BLOCK-TRANSITIVE ALGEBRAIC GEOMETRY CODES ATTAINING THE TSFASMAN-VLADUT-ZINK BOUND

MARÍA CHARA, RICARDO PODESTÁ, RICARDO TOLEDANO

October 5, 2017

ABSTRACT. We study the asymptotic behaviour of a family of algebraic geometry codes, which we call block-transitive, that generalizes the classes of transitive and quasi-transitive codes. We prove, by using towers of algebraic function fields, that there are sequences of codes in this family attaining the Tsfasman-Vladut-Zink bound over finite fields of square cardinality. We give the exact length of these codes as well as explicit lower bounds for their parameters.

1. INTRODUCTION

Let $\mathbb{F}_q$ denote a finite field with q elements. In 1982, Tsfasman, Vladut and Zink proved, in their remarkable paper [19], that there are sequences of linear codes over $\mathbb{F}_{p^2}$, p a prime number, whose transmission rates satisfy what is known today as the Tsfasman-Vladut-Zink bound. For finite fields of square cardinality bigger than 49, this bound is above the well kwown Gilbert-Varshamov bound in some interval and thus the work [19] showed, for the first time, the existence of a sequence of linear codes beating the Gilbert-Varshamov bound for infinitely many finite fields. This important result was achieved by considering algebraic geometry codes associated to towers of modular curves over $\mathbb{F}_{p^2}$. However, as of today, little is known about the structure of these codes besides linearity and the more we know about structural properties of a family of codes the better because they can be very helpful for the design of efficient coding and decoding methods.

Almost a quarter of a century later, a further step in this direction was given by Stichtenoth in [16]. There, he reproved the result of Tsfasman, Vladut and Zink by showing that there are sequences of transitive codes and self-dual codes (among others) over finite fields $\mathbb{F}_q$ of square cardinality $q > 4$ attaining the Tsfasman-Vladut-Zink bound. Since he used the Galois closure of a recursive tower of function fields over $\mathbb{F}_q$, there is an improvement with respect to the codes given in [19]. Namely, we have, on the one side, a sequence of linear codes with a richer structure and, on the other side, a sequence of function fields which is more manageable, in principle, than the sequence of modular towers used in [19].

In this paper, we give another step by considering a different family of linear codes and showing that there are sequences of codes in this family attaining the Tsfasman-Vladut-Zink bound over finite fields of square cardinality $\mathbb{F}_{q^2}$ with q a prime power. These codes are finite direct sums of transitive codes and we call them *block-transitive* (see Definition 4.1). The advantage we have with this family of codes, with respect to others in previous works, lies in that we use the Galois closure of optimal towers, tamely and wildly ramified, defined in [10] and [8] which have been studied in detail in [3] and [4]. Thus we know explicitly, for instance, the degree of every

extension as well as the structure of the Galois groups associated to these extensions, which are subgroups of the group of automorphisms of these codes. This is a valuable feature because we now have at our disposal more tools for a better and deeper understanding of the structure of these codes. At this point it is worth to mention that this is not available, to the best of our knowledge, for the transitive codes given in [16] because the Galois closure of the function fields of an optimal tower with respect to a proper subfield of the original field of rational functions was considered, and this is not the case treated in [4]. Another point worth mentioning is that the use of block-transitive codes allow us to use simpler arguments in more general results.

An outline of the paper is as follows. Sections 2–3 are preparatoty while the main results are in Sections 4–7. More precisely, in Section 2 we briefly recall the basic definitions on algebraic codes and towers of algebraic function fields and their corresponding asymptotic behaviours. Also, in Definition 2.1 we introduce the notion of a (λ, δ)-bound, with the famous Tsfasman-Vladut-Zink bound being a particular case. In the next section we review algebraic-geometry codes (AG-codes for short) and the standard way to get asymptotically good sequences of AG-codes from sequences of towers, attaining such a (λ, δ)-bound. We also present some concrete realizations of good AG-codes using either recursive towers (Example 3.5) or lower bounds for the Ihara function (Examples 3.6 and 3.7).

Section 4 begins with the definition of block-transitive codes, that we use throughout the paper, together with some examples. Then, in Theorem 4.5 we give sufficient conditions on the splitting and ramification locus of a tower of function fields to be suitable for the construction of good r-block transitive codes over a given finite field. In the next 2 sections we apply this result to prove the existence of families of block-transitive codes that are asymptotically good. In fact, using Theorem 4.5 and two quadratic optimal towers given in [8] and [10] we prove, in Theorem 5.1, the existence of sequences of r-block transitive codes with $r = q^2 - q$ (resp. $r = 2(p - 1)$, p an odd prime) attaining the Tsfasman-Vladut-Zink bound over $\mathbb{F}_{q^2}$ (resp. $\mathbb{F}_{p^2}$). Then, in Theorem 6.1 we use good tamely ramified Hilbert class field towers with non zero splitting rate, given in [1], to prove the existence of good r-block transitive codes over certain finite fields, not necessarily of square cardinality, of both odd and even characteristic and for $r = 2n$ or $r = 3n$, respectively. The price we must pay for considering a wider class of finite fields is reflected in that we get weaker lower bounds for their performance compared to the ones obtained in Theorem 5.1 and [16] for the case of transitive codes. Finally we make some remarks on the existence of sequences of algebraic geometry codes with good performance over prime fields.

2. Asymptotic behaviour of codes and towers

A linear code of *length* n, *dimension* k and *minimum distance* d over $\mathbb{F}_q$ is an $\mathbb{F}_q$-linear subspace $\mathcal{C}$ of $\mathbb{F}_q^n$ with $k = \dim \mathcal{C}$ and $d = \min\{d(c, c') : c, c' \in \mathcal{C}, c \neq c'\}$, where d is the Hamming distance in $\mathbb{F}_q^n$. The elements of $\mathcal{C}$ are usually called codewords and it is customary to say that $\mathcal{C}$ is an $[n, k, d]$-*code* over $\mathbb{F}_q$.

It is convenient to normalize the dimension and minimum distance of a code $\mathcal{C}$ with respect to the length, so that the *information rate* $R = R(\mathcal{C}) := k/n$ and the *relative minimum distance* $\delta = \delta(\mathcal{C}) := d/n$ of $\mathcal{C}$ are in the unit interval for any $[n, k, d]$-code $\mathcal{C}$. The goodness of an $[n, k, d]$-code over $\mathbb{F}_q$ is usually measured according to how big the sum

$$0 < R + \delta = \frac{k}{n} + \frac{d}{n} < 1$$

is. Since k and d can not be arbitrarily large for fixed n it is natural to allow arbitrarily large lengths. One way to do this is by considering a sequence $\{\mathcal{C}_i\}_{i=0}^{\infty}$ of $[n_i, k_i, d_i]$-codes over $\mathbb{F}_q$ such that $n_i \to \infty$ as $i \to \infty$ and see how big the sum $k_i/n_i + d_i/n_i$ can be as $n_i \to \infty$.

On (ℓ, δ)-bounds for codes. A sequence $\{\mathcal{C}_i\}_{i=0}^{\infty}$ of $[n_i, k_i, d_i]$-codes over $\mathbb{F}_q$ is *asymptotically good over $\mathbb{F}_q$* if

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

where $n_i \to \infty$ as $i \to \infty$. In view of this, we propose the following

Definition 2.1. Let $\ell, \delta \in (0, 1)$ such that $\ell > \delta$. A sequence $\{\mathcal{C}_i\}_{i=0}^{\infty}$ of $[n_i, k_i, d_i]$-codes over $\mathbb{F}_q$ is said to attain an *(ℓ, δ)-bound over $\mathbb{F}_q$* if

$$\liminf_{i \to \infty} \frac{k_i}{n_i} \geq \ell - \delta \qquad \text{and} \qquad \liminf_{i \to \infty} \frac{d_i}{n_i} \geq \delta \,.$$

In particular, $\{\mathcal{C}_i\}_{i=0}^{\infty}$ is asymptotically good.

Thus, a lower bound for the above mentioned goodness of a code is obtained for a sufficiently large index i since, as $i \to \infty$ we have

$$\frac{k_i}{n_i} + \frac{d_i}{n_i} \sim \ell - \delta + \delta = \ell.$$

In other words, an (ℓ, δ)-bound says more than the good asymptotic behaviour of the sequence of codes $\{\mathcal{C}_i\}_{i=0}^{\infty}$. In fact, any (ℓ, δ)-bound gives a linear function as a lower bound for the *Manin's function $\alpha_q(\delta)$*; namely, for $0 \leq \delta \leq 1$, we have

$$(2.1) \qquad\qquad \alpha_q(\delta) \geq \ell - \delta.$$

Consider now the so called *Ihara's function* (see, for instance, [13] and [17])

$$(2.2) \qquad\qquad A(q) := \limsup_{g \to \infty} \frac{N_q(g)}{g} \,,$$

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

$$(2.3) \qquad\qquad c \log q \leq A(q) \leq \sqrt{q} - 1$$

for some positive constant c, where the first inequality is due to Serre ([14]) and the second one to Drinfeld and Vladut ([7]). Moreover, the equality holds in the upper bound for fields of square cardinality, i.e.

$$(2.4) \qquad\qquad A(q^2) = q - 1.$$

There are some improvements and refinements of lower bounds for $A(q)$, as can be seen in [13].

The famous *Tsfasman-Vladut-Zink bound over $\mathbb{F}_q$* (*TVZ-bound* for short) is an example of an (ℓ, δ)-bound with $\delta > 0$ and

$$(2.5) \qquad\qquad \ell = 1 - A(q)^{-1}$$

if $A(q) > 1$. For squares $q \geq 49$, the TVZ-bound over $\mathbb{F}_q$ improves the Gilbert-Varshamov bound which was considered, for some time, the best lower bound for Manin's function (see [17], [16] and [18]). The GV-bound can also be seen as an (ℓ, δ)-bound with

$$\ell = \delta + 1 - H_q(\tfrac{\delta}{2}),$$

where H_q is the q-ary entropy function $H_q(x) = x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x)$ for $0 \leq x \leq 1 - \frac{1}{q}$ and $H_q(0) = 0$.

Towers. A function field (of one variable) over K is a finite algebraic extension F of the rational function field $K(x)$, where x is a transcendental element over K. Following [17], a sequence $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ of function fields over a K is called a *tower* if for every $i \geq 0$ we have

   (1) $F_i \subsetneq F_{i+1}$;
   (2) the extension F_{i+1}/F_i is finite and separable;
   (3) K is perfect and algebraically closed in F_i; and
   (4) the genus $g(F_i)$ of F_i tends to infinity, for $i \to \infty$.

A tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over K is called *recursive* if there exist a sequence of transcendental elements $\{x_i\}_{i=0}^{\infty}$ over K and a polynomial $H(X, Y) \in K[X, Y]$ such that $F_0 = K(x_0)$ and

$$F_{i+1} = F_i(x_{i+1}) \quad \text{where} \quad H(x_i, x_{i+1}) = 0 \quad \text{for all } i \geq 0.$$

Now we define the concept of asymptotic behaviour of a tower. Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be a tower of function fields over K. The *genus* of $\mathcal{F}$ over F_0 is defined as

$$(2.6) \qquad\qquad\qquad\qquad \gamma(\mathcal{F}) := \lim_{i \to \infty} \frac{g(F_i)}{[F_i : F_0]}.$$

where $g(F_i)$ stands for the genus of F_i. Notice that $0 < \gamma(\mathcal{F}) \leq \infty$. When K is finite, we denote by $N(F_i)$ the number of rational places (i.e., places of degree one) of F_i and the *splitting rate* of $\mathcal{F}$ over F_0 is defined as

$$(2.7) \qquad\qquad\qquad\qquad \nu(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{[F_i : F_0]}.$$

Notice that $0 \leq \nu(\mathcal{F}) < \infty$.

A tower $\mathcal{F}$ is called *asymptotically good* over a finite field K if

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

Otherwise is called *asymptotically bad*. Equivalently, $\mathcal{F}$ is asymptotically good over K if and only if *the limit* of the tower $\mathcal{F}$ is positive, i.e.

$$(2.8) \qquad\qquad\qquad\qquad \lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)} = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})} > 0.$$

Notice that if $\mathcal{F}$ is a tower of function fields over $\mathbb{F}_q$ then $\lambda(\mathcal{F}) \leq A(q)$. The tower is said to be *optimal* if $\lambda(\mathcal{F}) = A(q)$.

