Reminders:
1. Register on piazza
2. Log on to Autolab
3. HW 0 out this Th (HW 0 is optional and will not be graded)

Recap:
- \((n, k, d)q\) code
- Block length
- Dimension
- Distance
- Alphabet size

Big Q: Given a distance \(d\), what is the largest rate for a code with distance \(d\)?

- Hamming code:
  \(C_1: (x_1, x_2, x_3, x_4)\)
  \[
  \begin{pmatrix}
  0 & 1 & 0 & 1;
  1 & 0 & 0 & 1;
  0 & 1 & 0 & 1
  \end{pmatrix}
  \]
  \((7, 4, 3)_2\) code

- Hamming distance:
  \(d(C_H) = \min wt(C)\)
  \[C_i \neq C_j \implies wt(C_i) \neq 0\]

- Hamming bound: For any \((n, k, d)q\) code, \(k \leq n - \log_q(n+1)\)

Volunteer for proof reading?

Linear codes

Q: How much space do we need to represent an \((n, k, d)q\) code?

A: In general nothing better than \(nq^k\) symbols. For \(q = p^s\) \(p\) prime. \(s \geq 1\) is an integer.

Today: A general class of codes that needs \(O(n^2)\) symbols.

**Definition (Linear codes)**: Let \(q\) be a prime power \((q = p^s: p\) prime. \(s \geq 1\) is an integer. \(C \subseteq \mathbb{F}_q^n\) is a linear code if it is a linear subspace. A linear \((n, k, d)q\) code is referred to as a \(\mathbb{F}_q^n, k(q, d)q\) code.

First: What set of "numbers"? What arithmetic operations?

Fields: \(\mathbb{F} = \langle \mathbb{Z}_p, +, \cdot \rangle\)
- Closure of \(+, \cdot\)
- Associativity of \(+, \cdot\)
- Commutativity of \(+, \cdot\)
Distributivity: \[ a \cdot (b + c) = a \cdot b + a \cdot c \]

Identities: \( O \) for +, \( 1 \) for \( \cdot \) \( \subseteq [0, 1] \subseteq \mathbb{R} \)

Inverses: \( \forall a \in \mathbb{R}, \exists -a \in \mathbb{R} \text{ s.t. } a + (-a) = 0 \)
\( \forall a \in \mathbb{R} \setminus \{0\}, \exists a' \in \mathbb{R} \text{ s.t. } a \cdot (a') = 1 \)

Ex: \( \mathbb{R} \) is a field, \( \mathbb{Z} \) is not

Finite fields \( \mathbb{F}_p \) are finite.

Thm 1: Any finite field \( \mathbb{F} \) has size \( \# \mathbb{F} = p^s \), where prime

Ex: \( (\{0, 1\}, \oplus, \land) \) \( \subseteq \) finite field of size 2
\( (\{0, \ldots, p-1\}, +_{\text{mod } p}, \cdot_{\text{mod } p}) \) \( \subseteq \) finite field of size \( p \).

Thm 2: There is a unique finite field for each prime power (up to isomorphism) \( \# \mathbb{F}_q \) for prime power \( q \)

Linear subspaces \( S \subseteq \mathbb{F}_q^n \) is a linear subspace if:
1. \( \forall x, y \in S, x + y \in S \)
2. \( \forall a \in \mathbb{F}_q, \forall x \in S, a \cdot x \in S \)

Ex 1: Subspace of \( \mathbb{F}_5^3 \):
\( S_1 = \{ (0,0,0), (1,1,1), (2,2,2), (3,3,3), (4,4,4) \} \)
\( \Rightarrow (1) \) \( (1,1,1) + (2,2,2) = (3,3,3) \in S_1 \)
\( (2) \) \( 2 \cdot (4,4,4) = (8,8,8) \mod 5 = (3,3,3) \in S_1 \)

