Lecture 8: From Classical to Quantum Codes

8.1 Block codes over finite fields

Recall: $\mathbb{F}_q = GF(q)$ denotes a finite field with $q = p^m$ (p prime, $m \geq 1$) elements.

Block code $\mathcal{B} \subseteq \mathbb{F}_q^n$, i.e. subsets of sequences of length n over $\mathbb{F}_q$.

Additionally, we require that $\mathcal{B}$ is closed under vector space operations, i.e

$$\forall x, y \in \mathcal{B} \; \forall \alpha, \beta \in \mathbb{F}_q : \quad \alpha \cdot x + \beta \cdot y \in \mathcal{B}$$

$\Rightarrow$ linear block code of length n over $\mathbb{F}_q$

As $\mathcal{B}$ is closed under vector space operations, it is a subspace of the vector space $\mathbb{F}_q^n$ of dimension k, $0 \leq k \leq n$

⇒ The code $\mathcal{C}$ is completely described by a basis of k linear independent vectors over $\mathbb{F}_q$, i.e only $k \times n$ elements over $\mathbb{F}_q$ describe in total q^k vectors.

9.2 Generator matrix

A generator matrix for a linear block code $C = [n, k]_q$ of length n and dimension k is a $k \times n$ matrix over $\mathbb{F}_q$ of rank k, whose row span equals the code.

Encoding an information sequence $i \in \mathbb{F}_q^k$ can be done by the linear mapping

$$i \mapsto i \cdot G = c$$

A generator matrix of the form $G = [I \,|\, A]$ with an $k \times k$ identity matrix I is called <u>systematic</u> as

$$i \mapsto (i, i \cdot A)$$

9.3 Parity check matrix

A linear subspace $C = [n,k] \in \mathbb{F}_q^n$ can also be described as the solution space of $n-k$ linear independent equations.

A parity check matrix H is an $(n-k) \times n$ matrix of full rank whose row-null space is the code.

Error syndrome: $s := v \cdot H^t \in \mathbb{F}_q^{n-k}$

for $v \in \mathbb{F}_q^n$

By definition: $c \in C \iff c \cdot H^t = 0$

Proposition: The error syndrome $s = v \cdot H^t$ depends only on the error.

Assume that $v = c + e$, $c \in C$, e error

$v \cdot H^t = (c+e) \cdot H^t = c \cdot H^t + e \cdot H^t = e \cdot H^t$

2.4 Dual code

Let $C = [n,k]_q$ be a linear code of length n, dimension k over $\mathbb{F}_q$. Then the dual code $C^\perp = [n, n-k]_q$ is a linear code of length n, dimension $n-k$ given by

$$C^\perp = \{v : v \in \mathbb{F}_q^n \mid v \cdot c = \sum_{i=1}^n v_i \cdot c_i = 0 \text{ for all } c \in C\}$$

If G and H are generator and parity check matrices for the code C, resp., then H and G are generator matrix and parity check matrix for the dual code $C^\perp$, i.e. the role of G and H is interchanged.

We have $G \cdot H^t = 0$.

$c = i \cdot G \implies c \cdot H^t = i \cdot G \cdot H^t = 0$

(5)

9.5 The minimum distance of a linear code

$$d_{min}(C) = \min \{ d_H(x,y) : x,y \in C \mid x \neq y \}$$

for linear codes

$$d_H(x,y) = d_H(x-y, \cancel{x}-y)$$
$$= d_H(x-y, 0)$$
$$= \mathrm{wgt}_H(x-y)$$

$$\Rightarrow d_{min}(C) = \min \{ \mathrm{wgt}_H(x) : x \in C \setminus \{0\} \}$$
$$=: \mathrm{wgt}_H(C)$$

bad news: Even for a linear code over $\mathbb{F}_2$ given by a parity check matrix $H \in \mathbb{F}_2^{(n-k)\times n}$, it is an NP complete problem to test whether there is a nonzero vector $c \in C$ with Hamming weight $\mathrm{wgt}_H(c) \leq w$.

$$c \cdot H^t = 0 \quad \text{with} \quad 0 < \mathrm{wgt}_H(c) \leq w$$

"Computing the minimum distance by linear algebra"

Proposition: If any $d-1$ columns in the parity check matrix H are linear independent, then the minimum distance of the code is at least d.

Proof: Let c be a non-zero codeword of weight $\leq d-1$, i.e. $c_{i_1}, \ldots, c_{i_{d-1}} \neq 0$.

$c \cdot H^t = 0$ implies that

$$c_{i_1} \cdot h^{(i_1)} + \ldots + c_{i_d} h^{(i_d)} = 0$$

where $h^{(j)}$ denotes the jth column of H.

$\Rightarrow$ contradiction to the assumption that any $d-1$ columns of H are linearly independent.

9.6 Hamming codes

A code can correct a single error if the minimum distance is at least $d = 3$. Then any two columns of H must be linearly independent, i.e. they are non-zero and not scalar multiples of each other.

The parity check matrix of the Hamming code of order m over $\mathbb{F}_q$ consists of all such vectors, i.e.

$$n = \frac{q^m - 1}{q - 1}$$

$$k = n - m$$

$$d = 3$$

Example: $q = 2$, $m = 3$

$$C = [7, 4, 3]_2 = [n, k, d]_q$$

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} = \left[\mathrm{bin}(i) \right]_{i=1}^{2^3-1}$$

binary expansion of i as column vector of length m

Let $e_i = (0, \ldots, 0, \underset{\uparrow i}{1}, 0 \ldots, 0)$ be a vector of weight one.

