WEEK 14: REED SOLOMON CODES (TEXTBOOK CHAPTER 14)

Prof. Michael Gastpar

Slides by Prof. M. Gastpar and Prof. em. B. Rimoldi

EPFL

Spring Semester 2025

OUTLINE

INTRODUCTION AND ORGANIZATION

ENTROPY AND DATA COMPRESSION

CRYPTOGRAPHY

CHANNEL CODING

- Error Detection and Error Correction
- Finite Fields and Vector Spaces
- Linear Codes
- Reed Solomon Codes
- Summary of Chapter 3

Today we learn about Reed Solomon Codes (Irving Reed and Gustave Solomon, 1960).

Why do we care?

- They are powerful (MDS)
- They are linear
- They let us choose various parameters (arbitrary $\mathbb{F}_q$ and $0 < k < n \leq q$)
- They have a nice construction
- They have elegant and efficient decoding algorithms

- They are used in many applications, namely:
  - Storage devices: tape, CDs, DVDs, bar codes, QR codes, . . .
  - Digital radio/television broadcast
  - High-speed modems: ADSL, xDSL, . . .
  - Deep space exploration modems (including Voyager 2, 1977, Jupiter, Saturn, Neptune)
  - Wireless mobile comm., including cellular phones and microwave links

POLYNOMIALS OVER FINITE FIELDS

Not surprisingly, the notion of polynomial extends to finite fields.

- Let $\vec{u} = (u_1, \ldots, u_k) \in \mathbb{F}^k$ for some finite field $\mathbb{F}$.
- We associate to $\vec{u}$ the polynomial

$$P_{\vec{u}}(x) = u_1 + u_2 x + \cdots + u_k x^{k-1}.$$

- $P_{\vec{u}}(x)$ can be evaluated at any $x \in \mathbb{F}$.
- The degree of a polynomial is the highest exponent i for which x^i has a non-zero coefficient.
- By convention, the zero polynomial has degree $-\infty$.

Example

- $\mathbb{F} = \mathbb{F}_5$;
- $P(x) = 2 + 4x + 3x^2$ is a polynomial of degree 2 over $\mathbb{F}_5$;
- $P(x) = P_{\vec{u}}(x)$ for $\vec{u} = (2, 4, 3) \in \mathbb{F}_5^3$;
- a polynomial $P(x)$ over a field $\mathbb{F}$ can be evaluated at any $x \in \mathbb{F}$: $P_{\vec{u}}(2) = 2 + 4 \cdot 2 + 3 \cdot 2^2 = 2 + 3 + 2 = 2$.

Example

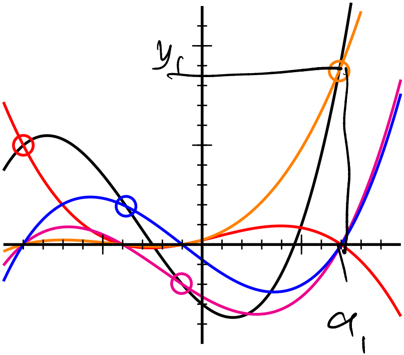
- $P(x) = 3x$ has degree 1.
- $P(x) = 3$ has degree 0.
- $P(x) = 0$ has degree $-\infty$.

Interpolation via Polynomials

Problem: given a field $\mathbb{F}$ and k pairs $(a_i, y_i) \in \mathbb{F}^2$, where the a_i are all distinct, is there a polynomial $P(x)$ over $\mathbb{F}$ of degree at most $k-1$ (hence described by at most k coefficients) such that

$$P(a_i) = y_i, \quad i = 1, \ldots, k?$$

$P(a_i) = y_i$



The answer is yes, obtained via Lagrange's interpolation polynomials.

LAGRANGE'S INTERPOLATION POLYNOMIALS

To simplify notation, we demonstrate how it works by means of examples.

EXAMPLE

- Fix a field $\mathbb{F}$ and distinct field elements a_1, a_2, a_3 as well as y_1, y_2, y_3 (not necessarily distinct).
- We seek a polynomial $P(x)$ of degree at most 2 and coefficients in $\mathbb{F}$ such that $P(a_i) = y_i$.
- Suppose we can find a polynomial $Q_1(x)$ of degree at most 2, such that

$$Q_1(x) = \begin{cases} 1, & x = a_1 \\ 0, & x = a_i \neq a_1 \end{cases}$$

Example (cont.)

- Suppose that $Q_2(x)$ behaves similarly for a_2 and $Q_3(x)$ for a_3.
- The desired polynomial is then $P(x) = y_1 Q_1(x) + y_2 Q_2(x) + y_3 Q_3(x)$.
- Back to the construction of $Q_1(x)$.
- $(x - a_2)(x - a_3)$ is 0 at all the a_i except at a_1 where it is $(a_1 - a_2)(a_1 - a_3)$.
- Hence $\frac{(x-a_2)(x-a_3)}{(a_1-a_2)(a_1-a_3)}$ is the desired $Q_1(x)$.
- We construct $Q_2(x)$ and $Q_3(x)$ similarly.

Example (concrete case)

Over $\mathbb{F}_5$, find the polynomial $P(x)$ of degree not exceeding 2, for which $P(a_i) = y_i$ for

i	(a_i, y_i)
1	$(2, 3)$
2	$(1, 0)$
3	$(0, 4)$

SOLUTION

We find the Lagrange interpolation polynomials $Q_1(x)$ and $Q_3(x)$ and then form $P(x) = y_1 Q_1(x) + y_3 Q_3(x)$. (Notice that $Q_2(x)$ is not needed because $y_2 = 0$.)

