Block-transitive algebraic geometry codes attaining the Tsfasman-Vladut-Zink bound

María Chara* , Ricardo Podestá, Ricardo Toledano***

* IMAL (CONICET) - Universidad Nacional del Litoral
** CIEM (CONICET) - Universidad Nacional de Córdoba

CIMPA Research Skol
Algebraic methods in Coding Theory

July 2 - 15, 2017 / Ubatuba, São Paulo, Brazil.

Based on the joint work

María Chara, Ricardo Podestá, Ricardo Toledano
Block-transitive algebraic geometry codes attaining the Tsfasman-Vladut-Zink bound.

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

Summary of the talk

1. 1. Codes
2. 2. Asymptotics
3. 3. Good BTC from towers
4. 4. GBTC from class field towers
5. 5. GBTC over prime fields

Motivation

Open question

Is the family of cyclic codes asymptotically good?

Block-transitive codes

Linear codes

- A **linear code** over $\mathbb{F}_q$ of *length* n, *dimension* k and *minimun distance* d is $\mathbb{F}_q$-linear subspace $\mathcal{C} \subset \mathbb{F}_q^n$ with

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

where d is the Hamming distance in $\mathbb{F}_q^n$.

- $\mathcal{C}$ is an $[n, k, d]$-code over $\mathbb{F}_q$.

Bounds

- Singleton bound

$$k + d \leq n - 1$$

- Griesmer bound

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$

- Hamming and Gilbert bounds

$$\sum_{i=0}^{[\frac{d-1}{2}]} \binom{n}{i}(q-1)^i \leq q^{n-k} \leq \sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i$$

Transitive and cyclic codes

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

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

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

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

- $\mathcal{C}$ is **transitive** if $Aut(\mathcal{C})$ acts transitively on $\mathcal{C}$, i.e. if for any $1 \leq i < j \leq n$ there is some $\pi \in Aut(\mathcal{C})$ s.t. $\pi(i) = j$.

- $\mathcal{C}$ is **cyclic** if $\sigma = (12 \cdots n) \in Aut(\mathcal{C})$, i.e.

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

Block-by-block actions

- If

$$n = m_1 + m_2 + \cdots + m_r$$

we can consider $v \in \mathbb{F}_q^n$ divided into r blocks of lengths m_i

$$v = (v_{1,1}, \ldots, v_{1,m_1}; \ldots; v_{r,1}, \ldots, v_{r,m_r})$$

- There is a block-by-block action of $\mathbb{S}_{m_1} \times \cdots \times \mathbb{S}_{m_r}$ on $\mathbb{F}_q^n$,

$$\pi \cdot v = (v_{1,\pi_1(1)}, \ldots, v_{1,\pi_1(m)}; \ldots; v_{r,\pi_r(1)}, \ldots, v_{r,\pi_r(m)})$$

where $\pi = (\pi_1, \ldots, \pi_r) \in \mathbb{S}_m \times \cdots \times \mathbb{S}_m$.

Block-transitive codes (BTC)

Definition

- A code $\mathcal{C}$ of length $n = m_1 + m_2 + \cdots + m_r$ is said to be **block-transitive** if for some $r \in \mathbb{N}$ there is a subgroup

$$\Delta = \{(\pi_1, \ldots, \pi_r)\} < \mathbb{S}_{m_1} \times \cdots \times \mathbb{S}_{m_r}$$

  acting transitively on the corresponding blocks in which the words of $\mathcal{C}$ are divided.

- If $m_1 = m_2 = \cdots = m_r = m$, hence $n = rm$, we say that $\mathcal{C}$ is an r-**block transitive** code.

- If $\pi_1 = \cdots = \pi_r = \pi$ we have an r-**quasi transitive** code.

Algebraic geometric codes

AG-codes: definition

We will use the language of 'algebraic function fields'.

- 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

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

where $x(P_i)$ stands for the residue class of x modulo P_i in the residual field $F_{P_i} = \mathcal{O}_{P_i}/P_i$.

AG-codes: parameters

- $C(D, G)$ is an $[n, k, d]$-code with

$$d \geq n - \deg G$$

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 $k = \deg G + 1 - g$.

Geometric block-transitive codes

Question

How can one construct (geometric) block-transitive codes?

Asymptotically good codes

Asymptotically good codes

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

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

- The goodness of $\mathcal{C}$ is usually measured according to how big is

$$0 < R + \delta < 1$$

- 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 $i \to \infty$. Otherwise the sequence is said to be *bad*.

