ST08 Lecture 05

2/20/08

Note Title 2/20/2008

Today: Algebraic Codes

- Algebra Review (Finite Fields)
- Codes from Polynomials
  - Reed-Solomon Codes
  - Reed-Muller Codes
  - Hadamard Codes
  - Hamming Codes

Finite Fields

(Don't need all this today, but will use some of these facts later)

Defn: $(F, +, \cdot)$ is a field if

- $+$ is commutative, associative, has identity (0), inverses.
- $\cdot$ is comm., associative, has identity (1), inverse for non-0 elements,
- $\cdot$ distributes over $+$

Defn: $(R, +, \cdot)$ ring if all properties above, except possibly multiplicative inverses hold.

Polynomial Rings

$\mathbb{F}[x]$: Ring of "polynomials in x with coefficients from $\mathbb{F}$."

Formally: elements of $\mathbb{F}[x]$ are just finite sequences of elements from $\mathbb{F}$

$$f \in \mathbb{F}[x] = (f_0, f_1, \ldots f_d) \approx \sum f_i x^i$$

with $f_d \neq 0$.

$d = \deg(f)$;

$f_d = 1 \Rightarrow f$ monic.

Addition, Multiplication: Polynomial addition, multiplication.

Factorization of Polynomials

- $f \in \mathbb{F}[x]$ is reducible if $\exists\, g, h$ $\deg(g), \deg(h) > 0$ s.t.

$$f = g \cdot h$$

and is irreducible otherwise.

- "Division Algorithm"

$\forall f, g \in \mathbb{F}[x]$ there exist unique $q, r \in \mathbb{F}[x]$ with $\deg(r) < \deg(g)$ s.t.

$$f = q \cdot g + r$$

q: quotient, r: remainder

- $\mathbb{F}[x]$ is a Unique Factorization Domain:

$$f = f_1 \cdots f_k = g_1 \cdots g_\ell$$

with $f_1 \cdots f_k, g_1 \cdots g_\ell$ irreducible;

$$\deg(f_1) \cdots \deg(f_k), \ldots \quad \deg(g_\ell) > 0$$

$\Rightarrow k = \ell$; $\exists$ permutation π, $\alpha_1 \cdots \alpha_k \in \mathbb{F}$

s.t. $f_i = \alpha_i \cdot g_{\sigma(i)}$.

- Evaluations: $f \in \mathbb{F}[x]$, $\alpha \in \mathbb{F}$

$\Rightarrow$ Evaluation of f at α,

$$f(\alpha) = \sum f_i \alpha^i$$

- α root of f if $f(\alpha) = 0$.

- Fundamental Theorem of Something :

  f has deg d

  $\Rightarrow$ # roots of $f \leq d$

Proof: Division Algorithm++ : $g = x - \alpha$

$\Rightarrow \forall f, \exists q$ s.t.

$$f(x) = q(x) \cdot (x-\alpha) + f(\alpha)$$

α root $\Rightarrow$ $f(x) = q(x) \cdot (x-\alpha)$

$\alpha_1 \cdots \alpha_d$ roots $\Rightarrow$

$$f(x) = \underbrace{\tilde{q}(x) \cdot (x-\alpha_1)\cdot(x-\alpha_2)\cdots(x-\alpha_d)}_{\deg \geq d}.$$

Cor: $f \neq g$, $\deg f, g \leq d \Rightarrow \#\{\alpha \mid f(\alpha) = g(\alpha)\} \leq d$.

