STO8 LECTURE 8

3/3/2008

Note Title 3/3/2008

TODAY: ALGEBRAIC GEOMETRY CODES

- Motivation: q-ary asymptotics
- Intuition: A concrete example
- Asymptotics: Assertions without full proofs.

---

q-ary Asymptotics

- Suppose you have R, δ in mind:
- Can you achieve this for some q?
- q-ary PLOTKIN bound:

$$R + \left(\frac{q}{q-1}\right)\delta \leq 1$$

← Problem Set 2

- Fixing R, δ s.t. $R + \delta < 1$

  get $R + \delta + \Omega\left(\frac{1}{q}\right) \leq 1$

- $q = \Omega(1 - R - \delta)$ necessary !

- Is this sufficient ?

- State of the art in the 1980

  GV bound : Exist $[n, k, d]_q$ codes with

$$q^k \cdot \mathrm{Vol}_q(n, d) \geq q^n$$

$$\mathrm{Vol}_q(n,d) \approx q^{H_q(d/n) \cdot n}$$

$$H_q(\delta) = \delta \log_q \frac{q-1}{\delta} + (1-\delta) \log_q \frac{1}{1-\delta}$$

$\exists$ q-ary codes with rate R & distance δ

s.t. $R + H_q(\delta) \geq 1$

- $H_q(\delta)$ complicated .... lets simplify by fixing $0 < \delta < 1$ and let $q \to \infty$

  Clearly $\lim_{q \to \infty} H_q(\delta) = 1 - \delta$

  Convergence = ? $H_q(\delta) = 1 - \delta - O\left(\frac{1}{\log q}\right)$

- $q = 2^{O\left(\frac{1}{1-R-\delta}\right)}$ suffices.

- Is this right? No real intuition!
- "Algebraic Geometry" Codes $q = \left(\frac{1}{1-R-\delta}\right)^2$ suffices!

History of AG Codes

- Concept suggested by V.D. Goppa
  (late 70's)
  - No concrete asymptotic improvement given
  - Merely optimism that something may be feasible.
- Early 80's : Breakthrough by
  [Tsfasman, Vladuts, Zink]
  based of "modular curves" ...
  acheived for every $q = p^k$, k even,
  q-ary codes of rate R & distance δ
  with $R + \delta \geq 1 - \frac{1}{\sqrt{q}-1}$

- '80s: Construction remained complex; even saying they were "explicit" in FORNEY sense required work: e.g. [MANIN, VLADUTS]

- 90s: [GARCIA - STICHTENOTH] gave much simpler family of codes.
  [Shum] shows these are $O(n^2)$ time constructible. Still not "JUSTESEN" explicit.

- Today: We'll see some of the ideas behind this line of work. & even if we don't prove it, the following is true ☺

Theorem: Let $q = p^{2t}$; Let $n \geq k + d + \frac{n}{\sqrt{q}-1}$;
Then $\exists$ $[n, k, d]_q$ code.

Univariate vs. Bivariate Polynomial Codes:

- Consider the evaluations of bivariate poly $Q(x, y)$ over $\mathbb{F}_q$ of degree at most ℓ in x and ℓ in y

- Distance of such codes

$$d \approx (q-\ell)^2$$

- Dimension $k \approx \ell^2$

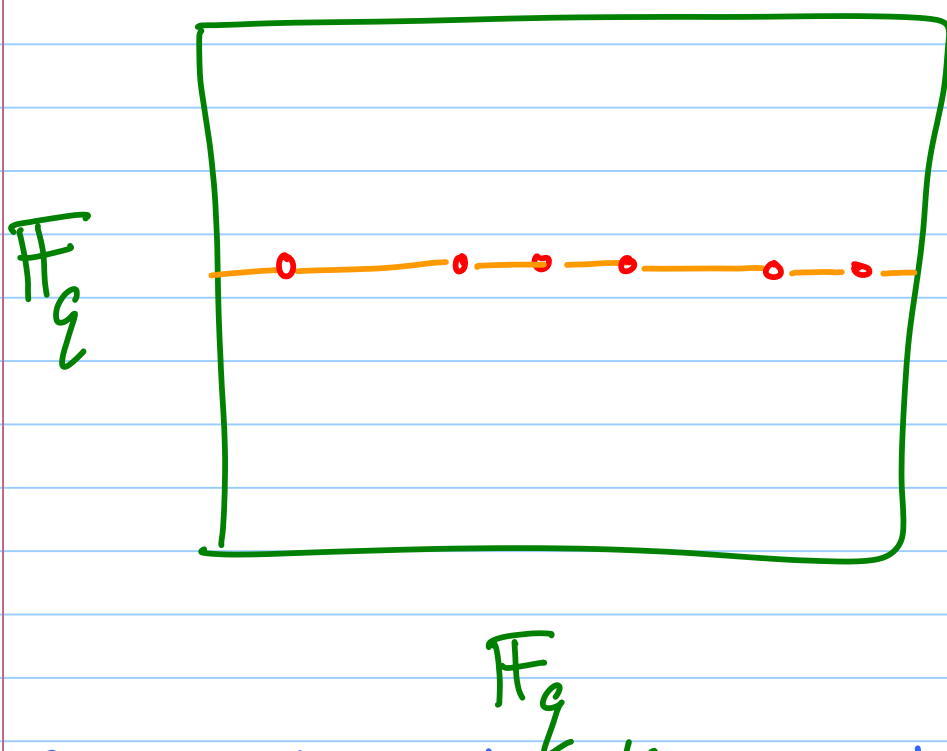
- $\Rightarrow \exists\ [q^2, \ell^2, q^2 - 2q\ell + \ell^2]_q$ code

- Contrast with RS code: $[q^2, \ell^2, q^2 - \ell^2]_{q^2}$

- "Deficit" of bivariate polynomials

$$= 2q\ell - 2\ell^2 = 2(q-\ell)\ell$$

- Why is this deficit coming up?



