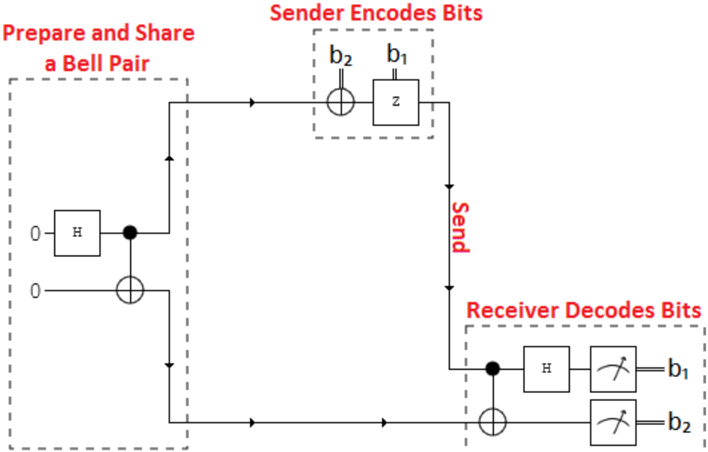
[CvDNT98] gave the following interpretation of Holevo's theorem that is more commonly used.

Theorem ([CvDNT98])

Suppose Alice wants to communicate a string to Bob. Then the following holds.

- *If Alice sents m qubits to Bob, and they* do not *have any prior entangled state, then Bob receives at most m bits of information about x.*
- *If Alice sents m qubits to Bob, and they* do *have some prior entangled state, then Bob receives at most $2m$ bits of information about x.*
- *If Alice sents m classical bits to Bob, and even if they have some prior entangled state, then Bob receives at most m bits of information about x.*

Superdense coding



From Holevo's Theorem to Low-dimensional Encodings

- Let $X \equiv U_N$, having values from $[N]$
- Encoding $E : x \in X \mapsto \rho_x$, some d-dimensional density matrix.
- Let $E_1, \ldots E_N$ be POVM operators.

From Holevo's Theorem to Low-dimensional Encodings

- Let $X \equiv U_N$, having values from $[N]$
- Encoding $E : x \in X \mapsto \rho_x$, some d-dimensional density matrix.
- Let $E_1, \ldots E_N$ be POVM operators.
- Probability of correct decoding: $p_x = Tr(E_x \rho_x) \leq Tr(E_x)$.

From Holevo's Theorem to Low-dimensional Encodings

- Let $X \equiv U_N$, having values from $[N]$
- Encoding $E : x \in X \mapsto \rho_x$, some d-dimensional density matrix.
- Let $E_1, \ldots E_N$ be POVM operators.
- Probability of correct decoding: $p_x = Tr(E_x \rho_x) \leq Tr(E_x)$.
- Sum of success probabilities:

$$\sum_{x=1}^{N} p_x \leq \sum_{x=1}^{N} Tr(E_x) = Tr(\sum_{i=1}^{N} E_x) = Tr(I) = d$$

From Holevo's Theorem to Low-dimensional Encodings

- Let $X \equiv U_N$, having values from $[N]$
- Encoding $E : x \in X \mapsto \rho_x$, some d-dimensional density matrix.
- Let $E_1, \ldots E_N$ be POVM operators.
- Probability of correct decoding: $p_x = Tr(E_x \rho_x) \leq Tr(E_x)$.
- Sum of success probabilities:

$$\sum_{x=1}^{N} p_x \leq \sum_{x=1}^{N} Tr(E_x) = Tr(\sum_{i=1}^{N} E_x) = Tr(I) = d$$

- Encode n uniformly random bits into m qubits, success probability after decoding is $\frac{2^m}{2^n}$

Quantum Random Access Code

- Given n bit string $X = X_1 X_2 \ldots X_n$ chosen uniformly at random

Quantum Random Access Code

- Given n bit string $X = X_1 X_2 \ldots X_n$ chosen uniformly at random
- Uniformly distributed by the encoding $E : X \mapsto \rho_X$

Quantum Random Access Code

- Given n bit string $X = X_1 X_2 \dots X_n$ chosen uniformly at random
- Uniformly distributed by the encoding $E : X \mapsto \rho_X$
- We want to decode individual bits X_i with probability $\geq \frac{1}{2} + \epsilon$

Quantum Random Access Code

- Given n bit string $X = X_1 X_2 \ldots X_n$ chosen uniformly at random
- Uniformly distributed by the encoding $E : X \mapsto \rho_X$
- We want to decode individual bits X_i with probability $\geq \frac{1}{2} + \epsilon$
- Equivalently, given i, return measurement $\{M_i, I - M_i\}$.

