Today

- Reed Solomon Codes
- MDS codes

CS3.318.1
Coding Theory
Lecture 6 (2022-9-16)
Instructor: Prahladh Harsha.

## Reed Solomon Codes:

$\mathbb{F}$ - finite field ($|\mathbb{F}| = q = p^\alpha$ prime power)

$S \subseteq \mathbb{F}$ - set of evaluation points, $|S| = n$

$k$ - degree parameter.

$$q \geq n \geq k \geq 1$$

$\mathbb{F}$ - alphabet. ; $S$ = ordered set $(\alpha_1, \alpha_2 \ldots, \alpha_n)$

$p$ - deg $< k$ polynomial w/ coeff from $\mathbb{F}$

$p(x) \in \mathbb{F}_{<k}[x]$

$$(p(\alpha_1), p(\alpha_2) \ldots, p(\alpha_n)) \in RS_{\mathbb{F}}[S, k]$$

$$p(x) = \sum_{i=0}^{k-1} p_i x^i$$

$$RS : \mathbb{F}^k \to \mathbb{F}^n$$
$$p \mapsto (p(\alpha_i))_{\alpha_i \in S}$$

Two settings:
- $S = \mathbb{F}$
- $S = \mathbb{F}^* = \mathbb{F} \setminus \{0\}$.

Observations:

1. $RS_{\mathbb{F}}[S,k]$ - $\mathbb{F}$-linear code.

Pf: Poly $\in \mathbb{F}_{<k}[x]$ closed under addition + scalar multiplication.

2. $RS_{\mathbb{F}}[S,k]$ meets the Singleton Bound

ie distance $= n-k+1$.

Claim: $p, q \in \mathbb{F}_{<k}[x]$, $p \neq q$, $\#\{\alpha \in S \mid p(\alpha) = q(\alpha)\} \leq k-1$

Claim [Degree Mantra]

$p \in \mathbb{F}_{\leq r}[x]$ & $p \neq 0$, $\Rightarrow$ $p$ has at most $r$ roots

Pf of previous claim: Working $p-q$

In short, $RS_{\mathbb{F}}[S,k]$ is a $[n, k, n-k+1]_q$-code

(A) Generator Matrix for RS:

$$\sum_{i=0}^{k-1} p_i x^i = p(x) \longmapsto (p(\alpha))_{\alpha \in S}$$

$\leftarrow$ monomials $\rightarrow$

Vandermonde Matrix $\leftarrow$

$$\begin{array}{c} \\ S \\ \\ \end{array}\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{k-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{k-1} \\ & & \vdots & & \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{k-1} \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_{k-1} \end{bmatrix} = \begin{bmatrix} p(\alpha_1) \\ p(\alpha_2) \\ \vdots \\ p(\alpha_n) \end{bmatrix}$$

## Maximum Distance Separable Codes (MDS codes)

A code is said to be MDS if it achieves the Singleton bound.

**Theorem:** Let $\mathcal{C} = [n,k,d]_q$-code be an MDS-code then $\forall\, T \subseteq [n]$, $|T| = k$ then $|\mathcal{C}_T| = q^k$

(where $\mathcal{C}_T = \{ c_T \mid c \in \mathcal{C} \}$

Pf: First for RS code

wlog $T = \{\alpha_1, \ldots, \alpha_k\}$

$\alpha$ – mon. $\rightarrow$

$$\begin{array}{c c} & i \\ \alpha\text{-}T \downarrow & \begin{bmatrix} \text{—} & \alpha^i & \text{—} \end{bmatrix} \\ & i \end{array} \begin{bmatrix} p_0 \\ \vdots \\ p_{k-1} \end{bmatrix} = \begin{bmatrix} p(\alpha_1) \\ \vdots \\ p(\alpha_k) \end{bmatrix}$$

$\hookrightarrow$ $k \times k$ Vandermonde is invertible.

Hence, the thm.

---

General case: $\mathcal{C}$ - $[n,k,d]_q$-code MDS

$d = n-k+1$.

$T \subseteq [n]$, Suppose $\exists\, c_1, c_2 \in \mathcal{C}$, st $c_1|_T = c_2|_T$

then $\Delta(c_1, c_2) \leq n-k$

$\Rightarrow \Leftarrow$

$\boxtimes$

# Primer on finite fields:

$\mathbb{F}$ - Set of elements equipped w/ 2 binary operⁿs

$+$ - addition

commutative, identity (0), associativity inverses.

$\cdot$ - multiplication (for nonzero elts).

commutative, identity (1), associativity inverses.

$a \cdot 0 = 0 \cdot a = 0 \quad \forall a \in \mathbb{F}$

- distributive

$a \cdot (b+c) = a \cdot b + a \cdot c.$

---

Ring: All the above except for multiplicative inverse.

eg: (fields)

$\mathbb{F}_p$ - prime fields.

$\mathbb{F}_q$ where $q = p^n$ p-prime, n-positive integer.

$\mathbb{F}_q \cong \mathbb{F}_p[X] / (E(x))$ E is an irreducible poly of deg exactly n

$\mathbb{F}[x]$ - polynomial rings.

Factorization: $f = g \cdot h$

$f \in \mathbb{F}[x]$ is reducible if $\exists$ $g, h$

$0 < \deg(g), \deg(h) < \deg(f)$

$f = g \cdot h$.

is irreducible otherwise

Unique-Factorization Domain (UFD)

$f = f_1 f_2 \dots f_r$ where $f_i, g_j$ are irreducible

$= g_1 \dots g_s$

then $r = s$ & there permutation

$\pi : [r] \to [s]$ &

$\alpha_1 \dots \alpha_r$ s.t $\prod \alpha_i = 1$

$f_i = \alpha_i g_{\pi(i)}$

Integers:

Division: Given $a, b \in \mathbb{Z}_{\geq 0}$

$\exists$ $q, r \in \mathbb{Z}_{\geq 0}$

$a = bq + r$ s.t $0 \leq r < b$.

