Quantum

Lecture 9

- Classical linear codes
- Quantum codes

Block Codes

An (n, M) block (channel) code over a field $\mathrm{GF}(q)$ is a set

$$\mathcal{C} = \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_M\}$$

of *codewords*, with $\mathbf{x}_m \in \mathrm{GF}^n(q)$

$\mathrm{GF}(q) =$ "set of $q < \infty$ objects that can be added, subtracted, divided and multiplied to stay inside the set"

- $\mathrm{GF}(2) = \{0, 1\}$ modulo 2
- $\mathrm{GF}(p) = \{0, 1, \dots, p-1\}$ modulo p, for a prime number p
- $\mathrm{GF}(q)$ for a non-prime q; polynomials...

Hamming distance: For $\mathbf{x}, \mathbf{y} \in \mathrm{GF}^n(q)$,

$$d(\mathbf{x}, \mathbf{y}) = \text{number of components where } \mathbf{x} \text{ and } \mathbf{y} \text{ differ}$$

Hamming weight: For $\mathbf{x} \in \mathrm{GF}^n(q)$,

$$w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$$

where $\mathbf{0} = (0, 0, \ldots, 0)$

Minimum distance of a code $\mathcal{C}$:

$$d_{\mathsf{min}} = d = \min \{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y};\ \mathbf{x}, \mathbf{y} \in \mathcal{C}\}$$

A code $\mathcal{C}$ is linear if

$$\mathbf{x}, \mathbf{y} \in \mathcal{C} \implies \mathbf{x} + \mathbf{y} \in \mathcal{C}, \quad \mathbf{x} \in \mathcal{C}, \alpha \in \mathrm{GF}(q) \implies \alpha \cdot \mathbf{x} \in \mathcal{C}$$

where $+$ and $\cdot$ are addition and multiplication in GF(q)

A linear code $\mathcal{C}$ forms a linear space $\subset \mathrm{GF}^n(q)$ of dimension $k < n$
$\Rightarrow$ exists a basis $\{\mathbf{g}_m\}_{m=1}^k$, $\mathbf{g}_m \in \mathcal{C}$, that spans $\mathcal{C}$, i.e.,

$$\mathbf{x} \in \mathcal{C} \iff \mathbf{x} = \sum_{m=1}^{k} u_m \mathbf{g}_m$$

for some $\mathbf{u} = (u_1, \ldots, u_k) \in \mathrm{GF}^k(q)$, and hence $M = |\mathcal{C}| = q^k$

Let $\{\mathbf{g}_m\}_{m=1}^k$ define the rows of a $k \times n$ matrix $\mathbf{G} \implies$

$$\mathbf{x} \in \mathcal{C} \iff \mathbf{x} = \mathbf{u}\mathbf{G}$$

for some $\mathbf{u} \in \mathrm{GF}^k(q)$

$\mathbf{G}$ is called a generator matrix for the code

Any $\mathbf{G}$ with rows that form a *maximal set of linearly independent codewords* is a valid generator matrix $\Rightarrow$ a code $\mathcal{C}$ can have different $\mathbf{G}$'s

An (n, M) linear code of dimension $k = \log_q M$ and with minimum distance d is called an $[n, k, d]$ code

Let $r = n - k$ and let the rows of the $r \times n$ matrix $\mathbf{H}$ span

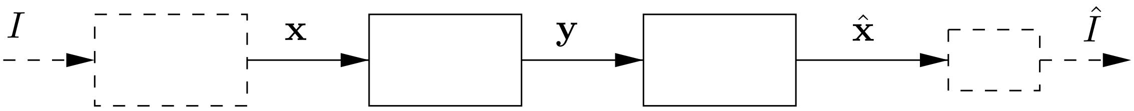
$$\mathcal{C}^\perp = \{\mathbf{v} : \mathbf{v} \cdot \mathbf{x} = 0,\ \ \mathbf{x} \in \mathcal{C}\}, \quad \mathbf{v} \cdot \mathbf{x} = \sum_{m=1}^{n} v_m x_m \ \text{ in } \mathrm{GF}(q)$$

Any such $\mathbf{H}$ is called a parity check matrix for $\mathcal{C}$

- $\mathbf{G}\mathbf{H}^T = \mathbf{0} \quad (= \{0\}^{k \times r}); \quad \mathbf{x} \in \mathcal{C} \iff \mathbf{H}\mathbf{x}^T = \mathbf{0}^T$
- $\mathbf{H}$ generates the *dual code* $\mathcal{C}^\perp$

$\mathcal{C}$ linear $\implies d_{\text{min}} = \min_{\mathbf{x} \in \mathcal{C}} w(\mathbf{x}) =$ minimal number of linearly dependent columns of $\mathbf{H}$

