(2, 1)-separating systems beyond the probabilistic bound

Hugues Randriambololona

April 6, 2011

Introduction

One of the most powerful tools to derive lower bounds in extremal combinatorics is the so called *probabilistic method* ([1]). Roughly speaking, to prove the existence of an object of a given size satisfying certain conditions, one shows that a random object of this size (maybe after being slightly modified) has a positive probability to satisfy these conditions.

In many problems the lower bound given by this method is conjectured exact, at least asymptotically, and sometimes one can prove it is indeed so. This means that optimal solutions to such problems are rather common. On the other hand, when the probabilistic lower bound is not asymptotically exact, optimal solutions tend to be rare and have some particular structure. So, from a theoretical point of view, it is of great importance to know whether a problem belongs to one or the other of these two classes.

Aside from this, a slight drawback of the probabilistic method is its non-constructiveness. One shows the existence of a solution, but one cannot exhibit it explicitly in a reasonnable time (say, polynomial in its size). So, it is often advantageous to complement it with constructive methods. Having a construction matching the probabilistic bound is always interesting, but of course, when possible, a construction going beyond the probabilistic bound is even better, since at the same time it also solves the alternative mentionned just above.

The problem we will be dealing with in this paper is that of $(2, 1)$-separation. As can be seen from [24], this problem, and more generally the theory of separating systems, has a quite long history. While its origins could be arguably traced back to [22], its first appearance, in the precise form we will be interested in, can be found in [8], motivated by a problem in electrical engineering. In fact the notion of separation there defined is very natural and ubiquitous, and several authors have introduced and studied equivalent versions, sometimes independently, in various contexts and in various languages.[1] We point out the following two elegant formulations which can be found in [14], the first being

[1] See the literature on: frameproof codes, intersecting codes, covering arrays, hash families...

in terms of information theory (dealing with binary sequences), the second in terms of extremal combinatorics (dealing with set systems):

Problem A. *How many different points can one find in the n-dimensional Hamming space so that no three of them are on a line?* [2]

Problem A*. *How many different subsets can one find in an n-set so that no three A, B, C of them satisfy $A \cap B \subset C \subset A \cup B$?*

The equivalence between these two formulations is seen by identifying each binary sequence with its support set.

We will take the condition in Problem A as the definition of a $(2, 1)$-separating system. It can be rephrased as saying that for any binary sequences x, y, z in the system, with $z \neq x, y$, there has to be a coordinate i such that $z_i \neq x_i, y_i$. Of course this condition could also be considered over larger alphabets, thus giving rise to the notion of $(2, 1)$-separating q-ary codes. For *linear* codes, this says in turn that any two non-zero codewords have intersecting supports. Such a code is then called a *linear intersecting code*.

Denote by $M(n)$ the common solution to Problems A and A*, and define its asymptotic exponent

$$\rho = \limsup_{n\to\infty} \frac{\log_2 M(n)}{n}. \tag{1}$$

It is shown in [14] that ρ satisfies the inequalities

$$1 - \frac{1}{2}\log_2 3 \leq \rho \leq \frac{1}{2} \tag{2}$$

where the derivation of the lower bound

$$1 - \frac{1}{2}\log_2 3 \approx 0.207518\ldots \tag{3}$$

is a typical example of use of the probabilistic method (it also follows from the earlier works [23][13][18][4], some of them of a more coding-theoretic nature, but still non-constructive).

The reader certainly noticed there is plenty of space for improvement between the two bounds in (2), and indeed the main aim of this paper will be to reduce this gap, although by an admittedly modest quantity:

Theorem 1. *The asymptotic exponent ρ satisfies the lower bound*

$$\rho \geq \frac{3}{50}\log_2 11 \approx 0.207565\ldots \tag{4}$$

[2]Here we say three points in a metric space are on a line if they satisfy the triangle inequality with equality. Recall also the n-dimensional Hamming space is the set of length n binary sequences, the Hamming distance between two sequences being the number of coordinates in which they differ.

As we will see, the proof of this theorem is fully constructive. And, however small the improvement from (3) to (4) might be, it is positive enough to ensure this new construction stands beyond the probabilistic bound. In fact, from the author's viewpoint, the tininess of this improvement makes it even nicer, since it results from an almost miraculous numerical coincidence. Do Mathematics have a sense of humour?

Up to now one of the best methods to construct good families of $(2,1)$-separating systems is by concatenation, since a concatenation of $(2,1)$-separating codes is also $(2,1)$-separating. A popular choice (see [5]) for the inner code is the binary non-linear *one-shortened Kerdock*[3] *code* of length $n = 15$ with $M = 128$ codewords. The only possible distances in this code are 0, 6, 8, and 10, so non-trivial equality in the triangular inequality is impossible, hence it is $(2,1)$-separating (see also [15]).

The outer code could then be taken in a family of $(2,1)$-separating or linear intersecting codes over $\mathbb{F}_{128}$, but as we will see, it can be more advantageous to take codes over the smaller field $\mathbb{F}_{121}$. This choice of $\mathbb{F}_{121}$, instead of $\mathbb{F}_{128}$ (or possibly $\mathbb{F}_{125}$), is motivated by the fact that algebraic geometry provides very good codes over fields of *square* order, and combines well with the intersecting support condition; although on the other hand this forces to use only 121 of the 128 codewords of the inner code.

So, denoting by R_q the asymptotic maximal achievable rate for linear intersecting codes over $\mathbb{F}_q$, we find (see [20] for more details):

$$\rho \geq \frac{7}{15} R_{128} \tag{5}$$

$$\rho \geq \frac{\log_2 121}{15} R_{121} \tag{6}$$

and any lower bound on R_{128} or R_{121} will translate in a lower bound for ρ. We recall and compare such known lower bounds on the R_q.

