Lower bounds on the minimum distance of long codes in the Lee metric

Hugues Randriam, Lin Sok, **Patrick Solé**, Telecom ParisTech

Workshop on "Non commutative rings and their applications"

Lens, July 1-4, 2013

Outline

1. Motivation
2. Background on algebraic geometry codes
3. Gilbert type bound
4. Asymptotic rate of new constructible codes
5. Comparison
6. Conclusion

Motivation for Lee metric

Lee weight $wt_L(a)$ of a symbol $a \in \mathbb{Z}_q$, $wt_L(a) := \min(a, q-a)$,

Lee weight of $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_q^n$, $wt_L(\mathbf{x}) = \sum_{i=1}^{n} wt_L(x_i)$

- Application:
- • phase modulation (Berlekamp's book)
- • run length limited coding (Roth's book, Siegel's papers)
- Development of Theory
- • generalizing Hamming case (technical!)
- • giving contructible methods

Affine space vs projective space

- $n-$dimensional affine space over $\mathbb{F}_q$:

$$\mathbb{A}^n(\overline{\mathbb{F}_q}) := \{(x_1, x_2, \ldots, x_n) | x_i \in \overline{\mathbb{F}_q}\}.$$

- $n-$dimensional projective space over $\mathbb{F}_q$:

$$\mathbb{P}^n(\overline{\mathbb{F}_q}) := \left(\mathbb{A}^{n+1}(\overline{\mathbb{F}_q})\right)^* / \sim \; = \{[\mathbf{x}] = (x_1 : \cdots : x_{n+1}) | \mathbf{x} \in \mathbb{A}^{n+1}(\overline{\mathbb{F}_q})\}$$

with $\sim$ defined by:
$\forall \mathbf{a}, \mathbf{b} \in \mathbb{A}^{n+1}(\overline{\mathbb{F}_q}), \mathbf{a} \sim \mathbf{b}$, if $\exists \lambda \in \overline{\mathbb{F}_q}^*$, $\mathbf{a} = \lambda \mathbf{b}$.

Algebraic curves

Let F be an irreducible homogeneous polynomial in $\overline{\mathbb{F}_q}[X_1, X_2, \ldots, X_{n+1}]$

- A projective algebraic curve defined by F over $\mathbb{F}_q$ is

$$\mathcal{X} := \{(x_1 : \cdots : x_{n+1}) \in \mathbb{P}^n(\overline{\mathbb{F}_q}) | F(x_1, \ldots, x_{n+1}) = 0\},$$

- The zeros of F with coordinate x_i in $\mathbb{F}_q$ are called rational points.
- The zeros of F with the last coordinate 0 are called points at infinity.

Example

Let $F(X, Y, Z) = X^3 + XZ^2 + Z^3 + YZ^2 \in \overline{\mathbb{F}_2}[X, Y, Z]$.

- Then the plane projective curve defined by F is

$$\mathcal{X} = \{(x : y : z) \in \mathbb{P}^2(\overline{\mathbb{F}_2}) | F^*(x, y, z) = x^3 + xz^2 + z^3 + yz^2 = 0\}.$$

- There is only one rational point $(1 : 0 : 0)$
- There is only one point at infinity $(1 : 0 : 0)$.

Divisors

$\mathcal{X}$: an algebraic curve over $\mathbb{F}_q$

- Divisor on $\mathcal{X}$:

$$D := \sum_{P \in \mathcal{X}} n_P P$$

with $n_p \in \mathbb{Z}$ all zero except finite many

- Degree of D:

$$\deg(D) := \sum_{P \in \mathcal{X}} n_P \deg(P),$$

where $\deg(P) = |P^\sigma|$ with P^σ as orbit of P under $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$.

- $D = \sum_{P \in \mathcal{X}} n_P P \succcurlyeq D' = \sum_{P \in \mathcal{X}} n'_P P$ if $n_P \geq n'_P$ for all P.

Example

$\mathcal{X} = \{(x:y:z) \in \mathbb{P}^3(\overline{\mathbb{F}_2}) | x^3 + xz^2 + z^3 + yz^2 = 0\}$, a projective plane algebraic curve over $\mathbb{F}_2$

- points of degree 1 over $\mathbb{F}_2$:($x, y \in \mathbb{F}_2$)
  $P_\infty = (0:1:0)$
- points of degree 2 over $\mathbb{F}_2$:($x, y \in \mathbb{F}_{2^2} = \{0, 1, \omega, \bar{\omega}\}$)
  $P_1 = \{(0:\omega:1), (0:\bar{\omega}:1)\}$,
  $P_2 = \{(1:\omega:1), (1:\bar{\omega}:1)\}$,
  where $\omega, \bar{\omega}$ are roots of $y^2 + y = 1$ in $\mathbb{F}_{2^2}$.
- $D = 2P_1 + 3P_2 - 7P_\infty$: a divisor on $\mathcal{X}$
- $\deg(D) = 2.2 + 3.2 - 7.1 = 3$

Rational functions

Let $\mathcal{X}$ be an algebraic curve defined by F. A rational function on $\mathcal{X}$ is a function $f = g/h$ where f and g are homogeneous polynomials of the same degree with $g \notin \langle F \rangle$.