Quantum Random Access Code

- Given n bit string $X = X_1 X_2 \dots X_n$ chosen uniformly at random
- Uniformly distributed by the encoding $E : X \mapsto \rho_X$
- We want to decode individual bits X_i with probability $\geq \frac{1}{2} + \epsilon$
- Equivalently, given i, return measurement $\{M_i, I - M_i\}$.
- For each $x \in \{0,1\}^n$, we want $Tr(M_i \rho_x) \geq p$ for $x_i = 1$ and $Tr(M_i \rho_x) \leq 1 - p$ for $x_i = 0$.

Quantum Random Access Code

- It is known that there exists $2 \mapsto^{0.85} 1$ and $3 \mapsto^{0.79} 1$ QRACs [ANTSV99, ANTSV02, HIN$^+$06, CGaS08].

Quantum Random Access Code

- It is known that there exists $2 \mapsto^{0.85} 1$ and $3 \mapsto^{0.79} 1$ QRACs [ANTSV99, ANTSV02, HIN$^+$06, CGaS08].
- Also, [HIN$^+$06] proved that there is no QRAC such that $4 \mapsto^{p} 1$ with $p > \frac{1}{2}$.

Quantum Random Access Code

- It is known that there exists $2 \mapsto^{0.85} 1$ and $3 \mapsto^{0.79} 1$ QRACs [ANTSV99, ANTSV02, HIN+06, CGaS08].
- Also, [HIN+06] proved that there is no QRAC such that $4 \mapsto^{p} 1$ with $p > \frac{1}{2}$.
- Can QRACs be shorter than classical case?

Quantum Random Access Code

- It is known that there exists $2 \mapsto^{0.85} 1$ and $3 \mapsto^{0.79} 1$ QRACs [ANTSV99, ANTSV02, HIN$^+$06, CGaS08].
- Also, [HIN$^+$06] proved that there is no QRAC such that $4 \mapsto^{p} 1$ with $p > \frac{1}{2}$.
- Can QRACs be shorter than classical case?
- Ambainis et al. [ANTSV99] show that if $m \mapsto^{p} n$ exists then $m = \Omega(\frac{n}{\log n})$, i.e. asymptotically QRACs can not be much smaller than classical counterparts.

Quantum Random Access Code

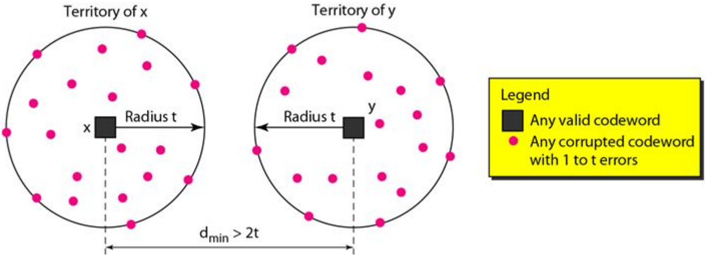
- It is known that there exists $2 \mapsto^{0.85} 1$ and $3 \mapsto^{0.79} 1$ QRACs [ANTSV99, ANTSV02, HIN⁺06, CGaS08].
- Also, [HIN⁺06] proved that there is no QRAC such that $4 \mapsto^{p} 1$ with $p > \frac{1}{2}$.
- Can QRACs be shorter than classical case?
- Ambainis et al. [ANTSV99] show that if $m \mapsto^{p} n$ exists then $m = \Omega(\frac{n}{\log n})$, i.e. asymptotically QRACs can not be much smaller than classical counterparts.
- Nayak [Nay99] tightened this by showing $m \geq (1 - H(p))n$.