$Q_1(x) = \frac{(x-1)(x-0)}{(2-1)(2-0)} = \frac{(x-1)x}{2} = 3(x-1)x;$

$Q_3(x) = \frac{(x-2)(x-1)}{(0-2)(0-1)} = \frac{(x-2)(x-1)}{2} = 3(x-2)(x-1);$

Finally

$$\begin{aligned} P(x) &= 3(3(x-1)x) + 4(3(x-2)(x-1)) \\ &= 4x^2 - 4x + 2x^2 - 6x + 4 \\ &= x^2 + 4. \end{aligned}$$

CONCLUSION

It should be obvious from the above example that we can proceed similarly for any field $\mathbb{F}$, for any positive integer *k*, and for any given set of *k* points with components in $\mathbb{F}$.

ROOTS OF POLYNOMIALS

Let $P(x)$ be a polynomial over a field $\mathbb{F}$. The roots of $P(x)$ are those $b \in \mathbb{F}$ for which $P(b) = 0$.

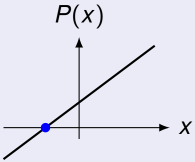
THEOREM (FUNDAMENTAL THM. OF ALGEBRA, TEXTBOOK THM 14.1)

Let $P(x)$ be a polynomial of degree at most $k - 1$ over a field. If $P(x) \neq 0$ then the number of its distinct[2] roots is at most $k - 1$.

[2] The theorem holds even for non-distinct roots if we account for their multiplicities. The stated version, which has an easier proof, is what we need.

Example

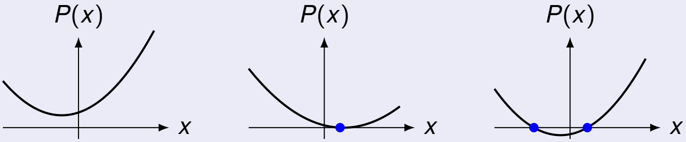
Let the field be $\mathbb{R}$ and $P(x) = ax + b$, $a \neq 0$. This polynomial has 1 root.



Example (cont.)

Let the field be $\mathbb{R}$ and $P(x) = ax^2 + bx + c$, $a \neq 0$.

This polynomial has 0, 1, or 2 roots.

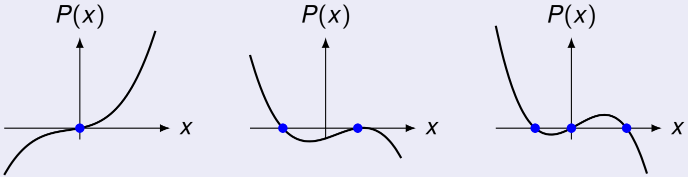


$b^2 - 4ac < 0$ $\qquad$ $b^2 - 4ac = 0$ $\qquad$ $b^2 - 4ac > 0$

Recall: The roots of $P(x)$ in $\mathbb{C}$ are $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Example (cont.)

Let the field be $\mathbb{R}$ and $P(x) = ax^3 + bx^2 + cx + d$, $a \neq 0$. This polynomial has 1, 2, or 3 roots.



Example

$P(x) = x^2 + x + 1$ has no roots in $\mathbb{F}_5$.

x	$P(x)$
0	1
1	3
2	2
3	3
4	1

Example

$P(x) = x^2 - 3x + 2$ has 2 roots in $\mathbb{F}_5$.

x	$P(x)$
0	2
1	0
2	0
3	2
4	1

PROOF (FUNDAMENTAL THM OF ALGEBRA)

LET $p(x)$ HAVE degree $\leq k-1$.

CLAIM: IF $p(x)$ HAS k (OR MORE) ROOTS, THEN $p(x) = 0 \ \forall x$ ("$p(x)$ IS THE ALL-ZERO POLYNOMIAL")

PROOF:

SPECIFY k POINTS:

$$\underbrace{(a_2, y_1)\ (a_2, y_2)\ \cdots\ (a_k, y_k)}$$

VIA LAGRANGE,

WE GET A POLYNOMIAL OF DEGREE $\leq k-1$:

$$p_{\vec{u}}(x) = u_1 + u_2 x + u_3 x^2 + .. + u_k x^{k-1}.$$

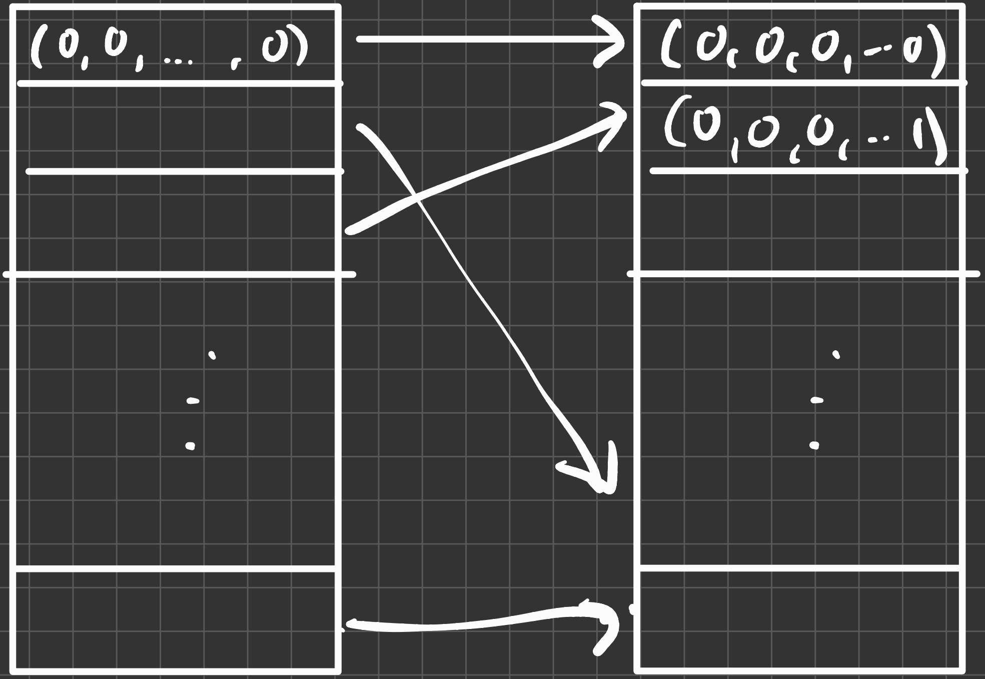
NOW CONSIDER THE MAPPING: (fix $a_1, a_2 .. a_k$)

$$\Psi: \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix} \longmapsto \begin{pmatrix} p_{\vec{u}}(a_1) \\ p_{\vec{u}}(a_2) \\ \vdots \\ p_{\vec{u}}(a_k) \end{pmatrix}$$

