Weierstrass semigroups and applications in Coding Theory

Giovanni Zini
(joint work with D. Bartoli and M. Montanucci)

Università di Milano-Bicocca

SandGAL 2019

Outline

1. error-correcting codes
2. algebraic curves and AG codes
3. Weierstrass semigroup at one point and AG codes
4. examples from the Suzuki curve
5. Weierstrass semigroup at many points and AG codes

Codes

$\mathcal{A}$: finite set $\qquad n$: positive integer $\qquad C \subset \mathcal{A}^n$

for any $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathcal{A}^n$:

$d(x, y) := |\{i \in \{1, \ldots, n\} : x_i \neq y_i\}|$ Hamming distance

$d = d(C) := \min\{d(x, y) \mid x, y \in C, x \neq y\} \qquad t := \lfloor \frac{d-1}{2} \rfloor$

- C is a block code of length n over the alphabet $\mathcal{A}$
- C has minimum distance d and corrects up to t errors
- $R := \frac{\log_{|\mathcal{A}|} |C|}{n}$ information rate $\qquad D := \frac{d}{n}$ relative minimum distance

Goal: maximize R and D

Singleton bound: $|C| \leq |\mathcal{A}|^{n-d+1}$

Linear codes

$\mathcal{A} = \mathbb{F}_q$ finite field with q elements

C : $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$

$k := \dim_{\mathbb{F}_q} C \Rightarrow |C| = q^k$

$d := \min_{x,y \in C,\, x \neq y} d(x,y) = \min_{x \in C} |\{i \in \{1,\ldots,n\} : x_i \neq 0\}|$

C is a linear $[n,k,d]_q$-code

Singleton bound: $k + n \leq n + 1$

relative Singleton defect: $\Delta := \frac{n+1-(k+d)}{n} \geq 0$

Goal: minimize Δ

Several families of linear codes:

Hamming, Golay, BCH, Reed-Solomon, Reed-Muller ...

Algebraic Geometry codes from algebraic curves over finite fields

Algebraic curves over finite fields

- $\mathcal{X} \subseteq \mathrm{PG}(r, \overline{\mathbb{F}}_q)$: projective, geometrically irreducible, algebraic curve defined over $\mathbb{F}_q$

$$\mathcal{X} : \begin{cases} f_1(X_1, \ldots, X_r) = 0 \\ \quad \vdots \\ f_{r-1}(X_1, \ldots, X_r) = 0 \end{cases} \qquad f_1, \ldots, f_{r-1} \in \mathbb{F}_q[X_1, \ldots, X_r]$$

- $g = g(\mathcal{X})$: (geometric) genus of $\mathcal{X}$
- $\mathcal{X}(\mathbb{F}_q)$: (finite) set of $\mathbb{F}_q$-rational places of $\mathcal{X}$

  If P is a non-singular points of $\mathcal{X}$:

  $\Rightarrow$ there is a unique place of $\mathcal{X}$ centered at P

  If $\mathcal{X}$ is non-singular:

  $\Rightarrow \mathcal{X}(\mathbb{F}_q) = \mathcal{X} \cap \mathrm{PG}(r, q)$: set of $\mathbb{F}_q$-rational points of $\mathcal{X}$

Algebraic Geometric codes: ingredients

- $\mathcal{X}$: $\mathbb{F}_q$-rational curve
- $\mathbb{F}_q(\mathcal{X})$: field of $\mathbb{F}_q$-rational functions over $\mathcal{X}$
  (field of fractions of the coordinate ring of $\mathcal{X}$ over $\mathbb{F}_q$)
- Group of $\mathbb{F}_q$-rational divisors of $\mathcal{X}$: $D = \sum_{P \in \mathcal{X}(\mathbb{F}_q)} n_P P$, $n_P \in \mathbb{Z}$
  (free group generated by the $\mathbb{F}_q$-rational places)
- Principal divisor of $f \in \mathbb{F}_q(\mathcal{X}) \setminus \{0\}$:
  collects zeros and poles of f, counted with multiplicity

$$(f) = (f)_0 - (f)_\infty = \sum_{P\,:\,P \text{ is a zero of } f} v_P P \;-\; \sum_{P\,:\,P \text{ is a pole of } f} (-v_P) P$$

