Asymptotically good quasi transitive AG-codes over prime fields

Ricardo A. Podestá

CIEM - CONICET
FaMAF - Universidad Nacional de Córdoba

XXI Coloquio Latinoamericano de Álgebra
Buenos Aires, Julio 25-29, 2016.

Based on the joint work

María Chara, Ricardo Podestá, Ricardo Toledano
Asymptotically good 4-quasi transitive algebraic geometry codes over prime fields, 2016.
arXiv:1603.03398v1 [math.NT]

Summary of the talk

1. Preliminaries on codes
   - Some classes of codes
   - Asymptotic behavior
2. Good AG-codes from sequences of algebraic function fields
   - Constructing good AG-codes from towers
   - Examples over non-prime fields
3. Good 4-quasi transitive AG-codes over prime fields
   - The main result
   - Over prime fields

Linear codes

- A **linear code** of *length* n over a finite field $\mathbb{F}_q$ is $\mathbb{F}_q$-linear subspace $\mathcal{C} \subset \mathbb{F}_q^n$. It is of *dimension* k and *minimum distance* d if $k = \dim \mathcal{C}$ and

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

  where d is the Hamming distance in $\mathbb{F}_q^n$. One says that $\mathcal{C}$ is an $[n, k, d]$-code over $\mathbb{F}_q$.

- The permutation group $\mathbb{S}_n$ acts naturally on $\mathbb{F}_q^n$

$$\mathbb{S}_n \times \mathbb{F}_q^n \to \mathbb{F}_q^n$$
$$\pi \cdot (v_1, \ldots, v_n) = (v_{\pi(1)}, \ldots, v_{\pi(n)})$$

Transitive and cyclic codes

The **permutation group** of a code $\mathcal{C}$ of length n is

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

- $\mathcal{C}$ is **transitive** if $Perm(\mathcal{C})$ acts transitively on $\mathcal{C}$, i.e. if for any $1 \leq i < j \leq n$ there is $\pi \in Perm(\mathcal{C})$ s.t. $\pi(i) = j$.
- $\mathcal{C}$ is **cyclic** if it is invariant by the cyclic shift $\sigma \in \mathbb{S}_n$, i.e.

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

  or in other words, if $\sigma = (12 \cdots n) \in Perm(\mathcal{C})$.
- Thus, cyclic codes are transitive codes.

Quasi transitive codes

- If $n = rm$ we can consider $v \in \mathbb{F}_q^n$ divided into r consecutive m-blocks

$$v = (v_{1,1}, \ldots, v_{1,m}, \ldots, v_{r,1}, \ldots, v_{r,m})$$

  There is a block-by-block action of $\mathbb{S}_m$ on $\mathbb{F}_q^n$ given by

$$\pi \cdot v = (v_{1,\pi(1)}, \ldots, v_{1,\pi(m)}, \ldots, v_{r,\pi(1)}, \ldots, v_{r,\pi(m)})$$

- The *r-permutation group* of $\mathcal{C}$ is

$$Perm_r(\mathcal{C}) = \{\pi \in \mathbb{S}_m \,:\, \pi(\mathcal{C}) = \mathcal{C}\}$$

- A code $\mathcal{C}$ is called r-**quasi transitive** if $Perm_r(\mathcal{C})$ acts transitively on each of the r blocks of every $c \in \mathcal{C}$.
- Note that 1-quasi transitive codes are just the transitive codes.

AG-codes: ingredients

- Let F be an algebraic function field over $\mathbb{F}_q$.
- Let $D = P_1 + \cdots + P_n$ and G be disjoints divisors of F, where $P_1, \ldots, P_n$ are different *rational* places.
- The Riemann-Roch space associated to G

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

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

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

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

AG-codes: parameters

- We have
$$d \geq n - \deg G$$
and $k = \dim \mathcal{L}(G) - \dim \mathcal{L}(D - G)$.

- If $\deg G < n$ then, by Riemann-Roch,
$$k = \dim \mathcal{L}(G) \geq \deg G + 1 - g$$
where g is the genus of F.

- If also $2g - 2 < \deg G$ then $k = \deg G + 1 - g$.

Asymptotically good codes

- The *information rate* and *relative minimum distance* of an $[n, k, d]$-code are

$$R = \frac{k}{n} \qquad \text{and} \qquad \delta = \frac{d}{n}$$

- A sequence $\{\mathcal{C}_i\}_{i=0}^{\infty}$ of $[n_i, k_i, d_i]$-codes over $\mathbb{F}_q$ is called **asymptotically good over** $\mathbb{F}_q$ if

$$\limsup_{i\to\infty} \frac{k_i}{n_i} > 0 \qquad \text{and} \qquad \limsup_{i\to\infty} \frac{d_i}{n_i} > 0$$

where $n_i \to \infty$ as $i \to \infty$.

