Some remarks on the asymptotic behavior of cyclic AG-codes

R. Toledano[1]

Facultad de Ingeniería Química - Univ. Nacional del Litoral

CLA 2016

[1] Joint work with M. Chara and R. Podestá

Linear codes

- A **linear code** $\mathcal{C}$ (over the alphabet $\mathbb{F}_q$) of **length** n is a linear subspace of $\mathbb{F}_q^n$. The elements of $\mathcal{C}$ are usually called **codewords**.

- If $k = \dim \mathcal{C}$ is the **dimension** of the code (as a vector space over $\mathbb{F}_q$) and

$$d = \min\{d(c, c') : c, c' \in \mathcal{C}, c \neq c'\}$$

is the **minimum distance** of $\mathcal{C}$, where d is the Hamming distance in $\mathbb{F}_q^n$, we shall say that $\mathcal{C}$ is an $[n, k, d]-$code.

- There is a natural action of the permutation group $\mathbb{S}_n$ on $\mathbb{F}_q^n$ given by

$$\pi \cdot (v_1, \ldots, v_n) = (v_{\pi(1)}, \ldots, v_{\pi(n)})$$

where $\pi \in \mathbb{S}_n$ and $(v_1, \ldots, v_n) \in \mathbb{F}_q^n$.

- The set of all $\pi \in \mathbb{S}_n$ such that $\pi \cdot c \in \mathcal{C}$ for all codewords c of $\mathcal{C}$ forms a subgroup $\mathrm{Perm}(\mathcal{C})$ of $\mathbb{S}_n$ which is called the **permutation group of $\mathcal{C}$**:

$$\mathrm{Perm}(\mathcal{C}) = \{\pi \in \mathbb{S}_n : \pi(\mathcal{C}) = \mathcal{C}\}.$$

Transitive and cyclic codes

Let $c = (c_1, \ldots, c_{n-1}, c_n)$ a codeword in $\mathcal{C}$.

- $\mathcal{C}$ is **transitive** if $\mathrm{Perm}(\mathcal{C})$ acts transitively on C, i.e. if for any $1 \leq i < j \leq n$ there is a $\pi \in \mathbb{S}_n$ such that $\pi(i) = j$.

- $\mathcal{C}$ is **cyclic** if it is invariant under the action of the cyclic shift $s \in \mathbb{S}_n$ defined as $s(1) = n$ and $s(i) = i - 1$ for $i = 2, \ldots, n$, i.e. if

$$s \cdot c = (c_n, c_1, \ldots, c_{n-1}) \in \mathcal{C}$$

  for every $c \in \mathcal{C}$.

Transitive and cyclic codes

Let $c = (c_1, \ldots, c_{n-1}, c_n)$ a codeword in $\mathcal{C}$.

- $\mathcal{C}$ is **transitive** if $\mathrm{Perm}(\mathcal{C})$ acts transitively on C, i.e. if for any $1 \leq i < j \leq n$ there is a $\pi \in \mathbb{S}_n$ such that $\pi(i) = j$.

- $\mathcal{C}$ is **cyclic** if it is invariant under the action of the cyclic shift $s \in \mathbb{S}_n$ defined as $s(1) = n$ and $s(i) = i - 1$ for $i = 2, \ldots, n$, i.e. if

$$s \cdot c = (c_n, c_1, \ldots, c_{n-1}) \in \mathcal{C}$$

  for every $c \in \mathcal{C}$.

Cycic codes are transitive codes

AG-codes

- Let F be an algebraic function field over $\mathbb{F}_q$, i.e. a finite extension of a rational function field $\mathbb{F}_q(x)$.
- Let D and G be disjoint divisors of F, with $D = P_1 + \cdots + P_n$ where $P_1, \ldots, P_n$ are different rational places.
- Let $\mathcal{L}(G)$ be the Riemann-Roch space associated to G

$$\mathcal{L}(G) = \{x \in F : (x) \geq -G\} \cup \{0\}$$

where (x) denotes the principal divisor associated to $x \in F$.

The AG-code defined by F, D and G is

$$\mathcal{C}(D, G) = \{(x(P_1), \ldots, x(P_n)) \in \mathbb{F}_q^n : x \in \mathcal{L}(G)\}$$

where $x(P_i)$ stands for the residue class of x modulo P_i.