• **Interpolation:** Given $\alpha_0 \dots \alpha_d \in \mathbb{F}$ distinct & $\beta_0 \dots \beta_d \in \mathbb{F}$

$\exists!\ f \in \mathbb{F}[x]$ with $\deg(f) \le d$

s.t. $f(\alpha_i) = \beta_i$

2 proofs

(1) $\Leftarrow$

$$\begin{bmatrix} 1 & \alpha_0 & \alpha_0^2 & \cdots & \alpha_0^d \\ 1 & \alpha_1 & \cdots & & \alpha_1^d \\ \vdots & & & & \\ 1 & \alpha_d & \cdots & & \alpha_d^d \end{bmatrix} \begin{bmatrix} f_0 \\ \vdots \\ f_d \end{bmatrix} = \begin{bmatrix} \beta_0 \\ \vdots \\ \beta_d \end{bmatrix}$$ is solvable

$\Leftarrow$ $\det(\downarrow) = \prod_{i<j} (\alpha_i - \alpha_j) \neq 0.$

Vandermonde Matrix

② (i) $\forall S \subseteq F$, $\alpha \in F - S$

$\exists \int_{\alpha, S} \in F[x]$ $\quad \deg(\int) \leq |S|$

s.t. $\int(\alpha) = 1$ & $\int(\beta) = 0$ $\forall \beta \in S$.

(use root ≤ deg to prove this)

(ii) Let $\int_i \triangleq \int_{\alpha_i, \{\alpha_0 \cdots \alpha_d\} - \alpha_i}$

Let $f = \sum_{i=0}^{d} \int_i \beta_i$ ....

- Multivariate Polynomials: $F[x_1 \ldots x_n]$ UFD;

Note curved bracket

Inherits nice structure from

$F(x_1 \cdots x_{n-1})[x_n]$ → ratios of polynomials

↑ field of rational functions in $x_1 \cdots x_{n-1}$

Finite Fields

- There is a unique field $\mathbb{F}_q$ with $|\mathbb{F}| = q$ iff $q = p^t$ for prime p & $+^{ve}$ integer t.

(Throughout $q = p^t$ with p prime)

- Computable Representations:

1. $\mathbb{F}_p$: integers modulo p.

   $\mathbb{F}_{p^t}$: given by irreducible polynomial $h(x)$, monic, $\deg(h) = t$,

   $$\mathbb{F}_{p^t} = \{ g \in \mathbb{F}_p[x], \deg(g) < t \}$$

   Addition, multiplication in $\mathbb{F}_p[x]$, modulo h.

[Shoup]: Given p, t can find irreducible h in det. time poly(p,t); in prob. time poly$(\log p, t)$.

(Reduction modulo h can be hard to think about ... so the following can be useful.)

2. $\mathbb{F}_{p^t}$ vs. $\mathbb{F}_p^t$ (field elements as vectors.)

ψ $\qquad$ ψ

$\alpha \longleftrightarrow V_\alpha$

$\alpha + \beta \iff V_{\alpha+\beta} = V_\alpha + V_\beta$

↑ vector addition

3. (field elements as matrices)

Continuing with repn. (2):

Say $\alpha \leftrightarrow V_\alpha$

Consider function

$$L_\beta : \mathbb{F}_p^t \to \mathbb{F}_p^t$$

$$V_\alpha \longmapsto V_{\alpha\beta}$$

L_β linear map $\Leftrightarrow \exists\ M_\beta \in \mathbb{F}_p^{t \times t}$

s.t. $V_{\alpha\beta} = M_\beta \cdot V_\alpha$

For this repn.

$$M_{\alpha+\beta} = M_\alpha + M_\beta$$

$$M_{\alpha\beta} = M_\alpha \cdot M_\beta$$

(2) + (3) can be quite useful.

Extension fields & polynomials

$$(x+y)^p = x^p + y^p$$

$$\left(\sum c_i x^i\right)^p = \sum c_i^p x^{ip}$$

Facts we most likely won't use

- $\exists$ multiplicative generator $w \in \mathbb{F}_q$ s.t.

$$\mathbb{F}_q = \{0, 1, w, w^2, \ldots w^{q-2}\}$$

- $\sum_{\alpha \in \mathbb{F}_q} \alpha^i = 0$ if $i \neq q-1$
  $= q-1$ if $i = q-1$

  } Fourier shift

- $\sum_{i=1}^{q-1} \alpha^i = 0$ if $\alpha \neq 1$
  $= q-1$ if $\alpha = 1$

Codes by Polynomials

General Idea

Message ≡ Coefficients of polynomial

Encoding ≡ Evaluation

Evaluation ⇒ Encoding

Interpolation ⇒ Decoding from no errors.

