Weierstrass semigroups, Pure gaps, and Codes on Function Fields

Erik A. R. Mendoza

IMECC - UNICAMP

June 16, 2023

Joint work with Alonso S. Castellanos and Luciane Quoos

EnCoRI 2023 - Encontro de Códigos Reticulados e Informação

Notation and preliminaries

- $\mathbb{F}_q$: finite field with q elements.
- K: algebraic closure of $\mathbb{F}_q$.
- $F/\mathbb{F}_q$: function field with full constant field $\mathbb{F}_q$ of genus g.
- $P_1, \ldots, P_N$: pairwise distinct rational places in $F/\mathbb{F}_q$.
- $D := P_1 + \cdots + P_N$.
- G: divisor of F such that $\mathrm{Supp}(D) \cap \mathrm{Supp}(G) = \emptyset$.

Algebraic Geometry Codes

Linear AG code:

$$C_{\mathcal{L}}(D, G) = \{(f(P_1), \ldots, f(P_N)) : f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^N.$$

Differential AG code:

$$C_{\Omega}(D, G) = \{(\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_N}(\omega)) : \omega \in \Omega(G - D)\} \subseteq \mathbb{F}_q^N.$$

Algebraic Geometry Codes

Linear AG code:

$$C_{\mathcal{L}}(D, G) = \{(f(P_1), \ldots, f(P_N)) : f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^N.$$

Differential AG code:

$$C_{\Omega}(D, G) = \{(\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_N}(\omega)) : \omega \in \Omega(G - D)\} \subseteq \mathbb{F}_q^N.$$

- The parameters of these codes are: N is the length of the code, k is its dimension over $\mathbb{F}_q$, and d is its minimum distance. We say that the code is an $[N, k, d]$-code.
- If $C_{\mathcal{L}}(D, G)$ (resp. $C_{\Omega}(D, G)$) is an $[N, k, d]$-code (resp. an $[N, k_\Omega, d_\Omega]$-code) then

$$d \geq N - \deg(G) \quad \text{and} \quad d_\Omega \geq \deg(G) - (2g - 2).$$

Weierstrass Semigroups and Pure Gaps

Definition

For a rational place P in F, the Weierstrass semigroup at P is defined by

$$H(P) = \{s \in \mathbb{N} : (z)_\infty = sP \text{ for some } z \in F\}.$$

The complement set $G(P) := \mathbb{N} \setminus H(P)$ is called the gap set at P.

Weierstrass Semigroups and Pure Gaps

Definition

For a rational place P in F, the Weierstrass semigroup at P is defined by

$$H(P) = \{s \in \mathbb{N} : (z)_\infty = sP \text{ for some } z \in F\}.$$

The complement set $G(P) := \mathbb{N} \setminus H(P)$ is called the gap set at P.

Analogously, the Weierstrass semigroup at two distinct rational places P_1, P_2 in F is defined by

$$H(P_1, P_2) = \{(s_1, s_2) \in \mathbb{N}^2 : (z)_\infty = s_1P_1 + s_2P_2 \text{ for some } z \in F\}.$$

Weierstrass Semigroups and Pure Gaps

Definition

For a rational place P in F, the Weierstrass semigroup at P is defined by

$$H(P) = \{s \in \mathbb{N} : (z)_\infty = sP \text{ for some } z \in F\}.$$

The complement set $G(P) := \mathbb{N} \setminus H(P)$ is called the gap set at P.