- Suppose two deg (ℓ, ℓ) polys agree on red points (say ℓ of them). Then they agree on entire line

- ℓ horizontal agreements

  $\Rightarrow$ q horizontal agreements.

- A "good" code should not have such redundancy!

- How to remove it?

  Don't evaluate Q on all points in plane but rather on some set $S \subseteq \mathbb{F}_q \times \mathbb{F}_q$.

- How to pick S?

  <u>Idea 1</u>: Pick S at random?

  - Will still need to do union bounds.
  - Will lead to GV bound.

  <u>Idea 2</u>: Algebraically?

GOPPA'S IDEA

- Pick some polynomial $R(x,y)$

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

But how to pick R ?

- Some bad ideas

  - $R(x,y) = ax + by + c$

    $\Rightarrow$ reduces to univariate poly !

  - $R(x,y) = 3x^2 + 2xy + y^2 + 7$

    $\Rightarrow$ still $|S| \leq 2q$ (Why ?)

  - $R(x,y) = \prod_{\alpha \in T} (x-\alpha) \cdot \prod_{\beta \in T'} (y-\beta)$

    $\Rightarrow$ still a collection of lines.

Goppa's suggestion:

Pick R irreducible;

of moderate degree;

Illustrative Example

- $q = 13$

- $R(x,y) = y^2 - 2(x-1)x(x+1)$

- Which polynomials? Ones supported by the monomials $\{1, x, x^2, x^3, y, xy\}$

- Suppose some poly

$$= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + b_1 y + b_2 xy$$

shares 7 zeros with $R(x,y)$

then $a_0 = a_1 = a_2 = a_3 = b_1 = b_2 = 0$

Proof: Bezout's theorem + careful analysis.

Bezout's Theorem: $R(x,y)$ & $Q(x,y)$ of degree D_1 & D_2 have more than $D_1 D_2$ common zeroes $\Rightarrow$ R & Q share common factor.

- Putting all this together $\Rightarrow$ $[19, 6, 13]_{13}$ code

  $(RS \Rightarrow [19, 6, 14]_{19}$ code $)$

Is this a big deal?

Are there some general ideas?

Traces & Norms

- $Tr: \mathbb{F}_{q^2} \to \mathbb{F}_q$

  $Tr(y) = y + y^q$

- $N: \mathbb{F}_{q^2} \to \mathbb{F}_q$

  $N(x) = x^{q+1}$

- Obvious that both map to $\mathbb{F}_{q^2}$, but do they really map to $\mathbb{F}_q$?

- $\mathbb{F}_q = \{ \alpha \in \mathbb{F}_{q^2} \mid \alpha^q = \alpha \}$

- $(y + y^q)^q = y^q + y^{q^2} = y^q + y$!

- $(x^{q+1})^q = x^{q^2+q} = x^{1+q}$!

Hermitian Example

- $R(x,y)$: $Tr(y) - N(x)$
- Useful facts: $\forall \gamma \neq 0 \quad \exists \; q+1 \; \alpha$ s.t
  $N(\alpha) = \gamma$

  $\forall \gamma \quad \exists \; q \quad \beta$ s.t.
  $Tr(\beta) = \gamma$

  $\Rightarrow \#\ (\alpha,\beta)$ s.t. $N(\alpha) = Tr(\beta)$

  $= (q-1)(q+1)\,q$

  $+ \; q \quad = \quad q^3$
- Using deg q poly in x,y

  $\Rightarrow \left[q^3, \binom{q+2}{2}, q^3 - q(q+1) \right]_{q^2}$ code.

- The point of this :
  - Same method to this "machine".
  - Asymptotics still not clear.

GARCIA - STICHTENOTH FAMILY

m-variate extension of previous example.

$$x_1 \quad x_2 \quad \cdots \quad x_{m+1}$$

- $S \subseteq \underbrace{\mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \times \cdots \mathbb{F}_{q^2}}_{m+1 \text{ times}}$

- $S = \Big\{ (x_1 \ldots x_{m+1}) \ \Big| \ \forall i \in [m] \quad Tr(x_{i+1}) = \dfrac{N(x_i)}{Tr(x_i)} \ldots \Big\}$

- **Claim:** $|S| \geq (q^2 - q) \cdot q^m$

Proof: Pick $x_1 \ldots x_i$ s.t. $Tr(x_1) \neq 0$

$\Rightarrow Tr(x_i) \neq 0$ & # x_{i+1} satisfying

$= q \cdot \ldots$

[WARNING ... THE FOLLOWING ARE NOT CORRECT CLAIMS ... BUT SOME SORT OF APPROX]

- Basis functions, roughly = deg q polys in $x_1 \ldots x_{m+1}$

- # zeroes in $S \leq q^{m+1}$ (roughly prod. of degrees)

$$= \frac{n}{q-1}$$

- Leads to $[n,k,d]_{q^2}$ codes with

$$n = q^{m+1}(q-1)$$

k = whatever you want

$$d \geq n - k - q^{m+1}$$

Summary

- Nice q-ary codes.
- Outperform GV bound for $q \geq 49$.
- What about binary codes?
    - Concatenation is still best.
    - Slightly nicer to concatenate

$$\underbrace{AG}_{q \approx \left(\frac{1}{\epsilon}\right)^2} \circ \text{ inner code}$$

- Questions: Why $\frac{1}{\sqrt{q}-1}$?
    - if $\frac{1}{q-100}$ $\Rightarrow$ what consequences?