3. Good AG-codes from sequences of function fields

Many families of $\mathbb{F}_q$-linear codes have been proved to attain the TVZ-bound using Goppa ideas for constructing linear codes from the set of rational points of algebraic curves over $\mathbb{F}_q$. They are called *algebraic geometry* codes (or simply AG-codes) and some standard references for them are the books [17], [18], [11], [12] and [15].

We now recall their construction using the terminology of function fields (instead of algebraic curves). Let F be an algebraic function field over $\mathbb{F}_q$, let G an $D = P_1 + \cdots + P_n$ be disjoint divisors of F, where $P_1, \ldots, P_n$ are different rational places of F. Consider now the Riemann-Roch space

$\mathcal{L}(G) = \{u \in F \setminus \{0\} : (u) \geq -G\} \cup \{0\}$ associated to G, where (u) denotes the principal divisor of $u \in F$. The algebraic-geometry code defined by F, D and G is

$$(3.1) \qquad \mathcal{C} = C_{\mathcal{L}}(D, G) = \left\{ \big(u(P_1), u(P_2), \ldots, u(P_n)\big) \in \mathbb{F}_q^n : u \in \mathcal{L}(G) \right\},$$

with $u(P_i)$ standing for the residue class of x modulo P_i.

An important feature of these $[n, k, d]$-codes is that lower bounds for k and d are available in terms of the genus $g = g(F)$ of F and the degree $\deg G$ of G. More precisely, $k \geq \deg G + 1 - g$ if $\deg G < n$ and $d \geq n - \deg G$. Furthermore, if $2g - 2 < \deg G < n$ then $k = \deg G + 1 - g$.

Good AG-codes from sequences. There is a standard way to construct a sequence of AG-codes over a finite field $\mathbb{F}_q$ attaining an (ℓ, δ)-bound, as we show next. We include the proof for the convenience of the reader.

Proposition 3.1. *Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be a sequence of algebraic function fields over $\mathbb{F}_q$ with $\mathbb{F}_q$ as their full field of constants and such that for each $i \geq 0$ there are n_i rational places $P_{i,1}, \ldots, P_{i,n_i}$ in F_i with $n_i \in \mathbb{N}$. Let $\lambda \in (0, 1)$ and suppose that the following three conditions hold:*

(a) $n_i \to \infty$ as $i \to \infty$;

(b) there exists an index i_0 such that $\frac{g(F_i)}{n_i} \leq \lambda$ for all $i \geq i_0$; and

(c) for each $i > 0$ there is a divisor G_i of F_i which is disjoint with $D_i := P_{i,1} + \cdots + P_{i,n_i}$ such that $\deg G_i \leq n_i \cdot \alpha(i)$, where $\alpha : \mathbb{N} \to \mathbb{R}$ with $\alpha(i) \to 0$ as $i \to \infty$.

Then, there exists a sequence $\{r_i\}_{i=N}^{\infty} \subset \mathbb{N}$, for certain N, such that $\mathcal{F}$ induces a sequence $\mathcal{G} = \{\mathcal{C}_i\}_{i=N}^{\infty}$ of asymptotically good AG-codes $\mathcal{C}_i = C_{\mathcal{L}}(D_i, r_i G_i)$ attaining an (ℓ, δ)-bound with $\ell = 1 - \lambda$. In particular, if $\lambda = A(q)^{-1}$ the sequence $\mathcal{G}$ attains the TVZ-bound.

Proof. Let $\delta \in (0, 1)$ be a fixed real number such that $1 - \delta > \lambda$. Note that δ depends only on λ. Since $\alpha(i) \to 0$ as $i \to \infty$ there exists an index i_1 such that $\alpha(i) < 1 - \delta$ for $i > i_1$. Clearly, we can find a positive integer r_i such that, for every $i \geq i_1$, we have

$$(3.2) \qquad 1 - \delta \geq r_i \frac{\deg G_i}{n_i} > 1 - \delta - \alpha(i).$$

Let us consider now the AG-code $\mathcal{C}_i = C_{\mathcal{L}}(D_i, r_i G_i)$ for $i \geq i_0$. This is a code of length n_i and we have that its minimum distance d_i satisfies $d_i \geq n_i - r_i \deg G_i$. From this and the first inequality in (3.2) we see that the relative minimum distance $\mathcal{C}_i$ satisfies

$$\frac{d_i}{n_i} \geq 1 - r_i \frac{\deg G_i}{n_i} \geq \delta.$$

On the other hand, for the dimension k_i of $\mathcal{C}_i$ we have

$$k_i \geq r_i \deg G_i + 1 - g(F_i) > r_i \deg G_i - g(F_i).$$

So that by (b) and the second inequality in (3.2) the information rate of $\mathcal{C}_i$ satisfies

$$\frac{k_i}{n_i} > \frac{r_i \deg G_i}{n_i} - \frac{g(F_i)}{n_i} \geq \frac{r_i \deg G_i}{n_i} - \lambda \geq 1 - \delta - \alpha(i) - \lambda$$

for $i \geq N = \max\{i_0, i_1\}$. Therefore,

$$\liminf_{i \to \infty} \frac{k_i}{n_i} \geq 1 - \lambda - \delta \qquad \text{and} \qquad \liminf_{i \to \infty} \frac{d_i}{n_i} \geq \delta,$$

showing that the sequence of AG-codes $\{\mathcal{C}_i\}_{i=N}^{\infty}$ attains an (ℓ, δ)-bound with $\ell = 1 - \lambda$. The remaining assertions follows directly from (2.5). $\qquad \square$

Remark 3.2. It is easy to see that in a concrete situation the crucial properties to have are conditions (a) and (b). In fact, once (a) and (b) are satisfied, condition (c) is not a problem unless we want the codes $\mathcal{C}_i$ to have some additional structure besides linearity. More precisely, if we have (a) and (b) and we are just looking for a good sequence of linear codes, it suffices to consider $G_i = P_i$, where P_i is a rational place of F_i which is not in the support of D_i. However, this choice of G_i may not be adequate when, for instance, the invariance of G_i under some F_0-embedding of F_i is needed as it happens in the cases of cyclic, transitive or block-transitive AG-codes (see Section 4 for details).

Remark 3.3. By the definition of the Ihara function we have $A(q) \geq \frac{n_i}{g(F_i)} \geq \lambda^{-1}$, where λ is the constant in (b) of Proposition 3.1. By the second inequality in (2.3), we see that

$$\lambda \geq \frac{1}{\sqrt{q} - 1}.$$

This bound tell us that the construction of asymptotically good AG-codes over $\mathbb{F}_q$ provided by Proposition 3.1 can not be carried out for $q \leq 4$, since $\lambda \in (0, 1)$.

Remark 3.4. Proposition 3.1 holds in the case of an asymptotically good tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ of function fields over $\mathbb{F}_q$ with limit $\lambda(\mathcal{F}) > 1$. In fact, if N_i is the number of rational places of F_i then we can take $n_i = N_i - 1$, $G_i = Q_i$ (where Q_i is the rational place of F_i not considered among the n_i chosen rational places) and $\alpha(i) = 1/n_i$. Then

$$\lim_{i \to \infty} \frac{n_i}{g(F_i)} = \lim_{i \to \infty} \frac{N_i - 1}{g(F_i)} = \lambda(\mathcal{F}) > 1,$$

so that there is an index i_0 such that (b) of Proposition 3.1 holds for all $i \geq i_0$ with $\lambda = \lambda(\mathcal{F})^{-1}$. Clearly, items (a) and (c) also holds. Further, notice that if (b) holds using the sequence of function fields of a tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_q$, then

$$\lim_{i \to \infty} \frac{N_i}{g(F_i)} \geq \liminf_{i \to \infty} \frac{n_i}{g(F_i)} \geq \lambda^{-1} > 1$$

so that the limit of the considered tower is bigger than 1.

Some examples. We now use Proposition 3.1 to give examples of asymptotically good AG-codes over $\mathbb{F}_{q^2}$, $\mathbb{F}_{q^3}$ and also over finite fields $\mathbb{F}_q$ of big enough cardinality. Of course, if we require something more than the linearity of the sequence of codes given by Proposition 3.1, the situation becomes much more delicate and restrictive (see the next Section).

Example 3.5. For each $q > 2$ there is a family of AG-codes over $\mathbb{F}_{q^2}$ which is asymptotically good. To show this we just use the function fields in the recursive tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_{q^2}$ of Garcia and Stichtenoth whose defining equation is

$$(3.3) \qquad\qquad y^q + y = \frac{x^q}{x^{q-1} + 1}.$$

It is known (see, for instance, [13, Example 5.4.1]) that $N(F_i) \geq q^{i-1}(q^2 - q) + 1$ and

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

Thus, by taking $n_i = q^{i-1}(q^2 - q)$, we have $n_i + 1$ rational places $P_{i,1}, \ldots, P_{i,n_i}, Q_i$ in F_i and

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

for all $i \geq 1$. We readily see that condition (a) in Proposition 3.1 holds and the same happens with condition (b) with $\lambda = (q-1)^{-1} = A(q^2)^{-1}$. Finally, by taking $G_i = Q_i$, we see that condition (c) also holds with $\alpha(i) = 1/n_i$. In this way, by Proposition 3.1, the sequence $\{\mathcal{C}_i\}_{i \in \mathbb{N}}$ of AG-codes $\mathcal{C}_i = C(D_i, Q_i)$, with $D_i = P_{i,1} + \cdots + P_{i,n_i}$, is asymptotically good and attains the TVZ-bound over $\mathbb{F}_{q^2}$ for $q \geq 3$.

Serre's type lower bound for $A(q)$ give us a way to prove that the family of AG-codes over $\mathbb{F}_q$ is asymptotically good for any q large enough.

Example 3.6. It is well known that $A(q) \geq \frac{1}{96} \log_2 q$, for any prime power q ([13, Theorem 5.2.9]). By definition of $A(q)$ there exists a sequence of function fields $\{F_i\}_{i=1}^{\infty}$ over $\mathbb{F}_q$ such that

$$\frac{N_i}{g(F_i)} \geq \tfrac{1}{96} \log_2 q > 1,$$

for $q > 2^{96}$, where $N_i = N(F_i)$. Take $n_i = N_i - 1$ and consider $\mathbb{F}_q$ with $q > 2^{96}$. Thus, condition (b) in Proposition 3.1 holds with $\lambda = \frac{96}{\log_2 q}$ and, since $g(F_i) \to \infty$ as $i \to \infty$, we must have that $N_i \to \infty$ as $i \to \infty$ so that condition (a) also holds. The divisor G_i is simply the remaining rational place of F_i after using the $N_i - 1$ rational places to define D_i. Clearly, condition (c) holds with $\alpha(i) = 1/n_i$. Thus, by Proposition 3.1, there is a sequence of asymptotically good AG-codes over $\mathbb{F}_q$ attaining an (ℓ, δ)-bound for any $q > 2^{96}$ with $\ell = 1 - \frac{96}{\log_2 q}$.

Example 3.7. There is a generalization of Zink's lower bound for $A(q^3)$ proved in [6], namely for any $q \geq 2$ we have

$$A(q^3) \geq \tfrac{2(q^2-1)}{q+2} > 1 \, .$$

A similar argument as in Example 3.6 shows that for any q there is an asymptotically good AG-code over $\mathbb{F}_{q^3}$ attaining an (ℓ, δ)-bound with $\ell = 1 - \frac{q+2}{2(q^2-1)}$.

In the previous examples we have obtained a sequence of AG-codes attaining the TVZ-bound without any additional structure other than linearity. Can one construct good AG-codes with a prescribed property such as for instance cyclicity, transitivity or self-duality? For self-dual and transitive codes this was done in [16]. The problem for cyclic codes is still open. We will show later that there are families of so called block-transitive codes, which we now introduce, attaining the TVZ-bound.

4. GOOD BLOCK-TRANSITIVE CODES

4.1. **Block-transitive codes.** There is a natural action of the group $\mathbb{S}_n$ on $\mathbb{F}_q^n$ given by

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

where $\pi \in \mathbb{S}_n$ and $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$. 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 $\mathcal{C}$ (sometimes denoted by $\mathrm{PAut}(\mathcal{C})$), that is

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

A code $\mathcal{C}$ is called *transitive* if there is a subgroup Γ of $\mathrm{Perm}(\mathcal{C})$ acting transitively on the co-ordinates of the codewords of $\mathcal{C}$, i.e. for any $c = (c_1, \ldots, c_n) \in \mathcal{C}$ and every $1 \leq i < j \leq n$ there exists $\pi \in \Gamma$ such that $c_{\pi(i)} = c_j$. An important subfamily of transitive codes is the class of *cyclic* codes. These are the codes which are invariant under the action of the cyclic shift $s \in \mathbb{S}_n$ defined by $s(1) = n$ and $s(i) = i - 1$ for $i = 2, \ldots, n$, i.e. a code $\mathcal{C}$ is cyclic if $s \cdot c = (c_{s(1)}, c_{s(2)}, \ldots, c_{s(n)}) = (c_n, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ for every $c = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$.