Coding over a DMC



Information variable: $I \in \mathcal{I}_M = \{1, \dots, M\}$ ($p(i) = 1/M$)

Encoding: $I = i \to \mathbf{x}_i = \alpha(i) \in \mathcal{C}$

- $\mathcal{C}$ linear with $M = q^k \implies$ any $i \in \mathcal{I}_M$ corresponds to some $\mathbf{u}_i \in \mathrm{GF}^k(q)$ and $\mathbf{x}_i = \mathbf{u}_i \mathbf{G}$

A DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ with $\mathcal{X} = \mathrm{GF}(q)$, used n times $\to \mathbf{y} \in \mathcal{Y}^n$

- potentially $\mathcal{Y} \neq \mathcal{X}$, but let's assume $\mathcal{Y} = \mathcal{X} = \mathrm{GF}(q)$

Decoding: $\hat{\mathbf{x}} = \beta(\mathbf{y}) \in \mathcal{C}$ ($\to \hat{I}$)

Probability of error: $P_e = \Pr(\hat{\mathbf{x}} \neq \mathbf{x})$

Decoding $\mathbf{x}$ transmitted $\implies$ $\mathbf{y} = \mathbf{x} + \mathbf{e}$ where $\mathbf{e} = (e_1, \dots, e_n)$ is the *error vector* corresponding to $\mathbf{y}$

The nearest neighbor (NN) decoder

$$\hat{\mathbf{x}} = \mathbf{x}' \quad \text{if} \quad \mathbf{x}' = \arg\min_{\mathbf{x} \in \mathcal{C}} d(\mathbf{y}, \mathbf{x})$$

- Equiprobable $I \in \mathcal{I}_M$ and a symmetric DMC such that $\Pr(e_m = 0) = 1 - p > 1/2$ and $\Pr(e_m \neq 0) = p/(q-1)$,

  NN $\iff$ *maximum likelihood* $\iff$ minimum P_e

With NN decoding, a code with $d_{\text{min}} = d$ can correct

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

errors; as long as $w(\mathbf{e}) \leq t$ the codeword $\mathbf{x}$ will *always* be recovered correctly from $\mathbf{y}$

Bounds

- *Hamming* (or sphere-packing): For a code with $t = \lfloor (d_{\min} - 1)/2 \rfloor$,

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \le M^{-1} q^n$$

  - equality $\implies$ *perfect* code $\implies$ can correct all $\mathbf{e}$ of weight $\le t$ and no others
  - *Hamming codes* are perfect linear binary codes with $t = 1$
- *Gilbert–Varshamov*: There exists an $[n, k, d]$ code over $\mathrm{GF}(q)$ with $r = n - k \le \rho$ and $d \ge \delta$ provided that

$$\sum_{i=0}^{\delta-2} \binom{n-1}{i} (q-1)^i < q^\rho$$

- *Singleton*: For any $[n, k, d]$ code,

$$r = n - k \ge d - 1$$

- $r = d - 1 \implies$ *maximum distance separable* (MDS)
- For MDS codes:
  - Any r columns in $\mathbf{H}$ are linearly independent
  - Any k columns in $\mathbf{G}$ are linearly independent

Two codes $\mathcal{C}$ and $\mathcal{D}$ of length n over $\mathrm{GF}(q)$ are equivalent if there exist n permutations $\pi_1, \dots, \pi_n$ of field elements and a permutation σ of coordinate positions such that

$$(x_1, \dots, x_n) \in \mathcal{C} \implies \sigma\big\{(\pi_1(x_1), \dots, \pi_n(x_n))\big\} \in \mathcal{D}$$

- In particular, swapping the same two coordinates in all codewords gives an equivalent code

For a linear code, $(\mathbf{G}, \mathbf{H})$ can be manipulated (add, subtract, swap rows, swap columns) into an equivalent linear code in systematic or standard form

$$\mathbf{G}_{\text{sys}} = \big[\mathbf{I}_k \big| \mathbf{A}\big] \qquad \mathbf{H}_{\text{sys}} = \big[-\mathbf{A}^T \big| \mathbf{I}_r\big]$$

For MDS codes: no swapping of columns needed

Cosets

For each $\mathbf{y} \in \mathrm{GF}^n(q)$, the coset of a linear code $\mathcal{C}$ (over $\mathrm{GF}(q)$) corresponding to $\mathbf{y}$ is the set

$$\mathcal{C}(\mathbf{y}) = \mathbf{y} + \mathcal{C} = \{\mathbf{y} + \mathbf{x} : \mathbf{x} \in \mathcal{C}\}$$

Every $\mathbf{z} \in \mathrm{GF}^n(q)$ belongs to $\mathcal{C}(\mathbf{y})$ for some $\mathbf{y}$