THIS MAPPING IS A BIJECTION!

polynomials $\vec{u} \in \mathbb{F}^k$

values at $(a_1, \dots, a_k)$



we have $|\mathbb{F}|^k$ homes

we have $|\mathbb{F}|^k$ holes

Proof: Fundamental Theorem of Algebra

Let $P(x)$ be a polynomial of degree at most $k-1$. We prove that if it has more than $k-1$ distinct roots, then it is the zero polynomial (contraposition).

Let $a_1, \ldots, a_k \in \mathbb{F}$ be k distinct numbers, and consider the map

$$\psi : \mathbb{F}^k \to \mathbb{F}^k, \qquad \vec{u} \mapsto \big(P_{\vec{u}}(a_1), \ldots, P_{\vec{u}}(a_k)\big).$$

By Lagrange, for every $y_1, \ldots, y_k \in \mathbb{F}$, there exists at least one $\vec{u} \in \mathbb{F}^k$, such that $P_{\vec{u}}(a_i) = y_i$, $i = 1, \ldots, k$. Hence the above map is surjective (onto).

Because the domain of ψ and its co-domain have the same cardinality, by the pigeonhole principle, ψ is bijective.

Hence there is a single $\vec{u} \in \mathbb{F}^k$ for which $a_1, \ldots, a_k$ are roots of $P_{\vec{u}}$: it is $\vec{u} = \vec{0}$. $\square$

REED - SOLOMON CONSTRUCTION

1) CHOOSE A FINITE FIELD $\mathbb{F}_q$.

2) CHOOSE n AND k S.T.

$$0 < k \leq n \leq q$$

3) CHOOSE n DISTINCT ELEMENTS

$$a_1, a_2, \dots a_n \in \mathbb{F}_q.$$

4) FOR INFORMATION WORD $\vec{u} \in \mathbb{F}_q^k$

$$\vec{c} = \left(P_{\vec{u}}(a_1), P_{\vec{u}}(a_2), \dots, P_{\vec{u}}(a_n) \right)$$

NOTE: $\text{degree}(P_{\vec{u}}(x)) \leq k-1.$

Reed Solomon (RS) Code Construction

- Choose a finite field $\mathbb{F}$ and integers k, n, such that $0 < k \leq n \leq q$, where $q = \text{card}(\mathbb{F})$.

- Choose n distinct elements $a_1, \ldots, a_n \in \mathbb{F}$. They exist because $n \leq q$.

- The codewords are defined via the following map:

$$\mathbb{F}^k \to \mathbb{F}^n, \qquad \vec{u} \mapsto \vec{c} = \big(P_{\vec{u}}(a_1), \ldots, P_{\vec{u}}(a_n)\big).$$

- This is a block code of length n over $\mathbb{F}$.

Ex: $k=2,\ n=3,\ q=3$

$\vec{u} \in \mathbb{F}_3^2$

$\vec{u} = (u_1, u_2)$

$p_{\vec{u}}(x) = u_1 + u_2 X$

$a_1 = 0$

$a_2 = 1$

$a_3 = 2$

$\vec{u}$	$p_{\vec{u}}(x)$	$\vec{z}$
00	0	000
01	x	012
02	$2x$	021
10	1	111
11	$1+x$	120
12	$1+2x$	1,0,2
20	2	222
21	$2+x$	201
22	$2+2x$	210

Example

- Let $(k, n, q) = (2, 3, 3)$. They fulfill $0 < k \leq n \leq q$.
- So we are in $\mathbb{F}_3$.
- Define $(a_1, a_2, a_3) = (0, 1, 2)$.

Write down all the codewords of the corresponding RS code.

Solution

We are looking for $q^k = 3^2 = 9$ codewords of length $n = 3$.

$\vec{u}$	$P_{\vec{u}}(x)$	$\vec{c}$
00	0	000
01	x	012
02	$2x$	021
10	1	111
11	$1 + x$	120
12	$1 + 2x$	102
20	2	222
21	$2 + x$	201
22	$2 + 2x$	210

__Ex:__ $q = 5$ $(\mathbb{F}_5)$

↳ Select from $n = (1), 2, 3, 4, 5$

$n =$

$k =$

$\vec{u}$	$p_{\vec{u}}(x)$	$\vec{c}$
00		
01		

Ex: $q = 5$ $(\mathbb{F}_5)$

↳ Select from $n = (1), 2, 3, 4, 5$

$n = 3$

$k = 2 \rightsquigarrow \mathbb{F}_5^2 \ni$

$\vec{u}$	$p_{\vec{u}}(x)$	$\vec{c}$
00		
01		
02		
03		
04		
10		
12	$1+2x$	$(3,2,4)$
⋮		
44		

Ex:

$a_1 = 1$, $a_2 = 3$, $a_3 = 4$

PROPERTY OF RS CODES

IF $\vec{u} \longmapsto \vec{c}_{\vec{u}} = (p_{\vec{u}}(a_1), \dots, p_{\vec{u}}(a_n))$