Suppose now that for a fixed $n \in \mathbb{N}$ we have a partition

(4.1) $$n = m_1 + m_2 + \cdots + m_r$$

where $m_1, \ldots, m_r$ are positive integers. There is a natural action of the direct product of the groups $\mathbb{S}_{m_1} \times \cdots \times \mathbb{S}_{m_r}$ on $\mathbb{F}_q^n = \mathbb{F}_q^{m_1} \times \mathbb{F}_q^{m_2} \times \cdots \times \mathbb{F}_q^{m_r}$, which restricts to $\mathcal{C}$ as well, as follows. Consider any $v \in \mathbb{F}_q^n$ divided into r consecutive blocks v_i of m_i coordinates each,

$$v = (v_1, \ldots, v_r) = (v_{1,1}, \ldots, v_{1,m_1}, \ldots, v_{r,1}, \ldots, v_{r,m_r}).$$

Then, if $\pi = (\pi_1, \ldots, \pi_r) \in \mathbb{S}_{m_1} \times \cdots \times \mathbb{S}_{m_r}$, we have the product action

$$\pi \cdot v = (\pi_1 \cdot v_1, \ldots, \pi_r \cdot v_r) = (v_{1,\pi_1(1)}, \ldots, v_{1,\pi_1(m_1)}, \ldots, v_{r,\pi_r(1)}, \ldots, v_{r,\pi_r(m_r)}).$$

In other words, each $\mathbb{S}_{m_i}$ acts transitively, and in an independent way, on the corresponding blocks in which the words of $\mathbb{F}_q^n$ are divided.

The set of all $(\pi_1, \ldots, \pi_r) \in \mathbb{S}_{m_1} \times \cdots \times \mathbb{S}_{m_r}$ such that $(\pi_1, \ldots, \pi_r) \cdot c \in \mathcal{C}$ for all codewords c of $\mathcal{C}$ forms a subgroup of $\mathbb{S}_{m_1} \times \cdots \times \mathbb{S}_{m_r}$. We call it the *r-block permutation group* of $\mathcal{C}$ and we denote it by $\mathrm{Perm}_r(\mathcal{C})$. Of course, we have $\mathrm{Perm}_r(\mathcal{C}) \leq \mathrm{Perm}(\mathcal{C})$.

Definition 4.1. Let $\mathcal{C}$ be a code over $\mathbb{F}_q$ of length n as in (4.1). In this case we say that $\mathcal{C}$ has length $(m_1, m_2, \ldots, m_r)$. $\mathcal{C}$ is said to be *block-transitive* if for some $r \in \mathbb{N}$ there is a subgroup Γ of $\mathbb{S}_{m_1} \times \cdots \times \mathbb{S}_{m_r}$ acting transitively on $\mathcal{C}$. In other words, if $c = (c_1, c_2, \ldots, c_r) \in \mathcal{C}$, and we consider any of its blocks, say $c_k = (c_{k,1}, \ldots, c_{k,m_k})$, and two indices $1 \leq i < j < m_k$, then there exists $\pi = (\pi_1, \ldots, \pi_r) \in \Gamma$ such that $\pi_k(i) = j$. Moreover, if $m_1 = \cdots = m_r = m$, so therefore $n = rm$, we say that $\mathcal{C}$ is an *r-block transitive* code. If further $\pi_1 = \cdots = \pi_r = \pi$ then we have the *r-quasi transitive* codes defined by Bassa in his Thesis [2]. Notice that 1-block transitive codes are just the transitive codes.

Remark 4.2. To have a transitive code $\mathcal{C}$, Definition 1.4 in [17] requires that the whole group of permutation automorphism of the code acts transitively in $\mathcal{C}$. We allow more general subgroups of $\mathrm{Perm}(\mathcal{C})$ in the definition of transitive codes.

We will next show how to construct geometric block transitive codes. We first recall some standard facts about places in Galois extensions. Let F be a function field over $\mathbb{F}_q$ and let E/F be a finite field extension. If Q is a place of E we will use the standard symbol $Q|P$ to denote that Q lies over the place P of F, i.e. $P = Q \cap F$. Now, assume that E is a separable extension and that $F = \mathbb{F}_q(x)$ is a rational function field over $\mathbb{F}_q$. It is well known (see, for instance, [17]) that the group $\mathrm{Aut}(E/F)$ of $\mathbb{F}_q(x)$-automorphisms of E acts on the set of all places of E and this action is extended naturally to divisors. Even more, if E/F is Galois and $\{P_1, \ldots, P_n\}$ is the set of all places of E lying above a place P of F, then for each $1 \leq i < j \leq n$ there exists $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(P_i) = P_j$. This means that $\mathrm{Gal}(E/F)$ acts transitively on the set $\{P_1, \ldots, P_n\}$.

Let $C_{\mathcal{L}}(D, G)$ be an AG-code as in (3.1). Suppose now that $\sigma(G) = G$ for any $\sigma \in H$ where H is a subgroup of $\mathrm{Aut}(E/F)$. Then, there is an action of H on $C_{\mathcal{L}}(D, G)$ defined as

$$\sigma \cdot \big(u(P_1), u(P_2), \ldots, u(P_n)\big) := \big(u(\sigma(P_1)), u(\sigma(P_2)), \ldots, u(\sigma(P_n))\big).$$

It is clear that all of this implies that the AG-code $C_{\mathcal{L}}(D, G)$ is transitive if H acts transitively on the set $\{P_1, \ldots, P_n\}$. Similarly, if H is a cyclic group then, under the above conditions, the AG-code $C_{\mathcal{L}}(D, G)$ is cyclic.

We first show how to construct a transitive AG-code. Let F be an algebraic function field over $\mathbb{F}_q$ and let P, Q be places in F with P rational. Consider any finite Galois extension E of F of degree n. If P splits completely in E, then the AG-code $\mathcal{C} = C_{\mathcal{L}}^E(D = P_1 + \cdots + P_n, G)$, where $P_i|P$ for $1 \leq i \leq n$ and $G = \sum_{Q'|Q} Q'$ is the divisor obtained by summing over all the

places in E above Q, is well defined since each P_i is rational and disjoint from G. Moreover, $\mathcal{C}$ is transitive, since $\Gamma = \mathrm{Gal}(E/F)$ acts transitively on D and G (hence, in particular, fixing them).

Now, to get r-block transitive AG-codes we proceed as follows. Let E be a finite Galois extension of degree m of a function field F over $\mathbb{F}_q$. Consider r rational places $P_1, \ldots, P_r$ in F which split completely in E and a divisor Q disjoint with all of them. Let $T(P_i) = \{P_{i,1}, \ldots, P_{i,m}\}$ be the places in E above P_i, for each $1 \le i \le r$. Let

$$D = P_{1,1} + \cdots + P_{1,m} + \cdots + P_{r,1} + \cdots + P_{r,m} \qquad \text{and} \qquad G = \sum_{Q'|Q} Q'.$$

Thus, all $P_{i,j}$ are rational and G is disjoint with D. Since $G = \mathrm{Gal}(E/F)$ acts transitively in each $T(P_i)$, $1 \le i \le r$ and fixes D and G, the AG-code $\mathcal{C} = C_{\mathcal{L}}^{E}(D, G)$ is an r-block transitive AG-code.

4.2. **Good block-transitive codes.**
In this subsection we will present sufficient conditions to get good block-transitive AG-codes from towers.

We first review some basic definitions on ramification in towers of algebraic function fields, which will be used throughout the rest of the paper. The standard reference for all of this is [17]. Let F be a function field over a perfect field K and let E be a field extension of F of finite degree. Let Q and P be places of E and F, respectively, with $Q|P$. Also, denote as usual by $e(Q|P)$ and $f(Q|P)$ the ramification index and the inertia degree of $Q|P$, respectively. We say that 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). We say that P *ramifies* in E if $e(Q|P) > 1$ for some place Q of E above P and that it is *totally ramified* in E if there is only one place Q of E lying over P and $e(Q|P) = [E : F]$ (hence $f(Q|P) = 1$). It is known that the different exponent $d(Q|P)$ satisfies $e(Q|P) - 1 \le d(Q|P)$. If $b \in \mathbb{R}$, the extension E/F is called *b-bounded* (see [9]) if for any place P of F and any place Q of E lying over P we have

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

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 $i \ge 1$. 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 $i \ge 1$. Notice that the set $R(\mathcal{F})$ could be empty, finite or even infinite whereas the set $Sp(\mathcal{F})$ could be empty or finite but never infinite. A place P of F_0 is *totally ramified* in the tower if for each $i \ge 1$ there is only one place Q of F_i lying over P and $e(Q|P) = [F_i : F_0]$. We introduce the following definition.

Definition 4.3. Given an integer $\mu > 1$ and a tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$, a place P of F_0 is *absolutely μ-ramified* in $\mathcal{F}$ if for each $i \ge 1$ and any place Q of F_i lying over P we have that $e(R|Q) \ge \mu$ for any place R of F_{i+1} lying over Q.

The tower $\mathcal{F}$ is called *tame* or *tamely ramified* if for any $i \ge 0$, 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 *wild* or *wildly ramified*. Furthermore, $\mathcal{F}$ has *Galois steps* if each extension F_{i+1}/F_i is Galois. One says that $\mathcal{F}$ 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 $\mathbb{F}_q$.

Conditions for the existence of good block-transitive AG-codes from towers. It is known that the class of transitive codes attains the TVZ-bound over $\mathbb{F}_{q^2}$ ([16]), i.e., by (2.4)–(2.5), an (ℓ, δ)-bound with

$$(4.2) \qquad \qquad \ell = 1 - \frac{1}{A(q^2)} = 1 - \frac{1}{q - 1}.$$

Also, from [2], the class of r-quasi transitive codes attains an (ℓ, δ)-bound over $\mathbb{F}_{q^3}$ with

$$\ell = 1 - \frac{q+2}{2r(q-1)}.$$

In both cases wildly ramified towers were used. We will later prove a general result for the case of r-block transitive codes by using both wildly and tamely ramified towers (see Section 6).

Remark 4.4. Note that, by definition, block-transitive codes are direct sums of transitive codes. It is clear that the direct sum of asymptotically good codes is again good. However, even though the family of transitive codes is asymptotically good, nothing can be said in general about the asymptotic behaviour of block-transitive codes, which are a direct sum of possibly different transitive codes.

We now present a general result giving sufficient conditions to have good r-block transitive AG-codes by using the Galois closure of a certain class of towers.

Theorem 4.5. *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 non empty splitting locus $Sp(\mathcal{F})$ and non empty ramification locus $R(\mathcal{F})$. 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*

$$(4.3) \qquad\qquad 0 < g_0 - 1 + \epsilon t < r,$$

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 there is a place $P_0 \in R(\mathcal{F})$ which is absolutely μ-ramified in $\mathcal{F}$ for some $\mu > 1$, then there exists a sequence $\mathcal{G} = \{\mathcal{C}_i\}_{i=0}^{\infty}$ of r-block transitive AG-codes over $\mathbb{F}_q$ attaining a (ℓ, δ)-bound with

$$(4.4) \qquad\qquad \ell = 1 - \frac{g_0 - 1 + \epsilon t}{r}.$$

In particular, the Manin's function satisfies $\alpha_q(\delta) \geq \ell - \delta$. Moreover, the sequence $\mathcal{G}$ is defined over the Galois closure $\mathcal{E}$ of $\mathcal{F}$ with limit $\lambda(\mathcal{E}) > 1$.

Proof. We divide the proof in several steps for clarity.

Step 1: the Galois closure $\mathcal{E}$ of $\mathcal{F}$. Let F_i' be the Galois closure of F_i over F_0, which is simply the compositum of fields of the form $\sigma(F_i)$ where σ ranges over the finitely many F_0-embeddings of F_i into an algebraic closure $\overline{F_0}$ of F_0. Denote by $\mathcal{E} = \{F_i'\}_{i=0}^{\infty}$ the tower which is the Galois closure of $\mathcal{F}$.

