MIT

6.440, LECTURE 08 3/4/2013

Note Title 4/24/2012

TODAY

Algebraic-Geometry Codes

- Motivation: ϵ-biased spaces
- General Principle
- AG code on Hermitian curve
  - Bezout's Theorem,
  - Trace, Norm etc.
- [TVZ] bound; Garcia-Stichtenoth curves

Next lecture:

Guest lecture by Prof. Eli Ben-Sasson.

- Upper bounds on list-decodability of Reed-Solomon codes.

ϵ-Biased Spaces

Will motivate later:

But amount to linear binary codes C of distance $\delta = \frac{1}{2} - \epsilon$, length $= n$, dimension k as large as possible,

★ extra condition: $1^n \in C$.

Random Code

$$k \approx \epsilon^2 \cdot n \iff n = k/\epsilon^2$$

Explicit Constructions - 1

Reed-Solomon concatenated with Hadamard.

$$[n, 2\epsilon n, (1-\epsilon)n]_n \circ [n, \log_2 n, \frac{n}{2}]_2$$

$$\Rightarrow \left[n^2, 2\epsilon n \log n, \left(\frac{1}{2} - \epsilon\right) n^2 \right]_2$$

$$\approx \left[N,\ \epsilon\sqrt{N}\log N,\ \left(\tfrac{1}{2}-\epsilon\right)N\right]_2 .$$

$$\Rightarrow K \approx \epsilon\sqrt{N} \quad \text{or} \quad N \approx \frac{K^2}{\epsilon^2}$$

Explicit Constructions - 2

RS concatenated with Random

$$\left[n,\ \tfrac{\epsilon}{2}n,\ \left(1-\tfrac{\epsilon}{2}\right)n\right]_n \circ \left[\ell,\ \log n,\ \left(\tfrac{1}{2}-\tfrac{\epsilon}{2}\right)\ell\right]_2$$

$\Downarrow$ where $\ell = O\left(\frac{\log n}{\epsilon^2}\right)$

$$\left[n\ell,\ \tfrac{\epsilon}{2}n\log n,\ \left(\tfrac{1}{2}-\epsilon\right)n\ell\right]_2$$

$\Downarrow$

$$\left[N,\ \ell(\epsilon^3 \cdot N),\ \left(\tfrac{1}{2}-\epsilon\right)N\right]_2$$

$$\Rightarrow K = \epsilon^3 N \quad \text{or} \quad N = K/\epsilon^3 .$$

Summary

- Best known ϵ-biased space has

$$n = k/\epsilon^2$$

- Best explicit code has

$$n = \frac{k^2}{\epsilon^2} \quad \text{or} \quad n = \frac{k}{\epsilon^3}$$

- Today: [Ben-Aroya & Ta-Shma]

$$n = \frac{k^?}{\epsilon^?}$$

by "AG code" & Hadamard.

AG Codes

General Idea:

- Message Space = Carefully chosen set of functions mapping

$$\mathbb{F}_q^m \to \mathbb{F}_q$$

- Coordinates = Carefully chosen set of points in $\mathbb{F}_q^m$

- Both careful choices dictated by "algebraic geometry"
  - In particular points determined by zeroes of nice algebraic curve

$$P_1(x_1 \cdots x_m) = 0 \quad \cdots \quad P_{m-1}(x_1 \cdots x_m) = 0.$$

History:

- Conceived by V.D. Goppa in late 70s.

70s (no dramatic constructions)

- Breakthroughs construction Tsfasman, Vladuts, Zink: Codes of rate R, distance δ

83? with $R \geq 1 - \delta - \frac{1}{\sqrt{q}-1}$ provided $q =$ square

- Simplified recently Garcia, Stichtenoth.

  Will show points, but not rate/distance

- Will show: Code on Hermitian curve

Code on Hermitian Curve

Basic Setup: q = prime power

- Alphabet = $\mathbb{F}_{q^2}$ (not $\mathbb{F}_q$!)

3 Ingredients:

I. Bezout's Theorem (in the plane)

if $f, g \in \mathbb{F}[x,y]$ have no common factors, then

$$\#\{(\alpha,\beta) \in \mathbb{F}\times\mathbb{F} \mid f(\alpha,\beta) = g(\alpha,\beta) = 0\}$$

$$\leq \deg(f) \cdot \deg(g)$$

II. Trace function: $Tr : \mathbb{F}_{q^t} \to \mathbb{F}_q$

$$Tr(x) = x + x^q + x^{q^2} + \dots x^{q^{t-1}}$$

Properties:

(1) $Im(Tr) \subseteq \mathbb{F}_q \iff \forall x \in \mathbb{F}_{q^t}$

$$Tr(x)^q = Tr(x)$$

(2) $Tr(x+y) = Tr(x) + Tr(y)$

(3) Tr is q^{t-1}-to-1 map from

$\mathbb{F}_{q^t} \to \mathbb{F}_q$

(follows from fact that $\forall \alpha, f$

$\#\{\beta \mid f(\beta) = \alpha\} \leq \deg(f)$ ...

