Towers and codes

Peter Beelen

Technical University of Denmark (DTU)

Workshop on Mathematics of Information - Theoretic Cryptography
Singapore
September 28, 2016

Evaluation codes

- $\mathbb{F}_q$: a finite field with q elements
- $P_1, \ldots, P_n$ points in m-dimensional space $\mathbb{F}_q^m$.

Definition

The evaluation map $\mathrm{Ev} : \mathbb{F}_q[x_1, \ldots, x_m] \to \mathbb{F}_q^n$ is defined by $\mathrm{Ev}(f) := (f(P_1), \ldots, f(P_n))$.
For any linear space $L \subset \mathbb{F}_q[x_1, \ldots, x_m]$, one obtains a linear code $\mathrm{Ev}(L)$.

Remarks:

1. This point of view advocated by Fitzgerald–Lax
2. Lagrange interpolation: any linear code can be obtained in this way.
3. If an ideal $I \subset \mathbb{F}_q[x_1, \ldots, x_m]$ satisfies $f(P_i) = 0$ for all $f \in I$ and all P_i, then we can define $\mathrm{Ev} : \mathbb{F}_q[x_1, \ldots, x_m]/I \to \mathbb{F}_q^n$.

Example

Choose $P_1, \ldots, P_n$ all $n = q^m$ points in $\mathbb{F}_q^m$ and choose $L \subset \mathbb{F}_q[x_1, \ldots, x_m]$ the polynomials of total degree up to r.

$\mathrm{Ev}(L) = \mathrm{RM}_q(r, m)$, the (generalized) Reed–Muller code of order r.

Dimension: $\binom{m+r}{r}$. Minimum distance $(q - r)q^{m-1}$ if $r < q$.

Geometrically:

- $\mathbb{F}_q^m$ is the m-dimensional (affine) space,
- $P_1, \ldots, P_n$ are the "rational points" of this space,
- L are functions on this space with restricted "behaviour at infinity"
- $n - w_H(\mathrm{Ev}(f))$ equals number of zeroes of f

AG codes

Choose:

1. $\mathcal{X}$: an algebraic curve,
2. $P_1, \ldots, P_n$ be rational points on $\mathcal{X}$,
3. G be a divisor on $\mathcal{X}$ s.t. $\deg G < n$.,

Write:

- g the genus of $\mathcal{X}$,
- $D = P_1 + \cdots + P_n$,
- $L(G)$ the Riemann–Roch space of G, of dimension $k := \ell(G)$,

Then:

Theorem (Goppa)

$C_L(D, G) := \mathrm{Ev}(L(G))$ is an $[n, k, d \geq n - k + 1 - g]_{\mathbb{F}_q}$ code and $C_L(D, G)^\perp$ is an $[n, n - k, d^\perp \geq k + 1 - g]_{\mathbb{F}_q}$ code.

Three examples

Reed–Solomon codes: Choose $\chi = \mathbb{P}^1$ and $G = aQ$, with Q the point "at infinity". Then $C_L(D, aQ)$ is a Reed–Solomon code.

Hermitian codes: Choose χ over $\mathbb{F}_{q^2}$ defined by $y^q + y = x^{q+1}$, Q the point at infinity, $P_1, \ldots, P_n$ up to q^3 rational points of χ. Then $C_L(D, aQ)$ is an $[n, k, d \geq n - k + 1 - g]$ code with $k = \ell(aQ)$ and $g = q(q-1)/2$.

Asymptotic good families: Choose χ over $\mathbb{F}_{q^2}$ from an "asymptotically optimal" family. Tfasman–Vladut–Zink found a family of codes with asymptotic rate $R = k/n$ and relative distance $\delta = d/n$:

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

Beats the Gilbert–Varshamov bound if $q \geq 7$.

Minimum distance AG codes

$$C_L(D, G): \ d \geq n - \deg(G) \geq n - k + 1 - g$$

- Choose $f \in L(G)$ such that $w_H(\mathrm{Ev}(f)) = d$.
- f has zeroes in $n - d$ rational points, say $P_1, \ldots, P_{n-d}$.
- $f \in L(G - P_1 - \cdots - P_{n-d})$
- $0 \leq \deg(G - P_1 - \cdots - P_{n-d}) = \deg(G) - n + d$
- $d \geq n - \deg(G) \geq n - k + 1 - g$, since $k = \ell(G) \geq \deg(G) - g + 1$.

$$C_L(D, G)^{\perp}: \ d^{\perp} \geq \deg(G) - 2g + 2 \geq n - k + 1 - g$$

- $C_L(D, G)^{\perp} = C_L(D, H)$ for a divisor H with $\deg(H) = n - \deg(G) + 2g - 2$.