Rational divisors

Let f be a nonzero rational function on $\mathcal{X}$.

- A rational divisor of f: $\mathrm{div}(f) := \sum_{P \in \mathcal{X}} v_P(f)P$.
- $\mathrm{div}(f) = \sum_{P:\text{zero of } f} v_P(f)P - \sum_{P:\text{pole of } f} (-v_P(f))P$.
- $\deg(div(f)) = 0$.

Vector space associated with a divisor

Let G be a divisor on $\mathcal{X}$.

- Define $L(G) := \{f | f = 0 \text{ or } \mathrm{div}(f) + G \succcurlyeq \mathbf{0}\}$
- Dimension of $L(G)$ is denoted by $l(G)$.
- Genus of $\mathcal{X}$ is $\min\{g | l(G) \geq \deg(G) - g + 1\}$.

Consequence of Riemann-Roch Theorem

Let G be a divisor on an algebraic curve $\mathcal{X}$ having genus g. if $\deg(G) > 2g - 2$ then

$$l(G) = \deg(G) + 1 - g.$$

Definitions

- For two divisors G and $D = P_1 + P_2 + \cdots + P_n$ s.t $supp(D) \cap supp(G) = \emptyset$, $L(G) := \{f | f = 0 \textbf{ or } div(f) + G \geq 0\}$ $C(D, G) := \{(f(P_1), f(P_2), \ldots, f(P_n)) | f \in L(G)\}$, the algebraic geometry code
- $[n, k]_q$: linear (Lee) code of length n and dimension k over $\mathbb{F}_q$
- For a genus g, $N_q(g)$: the largest number of rational points
- $A(q) := \limsup_{g \to \infty} \frac{N_q(g)}{g}$, the Ihara function

Definitions

C_i: $[n_i, k_i]_q$ of Lee distance $d_L(C_i)$ such that $n_i \to \infty$.

- Rate: $R = \lim_{i\to\infty} \sup \frac{k_i}{n_i}$.
- Relative Lee distance: $\delta = \lim_{i\to\infty} \sup \frac{d_L(C_i)}{n_i s}$,

  with $s = \lfloor q/2 \rfloor$.

Asymptotic rates of AG codes

Theorem

There are families of geometric codes over $\mathbb{F}_{\mathcal{Q}}$ with rate $\mathcal{R}$ and relative Hamming distance Δ satisfying

$$\mathcal{R} + \Delta \geq 1 - \frac{1}{A(\mathcal{Q})}.$$

Asymptotic rate of AG code

- Theorem (Tsfasman-Vladut-Zink 1981)
  If $\mathcal{Q}$ is a square then
$$\mathcal{R} + \Delta \geq 1 - \frac{1}{\sqrt{\mathcal{Q}} - 1}.$$
- Theorem (Drinfeld-Vladut 1983)
  For any $\mathcal{Q}$,
$$A(\mathcal{Q}) \leq \sqrt{\mathcal{Q}} - 1.$$

Asymptotic rate of AG code

$$\mathcal{R} + \Delta \geq 1 - \frac{1}{A(\mathcal{Q})}.$$

- To get a lower bound for $\mathcal{R}$, we need the exact value of $A(\mathcal{Q})$ or a lower bound for $A(\mathcal{Q})$.
- If $\mathcal{Q}$ is a square then $A(\mathcal{Q}) = \sqrt{\mathcal{Q}} - 1$.
- For $\mathcal{Q}$ being prime, are there any methods to calculate $A(\mathcal{Q})$ or to lower-bound $A(\mathcal{Q})$?