(and some counting & part (1)))

III: Norm function

- $N: \mathbb{F}_{q^t} \to \mathbb{F}_q$

$$N(x) = x^{1+q+q^2+\cdots q^{t-1}}$$

Properties

① $\forall \alpha \in \mathbb{F}_{q^t} \quad N(\alpha)^q = N(\alpha)$

$\Rightarrow N(\alpha)$ does map to $\mathbb{F}_q$

② $N(x \cdot y) = N(x) \cdot N(y)$

③ $\forall \alpha \in \mathbb{F}_{q^t}^*$

$$\#\{\beta \mid N(\beta) = \alpha\} = 1+q+\cdots q^{t-1}$$

so on non-zero elements

N is a $1+q+q^2+\cdots q^{t-1}$-to-1 map.

Hermitian Curve

$$S \subseteq \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$$

$$S \triangleq \{ (\alpha, \beta) \mid N(\beta) = Tr(\alpha) \}$$

Claim: $|S| = q^3$

Proof: Fix β & let $\gamma = Tr(\beta)$

$$\# \{ \alpha \mid Tr(\alpha) = \gamma \} = q$$

$\boxtimes$

will let $R(x,y) \triangleq N(y) - Tr(x)$ so that

$$S = \{ (\alpha, \beta) \mid R(\alpha, \beta) = 0 \}$$

Claim (without proof): R is irreducible.

Code on Curve

- Parameter: $r \leq q$
- Message space:

$$\{ f \in \mathbb{F}_{q^2}[x,y] \mid \deg(f) \leq r \quad \deg_y(f) \leq q \}$$

- Coordinates: points on Hermitian Curve $\leq$
- Encoding = Evaluations.

Code Parameters

- length $= n = q^3$
- alphabet $= q^2 = n^{2/3}$
- dimension $= k \geq r^2/2$

Distance Lemma: $d \geq n - r(q+1)$

Proof (Immediate from Bezout's Theorem. Details below.)

- fix f s.t. $\deg(f) \leq r$
- Note f & R have no common factors since R is irreducible & $\deg_y(f) < \deg_y(R)$
- Follows from Bezout Thm

$$\#\{(\alpha,\beta) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \mid f(\alpha,\beta) = R(\alpha,\beta) = 0\}$$
$$\leq r \cdot (q+1)$$

∎

Summary: $\forall\, r, q$

$$\exists \left[q^3, \frac{r^2}{2}, q^3\left(1 - \frac{r}{q^2}\right) \right]_{q^2} \text{ - code}$$

Concatenations with Hadamard $[q^2, \log q^2, \frac{1}{2}q^2]_2$

$$\Downarrow$$

$$\left[q^5,\ r^2,\ \frac{q^5}{2}\left(1-\frac{r}{q^2}\right)\right]_2 \text{ - code}$$

To get ϵ-Biased code of dimension k

Set $r^2 = k \Rightarrow r = \sqrt{k}$

& $\frac{r}{q^2} = \epsilon \Rightarrow q = \sqrt{\frac{r}{\epsilon}} = \frac{k^{1/4}}{\epsilon^{1/2}}$

Yields $n = q^5 = \frac{k^{5/4}}{\epsilon^{5/2}}$

(Btw, need $r \le q \Rightarrow r \le \sqrt{\frac{r}{\epsilon}} \Rightarrow r \le \frac{1}{\epsilon}$

$\Rightarrow \sqrt{k} \le \frac{1}{\epsilon}$)

Best known explicit const., when $\epsilon = \frac{1}{k}$ ⊠

Garcia - Stichtenoth Codes

$$S \subseteq \mathbb{F}_{q^2}^{m}$$

$$S \triangleq \left\{ (x_1 \dots x_m) \;\middle|\; \begin{array}{l} P_1(\bar{x}) = 0 \\ P_2(\bar{x}) = 0 \\ \vdots \\ P_{m-1}(\bar{x}) = 0 \end{array} \right\}$$

$$P_i(x_1 \dots x_m) = N(x_i) - Tr(x_i) \cdot Tr(x_{i+1})$$

Claim (Easy / Omitted): $|S| \geq q^{m+1}$.

Claim: (Hard / Omitted) $\exists$ spaces of functions

$$C_1 \subseteq C_2 \subseteq C_3 \cdots C_n$$

where $n = q^{m+1}$ s.t.

① $\Delta(C_i) \geq n - i$

② $\#\{i \mid C_i = C_{i+1}\} \leq \frac{n}{q-1}$

③ (for later use)

$\forall x \in C_i, y \in C_j$

$x * y \triangleq (x_1 y_1, x_2 y_2 \cdots, x_n y_n) \in C_{i+j}$

move or less $\Rightarrow$ polynomials

Asymptotically

$$R + \delta \geq 1 - \frac{1}{q-1}$$

for code over $\mathbb{F}_{q^2}$.

⊠