Analogously, the Weierstrass semigroup at two distinct rational places P_1, P_2 in F is defined by

$$H(P_1, P_2) = \{(s_1, s_2) \in \mathbb{N}^2 : (z)_\infty = s_1P_1 + s_2P_2 \text{ for some } z \in F\}.$$

The elements of the gap set $G(P_1, P_2) := \mathbb{N}^2 \setminus H(P_1, P_2)$ can be characterized as follows:

$$(s_1, s_2) \in G(P_1, P_2) \Leftrightarrow \ell(s_1P_1 + s_2P_2) = \ell(s_1P_1 + s_2P_2 - P_j) \text{ for some } j \in \{1, 2\}.$$

Definition

A pair $(s_1, s_2) \in G(P_1, P_2)$ is called a pure gap at P_1, P_2 if

$$\ell(s_1P_1 + s_2P_2) = \ell(s_1P_1 + s_2P_2 - P_j) \text{ for each } j \in \{1, 2\}.$$

The set of pure gaps at P_1, P_2 is denoted by $G_0(P_1, P_2)$.

Definition

A pair $(s_1, s_2) \in G(P_1, P_2)$ is called a pure gap at P_1, P_2 if

$$\ell(s_1P_1 + s_2P_2) = \ell(s_1P_1 + s_2P_2 - P_j) \text{ for each } j \in \{1, 2\}.$$

The set of pure gaps at P_1, P_2 is denoted by $G_0(P_1, P_2)$.

Consider the bijective map

$$\begin{array}{rccc} \tau_{P_1,P_2}: & G(P_1) & \to & G(P_2) \\ & \beta & \mapsto & \min\{\gamma \in \mathbb{N}_0 : (\beta, \gamma) \in H(P_1, P_2)\} \end{array}$$

The graph of τ_{P_1,P_2} given by

$$\Gamma(P_1, P_2) := \{(\beta, \tau_{P_1,P_2}(\beta)) : \beta \in G(P_1)\}$$

is called the minimal generating set of $H(P_1, P_2)$.

For $\mathbf{x} = (x_1, x_2)$ and $\mathbf{y} = (y_1, y_2)$, define

$$\mathrm{lub}(\mathbf{x}, \mathbf{y}) = (\max\{x_1, y_1\}, \max\{x_2, y_2\}) \quad \text{and} \quad \mathrm{glb}(\mathbf{x}, \mathbf{y}) = (\min\{x_1, y_1\}, \min\{x_2, y_2\}).$$

For $\mathbf{x} = (x_1, x_2)$ and $\mathbf{y} = (y_1, y_2)$, define

$$\mathrm{lub}(\mathbf{x}, \mathbf{y}) = (\max\{x_1, y_1\}, \max\{x_2, y_2\}) \quad \text{and} \quad \mathrm{glb}(\mathbf{x}, \mathbf{y}) = (\min\{x_1, y_1\}, \min\{x_2, y_2\}).$$

Lemma [Kim (1994)]

Let P_1 and P_2 be two distinct rational places in F. Then

$$H(P_1, P_2) = \{\mathrm{lub}(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \Gamma(P_1, P_2) \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2))\}.$$

For $\mathbf{x} = (x_1, x_2)$ and $\mathbf{y} = (y_1, y_2)$, define

$$\mathrm{lub}(\mathbf{x}, \mathbf{y}) = (\max\{x_1, y_1\}, \max\{x_2, y_2\}) \quad \text{and} \quad \mathrm{glb}(\mathbf{x}, \mathbf{y}) = (\min\{x_1, y_1\}, \min\{x_2, y_2\}).$$

Lemma [Kim (1994)]

Let P_1 and P_2 be two distinct rational places in F. Then

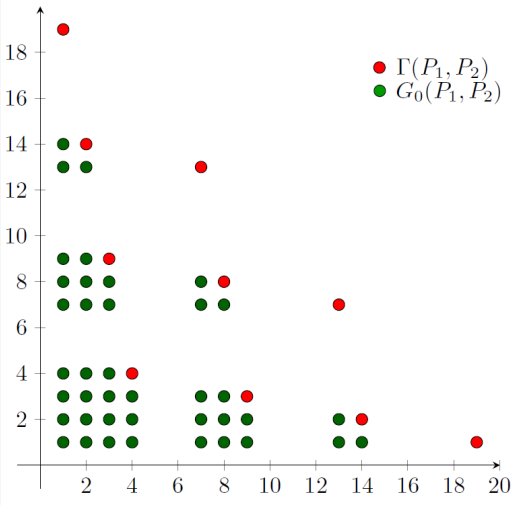
$$H(P_1, P_2) = \{\mathrm{lub}(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \Gamma(P_1, P_2) \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2))\}.$$