Gilbert type bound

Theorem (Astola 1984)

If $q = 2s + 1$, *then* $R(\delta) \geq 1 + \log_q \alpha\beta^{\delta s}$, *where* α, β *are defined by*

$$\begin{aligned} \alpha + 2\alpha \sum_{i=1}^{s} \beta^i &= 1, \\ \alpha \sum_{i=1}^{s} i\beta^i &= \frac{\delta s}{2} \end{aligned}$$

Construction methods

- Concatenation
- Victoria
- Victoria+descent of the base field

Concatenation

Proposition

Let C_1 and C_2 be an $[N, K, D]_{q^k}$ and $[n, k]_q$ code with Lee distance d_L, respectively. Let Φ be a map defined by

$$\Phi : \mathbb{F}_{q^k} \longrightarrow C_2,$$

and

$$\Phi^* : (\mathbb{F}_{q^k})^N \longrightarrow C_2, \ s.t \ \Phi^*(v_1, \ldots, v_N) = (\Phi(v_1), \ldots, \Phi(v_N)).$$

Then $C = \Phi^*(C_1)$, called concatenated code, is an $[Nn, Kk]_q$ code with Lee distance Dd_L.

We call C_1 the outer code and C_2 the inner code.

Concatenation bound

- Proposition

  The rate R and the relative Lee distance δ of the concatenated code satisfy

$$\frac{R}{k/n} + \frac{\delta s}{d_L/n} \geq 1 - \frac{1}{q^{k/2} - 1}.$$

- Corollary

  For each prime $p \geq 7$ and every integer $1 \leq t \leq (p+1)/2$, such that p is congruent to $t+1 \mod 2$, there is a family of Lee codes over $\mathbb{Z}_p$ with rate R and relative Lee distance δ satisfying

$$\frac{R(p-1)}{p-1-t} + \frac{\delta s(p-1)}{2t} \geq 1 - \frac{1}{p^{(p-t-1)/2} - 1},$$

Victorian construction

- Take $G = rP$, i.e
  $C(D, rP) := \{(f(P_1), f(P_2), \ldots, f(P_n)) | f \in L(rP)\}$.
  Then
- • f has no pole except P whose order is at most r and
- • the number of zeros of f is at most r.
- The occurence of $f(P_i)$ in the codeword of $C(D, rP)$ is at most r times.
- Hence the minimum Lee distance d_L of $C(D, rP)$ is lower bounded by the Lee weight of a word whose entries are filled up with the first small Lee weights.

Victorian construction

Construct a word $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n$ as follows:

- the first components a_i with $0^r, (\pm 1)^r, \ldots, (\pm M)^r$,
- the remaining components with $(M+1)$.
- Hence $d_L \geq wt_L(\mathbf{a})$.

Victorian bound

- Theorem (Wu-Kuijper-Udaya 2007)

  Given an algebraic curve of genus g over $\mathbb{F}_q$ having at least $n+1$ rational points, there are codes of parameters $[n-1, r-g]$ over $\mathbb{F}_q$ with Lee distance

  $$d_L \geq \frac{n^2 - r^2}{4r},$$

  for any integer r in the range $(2g-2, n)$.

- Corollary

  For a family of curves of genus $g \sim \gamma n$, the rate R of the attached family of codes of relative distance δ is

  $$R \geq -\gamma - 2\delta s + \sqrt{4\delta^2 s^2 + 1}.$$

Construction using descent of the base field

Let p be an odd prime and $\{1, \alpha\}$ a basis of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$.

- Then $\mathbb{F}_{p^2} = \mathbb{F}_p \cdot 1 + \mathbb{F}_p \cdot \alpha \cong \mathbb{F}_p \times \mathbb{F}_p$.
- We identify a word $c \in (\mathbb{F}_{p^2})^n$ with a word $\widetilde{c} \in (\mathbb{F}_p)^{2n}$.
- We identify an $[n, k]_{p^2}$ code C with an an $[2n, 2k]_p$ code $\widetilde{C}$.
- We extend the definition of the Lee weight to $\mathbb{F}_{p^2}$ by setting the weight of a symbol $z = x + y\alpha \in \mathbb{F}_{p^2}$ (where $x, y \in \mathbb{F}_p$) as

$$wt_L(z) = wt_L(x) + wt_L(y).$$

Construction using descent of the base field

The minimum Lee distance d_L of the $[n,k]_{p^2}$ code C is lower-bounded $wt_L(a)$ where $a = (a_1, a_2, \ldots, a_n) \in (\mathbb{F}_{p^2})^n$ is constructed as follows:

- all symbols $z \in \mathbb{F}_{p^2}$ of Lee weight $0, 1, \ldots, M$ occur in a exactly r times each
- some symbols of Lee weight $M+1$ could occur in a, but not more than r times each, and at least one of them less than r times
- no symbol of Lee weight greater than $M+1$ occur in a

Lower bounds on minimum Lee distance

Theorem

Let $M = \begin{cases} \left\lfloor \frac{1}{2}(-1+\sqrt{2n/r-1}) \right\rfloor & \text{if } 1 \leq n/r \leq \frac{p^2+4p-3}{2} \\ \left\lfloor p - \frac{1}{2}(1+\sqrt{2p^2+1-2n/r}) \right\rfloor & \text{if } \frac{p^2+4p-3}{2} < n/r \leq p^2. \end{cases}$