- Riemann-Roch space of the $\mathbb{F}_q$-rational divisor D : $\mathbb{F}_q$-vector space

$$\mathcal{L}(D) = \{ f \in \mathbb{F}_q(\mathcal{X}) \setminus \{0\} \mid (f) + D \geq 0 \} \cup \{0\}$$

Algebraic Geometric codes

- $\mathcal{X}$: $\mathbb{F}_q$-rational curve
- $D = P_1 + \cdots + P_n$ with $P_i \in \mathcal{X}(\mathbb{F}_q)$, $P_i \neq P_j$ for $i \neq j$
- G : another $\mathbb{F}_q$-rational divisor with $P_1, \ldots, P_n \notin \mathrm{supp}(G)$
- $\mathbb{F}_q$-linear evaluation map

$$e_D : \mathcal{L}(G) \to \mathbb{F}_q^n, \quad f \mapsto e_D(f) = (f(P_1), \ldots, f(P_n))$$

- $C_{\mathcal{L}}(D, G) := \mathrm{Im}(e_D)$: (functional) Algebraic Geometric code

Algebraic Geometric codes: parameters

$\mathcal{X}$: $\mathbb{F}_q$-rational curve, $D = \sum_{i=1}^{n} P_i$, $P_i \in \mathcal{X}(\mathbb{F}_q)$ distinct places
G : $\mathbb{F}_q$-rational divisor of $\mathcal{X}$ with $P_i \notin \mathrm{supp}(G)$

$C_{\mathcal{L}}(D, G)$ is an $[n, k, d]_q$-code

- If $\deg(\mathcal{X}) > 2g - 2$, then rel. Singleton defect $\Delta \leq g/n$
  $\Rightarrow$ use curves with many $\mathbb{F}_q$-rat. points w.r.t. $g \Rightarrow \mathbb{F}_q$-maximal curves
- Goppa lower bound on the minimum distance: $d \geq n - \deg(G)$
- Distance: $k = \dim(\mathcal{L}(G)) - \dim(\mathcal{L}(G - D))$
- If $deg(G) < n$, then $k = \dim(\mathcal{L}(G))$

We focus on **one-point** codes: $\mathbf{G = m\,P}$ with $P \in \mathcal{X}(\mathbb{F}_q)$ and $m < n$

Weierstrass semigroup

$g(\mathcal{X}) > 0$, $P \in \mathcal{X}(\mathbb{F}_q)$, $D = \sum_{i=1}^{n} P_i$, $G = mP$, $m < n$, $k = \dim(\mathcal{L}(mP))$

- $\mathcal{L}(mP) = \{f \in \mathbb{F}_q(\mathcal{X}) \mid (f) \geq -mP\}$:
  functions with P as unique pole, with multiplicity at most m
- $H(P) = \{s \geq 0 \mid \exists f \in \mathbb{F}_q(\mathcal{X}) : (f)_\infty = sP\}$
  Weierstrass semigroup at P, set of non-gaps (or pole numbers) at P
- $G(P) = \mathbb{N} \setminus H(P)$ set of gaps at P.
- $|G(P)|$: genus of the semigroup
- Weierstrass Gap Theorem:
  $|G(P)| = g(\mathcal{X})$, $\quad \min(G(P)) = 1$, $\quad \max(G(P)) \leq 2g(\mathcal{X}) - 1$
- $H(P)$ is the same for almost all places P of $\mathcal{X}$
- Weierstrass points : places with Weierstrass semigroup different from the one of almost all other places of $\mathcal{X}$

Weierstrass semigroup and dimension k of the code

$$g(\mathcal{X}) > 0,\ P \in \mathcal{X}(\mathbb{F}_q),\ D = \sum_{i=1}^{n} P_i,\ G = mP,\ m < n,\ k = \dim(\mathcal{L}(mP))$$

$$H(P) = \{\rho_1 = 0 < \rho_2 < \rho_3 < \dots\}$$

$$i > 0, \qquad \dim\mathcal{L}(\ell P) = \begin{cases} \dim\mathcal{L}((\ell-1)P) + 1 & \text{if } \ell \in H(P) \\ \dim\mathcal{L}((\ell-1)P) & \text{if } \ell \in G(P) \end{cases}$$

$$k = |\{\ell \in H(P) : \ell \leq m\}|$$

Weierstrass semigroup $\Rightarrow$ dimension of the code

explicit descrption of $H(P)$, explicit description of $G(P)$,

minimal set of generator, Frobenius number, multiplicity...