Proposition [Castellanos, - , and Quoos (2023)]

Let P_1 and P_2 be two distinct rational places in F. Then

$$G_0(P_1, P_2) = \{\mathrm{glb}(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \Gamma(P_1, P_2)\} \setminus \Gamma(P_1, P_2).$$

Example: Hermitian curve $y^6 = x^5 + x$.



Theorem [García, Kim, and Lax (1993)]

Suppose that $\gamma - t, \gamma - t + 1, \ldots, \gamma - 1, \gamma$ is a sequence of $t + 1$ consecutive gaps at a rational place Q. Let $G = \gamma Q$ and $D = P_1 + P_2 + \cdots + P_N$, where P_i is a rational place not in the support of G for each $i = 1, \ldots, N$. If the code $C_{\mathcal{L}}(D, G)$ has positive dimension, then

$$d \geq N - \deg(G) + t + 1.$$

Theorem [García, Kim, and Lax (1993)]

Suppose that $\gamma - t, \gamma - t + 1, \ldots, \gamma - 1, \gamma$ is a sequence of $t + 1$ consecutive gaps at a rational place Q. Let $G = \gamma Q$ and $D = P_1 + P_2 + \cdots + P_N$, where P_i is a rational place not in the support of G for each $i = 1, \ldots, N$. If the code $C_{\mathcal{L}}(D, G)$ has positive dimension, then

$$d \geq N - \deg(G) + t + 1.$$

Theorem [Homma and Kim (2001)]

Let $P_1, \ldots, P_N, Q_1, Q_2$ be pairwise distinct rational places on $F/\mathbb{F}_q$. Let $(\alpha_1, \alpha_2), (\beta_1, \beta_2)$ in $\mathbb{N}^2$ be such that $\alpha_i \leq \beta_i$ for $i = 1, 2$. Suppose each pair (γ_1, γ_2) with $\alpha_i \leq \gamma_i \leq \beta_i$ for $i = 1, 2$ is a pure gap at Q_1, Q_2. Consider the divisors $D = P_1 + \cdots + P_N$ and $G = \sum_{i=1}^{2} (\alpha_i + \beta_i - 1) Q_i$. Then the minimum distance d_Ω of the code $C_\Omega(D, G)$ satisfies

$$d_\Omega \geq \deg(G) - (2g - 2) + \textstyle\sum_{i=1}^{2} (\beta_i - \alpha_i) + 2.$$

Kummer extensions

Consider the curve $\mathcal{X}$ defined by the affine equation

$$\mathcal{X}: \quad y^m = \prod_{i=1}^{r}(x-\alpha_i)^{\lambda_i}, \quad \lambda_i \in \mathbb{N}, \quad 1 \leq \lambda_i < m \quad \text{and} \quad p \nmid m,$$

where $m \geq 2$, $\alpha_1, \ldots, \alpha_r \in K$ are pairwise distinct elements, $\lambda_0 := \sum_{i=1}^{r} \lambda_i$, and $(m, \lambda_0) = 1$. Let $K(\mathcal{X})$ be its function field. Then $K(\mathcal{X})/K(x)$ is a Kummer extension with one place at infinity Q_∞. If $(m, \lambda_i) = 1$, we denote by Q_i the only place in $K(\mathcal{X})$ corresponding to $x = \alpha_i$.