(λ, δ)-bounds

Definition

Let

$$0 < \delta < \lambda < 1 \qquad \text{and} \qquad r = \lambda - \delta > 0.$$

A sequence $\{\mathcal{C}_i\}_{i=0}^{\infty}$ of $[n_i, k_i, d_i]$-codes over $\mathbb{F}_q$ is said to **attain a** (λ, δ)-**bound** over $\mathbb{F}_q$ if

$$\limsup_{i\to\infty} \frac{k_i}{n_i} \geq r \qquad \text{and} \qquad \limsup_{i\to\infty} \frac{d_i}{n_i} \geq \delta$$

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_{i+1}/F_i is finite and separable of degree > 1 for all $i \geq 1$.
  - $\mathbb{F}_q$ is algebraically closed in F_i for all $i \geq 0$.
  - $g(F_i) \to \infty$ for $i \to \infty$.
- A tower $\mathcal{F}$ is **recursive** if there exist a sequence $\{x_i\}_{i=0}^{\infty}$ of transcendental elements over $\mathbb{F}_q$ and $H(X, Y) \in \mathbb{F}_q[X, Y]$ such that $F_0 = \mathbb{F}_q(x_0)$ and

$$F_{i+1} = F_i(x_{i+1}), \qquad H(x_i, x_{i+1}) = 0, \qquad i \geq 0.$$

Asymptotically good AG-codes from towers

Proposition

Let $\ell \in (0,1)$ and let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be a sequence of AFF's over $\mathbb{F}_q$ with $\mathbb{F}_q$ as their full field of constants and such that for each $i \geq 1$ there are n_i rational places $P_1^{(i)}, \ldots, P_{n_i}^{(i)}$ in F_i satisfying

(a) $n_i \to \infty$ *as* $i \to \infty$,

(b) *there is* i_0 *such that* $\frac{g(F_i)}{n_i} \leq \ell$ *for all* $i \geq i_0$, *and*

(c) *for each* $i > 0$ *there exists a divisor* G_i *of* F_i *disjoint from*

$$D_i := P_1^{(i)} + \cdots + P_{n_i}^{(i)}$$

such taht $\deg G_i \leq n_i\, s(i)$ *where* $s : \mathbb{N} \to \mathbb{R}$ *with* $s(i) \to 0$ *as* $i \to \infty$.

Asymptotically good AG-codes from towers

Proposition (continued)

Then, there exists a sequence $\{r_i\}_{i=m}^{\infty} \subset \mathbb{N}$ *such that* $\mathcal{F}$ *induces a sequence*

$$\mathcal{G} = \{\mathcal{C}_i\}_{i=m}^{\infty}$$

of **asymptotically good** *AG-codes of the form*

$$\mathcal{C}_i = C_{\mathcal{L}}(D_i, r_i G_i)$$

attaining a (λ, δ)**-bound** *with*

$$\lambda = 1 - \ell \quad \text{and} \quad 0 < \delta < \lambda.$$

Example

For each $q > 2$ there is a family of asymptotically good AG-codes over $\mathbb{F}_{q^2}$.

- Consider the recursive tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_{q^2}$ of Garcia and Stichtenoth defined by

$$y^q + y = \frac{x^q}{x^{q-1} + 1}$$

- It is known [Niederreiter-Xing, 2001] that

$$N(F_i) \geq q^{i-1}(q^2 - q) + 1$$

and

$$g(F_i) = \begin{cases} (q^{\frac{i}{2}} - 1)^2 & \text{for } i \text{ even,} \\ (q^{\frac{i-1}{2}} - 1)(q^{\frac{i+1}{2}} - 1) & \text{for } i \text{ odd.} \end{cases}$$

Example

- If $n_i = q^{i-1}(q^2 - q)$, we have at least $n_i + 1$ rational places, say $P_1^{(i)}, \ldots, P_{n_i}^{(i)}, Q_i$ in F_i, and

$$\frac{n_i}{g(F_i)} \geq q - 1 \qquad (i \geq 1)$$

- The conditions in the Proposition holds:
  - $n_i \to \infty$ and hence (a) holds.
  - (b) holds with $\ell = (q-1)^{-1} = A(q)^{-1}$.
  - By taking $G_i = Q_i$, (c) holds with $s(i) = 1/n_i$.