From Proposition 2.1, Theorem 2.2 and Remark 2.4 of [9] we have that $\mathcal{E}$ is also a tamely ramified tower of function fields over $\mathbb{F}_q$ with Galois steps or a 2-bounded tower with $\mathbb{F}_q$ as the full field of constants of each F_i'; with the same splitting and ramification locus of $\mathcal{F}$, i.e. $Sp(\mathcal{F}) = Sp(\mathcal{E})$ and $R(\mathcal{F}) = R(\mathcal{E})$, and also

$$(4.5) \qquad \gamma(\mathcal{E}) = \lim_{i \to \infty} \frac{g(F_i')}{[F_i' : F_0]} \leq g(F_0) - 1 + \epsilon \sum_{P \in R(\mathcal{E})} \deg P \leq g_0 - 1 + \epsilon t.$$

On the other hand, each place of Ω also splits completely in the Galois closure F_i' of F_i over F_0, so that we have $n_i = r[F_i' : F_0]$ rational places of F_i'

$$(4.6) \qquad\qquad S_{i,1}, S_{i,2} \ldots, S_{i,n_i}.$$

lying over the places of Ω. Thus, $\nu(\mathcal{E}) \geq r$. Therefore, by hypothesis, (4.5) and (2.8), we get

$$\lambda(\mathcal{E}) \geq \frac{r}{g_0 - 1 + \epsilon t} > 1.$$

Step 2: the codes over $\mathcal{E}$. Now we define a family of AG-codes associated to the tower $\mathcal{E}$. For each $i \geq 1$ let us consider the AG-code

$$(4.7) \qquad\qquad\qquad \mathcal{C}_i = C_{\mathcal{L}}(D_i, r_i G_i),$$

with $r_i \in \mathbb{N}$,

$$(4.8) \qquad\qquad D_i = S_{i,1} + \cdots + S_{i,n_i} \qquad \text{and} \qquad G_i = R_{i,1} + \cdots + R_{i,k_i}.$$

Here the rational places $S_{i,j}$ are the ones given in (4.6) while $R_{i,1}, \ldots, R_{i,k_i}$ are all the places of F_i' lying over P_0. We will show later (see Remark 4.6) an upper bound for the integers r_i, whose existence is given by Proposition 3.1.

Step 3: induction on the degree of the places. Let T_1 be the set of places of F_1 lying over P_0, which is rational by hypothesis. Since F_1/F_0 is Galois and P_0 is absolutely μ-ramified in the tower, for every place $P \in T_1$ we have that $P|P_0$ is ramified with ramification index $e = e(P|P_0) \geq \mu$ and relative degree $f = f(P|Q)$ so that $def = [F_1 : F_0]$ where $d = |T_1|$. Then

$$\deg \sum_{P \in T_1} P = df = \frac{[F_1 : F_0]}{e} \leq \frac{[F_1 : F_0]}{\mu} .$$

Now suppose that

$$\deg \sum_{P \in T_{i-1}} P \leq \frac{[F_{i-1} : F_0]}{\mu^{i-1}} ,$$

where T_{i-1} is the set of places of F_{i-1} lying over P_0. Let $P \in T_{i-1}$ and let $R_1, \ldots, R_{r_P}$ be all the places of F_i lying over P. Since F_i/F_{i-1} is a Galois extension, every place R_j over P is ramified with the same ramification index e_P and relative degree f_P. Thus $r_P e_P f_P = [F_i : F_{i-1}]$ and

$$r_P f_P = \frac{[F_i : F_{i-1}]}{e_P} \leq \frac{[F_i : F_{i-1}]}{\mu} .$$

Hence, by inductive hypothesis, we have

$$\deg \sum_{R \in T_i} R = \sum_{P \in T_{i-1}} r_P f_P \deg P \leq \frac{[F_i : F_{i-1}]}{\mu} \sum_{P \in T_{i-1}} \deg P$$

$$\leq \frac{[F_i : F_{i-1}]}{\mu} \frac{[F_{i-1} : F_0]}{\mu^{i-1}} = \frac{[F_i : F_0]}{\mu^i} ,$$

where T_i is the set of places of F_i lying over P_0. We have proved that if T_i is the set of places of F_i lying over P_0 then

$$(4.9) \qquad\qquad\qquad \deg \sum_{P \in T_i} P \leq \frac{[F_i : F_0]}{\mu^i},$$

for all $i \in \mathbb{N}$.

Step 4: estimating the degree of G_i. We can now give an upper bound for the degree of the divisors G_i. Note that $\operatorname{Sup} G_i \cap F_i = T_i$ and if we denote by $R_{i,1}^P, \ldots, R_{i,n_P}^P$ all the places in $\operatorname{Sup} G_i$ lying

over a place $P \in T_i$, we have that

$$\deg G_i = \sum_{j=1}^{k_i} \deg R_{i,j} = \sum_{P \in T_i} \sum_{t=1}^{n_P} \deg R_{i,t}^P$$

(4.10)
$$= \sum_{P \in T_i} \sum_{t=1}^{n_P} f(R_{i,t}^P|P)\, f(P|P_0) = \sum_{P \in T_i} f(P|P_0) \sum_{t=1}^{n_P} f(R_{i,t}^P|P)$$

$$\leq \sum_{P \in T_i} f(P|P_0)[F_i' : F_i] = [F_i' : F_i] \deg \sum_{P \in T_i} P \leq \frac{[F_i' : F_0]}{\mu^i},$$

where in the last inequality we have used (4.9).

Step 5: obtaining the (ℓ, δ)-bound. We will now apply Proposition 3.1 to the tower $\mathcal{E}$ and the sequence of codes $\mathcal{C}$ given in (4.7) and (4.8). Since $n_i = r[F_i' : F_0]$, condition (a) in the proposition holds. Also, by (4.5) and the hypothesis (4.3), we have

$$\frac{g(F_i')}{n_i} \leq \frac{g_0 - 1 + \epsilon t}{r} < 1$$

for n_i big enough and, hence, condition (b) holds with $\lambda = \frac{1}{r}(g_0 - 1 + \epsilon t) < 1$. Furthermore, from the above upper bound (4.10) for $\deg G_i$ we also have

$$\frac{\deg G_i}{n_i} \leq \frac{1}{\mu^i r},$$

so that condition (c) holds by taking $\alpha(i) = 1/\mu^i r$. In this way, by Proposition 3.1, the sequence $\{\mathcal{C}_i\}_{i=1}^\infty$ of AG-codes $\mathcal{C}_i = C_{\mathcal{L}}(D_i, r_i G_i)$, for certain integers $r_i > 0$ provided by the proof of the proposition, is asymptotically good over $\mathbb{F}_q$ attaining a (ℓ, δ)-bound with

$$\ell = 1 - \frac{g_0 - 1 + \epsilon t}{r}.$$

Final step: block transitivity. Finally, notice that both divisors D_i and G_i are invariant under $\mathrm{Gal}(F_i'/F_0)$ so that by the definition of D_i and the action of $\mathrm{Gal}(F_i'/F_0)$ on the places in the support of D_i, we see at once that $C_{\mathcal{L}}(D_i, r_i G_i)$ is an r-block transitive AG-code over $\mathbb{F}_q$.   □

Now we give a lower bound for the numbers r_i in (4.7), in terms of the parameters given in the hypothesis and the parameter δ, which represents the desired relative minimum distance of the codes $\mathcal{C}_i = C(D_i, r_i G_i)$ in the sequence (as can be seen in the proof of Proposition 3.1). We have

(4.11)
$$r_i \geq (1 - \delta) r \mu^i - 1$$

and hence they are bounded by r, δ and μ for every i.

To see this, without loss of generality we can take $0 < \delta < 1 - q^{-1}$, since Manin's function $\alpha_q(\delta) = 0$ for $1 - q^{-1} \leq \delta < 1$. Let $N = \log_\mu(\frac{q}{r})$. Then, for $i \geq N$ we have $\alpha(i) = \frac{1}{r\mu^i} \leq \frac{1}{q} < 1 - \delta$, and thus (3.2) tell us that

(4.12)
$$\left\lceil (1 - \delta - \frac{1}{\mu^i r}) \frac{n_i}{\deg G_i} \right\rceil \leq r_i \leq \left\lfloor (1 - \delta) \frac{n_i}{\deg G_i} \right\rfloor.$$

Therefore, for $i \geq N$ we get $r_i \geq (1 - \delta - \frac{1}{\mu^i r}) \frac{n_i}{\deg G_i} \geq (1 - \delta) r \mu^i - 1$.

Remark 4.6. At first, it seems that the condition of having an absolutely μ-ramified place in the tower $\mathcal{F}$ in Theorem 4.5 is only for technical reasons, but the above lower bound shows that μ has something to do also with the AG-codes constructed from $\mathcal{F}$.

5. Good block-transitive codes attaining the TVZ-bound

As a consequence of Theorem 4.5, we will next show that the TVZ-bound can be attained by sequences of certain block-transitive codes (constructed from towers of function fields) whose lengths can be computed explicitly while their minimum distances and dimensions can be estimated in terms of the cardinality of the considered finite field $\mathbb{F}_q$. The structure of the Galois groups acting on the codes is also known.

From wildly ramified towers. We will construct good r-block transitive codes over finite fields of square cardinality $\mathbb{F}_{q^2}$, with $r = q^2 - q$. We will need the following notation; let $q > 2$ and put

$$(5.1) \qquad m_i = \begin{cases} q^{2i-1} & (\text{resp. } q^{2i-1-\lfloor i/2 \rfloor}) & \text{if } 1 \le i \le 2 \text{ and } q \text{ is odd (resp. even)}, \\ q^{3i-3} & (\text{resp. } q^{3i-3-\lfloor i/2 \rfloor}) & \text{if } i \ge 3 \text{ and } q \text{ is odd (resp. even)}, \end{cases}$$

for each $i \in \mathbb{N}$.

Theorem 5.1. *Let $q > 2$ be a prime power. Then, there exists a sequence $\mathcal{G} = \{\mathcal{C}_i\}_{i=1}^{\infty}$ 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, where m_i is as in (5.1). By fixing $0 < \delta < 1 - q^{-2}$, we also have that*

$$(5.2) \qquad d_i \ge \delta\,(q^2 - q)m_i \qquad and \qquad k_i \ge \{(1-\delta)(q^2 - q) - (q + q^{-i})\}m_i$$

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

Proof. Let us consider now the wildly ramified tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_{q^2}$ recursively defined by the equation

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

whose optimality was first proved in [8] (see also Section 7.4 of [17]). From these works we know that $\mathcal{F}$ 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. $q^2 - q \le |Sp(\mathcal{F})|$ and $|R(\mathcal{F})| \ge q + 1$.

Thus, we are in the conditions of Theorem 4.5 with

$$\mu = q, \qquad \epsilon = 1, \qquad g_0 = 0, \qquad r = q^2 - q \qquad and \qquad t = q + 1.$$

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

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

which means that this sequence of codes over $\mathbb{F}_{q^2}$ attains the TVZ-bound (see (4.2)). Notice that this can also be checked directly since, from (5.2), we have $\delta_i + R_i \ge 1 - \frac{1}{q-1}$ for every i.

The codes in $\mathcal{G}$ are of the form $\mathcal{C}_i = C_{\mathcal{L}}(D_i, r_i G_i)$ as in (4.7). From [4, Corollary 27] we have that the degree of the extension F_i'/F_0 is given by the number m_i in (5.1), where F_i' is the Galois closure of F_i over F_0. Thus, from the proof of Theorem 4.5, for each $i \ge 1$ we have

$$n_i = r[F_i' : F_0] = (q^2 - q)m_i = rm_i.$$

Now, fix $0 < \delta < 1 - q^{-2}$. Since $\mu = q$, the right hand side of (4.12) is valid for $i \ge 1$, because $\log_q(\frac{q^2}{r}) = \log_q(\frac{q}{q-1}) = 1 - \log_q(q-1) < 1$, and thus

$$d_i \ge n_i - r_i \deg G_i \ge n_i - (1-\delta)n_i = \delta n_i$$

for $i \geq 1$, as desired.