$\vec{v} \longmapsto \vec{c}_{\vec{v}} = (p_{\vec{v}}(a_1), \dots, p_{\vec{v}}(a_n))$

THEN $\alpha\vec{u} + \beta\vec{v} \longmapsto \alpha\vec{c}_{\vec{u}} + \beta\vec{c}_{\vec{v}}$ $(\alpha, \beta \in \mathbb{F})$

<u>PROOF</u>:

$$\alpha\vec{u} + \beta\vec{v} \longmapsto (P_{\alpha\vec{u}+\beta\vec{v}}(a_1), \dots, P_{\alpha\vec{u}+\beta\vec{v}}(a_n))$$

$$
\begin{aligned}
& p_{\alpha\vec{u}+\beta\vec{v}}(x) \\
&= (\alpha u_1 + \beta v_1) + (\alpha u_2 + \beta v_2)x \\
&\quad + (\alpha u_3 + \beta v_3)x^2 \\
&\quad + \dots + (\alpha u_k + \beta v_k)x^{k-1} \\
&= \alpha\left[u_1 + u_2 x + u_3 x^2 + \dots + u_k x^{k-1}\right] \\
&\quad + \beta\left[v_1 + v_2 x + v_3 x^2 + \dots + v_k x^{k-1}\right] \\
&= \alpha\, p_{\vec{u}}(x) + \beta\, p_{\vec{v}}(x)
\end{aligned}
$$

$$P_{\alpha\vec{u}+\beta\vec{v}}(x) = \alpha u_1 + \beta v_1 + (\alpha u_2 + \beta v_2)x$$

$$+ (\alpha u_3 + \beta v_3)x^2$$

$$+ \cdots$$

$$+ (\alpha u_k + \beta v_k)x^{k-1}$$

$$\vec{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}, \quad \vec{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix}$$

$$\hookrightarrow \alpha\vec{u} + \beta\vec{v} = \begin{pmatrix} \alpha u_1 + \beta v_1 \\ \vdots \\ \alpha u_k + \beta v_k \end{pmatrix}$$

$$= \alpha\, p_{\vec{u}}(x) + \beta\, p_{\vec{v}}(x)$$

Hence

$$\xrightarrow{\alpha\vec{u}+\beta\vec{v}} \left(\alpha p_{\vec{u}}(a_1) + \beta p_{\vec{v}}(a_1), \ldots \alpha p_{\vec{u}}(a_n) + \beta p_{\vec{v}}(a_n) \right)$$

$$= \alpha \left(p_{\vec{u}}(a_1), p_{\vec{u}}(a_2), \dots p_{\vec{u}}(a_n) \right)$$

$$+ \beta \left(p_{\vec{v}}(a_1), \dots \; p_{\vec{v}}(a_n) \right)$$

$$= \alpha \, \vec{c}_{\vec{u}} + \beta \, \vec{c}_{\vec{v}}$$

$$\square$$

KEY PROPERTIES OF RS CODES

1) THEY ARE **LINEAR**

2) THEIR DIMENSION IS INDEED k, I.E. THEY HAVE q^k CODEWORDS.

3) THEY ARE MDS CODES:

$$d_{min} = n - k + 1.$$

RS CODES ARE LINEAR

PROOF: IF $\vec{c}_1$ AND $\vec{c}_2 \in \mathcal{C}$

THEN $\alpha \vec{c}_1 + \beta \vec{c}_2 \in \mathcal{C}$

(HOLDS FOR ALL CODEWORDS)

IF $\vec{c}_1 \in \mathcal{C}$ THEN $\exists \; \vec{u} : \vec{c}_1 = (P_{\vec{u}}(a_1), \dots P_{\vec{u}}(a_n))$

$\vec{c}_2 \in \mathcal{C}$ THEN $\exists \; \vec{v} : \vec{c}_2 = (P_{\vec{v}}(a_1) \dots)$

THEN CONSTRUCT THE CODEWORD FOR

$\alpha \vec{u} + \beta \vec{v} \Rightarrow \vec{c} = \alpha \vec{c}_1 + \beta \vec{c}_2$.

Proof: RS Codes are Linear

Let $\vec{u}$, $\vec{v}$ be in $\mathbb{F}^k$ and $\alpha \in \mathbb{F}$. Notice that

$$P_{\alpha\vec{u}}(x) = \alpha u_1 + \alpha u_2 x + \cdots + \alpha u_k x^{k-1} = \alpha P_{\vec{u}}(x);$$
$$P_{\vec{u}+\vec{v}}(x) = (u_1 + v_1) + (u_2 + v_2)x + \cdots + (u_k + v_k)x^{k-1} = P_{\vec{u}}(x) + P_{\vec{v}}(x).$$

Hence

$$P_{\alpha\vec{u}+\vec{v}}(x) = \alpha P_{\vec{u}}(x) + P_{\vec{v}}(x).$$

This proves that if

$$\vec{u} \mapsto \vec{x} \in \mathcal{C}$$
$$\vec{v} \mapsto \vec{y} \in \mathcal{C}$$

then $\alpha\vec{u} + \vec{v} \mapsto \alpha\vec{x} + \vec{y} \in \mathcal{C}.$

Hence the code is linear. □

RS CODES HAVE q^k CODEWORDS

PROOF:

1) CLEARLY NO MORE THAN q^k.

2) COULD $\vec{u}$ AND $\vec{v}$ LEAD TO THE SAME CODEWORD?

$$\vec{c}_{\vec{u}} = \vec{c}_{\vec{v}}$$

$$\Leftrightarrow \quad p_{\vec{u}}(a_i) = p_{\vec{v}}(a_i)$$

$$\text{for } i = 1, 2, \dots, n.$$

$$\Leftrightarrow \quad \underbrace{p_{\vec{u}}(a_i) - p_{\vec{v}}(a_i)} = 0$$

for $i = 1, 2, \dots, n$

THIS IS A POLYNOMIAL

OF DEGREE $\leq k-1$.