Local Decoding

- Error correcting codes

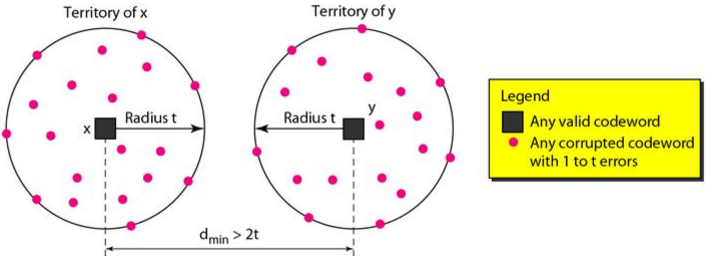
Local Decoding

- Error correcting codes



Local Decoding

- Error correcting codes



Definition (Local Decoding)

A map $E : \{0,1\}^n \to \{0,1\}^m$ is called an (q, δ, ϵ)-LDC if there exists a classical randomized decoding algorithm D satisfying the properties:

- For each $x \in \{0,1\}^n$ and $\forall y \in \{0,1\}^m$, $Ham(E(x), y) \leq \delta n$, we have $\forall i \in [n]$, $Pr[D(y,i) = x_i] \geq \frac{1}{2} + \epsilon$
- D makes at most non-adaptive q queries to y

Local Decoding

- Trade off between code length and number of queries

Local Decoding

- Trade off between code length and number of queries

Walsh-Hadamard Code

Given $x \in \{0,1\}^n$, we encode it into a string $y \in \{0,1\}^m$ with $m = 2^n$, where $y_i := x \cdot bin(i) \mod 2$.

Local Decoding

- Trade off between code length and number of queries

Walsh-Hadamard Code

Given $x \in \{0,1\}^n$, we encode it into a string $y \in \{0,1\}^m$ with $m = 2^n$, where $y_i := x \cdot bin(i) \mod 2$.

Example $n = 2$. For $x = 01$,
$E(x) = (x \cdot 00, x \cdot 01, x \cdot 10, x \cdot 11) = 0101.$

Local Decoding of WH Codes

- We can decode x_i of WH codes with $q = 2$ queries.

Local Decoding of WH Codes

- We can decode x_i of WH codes with $q = 2$ queries.
- Query the codeword at indices z and $z \oplus i$.

Local Decoding of WH Codes

- We can decode x_i of WH codes with $q = 2$ queries.
- Query the codeword at indices z and $z \oplus i$.
- Each of z and $z \oplus i$ is uniformly distributed. The probability of both queries returning uncorrupted bit is $\geq 1 - 2\delta$.

Local Decoding of WH Codes

- We can decode x_i of WH codes with $q = 2$ queries.
- Query the codeword at indices z and $z \oplus i$.
- Each of z and $z \oplus i$ is uniformly distributed. The probability of both queries returning uncorrupted bit is $\geq 1 - 2\delta$.
- Now, we have $E(x)_z$ and $E(x)_{z \oplus e_i}$. From this,

$$E(x)_z \oplus E(x)_{z \oplus e_i} = (x \cdot z) \oplus (x \cdot (z \oplus e_i)) = x.e_i = x_i$$

Local Decoding of WH Codes

- We can decode x_i of WH codes with $q = 2$ queries.
- Query the codeword at indices z and $z \oplus i$.
- Each of z and $z \oplus i$ is uniformly distributed. The probability of both queries returning uncorrupted bit is $\geq 1 - 2\delta$.
- Now, we have $E(x)_z$ and $E(x)_{z \oplus e_i}$. From this,

$$E(x)_z \oplus E(x)_{z \oplus e_i} = (x \cdot z) \oplus (x \cdot (z \oplus e_i)) = x.e_i = x_i$$

- WH is $(2, \delta, \frac{1}{2} - 2\delta)$-LDC.

Local Decoding: Lower Bounds

Theorem ([KT00])

For every (q, δ, ϵ)-LDC with encoding $E : \{0,1\}^n \to \{0,1\}^m$, and each $i \in [n]$, there exists a set $\mathcal{M}_i$ of $\Omega(\delta\epsilon m/q^2)$-many disjoint tuples. Each tuple $t \in \mathcal{M}_i$ consist of q indices from $[m]$, and a bit $a_{i,t}$ such that

$$Pr_{x\in\{0,1\}^n}\left[x_i = a_{i,t} \oplus \sum_{j\in t} E(x)_j\right] \geq \frac{1}{2} + \Omega(\frac{\epsilon}{2^q})$$

Local Decoding: Lower Bounds

Theorem ([KT00])

For every (q, δ, ϵ)-LDC with encoding $E : \{0,1\}^n \to \{0,1\}^m$, and each $i \in [n]$, there exists a set $\mathcal{M}_i$ of $\Omega(\delta \epsilon m / q^2)$-many disjoint tuples. Each tuple $t \in \mathcal{M}_i$ consist of q indices from $[m]$, and a bit $a_{i,t}$ such that

$$Pr_{x \in \{0,1\}^n} \left[x_i = a_{i,t} \oplus \sum_{j \in t} E(x)_j \right] \geq \frac{1}{2} + \Omega(\frac{\epsilon}{2^q})$$

Probability boosted by enumerating over t's randomly.