Ex 2: Subspace of \( \mathbb{F}_3^3 \):
\( S_2 = \{ (0,0,0), (1,0,1), (2,1,2), (0,1,1), (0,1,2), (2,2,1), (1,1,2), (2,2,1), (1,2,0), (2,1,0) \} \)
Def (Span) \( B = \{ u_1, \ldots, u_k \} \subset \mathbb{F}_q^n \), its span
\[ \text{span}(B) = \{ \sum_{i=1}^k q_i u_i \mid q_i \in \mathbb{F}_q \} \]

For \( \mathbb{F}_5 \): \( S_1 = \text{span}\{ (1,1,1) \} \)

Def (Linear Independence) \( \{ u_1, \ldots, u_k \} \subset \mathbb{F}_q^n \) are linearly independent if \( \forall i \in [k] \)
\( u_i \notin \text{span}(\{ u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_k \}) \)

Ex: Over \( \mathbb{F}_3 \) \( (1,0,1) \) & \( (0,1,1) \) are lin indep.

Def (Rank): Rank of a matrix \( M \in \mathbb{F}_q^{r \times k} \) is the largest \( r \) of linearly independent rows (or columns)
\( M \in \mathbb{F}_q^{r \times n} \) is full rank if it has rank \( \min(r,n) \)

Eq: \( \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \) is full rank over \( \mathbb{F}_3 \)

Thm: \( S \subset \mathbb{F}_q^n \) be a linear subspace \( \implies \)
(i) \( |S| = q^k \) \( 0 \leq k \leq n \) integer (\( k \): dimension of \( S \))
(ii) \( \exists u_1, \ldots, u_k \) lin. independent (basis of \( S \))
\( S \cap \mathbb{F}_q^n \)
\( \overline{x} = a_1 u_1 + a_2 u_2 + \ldots + a_k u_k \); \( a_i \in \mathbb{F}_q \)

(iii) \( \exists \) a full rank \( (n-k) \times n \) matrix \( H \) s.t. \( \forall x \in S \)
\( Hx^T = \mathbf{0} \in \mathbb{F}_q^{n-k} \)

(iv) \( S \) & \( H \) are orthogonal: \( G \cdot HT = 0 \)

\( S_1 : S_1 = (1,1,1) \quad H_1 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix} \) over \( \mathbb{F}_5 \)
\( S_2 : S_2 = (1,0,1) \quad H_2 = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 2 \end{pmatrix} \) over \( \mathbb{F}_5 \)

Lemma: \( S \) is gen matrix for \( S \); \( \mathbb{F}_q^n \); \( H \) is parity check matrix for \( S \); \( \mathbb{F}_q^n \); \( S \) is lin indep.
Properties of linear codes:

\([7,4,3]_2\) Hamming code

\[
\begin{align*}
G_{\text{Ham}} &= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
\end{pmatrix} \\
H_{\text{Ham}} &= \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\end{pmatrix} 
\end{align*}
\]

Prop 1: Any \([n,k]_q\) code can be represented with \(\min (kn, (n-k)n)\) symbols from \(\mathbb{F}_q\).

Prop 2: Any \([n,k]_q\) code has \(O(kn)\) operations over \(\mathbb{F}_q\) encoding.

Prop 3: \(O( (n-k)n) \) error detection.

Lemma: For any \([n,k,d]_q\) code \(C\)

\[
d = \min_{\mathbf{c} \neq \mathbf{0}} w(+(\mathbf{c}))
\]

\[
\exists \mathbf{d} \leq \Delta C(\mathbf{0}, \mathbf{c}') = \Delta C(\mathbf{c}_1, \mathbf{c}_2)
\]

\[
\exists \mathbf{d} = \Delta C(\mathbf{c}_1, \mathbf{c}_2) = w(\mathbf{c}_1 - \mathbf{c}_2) \geq \Delta
\]

Claim: \(\mathbf{c}_1 - \mathbf{c}_2 \in C\)

Proof: By scalar mult prop of linear subspace

\[\begin{align*}
\mathbf{c}_1 + (-\mathbf{c}_2) & \in C \\
\mathbf{c}_1 - \mathbf{c}_2 & \in C
\end{align*}\]