- Thus, the sequence $\{\mathcal{C}_i\}_{i \in \mathbb{N}}$ of codes $\mathcal{C}_i = C(D_i, Q_i)$, with $D_i = P_1^{(i)} + \cdots + P_{n_i}^{(i)}$, is asymptotically good and attains the TVZ-bound over $\mathbb{F}_{q^2}$ for $q \geq 3$.

Good (quasi) transitive AG-codes over non-prime fields

- The class of transitive codes attains the TVZ-bound over $\mathbb{F}_{q^2}$ (Stichtenoth, IEEE, 2006).
- The class of r-quasi transitive codes attains an (λ, δ)-bound over $\mathbb{F}_{q^3}$ with

$$\lambda = 1 - \frac{q+2}{2r(q-1)}, \qquad 0 < \delta < \lambda$$

  (Bassa, PhD Thesis, 2006).
- We will next give a result for 4-quasi transitive AG-codes over an arbitrary field $\mathbb{F}_q$.

The Theorem

By considering the Galois closure of an infinite Hilbert class field tower we get the following result in odd characteristic.

Theorem (Chara-P.-Toledano)

Let q be an odd prime power. Suppose that

- *there is $h(t) \in \mathbb{F}_q[t]$ monic of degree 9 which splits into (different) linear factors over $\mathbb{F}_q$, and*
- *$h(\alpha)$ and $h(\beta)$ are nonzero squares in $\mathbb{F}_q$ for two different elements $\alpha, \beta \in \mathbb{F}_q$.*

Then, there is a sequence of **asymptotically good 4-quasi transitive codes** *over $\mathbb{F}_q$ attaining a $(\frac{1}{8}, \delta)$-bound for $0 < \delta < \frac{1}{8}$.*

Sketch of proof. Step 1 - The base extension

- Consider the extension $F = \mathbb{F}_q(x, y)$ of $\mathbb{F}_q(x)$ given by

$$y^2 = h(x) = (x - a_1) \cdots (x - a_9)$$

- By a result on tame cyclic extensions of rational ff's
  - $F/\mathbb{F}_q(x)$ is a cyclic Galois extension of degree 2,
  - F has genus $g = 4$ and $\mathbb{F}_q$ is its full constant field,
  - $\mathbb{F}_q(x)$ has exactly 10 rational places, totally ramified in F,

$$P_i = P_{x-a_i}, \quad 1 \leq i \leq 9, \qquad \text{and} \qquad P_\infty.$$

Step 2 - The Hilbert class field tower

- By Kummer's theorem, $P_\alpha = P_{x-\alpha}$ and $P_\beta = P_{x-\beta}$ split completely into 2 rational places Q_1, Q_2 and Q_3, Q_4 respectively.
- Put $S_{\mathbb{F}_q} = \{P_\alpha, P_\beta\}$,

$$T = \{Q_\infty\} \qquad \text{and} \qquad S = \{Q_1, Q_2, Q_3, Q_4\}$$

- By a result in [Angles-Maire, 2002], the bound

$$\#\{P \in \mathbb{P}(\mathbb{F}_q(x)) : P \text{ ramifies in } F\} \geq 3 + |S_{\mathbb{F}_q}| + 2\sqrt{|S|} = 9$$

implies that the T-tamely ramified and S-decomposed Hilbert tower $\mathcal{H}_S^T$ of F is *infinite*.

Step 3 - The Galois closure of the tower

- That is, there is a sequence $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ of function fields over $\mathbb{F}_q$ such that $F_0 = F$, $\mathcal{H}_S^T = \bigcup_{i=1}^{\infty} F_i$ and for any $i \geq 1$:
  - F_i/F_{i-1} is finite abelian,
  - $[F_i : F] \to \infty$ as $i \to \infty$,
  - $\mathbb{F}_q$ = the full constant field of F_i,
  - each place $Q \in S$ splits completely in F_i, $N(F_i) \geq 4[F_i : F]$,
  - F_i/F is unramified outside T, and
  - Q_∞ is tamely ramified in F_i.
- Let F_i' be the **Galois closure** of F_i over F. By Hurwitz' genus formula and Abhyankar's Lemma we have

$$g_i' \leq \tfrac{7}{2}[F_i' : F] + 1$$

Step 4 - The codes $\mathcal{C}_i$

- Since the 4 rational places of S split completely in F_i', we have $n_i = 4[F_i' : F]$ rational places $S_1^{(i)}, \ldots, S_{n_i}^{(i)}$ of F_i' which are the ones lying over the places of S.
- We define the codes

$$\mathcal{C}_i = C_{\mathcal{L}}^{F_i'}(D_i, r_i G_i)$$

over $\mathbb{F}_q$ with

$$D_i = S_1^{(i)} + \cdots + S_{n_i}^{(i)} \qquad \text{and} \qquad G_i := R_1^{(i)} + \cdots + R_{k_i}^{(i)}$$

where $R_1^{(i)}, \ldots, R_{k_i}^{(i)}$ are all the places of F_i' lying above Q_∞.

