Coding Theory
Lecture 3

Lecture by Dr. Elette Boyle
Typeset by Steven Karas

2017-11-16
Last edited 18:41:52 2017-11-16

Disclaimer These lecture notes are based on the lecture for the course Coding Theory, taught by Dr. Elette Boyle at IDC Herzliyah in the fall semester of 2017/2018. Sections may be based on the lecture slides written by Dr. Elette Boyle.

Admin

Short Review

- $n, k, d,\ \Sigma, q,\ \Delta$
- Finite fields $\mathbb{F}_q \quad (q = p^s)$
- Linear codes = linear subspaces in ${\mathbb{F}_q}^n$. Note: $[n, k, d]_q$ code vs $(n, k, d)_q$ code.
- Nice properties of linear codes (generator matrix $G \in {\mathbb{F}_q}^{k \times n}$, parity check matrix $H \in {\mathbb{F}_q}^{n-k \times n}$)

Agenda

- Singleton Bound[1]
- Reed-Solomon Codes
- Maximum Distance Separable (MDS) codes
- Finite fields beyond $\mathbb{F}_p$ p is prime

1 Singleton Bound

Basically, this is the loose bound that you cannot provide a code better than the total size of the code space divided by the size of the Hamming ball.

Theorem For every $(n, k, d)_q$ code, $k \leq n - d + 1$.

This means any code, not just linear codes

Proof Let C be an $(n, k, d)_q$ code. Let $\vec{c}_1, \ldots, \vec{c}_M$ be all the codewords in C, where $k = \log_q M$.

We want to show that if C has distance d, then $M \leq q^{n-d+1}$.

For each $i \in [M]$, mark $\vec{c'}_i$ as the prefix of $\vec{c}_i$ of length $n - d + 1$.

We want to show that $\forall i \neq j \in [M] : \vec{c'}_i \neq \vec{c'}_j$. Suppose the contradiction. Thus, $\exists \vec{c'}_i = \vec{c'}_j$. This implies that $\Delta(\vec{c}_i, \vec{c}_j) \leq d - 1$ because the suffixes are of size $d - 1$. This contradicts that d is the distance of C.

[1] This is covered in chapter 4 of the book

2 Reed-Solomon Codes

The intuition is that we can map messages into polynomials and encode extra interpolation points. This allows us to recover from erasures. In future lectures, we will introduce efficient algorithms for recovering from general errors.

Basically, oversampling low degree polynomials.

2.1 Polynomials

For a finite field $\mathbb{F}_q$, a function $F(x) = \sum_{i=0}^{\infty} f_i x^i$ with $f_i \in \mathbb{F}_q$ is called a polynomial over $\mathbb{F}_q$.

For $F(x) = \sum_{i=0}^{d} f_i x^i \quad (f_d) \neq 0$ the degree of f is d, marked as $\deg(F) = d$.

$\alpha \in \mathbb{F}_q$ is a root of $F(x)$ if $F(\alpha) = 0$.

Note that adding and multiplying polynomials is as usual, with coefficient arithmetic over $\mathbb{F}_q$.

Bound on the possible roots of polynomials A nonzero polynomial $F(x)$ of degree t over $\mathbb{F}_q$ can have at most t roots in $\mathbb{F}_q$.

Proof Proof by induction on t. If $t = 0$, it is trivially true.

Say that $F(x)$ is a nonzero polynomial of degree $t \geq 1$. If $F(x)$ has no roots, then done. Otherwise, let $\alpha \in \mathbb{F}_q$ be a root of F.

We claim that $F(x) = (x - \alpha)g(x)$ where $\deg(g) = \deg(f) - 1$.

It always holds that $F(x) = (x-\alpha)g(x)+R(x)$ where $\deg(g) \leq \deg(f)-1$, and $\deg(R) \leq 1-1$[2]. Therefore, $\deg R = 0$, which means that R is constant. Because α is a root, $F(\alpha) = 0$, and therefore:

$$\begin{aligned} \underbrace{(\alpha - \alpha)}_{=0} g(\alpha) + R(\alpha) &= 0 \\ R(\alpha) &= 0 \\ R &\equiv 0 \end{aligned}$$

By inductive hypothesis, g has at most $\deg(g) \leq \deg(f) - 1$ roots. The roots of f are the roots of g and α. Thus, the number of roots of $f \leq \deg(f)$.

2.2 Formally

Let $\mathbb{F}_q$ be a finite field. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be distinct elements (sometimes called the evaluation points). Define an encoding procedure $\text{RS} : {\mathbb{F}_q}^k \to {\mathbb{F}_q}^n$ for a chosen $k \leq n \leq q$:

1. An input message $\vec{m} = (m_0, \ldots, m_{k-1}) \in {\mathbb{F}_q}^k$. This message is mapped to a degree $\leq k-1$ polynomial where $F_{\vec{m}}(x) = \sum_{i=0}^{k-1} m_i x^i$.
2. The output $\text{RS}(\vec{m})$ is the evaluation of $f_{\vec{m}}(x)$ on all n evaluation points α_i: $\text{RS}(\vec{m}) = (F_{\vec{m}}(\alpha_1), \ldots, F_{\vec{m}}(\alpha_n))$. The image of this mapping is the RS code.