Asymptotically good families

Definition: A family of codes

- is *asymptotically good* if there is a sequence in the family which is asymptotically good.
- is *asymptotically bad* if there is no asymptotically good sequence in the family.

Examples:

- Self-dual codes are asymptotically good.
- Transitive codes are asymptotically good.
- Quasi-cyclic groups are asymptotically good.
- BCH codes are asymptotically bad.
- Cyclic codes? We don't know.

The Ihara function

- The *Ihara's function* is

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}$$

  where $N_q(g)$ is the maximum number of rational places that a function field over $\mathbb{F}_q$ of genus g can have.

- By the Serre and Drinfeld-Vladut bounds

$$c \log q \leq A(q) \leq \sqrt{q} - 1$$

  for some $c > 0$.

- For $\mathbb{F}_{q^2}$ one has

$$A(q^2) = q - 1$$

Manin's function

- Consider the map $\psi : \{\text{linear codes over } \mathbb{F}_q\} \to [0,1] \times [0,1]$

$$\mathcal{C} \mapsto (\delta_{\mathcal{C}}, R_{\mathcal{C}})$$

- For $\delta \in [0,1]$, consider the accumulation points of $\psi(C)$ in the line $x = \delta$. Define $\alpha_q(\delta)$ to be the greatest second coordinate of these points.

Theorem

The Manin's function $\alpha_q : [0,1] \to [0,1]$ is continuous with

- $\alpha_q(0) = 1$,
- α_q *is decreasing on* $[0, 1 - \frac{1}{A(q)}]$ *and,*
- $\alpha_q = 0$ *in* $[1 - \frac{1}{A(q)}, 1]$.

Asymptotic bounds for $\alpha_q(\delta)$

- Singleton bound

$$\alpha_q(\delta) \leq 1 - \delta$$

- Griesmer bound

$$\alpha_q(\delta) \leq 1 - \frac{q}{q-1}\delta$$

- Hamming and Gilbert-Varshamov bounds

$$1 - H_q(\tfrac{\delta}{2}) \leq \alpha_q(\delta) \leq 1 - H_q(\delta)$$

where $H_q : [0, 1 - \frac{1}{q}] \to \mathbb{R}$ is the q-ary entropy function

$$H_q(x) = x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x)$$

and $H_q(0) = 0$.

Tsfasman-Vladut-Zink bound

Theorem (Tsfasman-Vladut-Zink bound)

Let q be a prime power. If $A(q) > 1$ then

$$\alpha_q(\delta) \geq 1 - \delta - \frac{1}{A(q)}$$

for $\delta \in [0, 1 - 1/A(q)]$.

- The TVZ-bound improves the GV-bound over $\mathbb{F}_{q^2}$, for $q^2 \geq 49$.

(ℓ, δ)-bounds

Definition

Let

$$0 < \delta < \ell < 1$$

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** (ℓ, δ)**-bound** over $\mathbb{F}_q$ if

$$\limsup_{i\to\infty} \frac{k_i}{n_i} \geq \ell - \delta \quad \text{and} \quad \limsup_{i\to\infty} \frac{d_i}{n_i} \geq \delta.$$

Example (Tsfasman-Vladut-Zink bound)

A sequence $\{\mathcal{C}_i\}_{i=0}^{\infty}$ of codes over $\mathbb{F}_q$ with $A(q) > 1$ attains the TVZ-bound over $\mathbb{F}_q$ if it attains a (ℓ, δ)-bound with

$$\ell = 1 - \frac{1}{A(q)}$$

Asymptotically good towers

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
  - $F_i \subsetneq F_{i+1}$ for all $i \geq 0$.
  - 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

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

Parameters of towers

Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be a tower of function fields over $\mathbb{F}_q$.

- The *genus* of $\mathcal{F}$ over F_0 is defined as

$$\gamma(\mathcal{F}) := \lim_{i \to \infty} \frac{g(F_i)}{[F_i : F_0]}$$

- The *splitting rate* of $\mathcal{F}$ over F_0 is defined as

$$\nu(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{[F_i : F_0]}$$

where $N(F_i)$ the number of rational places of F_i

Asymptotic behavior of towers

- *the limit* of the tower $\mathcal{F}$ is

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)} = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})}$$

- Note that $0 \leq \lambda(\mathcal{F}) \leq A(q) < \infty$.
- A tower $\mathcal{F}$ is called **asymptotically good** over $\mathbb{F}_q$ if

$$\nu(\mathcal{F}) > 0 \qquad \text{and} \qquad \gamma(\mathcal{F}) < \infty$$

Otherwise is called **asymptotically bad**.