Step 5 - The sequence $\{\mathcal{C}_i\}$ is asymptotically good

- We have

$$\deg G_i \leq [F_i' : F_i] \deg \sum_{P \in T_i} P \leq \frac{[F_i' : F_i][F_i : F]}{2^i} \leq \frac{[F_i' : F]}{2^i}$$

where $T_i = \{Q \in P(F_i) : Q \mid Q_\infty\}$, for every $i \in \mathbb{N}$. and

$$\frac{g_i'}{n_i} = \frac{\frac{7}{2}[F_i' : F] + 1}{4[F_i' : F]} \leq \frac{7}{8} + \frac{1}{n_i} \sim \frac{7}{8}$$

for n_i big enough.

- In this way, condition: (a) holds, (b) holds with $\ell \sim 7/8 < 1$, (c) holds by taking $s(i) = 1/2^{i-2}$.
- Thus, the sequence $\{\mathcal{C}_i\}_{i=1}^{\infty}$ is **asymptotically good** over $\mathbb{F}_q$ attaining a $(\frac{1}{8}, \delta)$-**bound** with $0 < \delta < 1/8$.

Step 6 - The codes $\mathcal{C}_i$ are 4-quasi transitive

- Both divisors D_i and G_i are invariant under $Gal(F_i'/F)$.
- Since $Gal(F_i'/F)$ acts transitively on the places in $\mathrm{Sup}(D_i)$,

$$C_{\mathcal{L}}(D_i, r_i G_i), \qquad r_i > 0$$

is a 4-**quasi transitive** AG-code over $\mathbb{F}_q$ for every i.

Explicit polynomials

Corollary

Let $q = p^r$ be an odd prime power. Suppose that:

- *there are 4 distinct elements $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{F}_q$ such that $\alpha_i^{-1} \notin \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ for $1 \leq i \leq 4$ and consider*

$$h(t) = (t+1)\prod_{i=1}^{4}(t-\alpha_i)(t-\alpha_i^{-1}) \in \mathbb{F}_q[t],$$

- *there is $\alpha \in \mathbb{F}_q^*$ such that $h(\alpha) = \gamma^2 \neq 0$, $\gamma \in \mathbb{F}_q$.*

Then there exists a sequence of 4-quasi transitive codes over $\mathbb{F}_q$ which is asymptotically good attaining a $(\frac{1}{8}, \delta)$-bound with $0 < \delta < \frac{1}{8}$.

Asymptotically good 4-quasi transitive AG-codes over $\mathbb{F}_{13}$

It is easy to see that there is no separable polynomial over $\mathbb{F}_{11}$ of degree 9 satisfying the required conditions.

Example

- $2, 3, 4, 5 \in \mathbb{F}_{13}$ satisfy the conditions of the Corollary.
- We have

$$h(t) = (t+1)(t-2)(t-7)(t-3)(t-9)(t-4)(t-10)(t-5)(t-8)$$

- $h(11) = 3 = 4^2$ in $\mathbb{F}_{13}$.
- Thus, there are asymptotically good sequences of 4-quasi transitive codes over $\mathbb{F}_{13}$ attaining a $(\frac{1}{8}, \delta)$-bound.

Infinitely many primes

Consider a prime $p \geq 29$.

- By Fermat's little theorem

$$h(t) = (t+1)\prod_{k=2}^{5}(t-k)(t-k^{p-2}) \in \mathbb{F}_p[t]$$

  has 9 different linear factors.

- "$h(a)$ is a nonzero square in $\mathbb{F}_p$ for $a \in \mathbb{F}_p^*$" iff $\left(\frac{h(a)}{p}\right) = 1$.