Then there are codes of parameters $[2(n-1), 2(r-g)]$ *over the prime field* $\mathbb{F}_p$ *with Lee distance* d_L *lower bounded by*

$$\begin{cases} (M+1)n + \frac{(M+1)(2M^2+4M+3)}{3} r & \text{if } n/r \leq \frac{p^2+4p-3}{2} \\ (M+1)n + \frac{2(M+1)(2M^2+4M-6pM-6p+3p^2)-p^3+p}{6} r & \text{if } n/r > \frac{p^2+4p-3}{2}. \end{cases}$$

Moreover, $d_L \geq \dfrac{n-r}{3}\sqrt{\dfrac{2n-r}{r}}$.

Lower bounds on rate

Corollary

Let $\gamma = \frac{1}{p-1}$, *R the code rate and δ relative distance. Then*

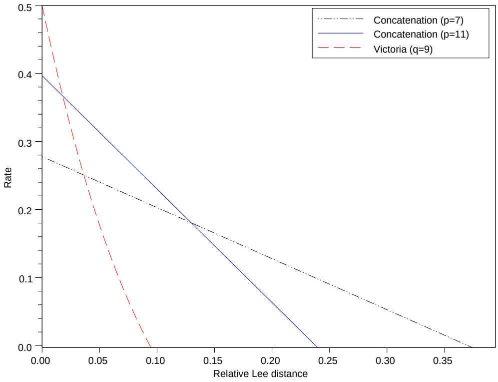
$$R \geq \begin{cases} 1 - 2\delta - \gamma & \text{if } 0 \leq \delta \leq \frac{2}{5} \quad (p \geq 3) \\ \frac{1}{3}(1-\delta) - \gamma & \text{if } \frac{2}{5} \leq \delta \leq \frac{10}{13} \quad (p \geq 5) \\ \text{etc.} & \\ c_M - d_M\delta - \gamma & \text{if } C(M) \leq \delta \leq C(M+1) \quad (p \geq 2M+3) \end{cases}$$

where $c_M = \frac{3}{2M^2+4M+3}$, $d_M = \frac{6}{(M+1)(2M^2+4M+3)}$, $C(M) = \frac{M+1}{2} - \frac{(M+1)(2M^2+4M+3)}{6(1+2M(M+1))}$.

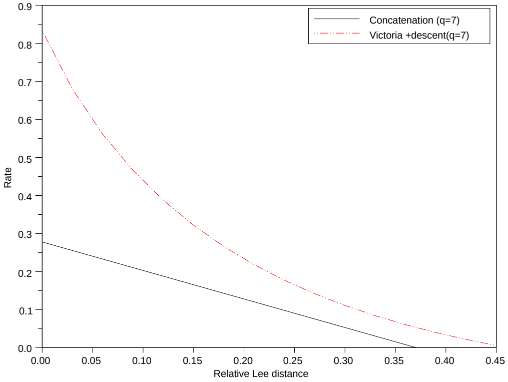
$$\text{Moreover}, R \geq \begin{cases} \left(\frac{-v-\sqrt{\Delta}}{2}\right)^{1/3} + \left(\frac{-v+\sqrt{\Delta}}{2}\right)^{1/3} + \frac{4}{3} - \gamma & \text{if } \Delta \geq 0 \\ 2\sqrt{\frac{-u}{3}}\cos\left(\frac{1}{3}\cos^{-1}\left(-\sqrt{\frac{27v^2}{-4u^3}}\right) + \frac{2\pi}{3}\right) + \frac{4}{3} - \gamma & \text{if } \Delta < 0 \end{cases}$$

with $\Delta = 6912\delta^6 + 2112\delta^4 - \frac{16\delta^2}{3}$, $u = 36\delta^2 - \frac{1}{3}$ *and* $v = (48\delta^2 - \frac{2}{7})$.

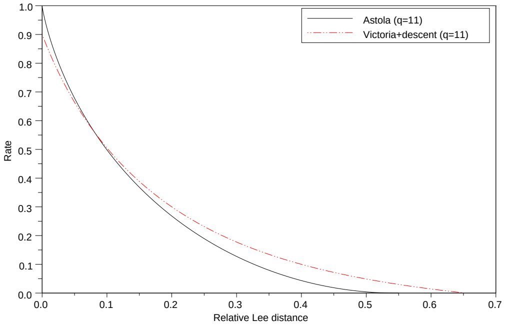
Concatenation vs Victoria



Concatenation vs Victoria+descent



Astola vs Victoria+descent



Thank you!