Two cosets $\mathcal{C}(\mathbf{y}_1)$ and $\mathcal{C}(\mathbf{y}_2)$ are either equal or disjoint

Thus, given $\mathcal{C}$ we can partition $\mathrm{GF}^n(q)$ into $q^n/|\mathcal{C}|$ different cosets

Quantum Error Correcting Codes

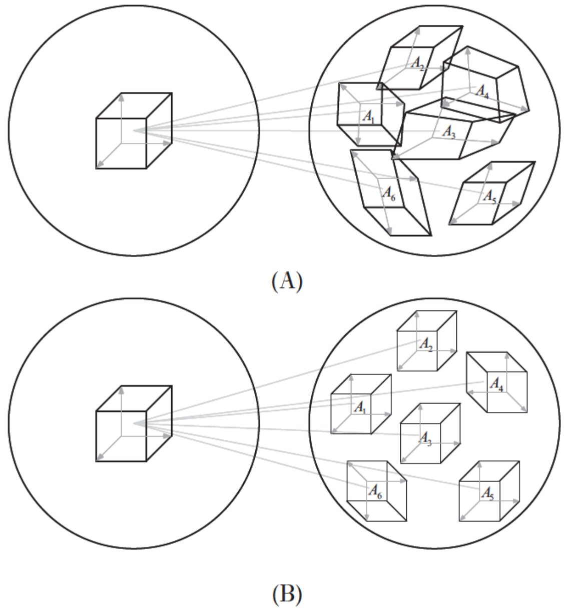


Figure 10.5. The packing of Hilbert spaces in quantum coding: (A) bad code, with non-orthogonal, deformed resultant spaces, and (B) good code, with orthogonal (distinguishable), undeformed spaces.

A code is a subspace $\mathcal{C}$ in a Hilbert space $\mathcal{H}$

Let $P_{\mathcal{C}}$ denote the projection on the code, $|\psi\rangle \in \mathcal{H} \Rightarrow P_{\mathcal{C}}|\psi\rangle \in \mathcal{C}$

A channel is represented by a quantum operation $\mathcal{E}$ from $\mathcal{H}$ to $\mathcal{H}'$, $\operatorname{Tr} \mathcal{E} = 1$, with operation elements $\{E_i\}$ called errors

A decoder is a mapping $\mathcal{D} : \mathcal{H}' \to \mathcal{H}$

The decoder is error-correcting if for $|\psi\rangle \in \mathcal{C}$, $\rho = |\psi\rangle\langle\psi|$,

$$\mathcal{D}(\mathcal{E}(\rho)) = \gamma\rho$$

for some $\gamma \in \mathbb{C}$

Error-correction conditions (finite dimensions)

There exists an error-correcting decoder iff

$$P_{\mathcal{C}} E_i^* E_j P_{\mathcal{C}} = \gamma_{ij} P_{\mathcal{C}}$$

for $\gamma_{ij} \in \mathbb{C}$ picked from a Hermitian matrix

If the condition is fulfilled, $\{E_i\}$ is a set of correctable errors

If the error-correction conditions are fulfilled for $\{E_i\}$ then they are also fulfilled for $\{F_i\}$, with

$$F_j = \sum_i c_{ij} E_i$$

for any $c_{ij} \in \mathbb{C}$

General error correction (finite dimensions)

Given $\mathcal{C}$, assume $\{E_i\}$ satisfies $P_{\mathcal{C}} E_i^* E_j P_{\mathcal{C}} = \gamma_{ij} P_{\mathcal{C}}$

The matrix $\gamma = (\gamma_{ij})$ is Hermitian $\Rightarrow \gamma = U^* D U$ for U unitary and $D = (d_{ij})$ diagonal

For $U = (u_{ij})$ let $F_j = \sum_i u_{ij} E_i \Rightarrow P_{\mathcal{C}} F_k^* F_\ell P_{\mathcal{C}} = d_{k\ell} P_{\mathcal{C}}$

$G_k = F_k P_{\mathcal{C}}$ can be written as $G_k = U_k \sqrt{G_k^* G_k}$ where U_k is unitary (polar decomposition), thus $F_k P_{\mathcal{C}} = \sqrt{d_{kk}} U_k P_{\mathcal{C}}$

Define the projector $P_k = U_k P_{\mathcal{C}} U_k^* \Rightarrow$ corresponding subspaces for different k orthogonal

Detection: Measure $\{P_k\}$

Correction: Apply U_k^*

Decoder: $\mathcal{D}(\sigma) = \sum_k U_k^* P_k \sigma P_k U_k$, $\sigma = \mathcal{E}(\rho)$

$\rho = |\psi\rangle\langle\psi|$ for $|\psi\rangle \in \mathcal{C} \Rightarrow \mathcal{D}(\sigma) = \sum_k d_{kk} \rho$