A common choice is $n = q - 1$ and $\alpha = \mathbb{F}_q \setminus \{0\}$.

2.3 Proof of linearity

We know for polynomials that $\vec{m}, \vec{m'} \in {\mathbb{F}_q}^k$, it holds that:

$$\begin{aligned} F_{\vec{m}}(x) + F_{\vec{m'}}(x) &= \sum_{i=0}^{k-1} m_i x^i + \sum_{i=0}^{k-1} m'_i x^i \\ &= \sum_{i=0}^{k-1} (m_i + m'_i) x^i \\ &= f_{\vec{m}+\vec{m'}}(x) \end{aligned}$$

For any $a \in \mathbb{F}_q$, $aF_{\vec{m}}(x) = F_{a\vec{m}}(x)$.

This implies:

[2] full proof elided for brevity

$$\begin{aligned}\mathrm{RS}(\vec{m}) + \mathrm{RS}(\vec{m'}) &= (F_{\vec{m}}(\alpha_1), \ldots) + (\ldots) \\ &= (F_{\vec{m}} + F_{\vec{m'}}(\alpha_1), \ldots) \\ &= (F_{\vec{m}+\vec{m'}}(\alpha_1), \ldots) + (\ldots) \\ &= \mathrm{RS}(\vec{m} + \vec{m'})\end{aligned}$$

Recall that the code is the image of RS on all ${\mathbb{F}_q}^k$ input so $\mathrm{RS}(\vec{m} + \vec{m'})$ is a codeword.
Similarly, $a \cdot \mathrm{RS}(\vec{m}) = \ldots = \mathrm{RS}(a \cdot \vec{m})$ is also a codeword.

2.4 Generator matrix

Note that $\vec{m}G = \mathrm{RS}(\vec{m})$.

This implies that some element of the codeword is $F_{\vec{m}}(\alpha_j) = \sum_{i=0}^{k-1} \vec{m}\alpha_j^i$. Therefore, we can define the elements of G as $G_{ij} = \alpha_i^j$.

We call this matrix the Vandermonde matrix, which is a full rank[3].

2.5 Equivalence to Singleton Bound

A Reed-Solomon code for parameters n, k, q is an $[n, k, (n-k+1)]_q$ code. That is, RS matches the singleton bound $k \leq n - d + 1$.

Proof Fix $\vec{m} \neq \vec{m'} \in {\mathbb{F}_q}^k$. Note that $F_{\vec{m}}$, $F_{\vec{m'}}$ are distinct, because they differ in at least 1 coefficient. Both of these polynomials are of degree $\leq k-1$.

$$\begin{aligned}\Delta(\mathrm{RS}(\vec{m}), \mathrm{RS}(\vec{m'})) &= \left|\{\alpha_i \mid F_{\vec{m}}(\alpha_i) \neq F_{\vec{m'}}(\alpha_i)\}\right| \\ &= \left|\{\alpha_i \mid F_{\vec{m}-\vec{m'}}(\alpha_i) \neq 0\}\right|\end{aligned}$$

We know that $F_{\vec{m}-\vec{m'}}$ is not the zero polynomial. We also know that $F_{\vec{m}-\vec{m'}}$ has degree $\leq k$, because $F_{\vec{m}-\vec{m'}} = F_{\vec{m}} - F_{\vec{m'}}$. From earlier, we know that the number of roots of $F_{\vec{m}-\vec{m'}}$ is $\leq (k-1)$.

$$\begin{aligned}\left|\{\alpha_i \mid F_{\vec{m}-\vec{m'}}(\alpha_i) \neq 0\}\right| &= n - \left|\{\alpha_i \mid F_{\vec{m}-\vec{m'}}(\alpha_i) = 0\}\right| \\ &\geq n - \text{the number of zeros of } F_{\vec{m}-\vec{m'}} \\ &\geq n - (k-1)\end{aligned}$$

2.6 Erasure decoding

Simple interpolation works, but we won't cover it at the moment.

2.7 Examples

Consider the finite case $F(x) = 2x^3 + x^2 + 5x + 6$ as a polynomial over $\mathbb{F}_7$.

$$\deg(2x^3 + x^2 + 5x + 6) = 3$$

Consider codewords of a $[\overbrace{3}^{n}, \overbrace{2}^{k}]_3$ over $\mathbb{F}_3$. There should be $q^k = 3^2 = 9$ such codewords. The codewords should be in ${\mathbb{F}_q}^n = \mathbb{F}_3^3$. We'll just enumerate by brute force from the input space: $\mathrm{RS} : \mathbb{F}_3^2 \to \mathbb{F}_3^3$

$$\begin{array}{ccc}
\underbrace{(000)}_{\vec{m}=00;F(\vec{m})=0} & \underbrace{(111)}_{\vec{m}=01;F(\vec{m})=1} & \underbrace{(222)}_{\vec{m}=02;F(\vec{m})=2} \\
\underbrace{(210)}_{\vec{m}=10;F(\vec{m})=x} & \underbrace{(021)}_{\vec{m}=11;F(\vec{m})=x+1} & \underbrace{(102)}_{\vec{m}=12;F(\vec{m})=x+2} \\
\underbrace{(120)}_{\vec{m}=20;F(\vec{m})=2x} & \underbrace{(201)}_{\vec{m}=21;F(\vec{m})=2x+1} & \underbrace{(012)}_{\vec{m}=22;F(\vec{m})=2x+2}
\end{array}$$