Finally, from [17, Lemma 7.2.3] we know that the sequence of rational numbers $\left\{ \frac{g(F_i')-1}{[F_i':F_0]} \right\}_{i=0}^{\infty}$ is monotonically increasing and its limit is the genus $\gamma(\mathcal{E})$ of the tower $\mathcal{E} = \{F_i'\}_{i=0}^{\infty}$. Also, from the proof of Theorem 4.5 we have an upper bound for the genus $\gamma(\mathcal{E})$ of $\mathcal{E}$. Therefore

$$\frac{g(F_i')-1}{[F_i':F_0]} \leq \gamma(\mathcal{E}) \leq g_0 - 1 + \mu t = q,$$

so that $g(F_i') \leq qm_i + 1$ for $i \geq 0$. From (3.2) we also have

$$r_i \deg G_i \geq (1 - \delta - \tfrac{1}{rq^i})rm_i,$$

for $i \geq 1$. Then, since $k_i \geq r_i \deg G_i + 1 - g(F_i')$, for every $i \geq 1$ we have

$$k_i \geq (1 - \delta - \tfrac{1}{rq^i})rm_i + 1 - (qm_i + 1) = \{(1-\delta)r - (q+q^{-i})\}m_i.$$

It is easy to check that $(1-\delta)r - (q+q^{-i}) > 0$ if $\delta < 1 - \tfrac{1}{r}(q+q^{-i})$. This proves the theorem. □

Example 5.2. By the previous theorem with $q = 3$, there are good sequences of 6-block transitive codes over $\mathbb{F}_9$ attaining a TVZ-bound with $0 < \delta < \tfrac{1}{2}$. Similarly, taking $q = 4$ there are good 12-block transitive codes over $\mathbb{F}_{16}$ with $0 < \delta < \tfrac{2}{3}$.

From tame towers. Here we construct good r-block transitive codes over $\mathbb{F}_{p^2}$, with $r = 2(p-1)$. For $i \in \mathbb{N}$ we put

$$(5.3) \qquad\qquad m_i = \begin{cases} 2^i & \text{if } i = 1, 2, 3, \\ 2^{2i-3} & \text{if } i = 4, 5, \\ 2^{3i-8} & \text{if } i \geq 6. \end{cases}$$

Theorem 5.3. *Let $p \geq 13$ be a prime and put $r = 2(p-1)$. Then, there exists a sequence $\mathcal{C} = \{\mathcal{C}_i\}_{i=1}^{\infty}$ of r-block transitive AG-codes over $\mathbb{F}_{p^2}$ attaining the TVZ-bound. Each $\mathcal{C}_i$ is an $[n_i = rm_i, k_i, d_i]$-code with with m_i as in (5.3). Moreover, by fixing $0 < \delta < 1 - p^{-2}$, we have*

$$(5.4) \qquad d_i \geq 2\delta(p-1)m_i \qquad and \qquad k_i \geq \{2(1-\delta)(p-1) - (2+2^{-i})\}m_i$$

for $i \geq \log_2(p)$, where the second inequality is non trivial if $\delta < 1 - \tfrac{1}{r}(2+2^{-i})$.

Proof. Let $q = p^2$ where p is an odd prime number. The tamely ramified tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_q$ recursively defined by the equation

$$y^2 = \frac{x^2+1}{2x},$$

was shown to be optimal over $\mathbb{F}_q$ in [10]. From [10, Proposition 5.3] we have that the ramification locus $R(\mathcal{F})$ consists of exactly 6 elements and also the pole P_∞ of x_0 in F_0 is totally ramified in the tower. Also, from [10, Theorem 5.5] and [9, Proposition 5.6] we have that there exists a set $\Omega \subset Sp(\mathcal{F})$ of cardinality $2(p-1)$. Thus we are in the conditions of Theorem 4.5 with

$$\mu = 2, \qquad b = \tfrac{1}{2}, \qquad g_0 = 0, \qquad r = 2(p-1) \qquad \text{and} \qquad t = 6.$$

Hence, there exists a sequence of r-block transitive codes over $\mathbb{F}_q$ attaining a (ℓ, δ)-bound with

$$\ell = 1 - \frac{2g_0 - 2 + t}{2r} = 1 - \frac{4}{4(p-1)} = 1 - \frac{1}{p-1},$$

which means that this sequence of codes over $\mathbb{F}_q$ attains the TVZ-bound. Again, this can be easily checked directly from (5.4), since $\delta_i + R_i \geq 1 - \tfrac{1}{p-1}(1 + \tfrac{1}{2^{i+1}})$ for every i.

On the other hand, from [3, Theorem 6.1] we have that if $p \geq 13$ the number m_i in (5.3) is the degree of the extension F_i'/F_0, where F_i' is the Galois closure of F_i over F_0. From the proof of Theorem 4.5 we have that $n_i = r[F_i' : F_0] = 2(p-1)m_i$ for $i \geq 1$ as stated.

Now, fix $0 < \delta < 1 - q^{-1}$. Since $\mu = 2$ the right hand side of (4.12) is valid for $i \geq \log_2(p)$ because

$$\log_2(\tfrac{q}{r}) = \log_2(\tfrac{p^2}{2(p-1)}) = \log_2(p) + \log_2(\tfrac{p}{p-1}) - 1 < \log_2(p).$$

Thus, for $i \geq \log_2(p)$ we have that

$$d_i \geq n_i - r_i \deg G_i \geq n_i - (1-\delta)n_i = \delta n_i,$$

as desired. Finally, as in the proof of Theorem 5.1, we have $\frac{g(F_i')-1}{[F_i':F_0]} \leq \gamma(\mathcal{E}) \leq g_0 - 1 + bt = 2$ for $i \geq 1$, where $\mathcal{E} = \{F_i'\}_{i=0}^\infty$. Then, $g(F_i') \leq 2m_i + 1$ for $i \geq 1$ and, from (3.2), we also have

$$r_i \deg G_i \geq (1 - \delta - \tfrac{2^{-i}}{r})rm_i,$$

for $i \geq \log_2(p)$. Therefore, since $k_i \geq r_i \deg G_i + 1 - g(F_i')$, for $i \geq \log_2(p)$ we have

$$k_i \geq (1 - \delta - \tfrac{2^{-i}}{r})rm_i + 1 - 2m_i - 1 = \{2(1-\delta)(p-1) - 2 - 2^{-i}\}m_i.$$

It is easy to check that $2(1-\delta)(p-1) - 2 - 2^{-i} > 0$ if $\delta < 1 - \frac{1}{r}(2 + 2^{-i})$, and the result follows. $\square$

Example 5.4. By the previous theorem with $p = 13$, there are good sequences of 24-block transitive codes over $\mathbb{F}_{13^2}$ attaining a TVZ-bound with $0 < \delta < \frac{11}{12}$. Also, by taking $p = 17$, there are good sequences of 32-block transitive codes over $\mathbb{F}_{17^2}$ attaining a TVZ-bound with $0 < \delta < \frac{15}{16}$.

Note that the dimensions of the codes in the good sequences of the previous theorems are in geometric progressions. In Theorem 5.1, the common ratio is q^3 if q is odd (if q is even, the ratio $\frac{n_{i+1}}{n_i}$ oscillates between q^3 and q^2 depending on the parity of i) while in Theorem 5.3 it is $2^3 = 8$.

6. Good block-transitive codes from class field towers

Now we prove the existence of good r-block transitive codes over finite fields, not necessarily of quadratic cardinality. This result will also allow us to give examples of asymptotically good r-block transitive codes for many values of r different from the ones given in Theorems 5.1 and 5.3. The price we must pay is that of having weaker bounds for the performance of the codes.

We will need the following notations. Given $n, m \in \mathbb{Z}$, we define the auxiliary function

$$(6.1) \qquad \varepsilon_n(m) = \begin{cases} 1 & \text{if } n \mid m, \\ 0 & \text{if } n \nmid m. \end{cases}$$

Also, for a polynomial $h \in \mathbb{F}_q[t]$, we define

$$(6.2) \qquad \begin{aligned} S_q^2(h) &= \{\beta \in \mathbb{F}_q : h(\beta) \text{ is a non zero square in } \mathbb{F}_q\}, \\ S_q^3(h) &= \{\beta \in \mathbb{F}_q : h(\beta) \text{ is a non zero cube in } \mathbb{F}_q\}. \end{aligned}$$

Theorem 6.1. *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 $\mathbb{F}_q$.*

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

$$(6.3) \qquad 2\sqrt{2u} \leq m - (u + 2 + \varepsilon_2(m)) < 3u.$$

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 $\ell = 1 - \frac{m-2-\varepsilon_2(m)}{4u}$.

(b) Let q be even of the form $q = 2^{2s}$. Suppose there is a set $\Sigma_e \subset S_q^3(h)$ such that $v = |\Sigma_e| > 0$ and

(6.4) $$2\sqrt{3v} \le m - (v + 2 + \varepsilon_3(m)) < 2v - \tfrac{1}{2}.$$

Then, there exists a tamely ramified Galois tower $\mathcal{F}'$ over $\mathbb{F}_q$ with limit $\lambda(\mathcal{F}') \ge \frac{6v}{2(m-\varepsilon_3(m))-3} > 1$. 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 $\ell = 1 - \frac{2m-3-2\varepsilon_3(m)}{6v}$.

Proof. Let x be a transcendental element over $\mathbb{F}_q$ and let $K = \mathbb{F}_q(x)$ the rational field over $\mathbb{F}_q$. We will use the extensions of K given by the super-elliptic equation

(6.5) $$y^n = h(x)$$

with $n = 2$ or 3, depending on whether q is odd or even, respectively.

We now divide the proof in three parts: (i) and (ii) consider the cases of q odd and even respectively, while in (iii) we prove items (a) and (b) of the theorem.

(i) Let q be odd. From our assumptions and Proposition 6.3.1 in [17] we have that the equation (6.5) with $n = 2$ defines a cyclic Galois extension $F_o = \mathbb{F}_q(x, y)$ of degree 2 of K with $\mathbb{F}_q$ as the full field of constants of F_o. Also, the rational places $P_1, \ldots, P_m$ of K, defined by the linear factors of $h(x)$, are totally ramified in F_o/K and no other places than $P_1, \ldots, P_m$ and P_∞ ramify in F_o/K, where P_∞ denotes the pole of x. Moreover, for every place Q_∞ in F over P_∞ we have $e(Q_\infty|P_\infty) = \frac{2}{d}$ with $d = (2, m)$ and the genus of F_o is given by $g(F_o) = \frac{1}{2}(m - d)$. Thus, if m is even then $e(Q_\infty|P_\infty) = 1$, hence there are exactly m (totally) ramified places of K in F_o and $g(F_o) = \frac{m-2}{2}$. On the other hand, if m is odd then we have $m + 1$ (totally) ramified places in F_o/K and $g(F_o) = \frac{m-1}{2}$.

Let P_β be the zero of $x - \beta$ in K with $\beta \in \Sigma_o$. Then, the residual class of $h(x)$ mod P_β is

$$h(x)(P_\beta) = h(\beta) = \gamma^2,$$

for some $\gamma \in \mathbb{F}_q^*$ by hypothesis, and we have that the separable polynomial

$$t^2 - \gamma^2 = (t - \gamma)(t + \gamma)$$

in $\mathbb{F}_q[t]$ corresponds to the reduction mod P_β of the right hand side of the equation $y^2 = h(x)$. By Kummer's theorem [17, Theorem 3.3.7] we see that P_β splits completely into 2 rational places of F_o for each $\beta \in \Sigma_o$.

Now pick a rational place P_0 of K defined by one of the linear factors of $h(x)$ and let Q_0 be the only place of F_o lying above P_0, let $Q_1, \ldots, Q_{2u}$ be the rational places of F_o lying over the places P_β with $\beta \in \Sigma_o$ and put

$$T_o = \{Q_0\} \qquad \text{and} \qquad S_o = \{Q_1, \ldots, Q_{2u}\}.$$

(ii) Suppose now that $q = 2^{2s}$. This condition is equivalent to have $q = 2^m$ and $q \equiv 1 \bmod 3$, which in turn is equivalent to the condition $3 \mid 2^m - 1$. But this last condition holds if and only if m is even, since $2^m - 1 = 2^{m-1} + 2^{m-2} + \cdots + 2^1 + 2^0$ and 3 divides the sum of two consecutive powers of 2 because $2^h + 2^{h-1} = 3 \cdot 2^{h-1}$.

Thus, from our assumptions and [17, Proposition 6.3.1], we have that the equation (6.5) with $n = 3$ defines a cyclic Galois extension $F_e = \mathbb{F}_q(x, y)$ of degree 3 of K, with constant field $\mathbb{F}_q$. Furthermore, any place Q_∞ in F_e over P_∞ satisfies $e(Q_\infty|P_\infty) = \frac{3}{d}$ with $d = (3, m)$ and the genus of F_e is given by $g(F_e) = (m - 1) - \frac{d-1}{2}$. Thus, if $3 \mid m$ then $d = 3$ and $e(Q_\infty|P_\infty) = 1$, hence there are exactly m (totally) ramified places of K in F_e and $g(F_e) = m - 2$. On the other hand, if $3 \nmid m$ then $d = 1$ and hence we have $m + 1$ (totally) ramified places in F_e/K and $g(F) = m - 1$.