Weierstrass semigroup and minimum distance d

$$g(\mathcal{X}) > 0, \quad P \in \mathcal{X}(\mathbb{F}_q), \quad D = \sum_{i=1}^{n} P_i, \quad G : \mathbb{F}_q\text{-rat. div.}, \; P_i \notin \operatorname{supp}(G)$$
$$H(P) = \{\rho_1 = 0 < \rho_2 < \rho_3 < \dots\}$$

$$C_{\mathcal{L}}(D,G)^{\perp} = \left\{x \in \mathbb{F}_q^n \mid \langle x, y\rangle = 0 \; \forall y \in C_{\mathcal{L}}(D,G)\right\}$$ dual code

$$n \perp = n \qquad k^{\perp} = n - k \qquad d^{\perp} \geq ?$$

$$\nu_{\ell} := |\{(i,j) \in \mathbb{N}^2 : \rho_i + \rho_j = \rho_{\ell+1}\}|$$
$$C := C_{\mathcal{L}}(D, \rho_{\ell})^{\perp} \qquad d_{\mathrm{ORD}}(C) := \min\{\nu_m : m \geq \ell\}$$

Order bound:

$$d^{\perp} \geq d_{\mathrm{ORD}}$$

Weierstrass semigroup $\Rightarrow$ minimum distance of the code

Weierstrass semigroups on the Suzuki curve

$s \geq 1, \quad q_0 = 2^s, \quad q = 2q_0^2 = 2^{2s+1}$ Suzuki curve over $\overline{\mathbb{F}}_q$:

$$\mathcal{S}_q : \quad Y^q + Y = X^{q_0}(X^q + X)$$

- $\mathrm{Aut}(\mathcal{S}_q) \cong {}^2B_2(q), \quad g = q_0(q-1), \quad |\mathcal{S}_q(\mathbb{F}_{q^4})| = q^4 + 1 + 2q^2 g$
  $\Rightarrow \mathcal{S}_q$ is $\mathbb{F}_{q^4}$-maximal
- $\mathbb{F}_{q^4}(\mathcal{S}_q) = \mathbb{F}_{q^4}(x,y), \;\; x, y$: coordinate functions
- $P_\infty \in \mathcal{S}_q(\mathbb{F}_q)$: unique point at infinity of $\mathcal{S}_q$
- in $\mathbb{F}_{q^4}(\mathcal{S}_q)$: $\quad x, \quad y, \quad v := y^{2q_0} + x^{2q_0+1}, \quad w := y^{2q_0}x + v^{2q_0}$
- $H(P_\infty) = \langle\, q, \quad q+q_0, \quad q+2q_0, \quad q+2q_0+1 \,\rangle$ (Matthews 2004)
  $\Rightarrow H(P) = H(P_\infty) \; \forall P \in \mathcal{S}_q(\mathbb{F}_q)$, as $\mathcal{S}_q(\mathbb{F}_q)$ is an orbit of $\mathrm{Aut}(\mathcal{S}_q)$
- for $P \in \mathcal{S}_q \setminus \mathcal{S}_q(\mathbb{F}_q)$: $H(P) = ?$

Weierstrass semigroups on the Suzuki curve

$$\mathcal{S}_q: \quad Y^q + Y = X^{q_0}(X^q + X)$$

- $\{$Weierstrass points of $\mathcal{S}_q\} = \mathcal{S}_q(\mathbb{F}_q)$ (Fuhrmann-Torres 1998)
  $\Rightarrow H(P)$ is the same for all $P \in \mathcal{S}_q \setminus \mathcal{S}_q(\mathbb{F}_q)$
  $\Rightarrow$ let $P = (a, b) \in \mathcal{S}_q(\mathbb{F}_{q^4}) \setminus \mathcal{S}_q(\mathbb{F}_q)$
- $\Phi : P \mapsto P^q$ Frobenius map on the places of $\mathcal{S}_q$
- there exists $f_P \in \overline{\mathbb{F}}_q(\mathcal{S}_q)$ such that

$$(f_P) = qP + 2q_0\Phi(P) + \Phi^2(P) - (q + 2q_0 + 1)P_\infty$$

$$\Rightarrow \ (f_{\Phi(P)}) = q\Phi(P) + 2q_0\Phi^2(P) + \Phi^3(P) - (q + 2q_0 + 1)P_\infty,$$
$$(f_P) = q\Phi^2(P) + 2q_0\Phi^3(P) + P - (q + 2q_0 + 1)P_\infty,$$
$$(f_P) = q\Phi^3(P) + 2q_0 P + \Phi(P) - (q + 2q_0 + 1)P_\infty.$$