- Equivalently, $\mathcal{F}$ is asymptotically good if and only if

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

and $\mathcal{F}$ is called **optimal** over $\mathbb{F}_q$ if $\lambda(\mathcal{F}) = A(q)$.

Asymptotically good codes from towers

Asymptotically good AG-codes from towers

Proposition

Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be a tower 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) *for* $\lambda \in (0,1)$ *there exists* i_0 *s.t.* $\frac{g(F_i)}{n_i} \leq \lambda$ *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 that

$$\deg G_i \leq n_i\, s(i)$$

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 (ℓ, δ)-**bound** *with*

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

Conditions for asymptotically good BT codes

Ramification

Let E/F be a function field extension of finite degree. Let Q and P be places of E and F, with $Q|P$.

- $e(Q|P)$ and $f(Q|P)$ the ramification index and the inertia degree of $Q|P$.
- P **splits completely** in E if $e(Q|P) = f(Q|P) = 1$ for any place Q of E lying over P (hence there are $[E:F]$ places in E above P).
- P **ramifies** in E if $e(Q|P) > 1$ for some place Q of E above P
- P is **totally ramified** in E if there is only one place Q of E lying over P and $e(Q|P) = [E:F]$ (hence $f(Q|P) = 1$).
- E/F is called b-**bounded** if for any place P of F and any place Q of E lying over P we have

$$e(Q|P) - 1 \leq d(Q|P) \leq b(e(Q|P) - 1)$$

Ramification

Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be a tower of function fields over $\mathbb{F}_q$.

- The **ramification locus** $R(\mathcal{F})$ of $\mathcal{F}$ is the set of places P of F_0 such that P is ramified in F_i for some $i \geq 1$.
- The **splitting locus** $Sp(\mathcal{F})$ of $\mathcal{F}$ is the set of rational places P of F_0 such that P splits completely in F_i for all $i \geq 1$.
- A place P of F_0 is **totally ramified** in the tower if for each $i \geq 1$ there is only one place Q of F_i lying over P and $e(Q|P) = [F_i : F_0]$.

Definition

A place P of F_0 is **absolutely μ-ramified** in $\mathcal{F}$ ($\mu > 1$) if for each $i \geq 1$ and any place Q of F_i lying over P we have that $e(R|Q) \geq \mu$ for any place R of F_{i+1} lying over Q.

Ramification

- The tower $\mathcal{F}$ is **tamely ramified** if for any $i \geq 0$, any place P of F_i and any place Q of F_{i+1} lying over P, the ramification index $e(Q|P)$ is not divisible by the characteristic of $\mathbb{F}_q$. Otherwise, $\mathcal{F}$ is called **wildly ramified**.
- $\mathcal{F}$ has **Galois steps** if each extension F_{i+1}/F_i is Galois.
- $\mathcal{F}$ is a **b-bounded tower** if each extension F_{i+1}/F_i is a b-bounded Galois p-extension where $p = \mathrm{char}(\mathbb{F}_q)$.
- If each extension F_i/F_0 is Galois, $\mathcal{F}$ is said to be a **Galois tower** over $\mathbb{F}_q$.

Theorem 1: general conditions for existence

Theorem

Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be either a tamely ramified tower with Galois steps or a 2-bounded tower over $\mathbb{F}_q$ with $Sp(\mathcal{F}) \neq \emptyset$ and $R(\mathcal{F}) \neq \emptyset$. Suppose there are finite sets Γ and Ω of rational places of F_0 such that $R(\mathcal{F}) \subset \Gamma$ and $\Omega \subset Sp(\mathcal{F})$ with

$$0 < g_0 - 1 + \epsilon t < r$$

where $g_0 = g(F_0)$, $t = |\Gamma|$, $r = |\Omega|$ and $\epsilon = \frac{1}{2}$ if $\mathcal{F}$ is tamely ramified or $\epsilon = 1$ otherwise.
If a place $P_0 \in R(\mathcal{F})$ is absolutely μ-ramified in $\mathcal{F}$ for some $\mu > 1$ then there exists a sequence $\mathcal{C} = \{\mathcal{C}_i\}_{i=0}^{\infty}$ of r-block transitive AG-codes over $\mathbb{F}_q$ attaining a (ℓ, δ)-bound with $\ell = 1 - \frac{g_0 - 1 + \epsilon t}{r}$.
In particular, the Manin's function satisfies $\alpha_q(\delta) \geq \ell - \delta$.
Moreover, the sequence $\mathcal{C}$ is defined over the Galois closure $\mathcal{E}$ of $\mathcal{F}$ with limit $\lambda(\mathcal{E}) > 1$.