IT HAS n ZEROS.

BUT $n > k-1$

HENCE

MUST BE ALL-ZERO POLYNOMIAL.

$$\Longrightarrow \quad \vec{u} = \vec{v}.$$

Proof: the design-parameter *k* is indeed the dimension of the RS-code

It suffices to prove that the encoding map is injective (one-to-one), implying that there are $[\mathsf{card}(\mathbb{F})]^k$ distinct codewords, hence that k is the dimension of the code.

When proving the fundamental theorem of algebra, we showed that the map

$$\begin{aligned} \psi : \mathbb{F}^k &\longrightarrow \mathbb{F}^k \\ \vec{u} &\mapsto \big(P_{\vec{u}}(a_1), \dots, P_{\vec{u}}(a_k)\big) \end{aligned}$$

is one-to-one.

This guarantees that the encoding map

$$\mathbb{F}^k \longrightarrow \mathcal{C}, \qquad \vec{u} \mapsto \big(P_{\vec{u}}(a_1), \dots, P_{\vec{u}}(a_k), P_{\vec{u}}(a_{k+1}), \dots, P_{\vec{u}}(a_n)\big)$$

is one-to-one. □

RS CODES ARE MDS

PROOF: LINEAR CODE

$\Rightarrow$ d_{min} = min weight.

$p_{\vec{u}}(x)$ IS A POLYNOMIAL OF DEGREE $\leq k-1$.

$\Downarrow$

$$\Big(\underbrace{p_{\vec{u}}(a_1),\ p_{\vec{u}}(a_2),\ \ldots,\ p_{\vec{u}}(a_n)}_{\leq k-1 \text{ zeros}}\Big)$$

$\leq k-1$ zeros (or all-zero)

$\Rightarrow$ $\geq n-(k-1)$ non-zeros

$\Rightarrow$ min weight $\geq n-k+1$

$\Rightarrow$ $d_{\min}(\mathcal{C}) \geq n-k+1.$

$\Rightarrow$ $\underline{\underline{\text{MDS code}}}$

$\square$

RS CODES ARE MDS

PROOF:

$p_{\vec{u}}(x)$ IS A POLYNOMIAL OF DEGREE $\leq k-1$.

$$\Downarrow$$

$$\Big(\underbrace{p_{\vec{u}}(a_1),\ p_{\vec{u}}(a_2),\ \dots\ p_{\vec{u}}(a_n)}_{\text{THERE CAN BE AT MOST } k-1 \text{ ZEROES}}\Big)$$

(SINCE a_i ARE ALL DIFFERENT)

Proof: RS codes are MDS

We want to prove that $d_{min} = n - k + 1$.

- Let $\vec{u} \in \mathbb{F}^k$ be a non-zero information vector. $P_{\vec{u}}(x)$ is a non-zero polynomial of degree at most $k - 1$. Hence it has at most distinct $k - 1$ roots.
- The corresponding codeword $\vec{c}$ (obtained by evaluating $P_{\vec{u}}(x)$ at n distince values) has at most $k - 1$ zeros.
- Hence $w(\vec{c}) \geq n - (k - 1) = n - k + 1$ for all $\vec{c}$.
- Since $\vec{c}$ is an arbitrary non-zero codeword, $d_{min} \geq n - k + 1$.
- By the Singleton's bound, $d_{min} \leq n - k + 1$.

Hence $d_{min} = n - k + 1$. □

To summarize, we have proved the following:

Theorem (Textbook Thm. 14.3)

A Reed Solomon code with design parameters k and n is a linear (n, k) code of minimum distance $d_{min} = n - k + 1$, i.e., it attains Singleton's bound with equality.

Note that the condition

$$\mathrm{card}(\mathbb{F}) \geq n$$

is necessary or else we can't find n distinct field elements $a_1, \ldots, a_n$.

LINEAR CODES : GENERATOR MATRIX?

$k=2$, $n=3$

$$G=\begin{pmatrix} 0 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\boxed{G \in \mathbb{F}_3^{2\times 3}}$$

$\vec{u}$	$p_{\vec{u}}(x)$	z
00	0	000
01	x	012
02	$2x$	021
10	1	111
11	$1+x$	120
12	$1+2x$	102
20	2	222
21	$2+x$	201
22	$2+2x$	210

LINEAR CODES : GENERATOR MATRIX?

$k = 2, \quad n = 3$

$$G = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix}$$

$$\boxed{G \in \mathbb{F}_3^{2\times 3}}$$

$$\Rightarrow H = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

$\vec{u}$	$p_{\vec{u}}(x)$	z
00	0	000
01	x	012
02	$2x$	021
10	1	111
11	$1+x$	120
12	$1+2x$	102
20	2	222
21	$2+x$	201
22	$2+2x$	210

Exercise

Find a generator matrix G for this code over $\mathbb{F}_3$.

Solution

We need to find two codewords that are linearly independent.

Here are a few choices:

$$G = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} \quad G = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \quad G = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}$$

$\vec{u}$	$P_{\vec{u}}(x)$	$\vec{c}$
00	0	000
01	x	012
02	$2x$	021
10	1	111
11	$1+x$	120
12	$1+2x$	102
20	2	222
21	$2+x$	201
22	$2+2x$	210

Recall that each generator matrix defines an input/output map.

The map that we originally used to define RS codes

$$\vec{u} \to P_{\vec{u}}(x) \to \vec{c} = P_{\vec{u}}(a_1), \ldots, P_{\vec{u}}(a_n)$$

is just one of many possible maps.