Basic decoding

Received word

$$r = (r_1, \ldots, r_n) = c + e,$$

sent codeword

$$c = \mathrm{Ev}(f) \text{ for } f \in L(G).$$

Find $Q(T) = Q_1 \cdot T + Q_0$ such that:

1. $Q_0 \in L(A + G)$, $Q_1 \in L(A)$, for a suitably chosen divisor A.
2. $Q_1(P_i)r_i + Q_0(P_i) = 0$ for all i.

Then $f = -Q_0/Q_1$ if $w_H(e) \leq (n - \deg(G) - 1 - g)/2$.

Extension to list decoding by Guruswami–Sudan.

Alternative proof of minimum distance $C_L(D, G)^\perp$

- $H(Q) = \{\gamma_0, \gamma_1, \gamma_2, \dots\}$ Weierstrass semigroup at Q.
- Given by the pole orders of $f_0, f_1, \dots$ of $f \in L(\infty Q)$
- $p(T) := \sum_i t^{\gamma_i}$

If $\chi = \mathbb{P}^1$, then

$$p(t) = 1 + t + t^2 + \cdots = \frac{1}{1-t}.$$

- $H_G(Q) = \{\delta_0, \delta_1, \dots\}$
- Given by pole orders of $g_0, g_1, \dots$ of $g \in L(G + \infty Q)$
- $p_G(T) := \sum_j t^{\delta_j}$.

If $\chi = \mathbb{P}^1$ and $G = aQ$, then

$$p_G(t) = 1 + t + t^2 + \cdots = \frac{1}{1-t}.$$

Alternative proof of minimum distance $C_L(D, G)^\perp$

Let $c \in C_L(D, G)^\perp \backslash C_L(D, G + Q)^\perp$

- $G = aQ + G'$: $v_Q(G) = a$
- Feng–Rao,Duursma:
  $w_H(c) \geq \nu_a := |\{(\gamma_i, \delta_j) \mid \gamma_i + \delta_j = a + 1\}|$
- This is the coefficient of t^{a+1} in $p(t) \cdot p_G(t)$.

If $\chi = \mathbb{P}^1$ and $G = aQ$:

$$p(t)p_G(t) = \frac{1}{(1-t)^2} = 1 + 2t + 3t^2 + \ldots,$$

hence $w_H(c) \geq a + 2$.

General: Using that $H(Q)$ and $H_G(Q)$ have g "gaps":
$w_H(c) \geq \deg(G) - 2g + 2$

Variations of the order bound

A global statement on $d^\perp$ was obtained by iterating:

$$C_L(D, G)^\perp \supset C_L(D, G + Q)^\perp \supset C_L(D, G + 2Q)^\perp \supset \cdots$$

$$d^\perp \geq d^* := \min_{\alpha \geq a} \nu_a \geq \deg(G) - 2g + 2.$$

In 2007, B. strengthened the method using more general filtrations:

$$C_L(D, G)^\perp \supset C_L(D, G + Q_1)^\perp \supset C_L(D, G + Q_1 + Q_2)^\perp \supset \cdots$$

Duursma generalized this further.

Decoding $C_L(D, G)^\perp$ by majority voting

Let $r = (r_1, \ldots, r_n)$ be the received word, $r = c + e$ for $c \in C_L(D, G)^\perp$.

- Consider the syndrome matrix $S = (\sum_\ell f_i(P_\ell) \cdot r_\ell \cdot g_j(P_\ell))_{i,j}$.
- Based on the structure of S, each of the, say ν_a, pairs in $\{(\gamma_i, \delta_j) \mid \gamma_i + \delta_j = a + 1\}$ "votes" in which coset of $C_L(D, G + Q)^\perp$ the error vector e lies.
- The vote is correct if $w_H(e) \leq (\nu_a - 1)/2$.

Iterating majority voting, we find c if $w_H(e) \leq (d^* - 1)/2$.

Fast decoding of AG-codes

- An RS-code of length n can be decoded in $O(n^2)$ using the Euclidean algorithm (or Berlekamp–Massey).
- Using the fast Euclidean algorithm (or BM) in $\tilde{O}(n)$.
- Majority voting: $O(n^3)$ in general, $O(n^{7/3})$ for Hermitian codes (Sakata).
- Basic algorithm for Hermitian codes: $\tilde{O}(n^2)$ (Brander, B.)
- Basic algorithm for Hermitian codes: $\tilde{O}(n^{5/3})$ (Rosenkilde né Nielsen, B.)
- **Central question: How to decode even faster?**

Curves with many rational points

Given a curve χ defined over $\mathbb{F}_q$, we define

$$g(\chi) \text{ genus }, \ N(\chi) \text{ number of rational points.}$$

Then (Hasse–Weil):

$$N(\chi) \leq q + 1 + 2\sqrt{q}g(\chi).$$

The Hermitian curve attains this bound, but curves with high genus cannot.

Ihara's constant: $A(q) := \limsup_{g(\chi)\to\infty} \frac{N(\chi)}{g(\chi)}$.