Block-transitive codes attaining the TVZ-bound

From wild towers

$$m_i = \begin{cases} q^{2i-1}(\text{resp. } q^{2i-1-\lfloor 1/2 \rfloor}) & \text{if } 1 \leq i \leq 2,\ q \text{ is odd (resp. even)}, \\ q^{3i-3}(\text{resp. } q^{3i-3\lfloor 1/2 \rfloor}) & \text{if } i \geq 3,\ q \text{ is odd (resp. even)}. \end{cases}$$

Theorem

Let $q > 2$ be a prime power. Then, there exists a sequence $\mathcal{C} = \{\mathcal{C}_i\}_{i=1}^{\infty}$ of r-block transitive codes over $\mathbb{F}_{q^2}$, with $r = q^2 - q$, attaining the TVZ-bound. Each $\mathcal{C}_i$ is an $[n_i = rm_i, k_i, d_i]$-code. By fixing $0 < \delta < 1 - q^{-2}$, we also have that

$$d_i \geq \delta n_i \qquad \text{and} \qquad k_i \geq \{(1-\delta)r - (q + q^{-i})\} m_i$$

for each $i \geq 1$, where the second inequality is non trivial if δ satisfies $0 < \delta < 1 - \frac{1}{r}(q + q^{-i})$.

Sketch of proof

Consider the wildly ramified tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_{q^2}$ recursively defined by the equation

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

which is optimal ([GS'96]).

- $\mathcal{F}$ is a 2-bounded tower over $\mathbb{F}_{q^2}$,
- the pole P_∞ of x_0 in $F_0 = \mathbb{F}_{q^2}(x_0)$ is totally ramified in $\mathcal{F}$, so that P_∞ is absolutely q-ramified in $\mathcal{F}$,
- at least $q^2 - q$ rational places of $\mathbb{F}_{q^2}$ split completely in $\mathcal{F}$ and
- the ramification locus $R(\mathcal{F})$ has at most $q+1$ elements,
- i.e. $q^2 - q \leq |Sp(\mathcal{F})|$ and $|R(\mathcal{F})| \geq q+1$.

Sketch of proof

- We are in the conditions of Theorem 1 with

$$\mu = q, \quad \epsilon = 1, \quad g_0 = 0, \quad r = q^2 - q \quad \text{and} \quad t = q + 1.$$

- Therefore, there exists a sequence $\mathcal{C} = \{\mathcal{C}_i\}_{i \in \mathbb{N}}$ of r-block transitive AG-codes over $\mathbb{F}_{q^2}$ attaining a (ℓ, δ)-bound with

$$\ell = 1 - \frac{g_0 - 1 + t}{r} = 1 - \frac{q}{q^2 - q} = 1 - \frac{1}{q - 1},$$

- Thus, $\mathcal{F}$ attains the TVZ-bound over $\mathbb{F}_{q^2}$. $\square$

Good block transitive from class field towers

GBTC from polynomials

- Given $n, m \in \mathbb{Z}$ we put

$$\varepsilon_n(m) = \begin{cases} 1 & \text{if } n \mid m, \\ 0 & \text{if } n \nmid m. \end{cases}$$

- For $h \in \mathbb{F}_q[t]$, we define

$$S_q^2(h) = \{\beta \in \mathbb{F}_q : h(\beta) \text{ is a non zero square in } \mathbb{F}_q\},$$
$$S_q^3(h) = \{\beta \in \mathbb{F}_q : h(\beta) \text{ is a non zero cube in } \mathbb{F}_q\}.$$

GBTC from polynomials

Theorem (case q odd)

Let q be an odd prime power and let $h \in \mathbb{F}_q[t]$ be a monic and separable polynomial of degree m such that it splits completely into linear factors over $\mathbb{F}_q$.

Suppose there is a set $\Sigma_o \subset S_q^2(h)$ such that $u = |\Sigma_o| > 0$ and

$$2\sqrt{2u} \leq m - (u + 2 + \varepsilon_2(m)) < 3u$$

Then, there exists a tamely ramified Galois tower $\mathcal{F}$ over $\mathbb{F}_q$ with limit $\lambda(\mathcal{F}) \geq \frac{4u}{m-2-\varepsilon_2(m)} > 1$. In particular, there exists a sequence of asymptotically good 2u-block transitive codes over $\mathbb{F}_q$, constructed from $\mathcal{F}$, attaining an (ℓ, δ)-bound, with

$$\ell = 1 - \frac{m - 3 + \varepsilon_2(m)}{4u}$$

.