- By multiplicativity

$$\left(\frac{h(t)}{p}\right) = \left(\frac{t+1}{p}\right)\prod_{k=2}^{5}\left(\frac{t-k}{p}\right)\left(\frac{t-k^{p-2}}{p}\right)$$

Infinitely many primes

- For $2 \leq j \leq \lfloor \frac{p-1}{5} \rfloor$ we have

$$h(p-j) = (p-(j-1)) \prod_{k=2}^{5} (p-(j+k))(p-(j+k^{p-2})) \neq 0$$

- By modularity and multiplicativity of the Legendre symbol:

$$\begin{aligned}
\left(\frac{h(p-j)}{p}\right) &= \left(\frac{1-j}{p}\right) \prod_{k=2}^{5} \left(\frac{j+k}{p}\right)\left(\frac{j+k^{p-2}}{p}\right) \\
&= \left(\frac{1-j}{p}\right) \prod_{k=2}^{5} \left(\frac{j+k}{p}\right)\left(\frac{k}{p}\right)^2\left(\frac{j+k^{p-2}}{p}\right) \\
&= \left(\frac{1-j}{p}\right) \prod_{k=2}^{5} \left(\frac{j+k}{p}\right)\left(\frac{k}{p}\right)\left(\frac{kj+1}{p}\right)
\end{aligned}$$

Infinitely many primes

For instance, for $j = 2$ we have

- $$\left(\frac{h(p-2)}{p}\right) = \left(\frac{-1}{p}\right)\prod_{k=2}^{5}\left(\frac{k+2}{p}\right)\left(\frac{k}{p}\right)\left(\frac{2k+1}{p}\right)$$
- Thus,

$$\left(\frac{h(p-j)}{p}\right) = \left(\frac{-1}{p}\right)\left(\left(\frac{4}{p}\right)\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)\right)\left(\left(\frac{5}{p}\right)\left(\frac{3}{p}\right)\left(\frac{7}{p}\right)\right)$$
$$\left(\left(\frac{6}{p}\right)\left(\frac{4}{p}\right)\left(\frac{9}{p}\right)\right)\left(\left(\frac{7}{p}\right)\left(\frac{5}{p}\right)\left(\frac{11}{p}\right)\right)$$

- and hence
$$\left(\frac{h(p-2)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)\left(\frac{11}{p}\right)$$

Infinitely many primes

- For $p \geq 37$ we can take the $2 \leq j \leq 7$ and we have

$$\left(\frac{h(p-2)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)\left(\frac{11}{p}\right)$$
$$\left(\frac{h(p-3)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)\left(\frac{13}{p}\right)$$
$$\left(\frac{h(p-4)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)\left(\frac{13}{p}\right)\left(\frac{17}{p}\right)$$
$$\left(\frac{h(p-5)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{11}{p}\right)\left(\frac{13}{p}\right)$$
$$\left(\frac{h(p-6)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right)\left(\frac{11}{p}\right)\left(\frac{13}{p}\right)\left(\frac{19}{p}\right)\left(\frac{31}{p}\right)$$
$$\left(\frac{h(p-7)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{29}{p}\right)$$

- This *reduces the search* of $\alpha \in \mathbb{F}_p^*$ such that $h(\alpha) = \gamma^2 \in \mathbb{F}_p^*$, to the *computation of Legendre symbols* $\left(\frac{\cdot}{p}\right)$.

Infinitely many primes

Proposition

There are asymptotically good 4-quasi transitive AG-codes over $\mathbb{F}_p$ for infinite primes p. For instance, this holds for primes of the form $p = 220k + 1$ or $p = 232k + 1$, $k \in \mathbb{N}$.

Proof.

- As before, consider the polynomial

$$h(t) = (t+1)\prod_{k=2}^{5}(t-k)(t-k^{p-2}) \in \mathbb{F}_p[t]$$

  for $p \geq 37$.

- It suffices to find infinitely many primes p, such that $\left(\frac{h(p-j)}{p}\right) = 1$, for a given j.

Infinitely many primes

- Consider first $j = 2$. We look for prime numbers p such that

$$\left(\frac{h(p-2)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)\left(\frac{11}{p}\right) = 1.$$

- Since $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1\,(4)$ and $\left(\frac{5}{p}\right) = 1$ if $p \equiv \pm 1\,(5)$, it is clear that if $p = 20k + 1$ then $\left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = 1$.
- In this way, if $p = (20 \cdot 11)k + 1$, $k \in \mathbb{N}$, then $\left(\frac{h(p-2)}{p}\right) = 1$ by quadratic reciprocity.
- By *Dirichlet's theorem* on arithmetic progressions, there are infinitely many prime numbers of the form $p = 220k + 1$, $k \in \mathbb{N}$. □

Asymptotically good 4-quasi transitive AG-codes over prime fields

Remark

- One checks computationally that the Corollary holds true for all primes $19 < p < 10^6$ with $\alpha_1 = 2$, $\alpha_2 = 3$, $\alpha_3 = 4$, $\alpha_4 = 5$, that is, using the polynomial

$$h(t) = (t+1)\prod_{k=2}^{5}(t-k)(t-k^{p-2}).$$

- In fact, these numerical experiments suggest that the Corollary holds true for any prime $p \geq 13$ (except for $p = 19$).

thanks!