Asymptotic result for codes:

$$R + \delta \geq 1 - \frac{1}{A(q)}.$$

Facts on $A(q)$

Serre:

$$A(q) > c \log(q).$$

Drinfeld–Vladut:

$$A(q) \leq \sqrt{q} - 1.$$

Ihara, Tsfasman–Vladut–Zink

$$A(p^{2m}) \geq p^m - 1.$$

Hence $A(p^{2m}) = p^m - 1$, but $A(p^{2m+1})$ is unknown.

Function fields

A curve χ defined over $\mathbb{F}_q$ gives rise to a function field $\mathbb{F}_q(\chi)$ consisting of all algebraic functions on χ.

Example: $\chi = \mathbb{P}^1$, then $\mathbb{F}_q(\chi) = \mathbb{F}_q(x)$.

Example: χ the Hermitian curve, then $\mathbb{F}_{q^2}(\chi) = \mathbb{F}_{q^2}(x, y)$ with $y^q + y = x^{q+1}$.

General: $\mathbb{F}_q(\chi)$ can be written as a finite algebraic extension of $\mathbb{F}_q(x)$ for some $x \in \mathbb{F}_q(\chi)$.

Towers of function fields

Tower of function fields:

$$\mathcal{F} = (F_0 \subseteq F_1 \subseteq \cdots \subseteq F_i \subseteq \cdots)$$

1. $F_0 = \mathbb{F}_q(x_0)$
2. F_{i+1}/F_i a finite extension, say $F_{i+1} = F_i(x_{i+1})$
3. $g(F_i) \to \infty$ as $i \to \infty$
4. $\overline{\mathbb{F}_q} \cap F_i = \mathbb{F}_q$

Limit of the tower $\mathcal{F}$:

$$\lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)}.$$

Then $A(q) \geq \lambda(\mathcal{F})$.

Recursive towers

- A recursive towers is obtained by an equation $0 = \varphi(X, Y) \in \mathbb{F}_q[X, Y]$ such that
  - $F_0 = \mathbb{F}_q(x_0)$,
  - $F_{i+1} = F_i(x_{i+1})$ with $\varphi(x_{i+1}, x_i) = 0$ for $i \geq 0$.
- Explicit recursive towers have given rise to good lower bounds on $A(q)$.
- Garcia, Stichtenoth introduced an explicit tower with the equation $(x_{i+1}x_i)^q + x_{i+1}x_i = x_i^{q+1}$ over $\mathbb{F}_{q^2}$ or equivalently

$$x_{i+1}^q x_i^{q-1} + x_{i+1} = x_i^q \text{ over } \mathbb{F}_{q^2}.$$

Garcia–Stichtenoth tower

$$(x_{i+1}x_i)^q + (x_i x_{i+1}) = x_i^{q+1} \text{ over } \mathbb{F}_{q^2}.$$

Using properties of norm and trace:
For an $x_i \in \mathbb{F}_{q^2} \backslash \{0\}$, there are q possibilities for $x_{i+1} \in \mathbb{F}_{q^2} \backslash \{0\}$.

Hence $N(F_i) \geq (q^2 - 1)q^i$.

A nontrivial computation gives $g(F_i) \leq (q+1)q^i$.

This tower is optimal: $\lambda(\mathcal{F}) = q - 1$.

Recent recursive towers

To show the recent result on $A(p^n)$, $n = 2m + 1$, Bassa, B., Garcia, Stichtenoth used a tower satisfying the recursion

$$\frac{x_{i+1}^{q^n-1} - 1}{x_{i+1}^{q^m-1}} = \frac{x_i^{q^n-1} - 1}{x_i^{q^n-q^{m+1}}}.$$

Using this tower, they showed:

$$A(p^n) \geq 2 \left(\frac{1}{p^m - 1} + \frac{1}{p^{m+1} - 1} \right)^{-1}.$$

Therefore the following holds for any n:

$$A(p^n) \geq 2 \left(\frac{1}{p^{\lceil n/2 \rceil} - 1} + \frac{1}{p^{\lfloor n/2 \rfloor} - 1} \right)^{-1}.$$

Results for codes: The asymptotic GV-bound can be improved for:

$$q = p^{2m+1} \text{ if } m > 0 \text{ and } q > 125.$$

Source of the equations

Tsfasman–Vladut–Zink found their results using modular curves.

The first Garcia–Stichtenoth tower was found in a completely different way.

Elkies showed though, that this and all other known optimal recursive towers are in fact modular as well.

The equation for the tower by Bassa–B.–Garcia–Stichtenoth was found using modular theory.

Conclusion

The past few years saw exciting developments in AG codes:

1. Fast decoding.
2. New results on $A(p^{2m+1})$.

Main open problems:

1. Faster decoding.
2. The case $A(p)$.

Conclusion

The past few years saw exciting developments in AG codes:

1. Fast decoding.
2. New results on $A(p^{2m+1})$.

Main open problems:

1. Faster decoding.
2. The case $A(p)$.

THANK YOU!