Cyclic AG-codes

An AG-code $C_{\mathcal{L}}(D, G)$ with $D = P_1 + \cdots + P_n$ is cyclic if for any codeword

$$(x(P_1), \ldots x(P_n)) \in C_{\mathcal{L}}(D, G),$$

where $x \in \mathcal{L}(G)$, we have that

$$(x(P_n), x(P_1), \ldots x(P_{n-1})) \in C_{\mathcal{L}}(D, G).$$

Cyclic AG-codes

An AG-code $C_{\mathcal{L}}(D, G)$ with $D = P_1 + \cdots + P_n$ is cyclic if for any codeword

$$(x(P_1), \ldots x(P_n)) \in C_{\mathcal{L}}(D, G),$$

where $x \in \mathcal{L}(G)$, we have that

$$(x(P_n), x(P_1), \ldots x(P_{n-1})) \in C_{\mathcal{L}}(D, G).$$

This happens if and only if there exists $z \in \mathcal{L}(G)$ such that

$$\begin{array}{rcl} z(P_1) & = & x(P_n)\,, \\ z(P_2) & = & x(P_1)\,, \\ & \vdots & \\ z(P_n) & = & x(P_{n-1})\,. \end{array} \tag{1}$$

Cyclic AG-codes

An AG-code $C_{\mathcal{L}}(D, G)$ with $D = P_1 + \cdots + P_n$ is cyclic if for any codeword

$$(x(P_1), \ldots x(P_n)) \in C_{\mathcal{L}}(D, G),$$

where $x \in \mathcal{L}(G)$, we have that

$$(x(P_n), x(P_1), \ldots x(P_{n-1})) \in C_{\mathcal{L}}(D, G).$$

This happens if and only if there exists $z \in \mathcal{L}(G)$ such that

$$\begin{array}{rcl} z(P_1) & = & x(P_n)\,, \\ z(P_2) & = & x(P_1)\,, \\ & \vdots & \\ z(P_n) & = & x(P_{n-1})\,. \end{array} \tag{1}$$

The existence of such an element $z \in \mathcal{L}(G)$ is a crucial question to answer in the theory of cyclic AG-codes.

Let E/F a finite cyclic extension of the function field $\mathbb{F}_q$ and $\mathcal{C}$ an AG-code such that

- every place in $\mathrm{Sup}(D) = \{P_1, \ldots, P_n\} \subset \mathbb{P}(E)$ lies over a unique place P of F;
- there is an element $\sigma \in \mathrm{Aut}(E/\mathbb{F}_q(x))$ such that

$$\sigma(G) = G \quad \text{and} \quad \sigma(P_i) = P_{i-1 \bmod n},$$

for $i = 1, \ldots, n$.

Let E/F a finite cyclic extension of the function field $\mathbb{F}_q$ and $\mathcal{C}$ an AG-code such that

- every place in $\mathrm{Sup}(D) = \{P_1, \ldots, P_n\} \subset \mathbb{P}(E)$ lies over a unique place P of F;
- there is an element $\sigma \in \mathrm{Aut}(E/\mathbb{F}_q(x))$ such that

$$\sigma(G) = G \quad \text{and} \quad \sigma(P_i) = P_{i-1 \bmod n},$$

for $i = 1, \ldots, n$.

$\mathcal{C}$ is a cyclic code

Let E/F a finite cyclic extension of the function field $\mathbb{F}_q$ and $\mathcal{C}$ an AG-code such that

- every place in $\mathrm{Sup}(D) = \{P_1, \ldots, P_n\} \subset \mathbb{P}(E)$ lies over a unique place P of F;
- there is an element $\sigma \in \mathrm{Aut}(E/\mathbb{F}_q(x))$ such that

$$\sigma(G) = G \quad \text{and} \quad \sigma(P_i) = P_{i-1 \bmod n},$$

for $i = 1, \ldots, n$.

$\mathcal{C}$ is a cyclic code

Take $z = \sigma^{-1}(x)$.

Cyclic AG-codes and cyclic extension

The previous situation can happen only in the presence of cyclic extensions:

Proposition

Let F be a function field over $\mathbb{F}_q$ and let $P_1, \ldots, P_n$ be n different places of F. Suppose there exists $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q(x))$ such that $\sigma(P_1) = P_n, \sigma(P_2) = P_1, \ldots, \sigma(P_n) = P_{n-1}$. Then there exist an intermediate field $\mathbb{F}_q(x) \subset E \subset F$ and a place P of E such that F/E is a cyclic extension of degree m divisible by n, and P decomposes exactly in F into the places $P_1, \ldots, P_n$ with $e(P_i|P)f(P_i|P) = \frac{m}{n}$ for $i = 1, \ldots, n$.