Kummer extensions

Consider the curve $\mathcal{X}$ defined by the affine equation

$$\mathcal{X}: \quad y^m = \prod_{i=1}^{r}(x-\alpha_i)^{\lambda_i}, \quad \lambda_i \in \mathbb{N}, \quad 1 \leq \lambda_i < m \quad \text{and} \quad p \nmid m,$$

where $m \geq 2$, $\alpha_1, \ldots, \alpha_r \in K$ are pairwise distinct elements, $\lambda_0 := \sum_{i=1}^{r} \lambda_i$, and $(m, \lambda_0) = 1$. Let $K(\mathcal{X})$ be its function field. Then $K(\mathcal{X})/K(x)$ is a Kummer extension with one place at infinity Q_∞. If $(m, \lambda_i) = 1$, we denote by Q_i the only place in $K(\mathcal{X})$ corresponding to $x = \alpha_i$.

Proposition

Suppose that $\lambda_1 = \lambda_2 = \cdots = \lambda_r$ and let Q be a totally ramified place in $K(\mathcal{X})/K(x)$ such that $Q \neq Q_\infty$. Then

$$G(Q) = \left\{ mj - i : 1 \leq j \leq r-1, \ \left\lfloor \frac{jm}{r} \right\rfloor + 1 \leq i \leq m-1 \right\}.$$

Proposition

Suppose that $\lambda_{\ell_1} = \lambda_{\ell_2}$ and $(m, \lambda_{\ell_1}) = 1$ for some $1 \leq \ell_1, \ell_2 \leq r$. Let λ be the inverse of λ_{ℓ_1} modulo m. Then

$$\Gamma(Q_{\ell_1}, Q_{\ell_2}) = \left\{ (i + mj_1, i + mj_2) : 1 \leq i < m,\ j_1, j_2 \geq 0,\ j_1 + j_2 = \sum_{k=1}^{r} \left\lceil \frac{i\lambda\lambda_k}{m} \right\rceil - \left\lceil \frac{i\lambda\lambda_0}{m} \right\rceil - 1 \right\}.$$

Proposition

Suppose that $\lambda_\ell = 1$ for some $1 \leq \ell \leq r$. Then

$$\Gamma(Q_\infty, Q_\ell) = \left\{ (mj_1 - i\lambda_0, i + mj_2) : 1 \leq i < m,\ j_1 \geq \left\lceil \frac{i\lambda_0}{m} \right\rceil,\ j_2 \geq 0,\ j_1 + j_2 = \sum_{k=1}^{r} \left\lceil \frac{i\lambda_k}{m} \right\rceil - 1 \right\}.$$

One-point AG codes

Theorem [Castellanos, - , and Quoos (2023)]

Suppose that $\lambda_1 = \cdots = \lambda_r$ and let Q be a totally ramified place in the extension $\mathbb{F}_q(\mathcal{X})/\mathbb{F}_q(x)$ such that $Q \neq Q_\infty$. For $a \in \{1, \ldots, r-1\}$, define the divisors

$$G_a := (am - \lfloor am/r \rfloor - 1)\, Q \quad \text{and} \quad D := \sum_{Q' \in \mathcal{X}(\mathbb{F}_q), Q' \neq Q} Q'$$

and assume that $\deg(G_a) < N := \deg(D)$. Then the AG code $C_{\mathcal{L}}(D, G_a)$ has parameters

$$\left[N, a + \sum_{i=1}^{a-1} \left\lfloor \frac{im}{r} \right\rfloor, d \geq N - m(a-1) \right].$$

Also, if $\#\{\gamma \in \mathbb{F}_q : P_\gamma \text{ splits completely in } \mathbb{F}_q(\mathcal{X})/\mathbb{F}_q(x)\} > a$, then $d = N - m(a-1)$.