In fact there are $(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})$ maps for a linear code of dimension k over $\mathbb{F}_q$.

Exercise

Which of the following is a valid parity-check matrix?

1. $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}$;
2. $B = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix}$;
3. $C = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$.

$\vec{u}$	$P_{\vec{u}}(x)$	$\vec{c}$
00	0	000
01	x	012
02	$2x$	021
10	1	111
11	$1+x$	120
12	$1+2x$	102
20	2	222
21	$2+x$	201
22	$2+2x$	210

Solution

A parity-check matrix for this code has $n - k = 1$ row, so only C is correctly sized.

Moreover, we can easily verify that $\vec{g}_i C^{\mathsf{T}} = 0$, where $\vec{g}_i$ is the ith row of G, hence $\vec{c}C^{\mathsf{T}} = 0$ for all codewords $\vec{c}$.

Therefore C is a parity-check matrix for the considered code.

$\vec{u}$	$P_{\vec{u}}(x)$	$\vec{c}$
00	0	000
01	x	012
02	$2x$	021
10	1	111
11	$1 + x$	120
12	$1 + 2x$	102
20	2	222
21	$2 + x$	201
22	$2 + 2x$	210

How about if we want the generator matrix for a specific encoding map?

Exercise

Find the generator matrix G that can be used as the encoder according to the given table.

$\vec{u}$	$P_{\vec{u}}(x)$	$\vec{c}$
00	0	000
01	x	012
02	$2x$	021
10	1	111
11	$1+x$	120
12	$1+2x$	102
20	2	222
21	$2+x$	201
22	$2+2x$	210

Solution

We want

- $(1,0)G = (1,1,1)$, so the first row of G is $(1,1,1)$.
- $(0,1)G = (0,1,2)$, so the second row of G is $(0,1,2)$.

Therefore

$$G = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

YESTERDAY

REED-SOLOMON CODES

$(n, k, q) \leftarrow \mathbb{F}_q$

$0 < k \le n \le q$

- LINEAR
- q^k CODEWORS

- $d_{min} = n - k + 1$

EXAMPLE:

$q = 13, \quad n = 4, \quad k = 2$

$a_1 = 0$

$a_2 = 1$

$a_3 = 2$

$a_4 = 3$

$q^k = 169$

$d_{min} = 3$

$\vec{u}$	$p_{\vec{u}}(x)$	$\vec{c}$
0, 0	0	0, 0, 0, 0
0, 1	x	0, 1, 2, 3
0, 2	$2x$	0, 2, 4, 6
⋮		⋮
0, 12	$12x$	0, 12, 11, 10
1, 0	1	1, 1, 1, 1
1, 1	$1+x$	⋮
1, 2	$1+2x$	
⋮	⋮	
1, 12	$1+12x$	
⋮	⋮	
12, 12	$12+12x$	12, 11, 10, 9

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix}$$

$$G' = \begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 2 & 3 \end{pmatrix}$$

$$\hookrightarrow H = \begin{pmatrix} 1 & \overset{11}{\overset{\nearrow}{-2}} & 1 & 0 \\ 2 & \underset{10}{\underset{\searrow}{-3}} & 0 & 1 \end{pmatrix}$$

A SPECIAL GENERATOR MATRIX

$\mathbb{F}_q^n$

$\vec{u}$	$p_{\vec{u}}(x)$	
$1\ 0\ 0\ 0\ 0\ \cdots\ 0$	1	$(1\ 1\ \cdots\ 1)$
$0\ 1\ 0\ 0\ 0\ \cdots\ 0$	x	$(a_1\ a_2\ \cdots\ a_n)$
$0\ 0\ 1\ 0\ 0\ \cdots\ 0$	x^2	$(a_1^2\ a_2^2\ \cdots\ a_n^2)$
$\vdots$	$\vdots$	$\vdots$
$\underbrace{0\ 0\ 0\ 0\ 0\ 0\ 0\ \cdot\ 1}_{\in \mathbb{F}_q^k}$	x^{k-1}	$(a_1^{k-1}\ a_2^{k-1}\ \cdots\ a_n^{k-1})$

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & & \cdots & a_n \\ a_1^2 & a_2^2 & & & & \\ \vdots & & & & & \\ a_1^{k-1} & a_2^{k-1} & & & & \end{pmatrix}$$

Vandermonde matrix.

More generally:

- We want a generator matrix for a given encoding map.

- It suffices to find the codewords that correspond to the following length-k information words:

$$\begin{array}{lcl}
(1,0,0,\ldots,0,0) & \rightsquigarrow & p_{\vec{u}}(x) = 1 \\
(0,1,0,\ldots,0,0) & \longrightarrow & p_{\vec{u}}(x) = x \\
(0,0,1,\ldots,0,0) & \longrightarrow & p_{\vec{u}}(x) = x^2 \\
\vdots & & \\
(0,0,0,\ldots,1,0) & \longrightarrow & p_{\vec{u}}(x) = x^{k-2} \\
(0,0,0,\ldots,0,1) & \longrightarrow & p_{\vec{u}}(x) = x^{k-1}
\end{array}$$

- The corresponding codewords are linearly independent (proof below) and are k in number. Hence they form a basis.

We prove that a linear encoding map sends linearly independent information vectors to linearly independent codewords.

Proof:

Let $\vec{u}_i \in \mathbb{F}^k$, $i = 1, \ldots, k$, be a collection of linearly independent information vectors and let $\vec{c}_i \in \mathbb{F}^n$ be the corresponding codewords.

We prove that the the codewords are linearly independent.

Suppose, to the contrary, that the codewords are linearly dependent, i.e.,

$$\sum_{i=1}^{k} \lambda_i \vec{c}_i = 0,$$

with some of the λ_i non-zero.