(GENERALIZED) REED SOLOMON CODES:

Specified by $\Sigma = \mathbb{F}_q$

$n \leq q$, $0 \leq k \leq n$, distinct $\alpha_1 \dots \alpha_n \in \mathbb{F}_q$

$m = (m_0 \dots m_{k-1}) \longmapsto \langle M(\alpha_1) \dots M(\alpha_n) \rangle$

$M(x) = \sum m_i x^i$

"Cor" $\Rightarrow$ $\Delta(RS_{\mathbb{F}_q, \alpha_1 \ldots \alpha_n, k}) \geq n - (k-1)$

$= n - k + 1$

Matches Singleton !!

[Classical RS : Set $\alpha_1 \ldots \alpha_n$ = all non-zero elements of $\mathbb{F}_q$]

Conclusion: if $q \geq n$ & $q = p^t$ then

can achieve "optimal" codes $[n, k, n-k+1]_q$

MDS - "Maximum Distance Seperable".

What about smaller alphabets ?

Multivariate Polynomials ⇔ Reed Muller Codes

Fix $\Sigma = \mathbb{F}_q$, degree r,

#variable m.

Then: message = coefficients of deg r poly

$r < q \Rightarrow k = \binom{m+r}{r}$

Generally $\rightarrow k \geq \left(\frac{r}{m}\right)^m \cdot \binom{m}{r} \cdots$

Encoding ≡ Evaluations

$n = q^m$

Distance? :

$r < q$: $\Delta(C) = \left(1 - \frac{r}{q}\right) \cdot n$

$r \geq q$: $\Delta(C) \geq q^{-\frac{r}{q-1}} \cdot n$

Example Choices:

(1) Given k

$q = \log^2 k$

$r = \frac{q}{2}$

m s.t. $\binom{m + q/2}{m} = k \Rightarrow m = \frac{\log k}{\log \log k}$

$n = q^m \approx k^2$

$\Rightarrow \left(k^2, k, \frac{1}{2}k^2\right)_{\log^2 k}$ code

Rate $\longrightarrow 0$; Dist $= \frac{1}{2}$

② Fix $m = O(1)$

Given k, pick $q = 2m \cdot k^{1/m}$

$r = q/2$

⋮

$\Rightarrow \left((2m)^m k, k, \frac{1}{2}(2m)^m k\right)_{2m k^{1/m}}$ code

Smaller alphabet than RS, smaller rate.

③ $q = 2$; $r = 1$; $m = m \to \infty$

coefficients $\triangleq k = m+1$

Gives $\left[2^k, k+1, 2^{k-1}\right]_2$ Code

$\Downarrow\Downarrow$

$\exists \left[2^k - 1, k, 2^{k-1}\right]_2$ code

Tight for Plotkin ↓ Simplex Code

Dual = $\left[2^k - k - 1, k, ?\right]$ code!

$?$ = 3 (= Hamming code!!)

Sometimes called "Hadamard Code"

Hadamard matrices & Codes

$n \times n$ matrix $H \in \{-1, +1\}^{n \times n}$

is a Hadamard matrix if

$$H \cdot H^T = n \cdot I$$

$H \Rightarrow$ binary codes as follows.

(1) w.l.o.g. first column of H is all $+1$'s
(if not flip entire row).

Drop first column, rest of rows form

$\left(n-1, \log n, \frac{n}{2}\right)_2$ code

(simplex code)

(2) Rows of H & their complements $-H$ form $\left(n, \log 2n, \frac{n}{2}\right)_2$ code

↑

$\mathbb{R}_m$ with $m = \log n$, $r=1$, $q=2$ is such a code.

Hadamard code.

Summary

- Algebra leads to nice codes;
- Matches Singleton, Plotkin (ii),
- But hasn't (yet) given $q = O(1)$, $R, \delta > 0$ ....
- But leads to Hens.