Local Decoding: Lower Bounds and connections to Quantum Computing

- Given $(2, \delta, \epsilon)$-LDC with encoding function $E : \{0, 1\}^n \mapsto \{0, 1\}^m$.
- **Spoiler:** Proof using QC to prove m is exponential in n!

Local Decoding: Lower Bounds and connections to Quantum Computing

- Given $(2, \delta, \epsilon)$-LDC with encoding function $E : \{0,1\}^n \mapsto \{0,1\}^m$.
- **Spoiler:** Proof using QC to prove m is exponential in n!
- **Strategy:** m-dimensional quantum encoding is a QRAC for x, with success probability $p > \frac{1}{2}$

Local Decoding: Lower Bounds and connections to Quantum Computing

- Given $(2, \delta, \epsilon)$-LDC with encoding function $E : \{0,1\}^n \mapsto \{0,1\}^m$.
- **Spoiler:** Proof using QC to prove m is exponential in n!
- **Strategy:** m-dimensional quantum encoding is a QRAC for x, with success probability $p > \frac{1}{2}$

$$x \mapsto |\phi_x\rangle = \frac{1}{\sqrt{m}} \sum_{j=1}^{m} (-1)^{E(x)_j} |j\rangle$$

Local Decoding: Lower Bounds and connections to Quantum Computing

- Given $(2, \delta, \epsilon)$-LDC with encoding function $E : \{0,1\}^n \mapsto \{0,1\}^m$.
- **Spoiler:** Proof using QC to prove m is exponential in n!
- **Strategy:** m-dimensional quantum encoding is a QRAC for x, with success probability $p > \frac{1}{2}$

$$x \mapsto |\phi_x\rangle = \frac{1}{\sqrt{m}} \sum_{j=1}^{m} (-1)^{E(x)_j} |j\rangle$$

(We know how to construct this oracle!)

Local Decoding: Lower Bounds and connections to Quantum Computing

- Given $(2, \delta, \epsilon)$-LDC with encoding function $E : \{0,1\}^n \mapsto \{0,1\}^m$.
- **Spoiler:** Proof using QC to prove m is exponential in n!
- **Strategy:** m-dimensional quantum encoding is a QRAC for x, with success probability $p > \frac{1}{2}$

$$x \mapsto |\phi_x\rangle = \frac{1}{\sqrt{m}} \sum_{j=1}^{m} (-1)^{E(x)_j} |j\rangle$$

(We know how to construct this oracle!)

- Number of qubits $= \log m$

Local Decoding: Lower Bounds and connections to Quantum Computing

- Given $(2, \delta, \epsilon)$-LDC with encoding function $E : \{0,1\}^n \mapsto \{0,1\}^m$.
- **Spoiler:** Proof using QC to prove m is exponential in n!
- **Strategy:** m-dimensional quantum encoding is a QRAC for x, with success probability $p > \frac{1}{2}$

$$x \mapsto |\phi_x\rangle = \frac{1}{\sqrt{m}} \sum_{j=1}^{m} (-1)^{E(x)_j} |j\rangle$$

(We know how to construct this oracle!)

- Number of qubits $= \log m$
- Holevo's Theorem says $m = (1 - H(p))n = \Omega(n)$

Local Decoding: Lower Bounds and connections to Quantum Computing

- Given $(2, \delta, \epsilon)$-LDC with encoding function $E : \{0,1\}^n \mapsto \{0,1\}^m$.
- **Spoiler:** Proof using QC to prove m is exponential in n!
- **Strategy:** m-dimensional quantum encoding is a QRAC for x, with success probability $p > \frac{1}{2}$

$$x \mapsto |\phi_x\rangle = \frac{1}{\sqrt{m}} \sum_{j=1}^{m} (-1)^{E(x)_j} |j\rangle$$

(We know how to construct this oracle!)