Let P_β be the zero of $x - \beta$ in $\mathbb{F}_q(x)$ where $\beta \in \Sigma_e$. Then the residual class of $h(x)$ mod P_β is

$$h(x)(P_\beta) = h(\beta) = \gamma^3,$$

for some $\gamma \in \mathbb{F}_q^*$ by hypothesis, and we have that the separable polynomial

$$t^3 - \gamma^3 = (t - \gamma)(t - \omega\gamma)(t - \omega^2\gamma)$$

in $\mathbb{F}_q[t]$ (where ω is a primitive 3-rd root of unity) corresponds to the reduction mod P_β of the right hand side of the equation $y^3 = h(x)$. By Kummer's theorem [17, Theorem 3.3.7] we see that P_β splits completely into 3 rational places of F_e for each $\beta \in \Sigma_e$.

Again, pick a rational place P_0 of K defined by one of the linear factors of $h(x)$ and let R_0 be the only place of F_e lying above P_0 and $R_1, \ldots, R_{3v}$ be the rational places of F_e lying over the places P_β with $\beta \in \Sigma_e$ and put

$$T_e = \{R_0\} \qquad \text{and} \qquad S_e = \{R_1, \ldots, R_{3v}\}.$$

(iii) Let Σ and F be either Σ_o and F_o or Σ_e and F_e, depending on the parity of q. Then,

$$\mathcal{R}(F/K) := \{P \in \mathbb{P}(K) : P \text{ ramifies in } F\}$$

has cardinality m or $m + 1$ depending on the parities of q and m. More precisely,

$$\#\mathcal{R}(F/K) = m + 1 - \varepsilon_n(m),$$

where $n = 2$ if q is odd and $n = 3$ if q is even. Therefore,

$$\#\mathcal{R}(F/K) \geq 2 + |\Sigma| + 2\sqrt{n|\Sigma|}$$

always holds, by (6.3) and (6.4). Therefore, the T-tamely ramified and S-decomposed Hilbert tower $\mathcal{H}_S^T$ of F is infinite, by Corollary 11 in [1], where $T = T_o$ and $S = S_o$ if q is odd or $T = T_e$ and $S = S_e$ otherwise.

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 that, for any $i \geq 1$, each place in S_o (resp. S_e) splits completely in F_i (hence $\mathbb{F}_q$ is the full constant field of F_i), the place Q_0 (resp. R_0) is tamely and absolutely ramified in the tower, F_i/F_{i-1} is an abelian extension with $[F_i : F] \to \infty$ as $i \to \infty$ and F_i/F_0 is unramified outside T. In particular, $T = R(\mathcal{H}_S^T)$ is the ramification locus of the tower $\mathcal{H}_S^T$.

Then, we are in the situation of Theorem 4.5 with $F_0 = F$, $\Gamma = T$ and $\Omega = S$. Let us check that $g(F) - 1 + \frac{1}{2}|\Gamma| = g(F) - \frac{1}{2} < |\Omega|$ holds in each case. We have seen before that

$$g(F_o) = \tfrac{1}{2}\{m - 1 - \varepsilon_2(m)\} \qquad \text{and} \qquad g(F_e) = m - 1 - \varepsilon_3(m).$$

Thus, by the hypothesis (6.3) and (6.4), we have

$$g(F) - \frac{1}{2} = \begin{cases} \tfrac{1}{2}\{m - 2 - \varepsilon_2(m)\} & < 2u = |S_o|, & \text{if } q \text{ is odd,} \\[2mm] m - \tfrac{3}{2} - \varepsilon_3(m) & < 3v = |S_e|, & \text{if } q \text{ is even.} \end{cases}$$

In this way, equation (4.3) holds and the conclusion in each case thus follows. Finally, note that $\lambda(\mathcal{F}) \geq |S|/\{g(F) - 1 + \frac{1}{2}\} > 1$ as we wanted to see, and also that by (4.4) we get the desired expressions for ℓ in (a) and (b) of the statement, respectively. $\qquad\square$

The case $q = 2^{2s+1}$, not covered in Theorem 6.1, cannot be handled with the method used in the proof. This is because the class field tower obtained in [1] is asymptotically good provided the first step F_0/K is cyclic and for this we need a primitive 3-rd root of unity in K.

We now give an example to show how Theorem 6.1 works.

Example 6.2. (i) Let $\mathbb{F}_{25} = \mathbb{F}_2(\alpha)$ where $\alpha^2 + 4\alpha + 2 = 0$. Since q is odd, (6.3) takes the form

$$2\sqrt{2u} + u + 2 \le m < 4u + 2.$$

Consider the polynomial $h(x) = (x - a_1)(x - a_2) \cdots (x - a_9) \in \mathbb{F}_{25}[x]$ whose roots a_i are given by 2, α, $\alpha + 3$, 2α, $2\alpha + 1$, $2\alpha + 2$, $3\alpha + 1$, $4\alpha + 1$ and $4\alpha + 3$. It is easy to check, using the software SAGE for instance, that

$$S^2_{25}(h) = \{\beta \in \mathbb{F}_{25} \; : \; h(\beta) \text{ is square in } \mathbb{F}^*_{25}\} = \{1, 3, \alpha + 1, 3\alpha + 4\}.$$

Thus, since $m = 9$, (6.3) only holds with $u = 2$. Therefore, by (a) of Theorem 6.1 there exists a sequence of 4-block transitive AG-codes over $\mathbb{F}_{25}$ attaining an (ℓ, δ)-bound with $\ell = 1 - \frac{6}{8} = \frac{1}{4}$, whose associated tamely ramified Galois tower $\mathcal{F}$ has limit $\lambda(\mathcal{F}) \ge \frac{8}{7} = 1.14285714\ldots > 1$.

(ii) Now, let $\mathbb{F}_{64} = \mathbb{F}_{2^6} = \mathbb{F}_2(\alpha)$ where $\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$ and consider the polynomial $h(x) = (x - b_1)(x - b_2) \cdots (x - b_{21})$ of degree 21 over $\mathbb{F}_{64}$ whose roots b_i are

$$0, \; \alpha^2, \; \alpha^2 + \alpha + 1, \; \alpha^3, \; \alpha^3 + 1, \; \alpha^3 + \alpha^2 + \alpha, \; \alpha^4, \alpha^4 + \alpha, \; \alpha^4 + \alpha + 1, \alpha^4 + \alpha^2 + \alpha + 1,$$

$$\alpha^4 + \alpha^3 + \alpha + 1, \alpha^5, \; \alpha^5 + \alpha^2, \; \alpha^5 + \alpha^2 + \alpha, \; \alpha^5 + \alpha^3 + 1, \; \alpha^5 + \alpha^4 + \alpha^2 + 1, \; \alpha^5 + \alpha^4 + \alpha^2 + \alpha,$$

$$\alpha^5 + \alpha^3 + \alpha^2 + \alpha, \; \alpha^5 + \alpha^4 + \alpha^3 + 1, \; \alpha^5 + \alpha^4 + 1, \; \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1.$$

Again, using SAGE, one checks that $\#S^3_{64}(h) = \#\{\beta \in \mathbb{F}_{64} \; : \; h(\beta) \text{ is a cube in } \mathbb{F}^*_{64}\} = 14$. For q even and $m = 21$ expression (6.4) reads

$$2\sqrt{3v} + v + 3 \le 21 < 3v + \tfrac{5}{2}$$

and holds for $v = 7$ and $v = 8$. Therefore, by (b) in the theorem and using $v = 8$ there is a sequence of 24-block transitive AG-codes over $\mathbb{F}_{64}$ attaining an (ℓ, δ)-bound with $\ell = \frac{9}{48}$. The limit of the associated tamely ramified Galois tower $\mathcal{F}'$ has limit $\lambda(\mathcal{F}') \ge 1 + \frac{11}{37} = 1,297\ldots > 1$.

We will now show, as a corollary of the previous theorem, that there are asymptotically good N-block transitive codes over $\mathbb{F}_q$, with N a multiple of 2 or 3, for q big enough depending on N.

Theorem 6.3. *Let $u \ge 2$ and $v \ge 5$. Then,*

(a) there are sequences $\mathcal{F}_u$ of asymptotically good $2u$-block transitive codes over $\mathbb{F}_q$ for every q odd with $q \ge 4(u + 2)^2$ and,

(b) there are sequences $\mathcal{F}_v$ of asymptotically good $3v$-block transitive codes over $\mathbb{F}_q$ for every $q = 2^{2s}$ even with $q \ge 4(2v + 5)^2$ if $v \equiv 0, 1 \bmod 3$ and $q \ge 4(2v + 4)^2$ if $v \equiv 2 \bmod 3$.

Proof. (a) Let q be odd. Given u, equation (6.3) holds for at least one m if $3u - 2\sqrt{2u} > 1$, hence $u \ge 2$. So, assuming $u \ge 2$, we have

(6.6) $$\lceil 2\sqrt{2u} + u + 2 \rceil \le m - \varepsilon_2(m) \le 4u + 1.$$

Note that we can always take $m = 2u + 5$ if m is odd or $m = 2u + 4$ if m is even.

Now, consider the hyperelliptic curve C given by the equation

$$y^2 = h(x) = (x - \alpha_1) \cdots (x - \alpha_m)$$

where $\alpha_i \in \mathbb{F}_q[x]$. It is well known that C has genus $g = [\frac{m-1}{2}]$. Without lost of generality, we will assume that m is odd.

The $\mathbb{F}_q$-rational points of C are $C(\mathbb{F}_q) = \{(\alpha, \beta) \in \mathbb{F}_q^2 : h(\alpha) = \beta^2\}$ and by the Hasse-Weil bound the number N of them is bounded by

$$N \ge q + 1 - 2g\sqrt{q} = q + 1 - (m - 1)\sqrt{q}.$$

There are exactly m rational points of the form $(\alpha, 0)$, i.e. the roots of $h(x)$, plus the point at infinity ∞. To apply Theorem 6.1 we need a set of cardinality $2u$ inside $S_q^2(h)$, so we look for rational points of the form (α, β) with $\beta \neq 0$ such that $h(\alpha) = \beta^2 \neq 0$. This is equivalent to solve the inequality

$$\{q + 1 - (m-1)\sqrt{q}\} - (m+1) \geq 2u.$$

Taking $x^2 = q$, we have to solve for the quadratic inequality

(6.7) $x^2 - (m-1)x - (m - 2u) \geq 0.$

Taking $m = 2u + 5$, (6.7) holds for $x \geq m = 2(u+2)$, that is for every $q > 4(u+2)^2$ odd.

(b) For $q = 2^{2s}$ we proceed similarly as before. Starting from (6.4), since $v \geq 5$, we can take $m = 2v + 5$ odd. Consider now the superelliptic curve $C: y^3 = h(x) = (x - \alpha_1) \cdots (x - \alpha_m)$. By the Riemann-Hurwitz formula, the genus of C is given by

$$g = \tfrac{1}{2}\{3(|R| - 2) - |R|\} + 1 = |R| - 2$$

where $R = \{a_1, \ldots, a_m\}$ if $3 \mid m$ and $R = \{a_1, \ldots, a_m\} \cup \{\infty\}$ if $3 \nmid m$. So, if $v \equiv 0, 1 \bmod 3$, then $3 \nmid m$ and $g = m - 1$ while if $v \equiv 2 \bmod 3$ then $3 \nmid m$ and $g = m - 2$. The number of rational points of C is $N \geq q + 1 - 2(m-1)\sqrt{q}$. Taking $q = x^2$, we have to solve the inequality

$$x^2 + 1 - 2(m - 1 - \varepsilon(m))x - (m + 1) \geq 3v.$$

Thus, if $v \equiv 0, 1 \bmod 3$, this is equivalent to $x^2 - 2(m-1)x - (2m - 1) \geq 0$ and holds true for $x \geq 2m = 2(2v + 5)$, so for every $\mathbb{F}_q$ with $q \geq 4(2v + 5)^2$ even of the form 2^{2s}. Similarly, if $v \equiv 2 \bmod 3$ we get $x \geq 2(m - 1) = 2(2v + 4)$, and the result thus follows. $\square$

Example 6.4. For instance, if q is odd there are families of asymptotically good 4-block transitive codes over $\mathbb{F}_{3^5}$. We give a table with the first values for u and q such that there are good families of $2u$-block transitive codes over $\mathbb{F}_q$, for the first prime characteristics, we give also the first prime field for which these codes exists.

u	$2u$-bt codes	$4(u+2)^2$	fields
2	4-bt codes	64	$\mathbb{F}_{3^4}, \mathbb{F}_{5^3}, \mathbb{F}_{7^3}, \mathbb{F}_{11^2}, \mathbb{F}_{13^2}, \mathbb{F}_{67}$
3	6-bt codes	100	$\mathbb{F}_{3^5}, \mathbb{F}_{5^3}, \mathbb{F}_{7^3}, \mathbb{F}_{11^2}, \mathbb{F}_{13^2}, \mathbb{F}_{101}$
4	8-bt codes	144	$\mathbb{F}_{3^5}, \mathbb{F}_{5^4}, \mathbb{F}_{7^3}, \mathbb{F}_{11^2}, \mathbb{F}_{13^2}, \mathbb{F}_{149}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
12	24-bt codes	784	$\mathbb{F}_{3^7}, \mathbb{F}_{5^5}, \mathbb{F}_{7^4}, \mathbb{F}_{11^3}, \mathbb{F}_{13^3}, \mathbb{F}_{787}$

If q is even, there are families of good 15-block transitive and 18-block and transitive codes in $\mathbb{F}_{2^{10}}$, and hence in $\mathbb{F}_{2^{2s}}$ for any $s \geq 5$. Similarly, there are $3v$-block transitive codes with $7 \leq v \leq 14$ over $\mathbb{F}_{2^{12}}$. In general, for $2^r - 1 \leq v \leq 2^{r+1} - 2$ with $r \geq 2$, there are good families of $3v$-block transitive codes over $\mathbb{F}_{2^{2(r+3)}}$.