"Division Algorithm" (for univariate polynomials)

Given $A(x), B(x) \in \mathbb{F}[x]$

$\exists$ $Q(x), R(x) \in \mathbb{F}[x]$

$A(x) = B(x) \cdot Q(x) + R(x)$

where $0 \leq \deg(R) < \deg(B)$.

(Proof of Degree Mantra).

$\alpha$ is a root of $P(x) \Leftrightarrow p(\alpha) = 0$

$P(x) = (x-\alpha) Q(x) + P(\alpha)$

$\alpha$ is a root of $P(x) \Rightarrow P(x) = (x-\alpha) Q(x)$

Continuing $\alpha_1 \ldots \alpha_n$ - roots

$P(x) = Q(x) \cdot \prod_{i=1}^{n} (x - \alpha_i)$

---

$\mathbb{F}_q$: All elements of $\mathbb{F}_q$ are roots of $x^q - x$

$\mathbb{F}_p$ - prime field.

$\{0, 1, 2, \ldots, p-1\}$

$\{0, 1 = 0+1, 2 = 1+1, \ldots, p-1 = p-2+1\}$

$0 = p-1+1$

$S = \mathbb{F}_p = (0, 1, 2, \ldots, p-1)$

$A \in \mathbb{F}_{<k}[x] \quad (A(0), A(1), \ldots, A(p-1))$

$B(x) = A(x-1)$

$(B(0), B(1), \ldots, B(p-1)) = (A(p-1), A(0), \ldots A(p-2))$

RS is cyclic.

non-prime fields.

$\mathbb{F}_q \qquad q = p^r \qquad r \neq 1$

$\forall q = p^r, \quad \exists\, \omega \in \mathbb{F}_q^*, \quad \mathbb{F}_q^* = \{1, \omega, \omega^2, \ldots, \omega^{q-2}\}$

$S = \mathbb{F}_q^*$

$$\left.\begin{array}{l} (A(1), A(\omega) \ldots \quad A(\omega^{q-2})) \\ B(x) = A(\omega x) \\ (B(1), \ldots \quad B(\omega^{q-2})) \\ = (A(\omega), \ldots \quad A(\omega^{q-2}), A(1)) \end{array}\right\} \text{RS is cyclic.}$$

## Parity Check Representation of the RS code

$S = \mathbb{F}_q$ (Evaluation points is the whole field)

Consider $\sum_{\alpha \in \mathbb{F}} \alpha^i \qquad 0 \leq i \leq q-1$

$i = 0$: $\quad \sum_{\alpha \in \mathbb{F}} \alpha^0 = \sum_{\alpha \in \mathbb{F}} 1 = 0$

$i = q-1$ $\quad \sum_{\alpha \in \mathbb{F}} \alpha^{q-1} = 0 + \sum_{\alpha \in \mathbb{F}_q^*} 1 = -1$

$0 < i < q-1$ $\quad \sum_{\alpha \in \mathbb{F}} \alpha^i = \sum_{\alpha \in \mathbb{F}^*} \alpha^i$ (since $i \neq 0$)

$$= \sum_{j=0}^{q-2} (\omega^j)^i$$

$$= \frac{(\omega^i)^{q-1} - 1}{\omega^i - 1} \quad \text{(since } i \notin \{0, q-1\}\text{)}$$

$= 0$

**Proposition:** $\displaystyle\sum_{\alpha\in\mathbb{F}} \alpha^i = \begin{cases} 0 & \text{if } i < q-1 \\ -1 & \text{if } i = q-1 \end{cases}$

**Cor:** $\forall\, i,j$ s.t. $0 \le i+j \le q-2$, $\displaystyle\sum_{\alpha\in\mathbb{F}} \alpha^i \alpha^j = 0$

**Cor:** $\forall\, f,g \in \mathbb{F}[x]$ s.t. $0 \le \deg(f) + \deg(g) \le q-2$,

$$\sum_{\alpha\in\mathbb{F}} f(\alpha)\cdot g(\alpha) = 0$$

Equivalently,

$$RS_{\mathbb{F}}[\mathbb{F}, k]^{\perp} \supseteq RS_{\mathbb{F}}[\mathbb{F}, q-k] \quad \text{where } |\mathbb{F}| = q$$

(since $k-1+q-k-1 = q-2$)

However $\dim\left(RS_{\mathbb{F}}[\mathbb{F}, k]^{\perp}\right)$

$= q - \dim\left(RS_{\mathbb{F}}[\mathbb{F}, k]\right)$

$= q-k$

Hence,

**Prop:** $RS_{\mathbb{F}}[\mathbb{F}, k]^{\perp} = RS_{\mathbb{F}}[\mathbb{F}, q-k]$

ie, When $S = \mathbb{F}$, the dual of RS is RS (of a different degree parameter)

The same is true for any $S$ (w/ some slight alterations) see PS2.

Thus, a parity check matrix for $RS_{\mathbb{F}}[\mathbb{F}, k]$ is

$$\begin{array}{cc}
 & \alpha \longleftarrow S = \mathbb{F} \longrightarrow \\
\begin{array}{c} i \\ \text{monomials} \\ x^i;\ 0 \le i < q-k \\ \downarrow \end{array} &
\begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
\alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\
\alpha_1^2 & \alpha_2^2 & \alpha_3 & \cdots & \alpha_n^2 \\
\vdots & & & & \\
\alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \alpha_3^{n-k-1} & \cdots & \alpha_n^{n-k-1}
\end{bmatrix}
\end{array} \quad \alpha$$

here $n = q = |\mathbb{F}|$

$\boxtimes$