- rational function t_P associated to the tangent line to $\mathcal{S}_q$ at P:
  $(t_P) = q_0 P + \Phi(P) + E - (q + q_0)P_\infty$ with $E \geq 0$, $P_\infty, \Phi^i(P) \notin \mathrm{supp}(E)$

Weierstrass semigroups on the Suzuki curve

$$\mathcal{S}_q : \quad Y^q + Y = X^{q_0}(X^q + X)$$

with suitable $h, i, j, k, \ell \tilde{i}, \tilde{h} \in \mathbb{N}$, $H(P)$ is given by the multiplicities at P of

$$\left(f^{i}_{\Phi(P)} \cdot f^{j}_{\Phi^2(P)} \cdot f^{k}_{\Phi^3(P)} \cdot t^{\ell}_{P} \right) \, / \, f^{h}_{P}\,, \qquad \left(f^{\tilde{i}}_{\Phi(P)} \cdot f^{\tilde{h}-q_0}_{\Phi^3(P)} \right) \, / \, \left(f^{\tilde{h}}_{P} \cdot f_{\Phi^2(P)} \right)$$

Theorem

$P \in \mathcal{S}_q \setminus \mathcal{S}_q(\mathbb{F}_q)$, minimal set of generator for $H(P)$:

$$\left\{ hq - kq_0 - \lfloor (2h-k-2)/2 \rfloor \ : \ h \in \{1, \ldots, q_0\}, k \in \{0, \ldots, 2h-2\} \right\}$$

$$\cup \quad \left\{ hq - (2(h-q_0)-1)q_0 - (q_0 - 1) \ : \ h \in \{q_0+1, \ldots, 2q_0\} \right\}$$

Application to the parameters of $C_{\mathcal{L}}(D, mP)$ and $C_{\mathcal{L}}(D, mP)^{\perp}$

with $D = \mathcal{S}_q(\mathbb{F}_{q^4}) \setminus \{P\} \Rightarrow$ get examples of good codes generalization:

$\mathcal{X}$: curve over $\mathbb{F}_q$, $P_1, \ldots, P_t$: distinct $\mathbb{F}_q$-rational places of $\mathcal{X}$

$H(P_1, \ldots, P_t)$: Weierstrass semigroup at $(P_1, \ldots, P_t)$:

$$\left\{(s_1, \ldots, s_t) \in \mathbb{N}^t \mid \exists f \in \mathbb{F}_q(\mathcal{X}) : (f)_\infty = s_1 P_1 + \cdots + s_t \in P_t\right\}$$

- Gaps at $(P_1, \ldots, P_t)$: $G(P_1, \ldots, P_t) = \mathbb{N}^t \setminus H(P_1, \ldots, P_t)$

$G(P_1, \ldots, P_t) = \{(s_1, \ldots, s_t) \in \mathbb{N}^t$ such that
$\dim \mathcal{L}\left(\sum_{i=1}^t s_i P_i\right) = \dim \mathcal{L}\left(\left(\sum_{i=1}^t s_i P_i\right) - P_j\right.$ for some $\left. j \in \{1, \ldots, t\}\right\}$

- Pure gaps at $(P_1, \ldots, P_t)$: $G_0(P_1, \ldots, P_t) = \{(s_1, \ldots, s_t) \in \mathbb{N}^t$ s.t.
$\dim \mathcal{L}\left(\sum_{i=1}^t s_i P_i\right) = \dim \mathcal{L}\left(\left(\sum_{i=1}^t s_i P_i\right) - P_j\right.$ for all $\left. j \in \{1, \ldots, t\}\right\}$

Pure gaps give better lower bounds on the minimum distance of
$C_{\mathcal{L}}(D, n_1 P_1 + \cdots + n_t P_t)$

Thank you for your attention!