7. Good block transitive codes over prime fields

Here we focus in more detail on the construction of asymptotically good sequences of block transitive codes over prime fields $\mathbb{F}_p$. Theorem 6.3 assures that good sequences of both $2u$ and $3u$-block transitive codes over $\mathbb{F}_p$ exist, but the minimum possible value of p grows quadratically with u. We want to find good sequences of r-block transitive codes for small values of r over the smallest prime fields possible. In particular, we want to produce good 4-block transitive codes (which are the more cyclic-like we can get) over small prime fields.

Restriction of good codes to prime fields. Let p be a prime. We respectively denote by k' and d' the dimension and minimum distance of the restriction code $\mathcal{C}'$ over $\mathbb{F}_p$ of an $[n, k, d]$-code $\mathcal{C}$ over $\mathbb{F}_{p^s}$. We clearly have $d' \geq d$ and, from [17, Lemma 9.1.3], also

$$(7.1) \qquad\qquad k' \geq k - (s-1)(n-k) = sk - (s-1)n.$$

Consider a sequence of $[n_i, k_i, d_i]$-codes $\{\mathcal{C}_i\}$ over $\mathbb{F}_{p^s}$ attaining an (ℓ, δ)-bound. Then, we have that $\frac{k_i}{n_i} \geq \ell - \delta$ and $\frac{d_i}{n_i} \geq \delta$, for i big enough. Thus, by (7.1),

$$(7.2) \qquad R'_i = \frac{k'_i}{n_i} \geq \frac{sk_i}{n_i} - s + 1 \geq s\ell - s + 1 - s\delta \qquad \text{and} \qquad \delta'_i = \frac{d'_i}{n_i} \geq \frac{d_i}{n_i} \geq \delta.$$

If $\{\mathcal{C}_i\}_{i=1}^{\infty}$ also attains the TVZ-bound over $\mathbb{F}_{p^{2m}}$, we have

$$\alpha_{p^{2m}}(\delta) \geq 1 - \frac{1}{p^m - 1} - \delta$$

where $\ell = 1 - \frac{1}{p^m-1}$. Then, by (2.1), (2.4) and (7.2), the following lower bound for Manin's function over the prime field $\mathbb{F}_p$ holds

$$(7.3) \qquad\qquad \alpha_p(\delta) \geq 1 - \frac{2m}{p^m - 1} - (2m-1)\delta.$$

That is, we cannot assure that the restricted sequence $\{\mathcal{C}'_i\}$ of codes satisfy an (ℓ', δ')-bound, but they still have a good performance. Furthermore, we have the following.

Lemma 7.1. *Let p be a prime and $\mathcal{G} = \{\mathcal{C}_i\}_{i=1}^{\infty}$ a sequence of codes over $\mathbb{F}_{p^{2m}}$ attaining the TVZ-bound. Then, if $p \geq 5$, the sequence of restricted codes $\mathcal{G}' = \{\mathcal{C}'_i\}_{i=1}^{\infty}$ is asymptotically good over $\mathbb{F}_p$. Also, $\mathcal{G}'$ is asymptotically good over $\mathbb{F}_2$ if $m \geq 3$ and over $\mathbb{F}_3$ if $m \geq 2$.*

Proof. By (7.2) we only need to show that $0 < 2m(\ell - \delta - 1) + 1 < 1$. Since $\mathcal{G}$ attains the TVZ-bound over $\mathbb{F}_{p^{2m}}$, we have $\ell = 1 - \frac{1}{p^m-1}$. This is equivalent to

$$0 < \tfrac{1}{2m} - \tfrac{1}{p^m-1} < 1.$$

This holds for $p = 2$ and $m \geq 3$, $p = 3$ and $m \geq 2$ and for $p \geq 5$ for every m. $\qquad\square$

Now, we show that there are sequences of asymptotically good r-block transitive codes over $\mathbb{F}_p$, for every prime p and some r depending on p.

Proposition 7.2. *Let p be a prime number and m an integer.*

(a) *There are asymptotically good $2(p-1)$-block transitive codes over $\mathbb{F}_p$, for any $p \geq 13$.*
(b) *There are asymptotically good $p^m(p^m - 1)$-block transitive codes over $\mathbb{F}_p$, for every $m \geq 3$ if $p = 2$, $m \geq 2$ if $p = 3$ and $m \geq 1$ if $p \geq 5$.*

Proof. The result follows directly from Theorems 5.1 and 5.3 and Lemma 7.1. $\qquad\square$

Remark 7.3. Notice that by the results in [16] and using Lemma 7.1 we can assure the existence of asymptotically good sequences of transitive codes and self-dual codes over prime fields.

Good 4-*block transitive codes.* Now we present a direct construction of good block-transitive AG-codes over certain prime fields by using Theorem 6.1 and properties of the Legendre symbol. We focus on the case of 4-block transitive codes. We have seen in the previous section (Example 6.4) that good 4-block transitive codes exist for every prime field $\mathbb{F}_p$ with $p \geq 67$. Here we will prove that they also exist for every prime $p \geq 13$ by using properties of Legendre symbols.

Given $m = 2n + 1$, let

$$R_m = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_q$$

such that $\alpha_i^{-1} \notin R_m$ for $i = 1, \ldots, n$. Let $h \in \mathbb{F}_q[t]$ be any separable polynomial of degre m. We know from the proof of Theorem (6.1) that if q is odd and u satisfies (6.3) then there exists a set

$$S_u = \{\beta_1, \ldots, \beta_u\} \in S_q^2(h),$$

that is $h(\beta_j) = \gamma_j^2 \in \mathbb{F}_q^*$ for $j = 1, \ldots, u$. Similarly, if q is even of the form $q = 2^{2s}$ and u satisfies (6.4), then there is $S_u = \{\beta_1, \ldots, \beta_v\} \in S_q^3(h)$, i.e. $h(\beta_j) = \gamma_j^3 \in \mathbb{F}_q^*$ for $j = 1, \ldots, u$. This allowed us to get asymptotically good sequences, say

(7.4) $$\mathcal{G} = \mathcal{G}_{R_n,S_u} := \{C_i^{n,u}\}_{i=1}^\infty,$$

of r-block transitive codes over $\mathbb{F}_q$. Given R_n as before define

(7.5) $$h(t) = h_{R_n}(t) := (t+1)\prod_{i=1}^n (t - \alpha_i)(t - \alpha_i^{-1}) \in \mathbb{F}_q[t].$$

Thus, if u satisfies (6.3) for the given m, then there exists a sequence of $2u$-block transitive codes over $\mathbb{F}_q$ which is asymptotically good. We will say that the sequence $\mathcal{G}$ in (7.4) is *generated* by R_n (or by h_{R_n}) and S_u.

We now want to produce good sequences of r-block transitive codes over prime fields for small values of r. For 4-block transitive codes we have the following result.

Proposition 7.4. *There are asymptotically good* 4-*block transitive codes over* $\mathbb{F}_p$, *for every prime* $p \geq 13$.

Proof. To get 4-btc from Theorem 6.1 we consider $u = 2$. For this u, (6.3) only holds for $m = 9$. So, consider the polynomial $h(t) = h_{S_4}(t) \in \mathbb{F}_p[t]$ given by (7.5) with $n = 4$. Note that we always have $h(0) = 1$, which is a nonzero square in $\mathbb{F}_q$. So, we only need to find an element $\beta \in \mathbb{F}_p$ such that $h(\beta)$ is a nonzero square in $\mathbb{F}_p$.

It is easy to check that for $p \leq 11$ there is no separable polynomial of degree 9 satisfying the required conditions. Let $p = 13, 17, 19$ and 23. It is straightforward to check that the elements $\alpha_1 = 2, \alpha_2 = 3, \alpha_3 = 4$ and $\alpha_4 = 5$ of $\mathbb{F}_p$ with $p = 13, 17$ or 23 satisfy $\alpha_i^{-1} \notin R_4 = \{2, 3, 4, 5\}$ for $i = 1, \ldots, 4$. and

$$h(t) = (t+1)(t-2)(t-7)(t-3)(t-9)(t-4)(t-10)(t-5)(t-8) \in \mathbb{F}_{13}[t],$$
$$h(t) = (t+1)(t-2)(t-9)(t-3)(t-6)(t-4)(t-13)(t-5)(t-9) \in \mathbb{F}_{17}[t],$$
$$h(t) = (t+1)(t-2)(t-12)(t-3)(t-8)(t-4)(t-6)(t-5)(t-14) \in \mathbb{F}_{23}[t].$$

Thus, by taking $\alpha = 11 \in \mathbb{F}_{13}$ we have that $h(11) = 3 = 4^2$ in $\mathbb{F}_{13}$. Similarly, by choosing $\alpha = 1 \in \mathbb{F}_{17}$ and $\alpha = 7 \in \mathbb{F}_{23}$ we get $h(1) = 13 = 8^2$ in $\mathbb{F}_{17}$ and $h(7) = 3 = 7^2$ in $\mathbb{F}_{23}$, respectively.

On the other hand, the inverses of the elements $\alpha_1 = 2, \alpha_2 = 3, \alpha_3 = 4$ and $\alpha_4 = 6$ of $\mathbb{F}_{19}$ are different from $2, 3, 4, 6$ and

$$h(t) = (t+1)(t-2)(t-10)(t-3)(t-13)(t-4)(t-5)(t-6)(t-16),$$

so that by taking $\alpha = 12 \in \mathbb{F}_{19}$ we have that $h(12) = 4 = 2^2$ in $\mathbb{F}_{19}$.

Therefore, there are sequences of 4-block transitive codes over $\mathbb{F}_p$ for $p = 13, 17, 19$ and 23 which are asymptotically good. Proceeding similarly one can find sets $R_4 \in \mathbb{F}_p$ an a nonzero element $\beta \in \mathbb{F}_p$ such that $h(\beta)$ is a nonzero square for p prime with $p \leq 61$. The result holds for $\mathbb{F}_p$ with $p \geq 67$ by Theorem 6.1 and Example 6.4, and thus we are done.   □

For small values of r, we will give asymptotically good sequences of r-bt codes over $\mathbb{F}_p$, generated by explicit sets R_n and S_u.

We now consider the case of an arbitrary prime $p \geq 29$. In this case we can take the same set of roots $R_4 = \{2, 3, 4, 5\}$ of h for every $\mathbb{F}_{p^s}$, s odd. Also, by Fermat's theorem the inverse of a in $\mathbb{F}_p$ is a^{p-2} and, hence, (7.5) takes the form

$$(7.6) \qquad h(t) = (t+1) \prod_{k=2}^{5} (t-k)(t-k^{p-2}) \in \mathbb{F}_{p^s}[t]$$

with s odd. We want to find an element $a \in \mathbb{F}_{p^s}^*$, s odd, such that $h(a)$ is a non zero square in $\mathbb{F}_p$. It suffices to check that $\left(\frac{h(a)}{p}\right) = 1$, where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol modulo p (Jacobi symbol for p odd not prime). Since the Jacobi and Legendre symbols are multiplicative, we have

$$(7.7) \qquad \left(\frac{h(t)}{p^s}\right) = \left(\frac{t+1}{p}\right) \prod_{k=2}^{5} \left(\frac{t-k}{p}\right) \left(\frac{t-k^{p-2}}{p}\right)$$

since s is odd and $\left(\frac{\cdot}{p}\right)^2 = 1$.