Then $s = e_i \cdot H^t = \mathrm{bin}(i)$

$\Rightarrow$ The error syndrome tells us the position of an error.

8

Goal: Use classical binary linear block codes to construct quantum codes.

The states $|c\rangle$, $c \in C = [n, k, d]$ can be used to correct up to $\lfloor \frac{d-1}{2} \rfloor$ bit-flip (σ_x) errors, e.g. $|000\rangle$, $|111\rangle$ corresponding to the linear code $C = [3, 1, 3]$ with $G = [1 1 1]$

8.7 Lemma:

$$\sum_{c \in C} (-1)^{x \cdot c} = \begin{cases} |C| & \text{for } x \in C^\perp \\ 0 & \text{for } x \notin C^\perp \end{cases}$$

Proof: $x \in C^\perp \Rightarrow x \cdot c = 0$ for all $c \in C$

$\Rightarrow \sum_{c \in C} (-1)^{x \cdot c} = \sum_{c \in C} 1 = |C|$

$x \notin C^\perp \Rightarrow D^\perp = \langle C^\perp, x \rangle$

$D < C$

$\Rightarrow C = D \,\dot\cup\, (D + c_0)$ $\quad c_0 \cdot x = 1$

$$\sum_{c \in C} (-1)^{x \cdot c} = \sum_{d \in D} (-1)^{x \cdot d} + \sum_{d \in D} (-1)^{x \cdot (d + c_0)} = 0$$

9.8 Let C be a linear code of length n over $\mathbb{F}_2$ and let $a, b \in \mathbb{F}_2^n$.

Define the following quantum state:

$$|\psi\rangle := \frac{1}{\sqrt{|C|}} \sum_{c \in C} (-1)^{a \cdot c} |c + b\rangle$$

Then the image of $|\psi\rangle$ under the Hadamard transformation $H_{2^n} = H^{\otimes n}$ where $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is given by

$$H_{2^n} |\psi\rangle = \frac{(-1)^{a \cdot b}}{\sqrt{|C^\perp|}} \sum_{c \in C^\perp} (-1)^{b \cdot c} |c + a\rangle$$

Proof:
$$H_{2^n} = \frac{1}{\sqrt{2^n}} \sum_{x, y \in \mathbb{F}_2^n} (-1)^{x \cdot y} |x\rangle\langle y|$$

direct calculation using Lemma 9.7

CSS code construction

Independently developed by Andrew Steane and R. Calderbank & P. Shor.

9.8 Let $C_1 = [n, k_1, d_1]$ and $C_2 = [n, k_2, d_2]$ be linear binary codes of equal length and additionally we require that $C_2^\perp \leq C_1$.

As $C_2^\perp$ is a subspace of C_1, we can write C_1 as the disjoint union of translates of $C_2^\perp$, i.e

$$C_1 = \dot{\bigcup_{w_i \in W}} (C_2^\perp + w_i)$$

Then the CSS code given by C_1, C_2 has basis states

$$|\psi_i\rangle = \frac{1}{\sqrt{|C_2^\perp|}} \sum_{c \in C_2^\perp} |c + w_i\rangle .$$

$\Rightarrow$ for $w_i \neq w_j$ ($w_i - w_j \notin C_2^\perp$) we have

$$\langle \psi_i | \psi_j \rangle = 0$$

There are $|W| = \frac{|C_1|}{|C_2^\perp|} = \frac{2^{k_1}}{2^{n-k_2}}$

$$= 2^{k_1+k_2-n}$$

mutually orthogonal basis states

notation: $\mathcal{C} = ((n, 2^{k_1+k_2-n})) \le (\mathbb{C}^2)^{\otimes n}$

$$= [[n, k_1+k_2-n]]$$

The CSS code can correct

up to $\left\lfloor \frac{d_1-1}{2} \right\rfloor$ spin-flip (σ_x) errors

<u>and</u> simultaneously

up to $\left\lfloor \frac{d_2-1}{2} \right\rfloor$ sign-flip (σ_z) errors

$\Rightarrow$ The code can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor = t$ where $d = \min(d_1, d_2)$ arbitrary Pauli errors (and hence any general error up to weight t).

$\Rightarrow$ The code has minimum distance (at least) d

$$\mathcal{C} = [[n, k, d]]$$

Sketch of a proof for CSS codes

Up to a phase factor, any Pauli error can be written as

$$e = \left(\sigma_x^{e_{x,1}} \sigma_z^{e_{z,1}}\right) \otimes \ldots \otimes \left(\sigma_x^{e_{x,n}} \sigma_z^{e_{z,n}}\right)$$

i.e. two binary vectors $e_x, e_z \in \mathbb{F}_2^n$ specify the error.

A general state of the CSS code:

$$|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle$$

$$= \sum_i \tilde{\alpha}_i \sum_{c \in C_2^\perp} |c + w_i\rangle = \sum_{c \in C_1} \beta_c |c\rangle$$

As superpositions of codewords of C_1, we can correct up to $\left\lfloor \frac{d_1 - 1}{2} \right\rfloor$ σ_x-errors.

The Hadamard transformed basis states are

$$H_{2^n} |\psi_i\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{c \in C_2} (-1)^{c \cdot w_i} |c\rangle$$

$\Rightarrow$ The Hadamard transformed general state of the CSS code is of the form

$$H_{2^n} |\psi\rangle = \sum_{c \in C_2} \gamma_c |c\rangle$$

As superposition of codewords of C_2, we can correct up to $\left\lfloor \frac{d_2 - 1}{2} \right\rfloor$ σ_x-errors in the Hadamard transformed basis, i.e. σ_z-errors in the original basis.

It remains to show that σ_x and σ_z errors can be corrected independently.