- Number of qubits $=\log m$
- Holevo's Theorem says $m = (1 - H(p))n = \Omega(n)$
- Put them together! $N \geq 2^{\Omega(\delta^2 \epsilon^4 n)}$

Local Decoding: Lower Bounds and connections to Quantum Computing

- How to recover x_i from $|\phi_x\rangle$?

Local Decoding: Lower Bounds and connections to Quantum Computing

- How to recover x_i from $|\phi_x\rangle$?
- Convert $\mathcal{M}_i$ into projective measurement by converting each pair $(j,k) \in \mathcal{M}_i$ into projector matrix $P_{jk} = |j\rangle\langle j| + |k\rangle\langle k|$ and another $P_{rest} = \sum_{j \notin \cup t \in \mathcal{M}_i} |j\rangle\langle j|$.

Local Decoding: Lower Bounds and connections to Quantum Computing

- How to recover x_i from $|\phi_x\rangle$?
- Convert $\mathcal{M}_i$ into projective measurement by converting each pair $(j, k) \in \mathcal{M}_i$ into projector matrix $P_{jk} = |j\rangle\langle j| + |k\rangle\langle k|$ and another $P_{rest} = \sum_{j \notin \cup t \in \mathcal{M}_i} |j\rangle\langle j|$.
- Notice that they sum to $I \implies$ valid projective measurement.

Local Decoding: Lower Bounds and connections to Quantum Computing

- How to recover x_i from $|\phi_x\rangle$?
- Convert $\mathcal{M}_i$ into projective measurement by converting each pair $(j,k) \in \mathcal{M}_i$ into projector matrix $P_{jk} = |j\rangle\langle j| + |k\rangle\langle k|$ and another $P_{rest} = \sum_{j \notin \cup t \in \mathcal{M}_i} |j\rangle\langle j|$.
- Notice that they sum to $I \implies$ valid projective measurement.
- State $P_{jk}|\phi_x\rangle$ with probability $\frac{2}{m}$ $\forall (j,k) \in \mathcal{M}_i$.

Local Decoding: Lower Bounds and connections to Quantum Computing

- How to recover x_i from $|\phi_x\rangle$?
- Convert $\mathcal{M}_i$ into projective measurement by converting each pair $(j,k) \in \mathcal{M}_i$ into projector matrix $P_{jk} = |j\rangle\langle j| + |k\rangle\langle k|$ and another $P_{rest} = \sum_{j \notin \cup t \in \mathcal{M}_i} |j\rangle\langle j|$.
- Notice that they sum to $I \implies$ valid projective measurement.
- State $P_{jk}|\phi_x\rangle$ with probability $\frac{2}{m}$ $\forall (j,k) \in \mathcal{M}_i$.
- $|\mathcal{M}_i| = \Omega(\delta\epsilon m)$, probability $|\mathcal{M}_i| \times \frac{2}{m} = \Omega(\delta\epsilon)$.

Local Decoding: Lower Bounds and connections to Quantum Computing

- How to recover x_i from $|\phi_x\rangle$?
- Convert $\mathcal{M}_i$ into projective measurement by converting each pair $(j,k) \in \mathcal{M}_i$ into projector matrix $P_{jk} = |j\rangle\langle j| + |k\rangle\langle k|$ and another $P_{rest} = \sum_{j \notin \cup t \in \mathcal{M}_i} |j\rangle\langle j|$.
- Notice that they sum to $I \implies$ valid projective measurement.
- State $P_{jk}|\phi_x\rangle$ with probability $\frac{2}{m}$ $\forall (j,k) \in \mathcal{M}_i$.
- $|\mathcal{M}_i| = \Omega(\delta\epsilon m)$, probability $|\mathcal{M}_i| \times \frac{2}{m} = \Omega(\delta\epsilon)$.
- Other case with probability $r = 1 - \Omega(\delta\epsilon)$. In this case, guess x_i using a fair coin.