Evaluating $h(t)$ at $t = p - j$ for $2 \leq j \leq \lfloor \frac{p-1}{5} \rfloor$ we ensure that $h(p-j) \neq 0$. Thus,

$$(7.8) \qquad h(p-j) = (p - (j-1)) \prod_{k=2}^{5} (p - (j+k))(p - (j+k^{p-2})) \neq 0.$$

Now, computing the Jacobi symbol of $h(p-j)$, we get

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

Note that this last expression involves only k and not its inverse. For instance, for $p \geq 37$ we can take the $j = 2, \dots, 7$ and

$$(7.9) \qquad \begin{aligned} \left(\frac{h(p-2)}{p^s}\right) &= \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) \left(\frac{11}{p}\right), \\ \left(\frac{h(p-3)}{p^s}\right) &= \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) \left(\frac{5}{p}\right) \left(\frac{13}{p}\right), \\ \left(\frac{h(p-4)}{p^s}\right) &= \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) \left(\frac{5}{p}\right) \left(\frac{13}{p}\right) \left(\frac{17}{p}\right), \\ \left(\frac{h(p-5)}{p^s}\right) &= \left(\frac{-1}{p}\right) \left(\frac{11}{p}\right) \left(\frac{13}{p}\right), \\ \left(\frac{h(p-6)}{p^s}\right) &= \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) \left(\frac{3}{p}\right) \left(\frac{5}{p}\right) \left(\frac{11}{p}\right) \left(\frac{13}{p}\right) \left(\frac{19}{p}\right) \left(\frac{31}{p}\right), \\ \left(\frac{h(p-7)}{p^s}\right) &= \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) \left(\frac{29}{p}\right), \end{aligned}$$

for every $s \geq 1$ odd. This reduces the search of a non zero element $\alpha \in \mathbb{F}_p$ such that $h(\alpha)$ is a non zero square in $\mathbb{F}_p$ to the computation of Legendre symbols for a given prime $p \geq 37$.

Corollary 7.5. *There are asymptotically good 4-block transitive AG-codes over $\mathbb{F}_{p^s}$, for any $s \geq 1$ odd, generated by the sets $S = \{2,3,4,5\}$ and $R = \{0, p-j\}$ in $\mathbb{F}_p$, with $2 \leq j \leq 7$, for infinitely many prime numbers p. For instance, for every prime of the form $p = 220k + \ell$, with $k \in \mathbb{N}$ and $\ell \in \{1,9,11,19\}$, the element $p-2$ together with the set S generates an asymptotically good sequence of 4-block transitive codes over $\mathbb{F}_{p^s}$ for every s odd.*

Proof. Consider the polynomial $h(t)$ given in (7.6). It suffices to find infinitely many primes p, such that $\left(\frac{h(p-j)}{p}\right) = 1$, for a given j. Consider first the case $j = 2$. We look for prime numbers p such that

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

We have $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ and $\left(\frac{5}{p}\right) = (-1)^{\lfloor\frac{p-1}{2}\rfloor}$. Hence, $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \bmod 4$, $\left(\frac{-1}{p}\right) = -1$ if $p \equiv 3 \bmod 4$, $\left(\frac{5}{p}\right) = 1$ if $p \equiv \pm 1 \bmod 5$ and $\left(\frac{5}{p}\right) = -1$ if $p \equiv \pm 2 \bmod 5$. As a first step, we find p's satisfying $\left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = 1$. The values $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = 1$ are obtained by taking $p = 20k + 1$ or $p = 20k + 9$ with $k \in \mathbb{N}$, while $\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = -1$ are obtained with $p = 20k + 3$ or $p = 20k + 7$ with $k \in \mathbb{N}$. Now, take $p = (20 \cdot 11)k + j$ with $j = 1,3,7$ or 9 and $k \in \mathbb{N}$. By the quadratic reciprocity law, we have

(7.10) $$\left(\frac{11}{p}\right) = (-1)^{\frac{(11-1)}{2}\frac{(p-1)}{2}}\left(\frac{(20\cdot 11)k+1}{11}\right) = \left(\frac{1}{11}\right) = 1$$

for $j = 1,9$. Similarly, we can do the same considering the cases of different parity in the symbols $\left(\frac{-1}{p}\right)$ and $\left(\frac{5}{p}\right)$. The pattern $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{5}{p}\right) = 1$ holds for $p = 20k + 11$ or $20k + 19$, $k \in \mathbb{N}$. By quadratic reciprocity, (7.10) above is also true for these values of p (however, the pattern $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{5}{p}\right) = -1$ does not lead to a solution of (7.10)).

That is, for every prime number of the form $p = 220k + j$, with $j = 1,9,11,19$ and $k \in \mathbb{N}$, we have that $\left(\frac{h(p-2)}{p}\right) = 1$. Proceeding similarly as before, from the expressions in (7.9) one can prove similar results for $R = \{p - j\}$ with $3 \leq j \leq 7$ and we leave it to the reader. By Dirichlet's theorem on arithmetic progressions, there are infinitely many prime numbers p of the form $220k + 1$, $220k + 9$, $220k + 11$ and $p = 220k + 19$ with $k \in \mathbb{N}$, and thus the result follows. $\square$

Notice that by using the same method as above, one can obtain asymptotically good sequences of 6-block transitive codes over $\mathbb{F}_{p^s}$ for every $s \geq 1$ odd, by considering any two of the expressions in (7.9) simultaneously. But now, since $u = 3$, we have to take $m = 11$ (by (6.3)) and hence we have to consider the polynomial $h(t)$ in (7.6) with $n = 6$, that is (7.7) with $2 \leq k \leq 6$. In other words,

$$\left(\frac{h_6(p-j)}{p^s}\right) = \left(\frac{1-j}{p}\right)\prod_{k=2}^{6}\left(\frac{j+k}{p}\right)\left(\frac{k}{p}\right)\left(\frac{kj+1}{p}\right) = \left(\frac{1-j}{p}\right)\left(\frac{h_5(p-j)}{p^s}\right)\left(\frac{j+6}{p}\right)\left(\frac{6}{p}\right)\left(\frac{6j+1}{p}\right).$$

So, for instance for $j = 2,3$, by (7.8), we have

$$\left(\frac{h_6(p-2)}{p^s}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)\left(\frac{11}{p}\right)\left(\frac{8}{p}\right)\left(\frac{6}{p}\right)\left(\frac{13}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right)\left(\frac{11}{p}\right)\left(\frac{13}{p}\right),$$

$$\left(\frac{h(p-3)}{p^s}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)\left(\frac{13}{p}\right)\left(\frac{9}{p}\right)\left(\frac{6}{p}\right)\left(\frac{19}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right)\left(\frac{13}{p}\right)\left(\frac{19}{p}\right).$$

It is known that $\left(\frac{3}{p}\right) = (-1)^{\lfloor\frac{p+1}{6}\rfloor}$, i.e. $\left(\frac{3}{p}\right) = 1$ if $p \equiv \pm 1 \bmod 12$ and $p \equiv \pm 5 \bmod 12$. Hence, for a prime of the form $p = 60k + 1$ we have that $\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right) = 1$. So, consider a prime of the form

$$p = (11 \cdot 13 \cdot 19 \cdot 60)k + 1 = 163021k + 1, \qquad k \in \mathbb{N}.$$

By applying quadratic reciprocity again, we get $\left(\frac{11}{p}\right) = \left(\frac{13}{p}\right) = \left(\frac{19}{p}\right) = 1$. In this way, for primes of the form $p = (11 \cdot 13 \cdot 19 \cdot 60)k + 1$, $k \in \mathbb{N}$, the sets $S = \{2, 3, 4, 5, 6\}$ and $R = \{0, p-2, p-3\}$ generates an asymptotically good sequence of 6-block transitive codes over $\mathbb{F}_{p^s}$ for every s odd. In particular, for $k = 1$ we get a good family of 6-block transitive codes over $\mathbb{F}_{163021}$.

References

[1] Bruno Angles, Christian Maire. *A note on tamely ramified towers of global function fields.* Finite Fields Appl., 8, no. 2, (207–215) 2002.

[2] Alp Bassa. *Towers of function fields over cubic fields.* PhD Thesis, Duisburg-Essen University, 2006.

[3] Alp Bassa, Peter Beelen. *On the construction of Galois towers.* Contemporary Mathematics, 9–20, Vol. 487, 2009.

[4] Alp Bassa, Peter Beelen. *The Galois closure of Drinfeld modular towers.* J. Number Theory, 131, (561–577) 2011.

[5] Alp Bassa, Peter Beelen, Arnaldo Garcia, Henning Stichtenoth. *An improvement of the gilbert-varshamov bound over nonprime fields.* IEEE Trans. Inform. Theory, 60, no. 7, (3859–3861) 2014.

[6] Juscelino Bezerra, Arnaldo Garcia, Henning Stichtenoth. *An explicit tower of function fields over cubic finite fields and Zink's lower bound.* J. Reine Angew. Math., 589, (159–199) 2005.

[7] S. G. Vlăduţ, V. G. Drinfel'd. *The number of points of an algebraic curve.* (Russian) Funktsional. Anal. i Prilozhen, 17, no. 1, (68–69) 1983.

[8] Arnaldo Garcia, Henning Stichtenoth. *On the asymptotic behaviour of some towers of function fields over finite fields.* J. Number Theory, 61, (248–273) 1996.

[9] Arnaldo Garcia, Henning Stichtenoth. *On the Galois closure of towers.* Recent trends in coding theory and its applications, vol. 41 of *AMS/IP Stud. Adv. Math.*, (83–92), Amer. Math. Soc., 2007.

[10] Arnaldo Garcia, Henning Stichtenoth, Hans-Georg Rück. *On tame towers over finite fields.* J. Reine Angew. Math., 557, (53–80) 2003.

[11] Edgar Martínez-Moro, Carlos Munuera, Diego Ruano, editors. *Advances in algebraic geometry codes*, vol. 5 of *Series on Coding Theory and Cryptology*. World Scientific Publishing, 2008.

[12] Carlos Moreno. *Algebraic curves over finite fields*, vol. 97 of Cambridge Tracts in Mathematics. Cambridge University Press, 1991.

[13] Harald Niederreiter, Chaoping Xing. *Rational points on curves over finite fields: Theory and Applications*, London Mathematical Society Lecture Note Series, 285. Cambridge University Press, Cambridge, 2001.

[14] Jean-Pierre Serre. *Rational points on curves over finite fields.* Unpublished lecture notes by F. Q. Gouvea, Harvard University, 1985.

[15] Serguei A. Stepanov. *Codes on algebraic curves.* Kluwer Academic/Plenum Publishers, New York, 1999.

[16] Henning Stichtenoth. *Transitive and self-dual codes attaining the Tsfasman-Vlăduţ-Zink bound.* IEEE Trans. Inform. Theory, 52, no. 5, (2218–2224), 2006.

[17] Henning Stichtenoth. *Algebraic function fields and codes*, Graduate Texts in Mathematics 254. Springer-Verlag, Berlin, second edition, 2009.

[18] Michael Tsfasman, Serge Vlăduţ, Dmitry Nogin. *Algebraic geometric codes: basic notions*, Mathematical Surveys and Monographs 139. American Mathematical Society, Providence, RI, 2007.

[19] M. A. Tsfasman, S. G. Vlăduţ, Th. Zink. *Modular curves, Shimura curves, and Goppa codes better than Varshamov-Gilbert bound.* Math. Nachrichten, 109, (21–28), 1982.

María Chara – Instituto de Matemática Aplicada del Litoral - UNL - CONICET, (3000) Santa Fe, Argentina. *E-mail: mchara@santafe-conicet.gov.ar*

Ricardo Podestá – CIEM - CONICET, FaMAF, Universidad Nacional de Córdoba, (5000) Córdoba, Argentina. *E-mail: podesta@famaf.unc.edu.ar*

Ricardo Toledano – Departamento de Matemática, Facultad de Ingeniería Química, UNL, (3000) Santa Fe, Argentina. *E-mail: ridatole@gmail.com*