Examples:

- Let n be an odd integer. Consider the $\mathbb{F}_{q^{2n}}$-maximal curve $y^{q^n+1} = x^q + x$. For $1 \leq a \leq q-1$, we have one-point AG codes over $\mathbb{F}_{q^{2n}}$ with parameters

$$\left[q^{2n+1}, a + \frac{a(a-1)q^{n-1}}{2}, q^{2n+1} - (q^n+1)(a-1)\right].$$

Examples:

- Let n be an odd integer. Consider the $\mathbb{F}_{q^{2n}}$-maximal curve $y^{q^n+1} = x^q + x$. For $1 \leq a \leq q-1$, we have one-point AG codes over $\mathbb{F}_{q^{2n}}$ with parameters

$$\left[q^{2n+1}, a + \frac{a(a-1)q^{n-1}}{2}, q^{2n+1} - (q^n+1)(a-1)\right].$$

- For $n \geq 2$, consider the Norm-Trace curve $y^{\frac{q^n-1}{q-1}} = x^{q^{n-1}} + x^{q^{n-2}} + \cdots + x$. For each $1 \leq a \leq q^{n-1} - 1$, we obtain one-point AG codes over $\mathbb{F}_{q^n}$ with parameters

$$\left[q^{2n-1}, \frac{a(a+1)}{2} + \sum_{i=1}^{a-1} \left\lfloor \frac{i(q^{n-1}-1)}{q^{n-1}(q-1)} \right\rfloor, q^{2n-1} - \frac{(a-1)(q^n-1)}{q-1}\right].$$

Two-point AG Codes

Example: For $q \geq 4$ even and $n \geq 3$ odd, consider the subcover of the BM curve given by

$$\mathcal{Y}_{q^n+1}: \quad y^{q^n+1} = x(x+1)\left(\frac{x^{q-1}+1}{x+1}\right)^{q+1}.$$

Let Q be a totally ramified place such that $Q \neq Q_\infty$. By previous results, we can determine the sets $\Gamma(Q_\infty, Q)$ and $G_0(Q_\infty, Q)$. Using Homma and Kim's theorem we get:

Two-point AG Codes

Example: For $q \geq 4$ even and $n \geq 3$ odd, consider the subcover of the BM curve given by

$$\mathcal{Y}_{q^n+1}: \quad y^{q^n+1} = x(x+1)\left(\frac{x^{q-1}+1}{x+1}\right)^{q+1}.$$

Let Q be a totally ramified place such that $Q \neq Q_\infty$. By previous results, we can determine the sets $\Gamma(Q_\infty, Q)$ and $G_0(Q_\infty, Q)$. Using Homma and Kim's theorem we get:

Proposition

For $\lfloor (q^{n+2} - 2q^{n+1} - q^3 + q^2 + 1)/(2q^3 - 3q - 1) \rfloor + 1 \leq a \leq (q^n - 2q - 1)/(q+1)$ it exists a $[N, k, d]$-code over $\mathbb{F}_{q^{2n}}$ with

$$N = q^{2n+1} - q^{n+2} + 2q^{n+1} - 1,$$
$$k = q^{2n+1} - q^{n+2} + (5q^{n+2} + q^n - q^3 + q^2 - 2q + 2)/(2q+2) - a(2q^2 - 2q - 1), \text{ and}$$
$$d \geq 2a(q^2 - q - 1) - q^2(q^n - 2q^{n-1} - q^{n-2} - q + 1)/(q+1).$$

References

- Goppa, V. D. (1977). Codes associated with divisors. Problemy Peredachi Informatsii, 13(1), 33-39.
- Garcia, A., Kim, S. J., & Lax, R. F. (1993). Consecutive Weierstrass gaps and minimum distance of Goppa codes. Journal of pure and applied algebra, 84(2), 199-207.
- Kim, S. J. (1994). On the index of the Weierstrass semigroup of a pair of points on a curve. Archiv der Mathematik, 62(1), 73-82.
- Homma, M., & Kim, S. J. (2001). Goppa codes with Weierstrass pairs. Journal of Pure and Applied Algebra, 162(2-3), 273-290.
- Castellanos, A. S., Mendoza, E. A., & Quoos, L. (2023). Weierstrass Semigroup, Pure Gaps and Codes on Function Fields. ArXiv:2304.02128.