Cyclic AG-codes and cyclic extension

The previous situation can happen only in the presence of cyclic extensions:

Proposition

Let F be a function field over $\mathbb{F}_q$ and let $P_1, \ldots, P_n$ be n different places of F. Suppose there exists $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q(x))$ such that $\sigma(P_1) = P_n, \sigma(P_2) = P_1, \ldots, \sigma(P_n) = P_{n-1}$. Then there exist an intermediate field $\mathbb{F}_q(x) \subset E \subset F$ and a place P of E such that F/E is a cyclic extension of degree m divisible by n, and P decomposes exactly in F into the places $P_1, \ldots, P_n$ with $e(P_i|P)f(P_i|P) = \frac{m}{n}$ for $i = 1, \ldots, n$.

Conversely, let F/E be a cyclic extension of function fields over $\mathbb{F}_q$ of degree m. Let P be a place of E and let $P_1, \ldots, P_n$ be all the places of F lying over P. Then, m is divisible by n and we have that $\sigma(P_1) = P_n, \sigma(P_2) = P_1, \ldots, \sigma(P_n) = P_{n-1}$ for any generator σ of $\mathrm{Gal}(F/E)$.

Towers of function fields

A sequence $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ of function fields over $\mathbb{F}_q$ is called a tower if

- $F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_i \subsetneq \cdots$;
- F_{i+1}/F_i finite and separable, $i \geq 0$;
- $\mathbb{F}_q$ is the full constant field of F_i, $i \geq 0$.
- $g(F_i) \to \infty$ for $i \to \infty$

Towers of function fields

A sequence $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ of function fields over $\mathbb{F}_q$ is called a tower if

- $F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_i \subsetneq \cdots$;
- F_{i+1}/F_i finite and separable, $i \geq 0$;
- $\mathbb{F}_q$ is the full constant field of F_i, $i \geq 0$.
- $g(F_i) \to \infty$ for $i \to \infty$

The limit of the tower is defined by

$$\lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)} \geq 0.$$

Towers of function fields

A sequence $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ of function fields over $\mathbb{F}_q$ is called a tower if

- $F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_i \subsetneq \cdots$;
- F_{i+1}/F_i finite and separable, $i \geq 0$;
- $\mathbb{F}_q$ is the full constant field of F_i, $i \geq 0$.
- $g(F_i) \to \infty$ for $i \to \infty$

The limit of the tower is defined by

$$\lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)} \geq 0.$$

The tower is asymptotically good if $\lambda(\mathcal{F}) > 0$.

Theorem

Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ *be an asymptotically good tower of function fields over* $\mathbb{F}_q$ *where* $F_0 = \mathbb{F}_q(x)$ *is a rational function field. For each* $i \in \mathbb{N}$*, let* n_i *be a positive integer and let* $P_1, \ldots, P_{n_i}$ *be different rational places of* F_i*. Suppose that for each* $i \in \mathbb{N}$ *there is an element* $\sigma_i \in \mathrm{Aut}(F_i/F_0)$ *such that*

$$\sigma(P_1) = P_{n_i},\ \sigma(P_2) = P_1,\ \ldots,\ \sigma(P_{n_i}) = P_{n_i-1}.$$

Then $n_i < [F_i : F_0]$ *and there exists a place* $P \in \mathrm{Ram}(\mathcal{F})$ *such that* $P_1, \ldots, P_{n_i}$ *are all the places of* F_i *lying over* P*.*

Theorem

Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be an asymptotically good tower of function fields over $\mathbb{F}_q$ where $F_0 = \mathbb{F}_q(x)$ is a rational function field. For each $i \in \mathbb{N}$, let n_i be a positive integer and let $P_1, \ldots, P_{n_i}$ be different rational places of F_i. Suppose that for each $i \in \mathbb{N}$ there is an element $\sigma_i \in \mathrm{Aut}(F_i/F_0)$ such that

$$\sigma(P_1) = P_{n_i},\ \sigma(P_2) = P_1,\ \ldots,\ \sigma(P_{n_i}) = P_{n_i-1}.$$

Then $n_i < [F_i : F_0]$ and there exists a place $P \in \mathrm{Ram}(\mathcal{F})$ such that $P_1, \ldots, P_{n_i}$ are all the places of F_i lying over P.

This theorem shows that the divisor D has to be defined with all the rational places lying over a place in the ramification locus of the tower.

Thanks!