[3]A formal proof is by expressing the determinant as a polynomial with each of the elements as roots

3 Maximum Distance Separable codes

A Maximum Distance Separable code is an $(n, k, q)_q$ code for which $d = n - k + 1$ (i.e. it meets the singleton bound). We've just shown that Reed-Solomon codes are MDS codes.

3.1 Finite fields beyond $\mathbb{F}_p$

Recall that there is exactly one finite field with a given cardinality, within isomorphism.

Recall polynomials over $\mathbb{F}_q$

A polynomial $F(x)$ over $\mathbb{F}_q$ is irreducible if $\forall G_1(x), G_2(x)$ for which $F(x) = G_1(x)G_2(x)$, it holds that $\min(\deg G_1, \deg G_2) = 0$ (i.e. one of them must be a constant).

Theorem Let $E(x)$ be an irreducible polynomial of degree $s \geq 2$ over $\mathbb{F}_p$, where p is prime. Then the set of polynomials $\mathbb{F}_p[x]$ modulo $E(x)$ denoted $\frac{\mathbb{F}_p}{(E(x))}$ is a field.

Proof Sketch The proof largely follows the proof that $\mathbb{F}_p = \frac{\mathbb{Z}}{(p)}$ is a field.

Note that the elements of $\frac{\mathbb{F}_p}{(E(x))}$ are all polynomials of degree $\leq s - 1$.

Recall that arithmetic over this field is $\mod E(x)$, which means that for any $G \mod E$: $G(x) = A(x)E(x) + R(x)$.

The additive identity is the zero polynomial.

The additive inverse $F(x) = \sum_{i=0}^{s-1} f_i x^i$ is $\sum_{i=0}^{s-1}(-f_i)x^i$.

The multiplicative identity is 1.

The multiplicative inverse can be shown to exist uniquely similar to how we proved for arithmetic $\mod p$ where p is prime.

The number of elements is the number of distinct deg $\leq s-1$ polynomials, which is p^s, because the coefficients are in $\mathbb{F}_p$.

Existence of irreducible polynomials For any $s \geq 2$ and $\mathbb{F}_p$ prime, there exists an irreducible polynomial over $\mathbb{F}_p$ of degree s. In fact, the number of such irreducible polynomials is $\Theta\left(\frac{p^2}{s}\right)$.

Note that given a polynomial $F(x)$ of degree s, then we can efficiently[4] determine if F is irreducible. We can do this by checking $\gcd(F(x), x^{q^s} - x) \underset{?}{=} F(x)$ since we knwo that $x^{q^s} - x = \prod_{F \text{ irreducible;deg } F=s} F$.

Because we can do this efficiently, we can start from $\mathbb{F}_p$, and find an irreducible polynomial to construct $\mathbb{F}_{p^s}$.

Recall that when we constructed the Reed Solomon codes, we defined them over a finite field, and if we consider our encoding field as acting on polynomials in F_{p^s}, we are effectively defining a field of polynomials over polynomials. However, while addition over the coefficient representation works naively, multiplication is non-trivial.

3.2 Examples

$1 + x^2$ over $\mathbb{F}_2$ is not irreducible, because:

$$\begin{aligned} 1 + x^2 &= (1 + x)(1 + x) \\ &= 1 + 2x + x^2 \\ &= 1 + x^2 \end{aligned}$$

$1 + x + x^2$ is irreducible over $\mathbb{F}_2$.

In order to have a nontrivial factorization over $\mathbb{F}$, either $\underbrace{x}_{a=0 \text{ is a root}} \mid 1+x+x^2$ and/or $\underbrace{(1+x)}_{1 \text{ is a root}} \mid 1 + x + x^2$. Neither is implied, and therefore $1 + x + x^2$ is irreducible.

Note that having no roots is not equivalent to being irreducible over finite fields:

$(1 + x + x^2)^2$ is clearly not irreducible, yet has no roots.

Suppose that we take $E(x) = 1 + x + x^2$, which is irreducible over $\mathbb{F}_2$. Taking $\mod E(x)$ is saying that $1 + x + x^2 = 0 \mod E(x)$, and $x^2 = -(1 + x)$.

For example, take $G(x) = x^5 + x^3 + x^2 + 1$. We can substitute the x^2 terms to reduce the degree and it's all arithmetic from there.

[4]The proof is interesting, and it is recommended to read up on it later.

4 Next week

I will be missing the lecture next week because of Thanksgiving.