Then

$$\sum_{i=1}^{k} \lambda_i \vec{u}_i = 0,$$

which contradicts the assumption that the information vectors are linearly independent. □

HOW SO ?

$\vec{c}_i$ IS GENERATED BY $p_{\vec{u}_i}(x)$

$$\underbrace{\sum_i \lambda_i \vec{c}_i}_{\text{WHICH POLYNOMIAL GENERATES THIS CODE WORD ?}} = 0$$

$$p_{\sum_i \lambda_i \vec{u}_i}(x)$$

HOW SO ?

$\vec{c}_i$ IS GENERATED BY $p_{\vec{u}_i}(x)$

$$\underbrace{\sum_i \lambda_i \vec{c}_i}_{\text{WHICH POLYNOMIAL GENERATES THIS CODE WORD ?}} = 0$$

↳ $p_{\sum_i \lambda_i u_i}(x)$

$\longrightarrow$ DEGREE $\leq k-1$

BUT WE KNOW IT HAS

n ZEROS!

HENCE IT MUST BE THE ALL-ZERO POLYNOMIAL!

THAT IS,

$$\sum_i \lambda_i \vec{u}_i = \vec{0}.$$

□

In particular, the map that we used to define the code sends $\vec{u} \in \mathbb{F}^k$ to

$$\vec{c} = \big(P_{\vec{u}}(a_1), \ldots, P_{\vec{u}}(a_n)\big).$$

If $\vec{u}$ has 1 at position i and 0 elsewhere, then $P_{\vec{u}}(x) = x^{i-1}$.

Hence, the map that we have used to defined RS codes has the generator matrix

$$G = \left(\begin{array}{ccccc} 1 & 1 & 1 & \ldots & 1 \\ a_1 & a_2 & a_3 & \ldots & a_n \\ (a_1)^2 & (a_2)^2 & (a_3)^2 & \ldots & (a_n)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (a_1)^{k-1} & (a_2)^{k-1} & (a_3)^{k-1} & \ldots & (a_n)^{k-1} \end{array}\right).$$

DECODING FROM ERASURES

- HOW MANY CAN BE TOLERATED?

(n, k, q) $n=7, k=3$

$d_{min} = n-k+1 = 5$

$\vec{c} = (c_1, c_2, c_3, c_4, c_5, c_6, c_7)$

$\vec{y} = (c_1, ?, c_3, c_4, ?, ?, ?)$

EX: $q = 13$, $n = 4$, $k = 2$, $a_1 = 0$, $a_2 = 1$, $a_3 = 2$, $a_4 = 3$

$$\vec{c} = (0, 2, 4, 6)$$

$$\vec{y} = (?, 2, ?, 6)$$

Q: WHICH $p_{\vec{u}}(x)$ GENERATED $\vec{c}$?

WE KNOW

1) $\deg(p_{\vec{u}}(x)) \leq 1$
2) $p_{\vec{u}}(x = 1) = 2$
3) $p_{\vec{u}}(x = 3) = 6$

$$p_2(x) = \frac{1}{-2}(x-3)$$

$$p_4(x) = \frac{1}{2}(x-1)$$

$$p_{\vec{u}}(x) = 2 \cdot \frac{1}{-2}(x-3) + 6 \cdot \frac{1}{2}(x-1)$$

$$= -(x-3) + 3(x-1)$$

$$= 2x$$

⇛ just do Lagrange interpolation!

works because we have k points.

(a_i, c_i)

which we know to be generated from a polynomial of degree $\leq k-1$.

Example (CD-ROM)

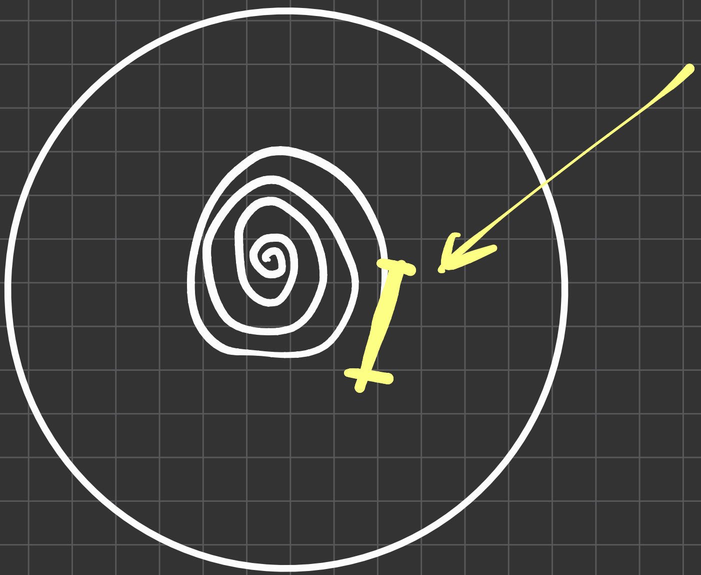
CDs use Cross-Interleaved Reed-Solomon Codes (CIRC) as follows:

- Each byte of the source is seen as an element of $\mathbb{F} = \mathbb{F}_{2^8}$.
- Source symbols, are encoded using a $(28, 24)$ RS code over $\mathbb{F}$.
- The elements of a sequence of many codewords are interleaved.
- The result is encoded using a $(32, 28)$ RS code over $\mathbb{F}$.

Notice that both codes have $d_{min} = 5$, but this small distance is compensated by the interleaver which distributes strings of errors among many codewords.

The end result is that error bursts up to 4000 bits can be corrected. We have roughly that many bits in a track segment of length 2.5mm.