Local Decoding: Lower Bounds and connections to Quantum Computing

- How to recover x_i from $|\phi_x\rangle$?
- Convert $\mathcal{M}_i$ into projective measurement by converting each pair $(j,k) \in \mathcal{M}_i$ into projector matrix $P_{jk} = |j\rangle\langle j| + |k\rangle\langle k|$ and another $P_{rest} = \sum_{j \notin \cup t \in \mathcal{M}_i} |j\rangle\langle j|$.
- Notice that they sum to $I \implies$ valid projective measurement.
- State $P_{jk}|\phi_x\rangle$ with probability $\frac{2}{m}$ $\forall (j,k) \in \mathcal{M}_i$.
- $|\mathcal{M}_i| = \Omega(\delta\epsilon m)$, probability $|\mathcal{M}_i| \times \frac{2}{m} = \Omega(\delta\epsilon)$.
- Other case with probability $r = 1 - \Omega(\delta\epsilon)$. In this case, guess x_i using a fair coin.

Local Decoding: Lower Bounds and connections to Quantum Computing

- For first case, current state after measurement is

$$\frac{(-1)^{E(x)_j}}{\sqrt{2}}(|j\rangle + (-1)^{E(x)_j \oplus E(x)_k} |k\rangle)$$

Local Decoding: Lower Bounds and connections to Quantum Computing

- For first case, current state after measurement is

$$\frac{(-1)^{E(x)_j}}{\sqrt{2}}(|j\rangle + (-1)^{E(x)_j \oplus E(x)_k} |k\rangle)$$

- Measure this in $|j\rangle + |k\rangle$ and $|j\rangle - |k\rangle$ basis to get $E(x)_j \oplus E(x)_k$.

Local Decoding: Lower Bounds and connections to Quantum Computing

- For first case, current state after measurement is

$$\frac{(-1)^{E(x)_j}}{\sqrt{2}}(|j\rangle + (-1)^{E(x)_j \oplus E(x)_k} |k\rangle)$$

- Measure this in $|j\rangle + |k\rangle$ and $|j\rangle - |k\rangle$ basis to get $E(x)_j \oplus E(x)_k$.
- Add $a_{i,(j,k)}$ to this using Katz-Trevisan Theorem.

Local Decoding: Lower Bounds and connections to Quantum Computing

- For first case, current state after measurement is

$$\frac{(-1)^{E(x)_j}}{\sqrt{2}}(|j\rangle + (-1)^{E(x)_j \oplus E(x)_k} |k\rangle)$$

- Measure this in $|j\rangle + |k\rangle$ and $|j\rangle - |k\rangle$ basis to get $E(x)_j \oplus E(x)_k$.
- Add $a_{i,(j,k)}$ to this using Katz-Trevisan Theorem.
- Success probability $p \geq \frac{r}{2} + \left(\frac{1}{2} + \Omega(\epsilon)\right)(1-r) = \frac{1}{2} + \Omega(\delta\epsilon^2)$

A. Ambainis, D. Leung, L. Mancinska, and M. Ozols.

Quantum random access codes with shared randomness.

ArXiv preprint, 2008.

A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani.

Dense quantum coding and a lower bound for 1-way quantum automata.

In *Proceedings of 31st ACM STOC*, pages 376–383, 1999.

A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani.

Dense quantum coding and quantum finite automata.

Journal of the ACM, 49(4):496–511, 2002.

A. Casaccino, E. F. Galvão, and S. Severini.

Extrema of discrete wigner functions and applications.

Physical Review A, 78, 2008.

R. Cleve, W. van Dam, M. Nielsen, and A. Tapp.

Quantum entanglement and the communication complexity of the inner product function.

In *Proccedings of 1st NASA QCQC conference*, pages 61–74, 1998.

R. de Wolf.

Quantum computing: Lecture notes.

CWI Netherlands, *https://homepages.cwi.nl/~rdewolf/qcnotes.pdf*, 2009.

M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita.

(4, 1)-quantum random access coding does not exist.

New Journal of Physics, (8):129, 2006.

A. S. Holevo.

Bounds for the quantity of information transmitted by a quantum communication channel.

Problemy Peredachi Informatsii, 9:177–183, 1973.

J. Katz and L Trevisan.

On the efficiency of local decoding procedures for error-correcting codes.

In *Proceedings of 32nd ACM STOC*, pages 80–86, 2000.

A. Nayak.

Optimal lower bounds for quantum automata and random access codes.

In *Proceedings of 40th IEEE FOCS*, pages 369–376, 1999.

R. O'Donell.

Course on "quantum computing and quantum information".

CMU, https://www.cs.cmu.edu/~odonnell/quantum15/, 2015.

Thank You!