GBTC from polynomials

Theorem (case q even)

Let $q = 2^{2s}$ and let $h \in \mathbb{F}_q[t]$ be a monic and separable polynomial of degree m such that it splits completely into linear factors over $\mathbb{F}_q$.

Suppose there is a set $\Sigma_e \subset S_q^3(h)$ such that $v = |\Sigma_e| > 0$ and

$$2\sqrt{3v} \leq m - (v + 2 + \varepsilon_3(m)) < 2v - \frac{1}{2}$$

Then, there exists a tamely ramified Galois tower $\mathcal{F}'$ over $\mathbb{F}_q$ with limit $\lambda(\mathcal{F}') \geq \frac{6v}{2(m-\varepsilon_3(m))-3} > 1$. In particular, there exists a sequence of asymptotically good $3v$-block transitive codes over $\mathbb{F}_q$, constructed from $\mathcal{F}'$, attaining an (ℓ, δ)-bound with

$$\ell = 1 - \frac{2m - 5 + 2\varepsilon_3(m)}{6v}$$

.

Sketch of proof

- Let $K = \mathbb{F}_q(x)$ and $F = \mathbb{F}_q(x, y)$ given by the equation

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

- F/K is cyclic Galois of degree 2.
- The rational places $P_{a_1}, \ldots, P_{a_m}$ of K are totally ramified in F/K and no other places than $P_{a_1}, \ldots, P_{a_m}$ and P_∞ ramify in F/K. Moreover, P_∞ is totally ramified if m is odd.
- There are $m + 1 - \varepsilon_2(m)$ places in K totally ramified in F.
- The genus $g(F) = \frac{1}{2}(m - 1 - \varepsilon_2(m))$.

Sketch of proof

- By Kummer's theorem, the place $P_\beta = P_{x-\beta}$ in K, $\beta \in \Sigma_o$, splits completely into 2 rational places of F for each $\beta \in \Sigma_o$.
- Let P_0 be some P_{a_i} and let Q_0 be the only place of F lying above P_0. Let $Q_1, \ldots, Q_{2u}$ be the rational places of F lying over the places P_β with $\beta \in \Sigma_o$ and put

$$T = \{Q_0\} \qquad \text{and} \qquad S = \{Q_1, \ldots, Q_{2u}\}$$

- Since

$$\#\{P \in \mathbb{P}(K) : P \text{ ramifies in } F\} = m + 1 - \varepsilon_2(m)$$

thus, by hypothesis,

$$\#\{P \in \mathbb{P}(K) : P \text{ ramifies in } F\} \geq 2 + |\Sigma| + 2\sqrt{n|\Sigma|}$$

Sketch of proof

- By a result of [AM], the T-tamely ramified and S-decomposed Hilbert tower $\mathcal{H}_S^T$ of F is infinite.
- This means that there is a sequence $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ of function fields over $\mathbb{F}_q$ such that $F_0 = F$,

$$\mathcal{H}_S^T = \bigcup_{i=0}^{\infty} F_i$$

  and for any $i \geq 1$
  - each place in S splits completely in F_i,
  - the place Q_0 is tamely and absolutely ramified in the tower,
  - F_i/F_{i-1} is an abelian extension, $[F_i : F] \to \infty$ as $i \to \infty$ and
  - F_i/F_0 is unramified outside T.

Sketch of proof

- Then, we are in the situation of Theorem 1 with

$$F_0 = F, \qquad \Gamma = T, \qquad \Omega = S$$

- Also,

$$g(F) = \frac{1}{2}\{m - 1 - \varepsilon_2(m)\} < 2u = |S|$$

- Thus, by Theorem 1, the result follows. $\square$

Good block transitive codes over prime fields

Explicit polynomials

Proposition

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-block transitive codes over $\mathbb{F}_q$ attaining a $(\frac{1}{8}, \delta)$-bound with $0 < \delta < \frac{1}{8}$.

Proof.

Take $m = 9$ and $u = 2$ in the previous Theorem and note that $h(0) = 1$ is a nonzero square in $\mathbb{F}_q$. □

Asymptotically good 4-block 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 proposition.*
- *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-block 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 $a \in \mathbb{F}_p^*$ $\Leftrightarrow$ $\left(\frac{h(a)}{p}\right) = 1.$
- By multiplicativity of the Legendre symbol

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

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:

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

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,

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

- 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-block transitive AG-codes over $\mathbb{F}_p$ *for infinitely many 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, for $p \geq 37$, consider the polynomial

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

- 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 $j = 2$. 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 $p = 220k + 1$, $k \in \mathbb{N}$ (the first being $p = 661$). $\square$

muito obrigado!