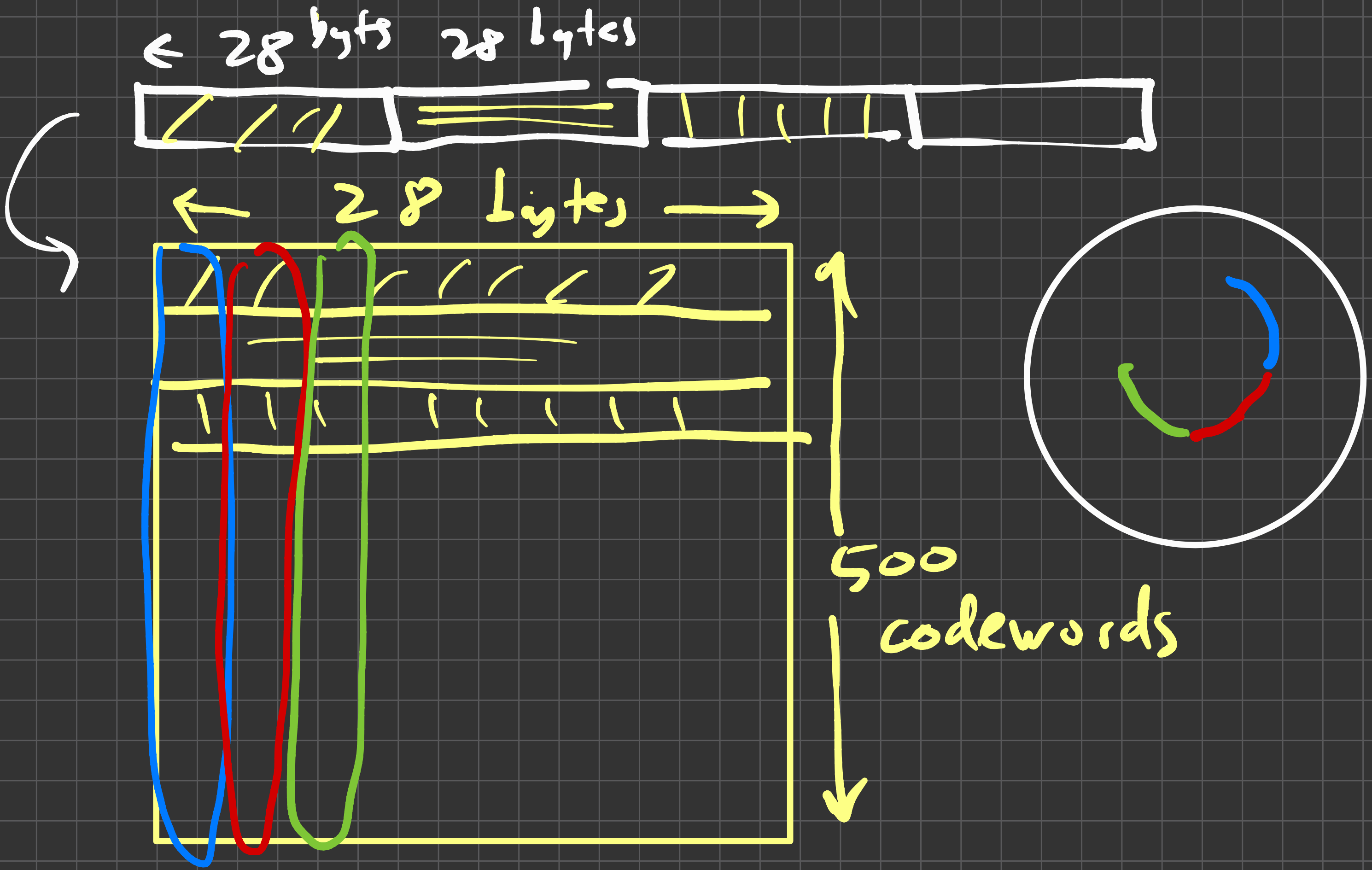
Source: Standard ECMA-130, "Data interchange on read-only 120mm optical data disks (CD-ROM)", 2nd Edition, 1996.



$\Rightarrow$ 4000 bits are erased

$\Rightarrow \frac{4000}{8} = 500$ symbols are erased

$\Rightarrow \frac{500}{28} = 17.85$ codewords erased


← 28 byts
28 bytes
← 28 bytes →
500 codewords

Outline

Introduction and Organization

Entropy and Data Compression

Cryptography

Channel Coding

- Error Detection and Error Correction
- Finite Fields and Vector Spaces
- Linear Codes
- Reed Solomon Codes
- Summary of Chapter 3

SUMMARY OF CHAPTER 3

Basic Concepts of Error Detection and Correction:

- Two basic channel models: Erasure channel and Error channel.
- Code $=$ subset of all possible sequences of length n (over D-ary alphabet).
  - Convenient to talk about the number of codewords via the parameter $k = \log_D |\mathcal{C}|$.
- Minimum Distance Decoding
- Minimum Distance of a code
- Singleton's bound: $d_{min} \leq n - k + 1$.
  - A code satisfying this bound with equality is called MDS code.

Summary of Chapter 3

Linear Codes: Basic Properties, Design, Decoding

- Finite field: A finite set with two operations (“sum” and “product”) satisfying the “natural” properties (as you know them over the reals).
  - Only exists if the cardinality of the finite set is a prime power, $\text{card}(\mathbb{F}) = p^m$.
- Vector spaces over finite fields. Subspaces. Basis.
- Linear Code $=$ Subspace of a vector space over a finite field
- Generator matrix ($=$ collection of vectors spanning the subspace)
  - Particularly desirable form: Systematic generator matrix.
- Parity check matrix
- Key example: Hamming codes

Summary of Chapter 3

Reed-Solomon Codes

- A very popular class of linear codes over a finite field $\mathbb{F}$. They are MDS!
- Block length has to be $n \leq |\mathbb{F}|$ (so we need large finite fields).
- They can be neatly described via *polynomials.*