First, one can use the probabilistic method to get ([6] Th. 8.1):

$$R_q \geq 1 - \frac{1}{2}\log_q(2q-1) = \frac{1}{2} - \frac{1}{2}\log_q\left(2 - q^{-1}\right) \tag{7}$$

hence $R_{128} \geq 0.428974$ and $\rho \geq 0.200188$, which is not very far from (3) while equally non-constructive.

Another try: it is easy to show that a linear code of relative minimum distance larger than one-half is intersecting. The Gilbert-Varshamov bound then gives

$$R_q \geq 1 - H_q\left(\frac{1}{2}\right) = \frac{1}{2} - \frac{1}{2}\log_q\left(4 - 4q^{-1}\right) \tag{8}$$

which is worse: $R_{128} \geq 0.357951$ and $\rho \geq 0.167043$.

[3] or Nordstrom-Robinson

If instead one combines the minimum distance criterion with the Tsfasman-Vladut-Zink bound, this gives intersecting AG codes with

$$R_q \geq \frac{1}{2} - \frac{1}{A(q)} \tag{9}$$

where $A(q) = q^{1/2} - 1$ if q is a *square*. Hence $R_{121} \geq 0.4$ and $\rho \geq 0.184503$, still not enough.

In [29] Xing gives a new criterion for an AG code to be intersecting, that does not rely on the minimum distance of the code. From this criterion and a (non-constructive) counting argument in the Jacobian of the curve he deduces

$$R_q \geq \frac{1}{2} - \frac{1}{A(q)} + \frac{1 - 2\log_q(2)}{2A(q)} \tag{10}$$

hence $R_{121} \geq 0.435546$ and $\rho \geq 0.200877$. This is better, but still below (3). However we will improve on Xing's bound (10) as follows:

Theorem 2. *Let q be a prime power with $A(q) > 4$. Then the asymptotic maximal achievable rate for linear intersecting codes over $\mathbb{F}_q$ satisfies*

$$R_q \geq \frac{1}{2} - \frac{1}{2A(q)}. \tag{11}$$

Moreover if $q \geq 25$ is a square, then $R_q \geq \frac{1}{2} - \frac{1}{2(q^{1/2}-1)}$.

This new bound was first conjectured in [20] and, as noted there, it implies Theorem 1. Indeed, it gives $R_{121} \geq \frac{9}{20} = 0.45$, hence combined with (6):

$$\rho \geq \frac{\log_2 121}{15}\frac{9}{20} = \frac{3}{50}\log_2 11 > 0.207565. \tag{12}$$

Thus the rest of this paper will be devoted to the proof of Theorem 2. We will do so by giving an effectively constructible family of linear intersecting codes attaining (11).[4]

As a final remark, it should be noted that there is no reason to believe that the new lower bound on ρ found in Theorem 1 should be exact, although it seems difficult to do significantly better with a concatenation argument similar to the one given here; so it is likely that further improvements will require substantially new methods. On the opposite side, concerning the upper bound $\rho \leq 0.5$, while its proof has been greatly simplified (see [2]), the problem of diminishing it (if possible) is still open.

Also note that the $(2,1)$-separating systems we construct reaching the lower bound in Theorem 1 are non-linear, so it might be instructive to compare with what is known in the linear case. Thus let ρ' be the analogue of ρ when restricting to linear codes, or with our previous notations, $\rho' = R_2$. Then the best lower

[4] at least, provided an effectively constructible family of curves attaining $A(q)$ is known, which will be true in our case of interest

bound on ρ' up to now is still the one given by the probabilistic method, namely 0.207518, while a much closer upper bound is known, 0.2835 (see [12]), and an even closer but conjectural upper bound, 0.2271, solution to $x = 1 - H_2(x)$, could be reasonnably guessed (see [4]: it holds if the binary Gilbert-Varshamov lower bound is exact).

To sum up, for possibly non-linear $(2,1)$-separating systems we have shown

$$0.207565 < \rho \leq 0.5 \tag{13}$$

while in the linear case it is known

$$0.207518 < \rho' < 0.2835 \tag{14}$$

and conjecturally

$$0.207518 < \rho' \overset{?}{<} 0.2271. \tag{15}$$

Obviously $\rho \geq \rho'$, however it is not known whether this inequality is strict or not. If one believes $\rho = \rho'$ (on which the author has no opinion), then it is not so surprising that the improvement in Theorem 1 was so tiny; indeed the room for improvement as suggested by (15) is then much smaller than the one that was given in (2).

The paper is organized as follows.

In section 1 we recall the definition of separating codes. Although perhaps unusual, and not logically necessary, we find it pleasant to express it in the language of metric convexity. This is one of the numerous aspects in which the discrete geometry of Hamming space admits striking similarities with the continuous geometry of Euclidean space, and does not appear to have been so much studied before.

In section 2 we turn to another type of geometry, namely algebraic geometry. We recall Xing's criterion for a generalized Goppa evaluation code to have the intersecting support property ([29]). In fact we give a slight variant of this criterion that allows to deal with pairs of mutually intersecting AG codes, and we use it to give a lower bound on the rates of such pairs. While easier, the proof of this result will serve as a model for the proof of Theorem 2 in the last section; and it is also certainly of independent interest.

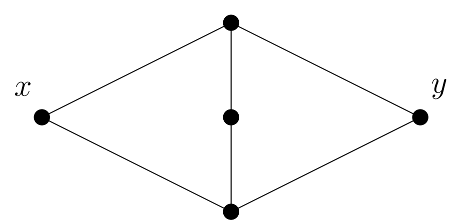
Finally in section 3 we give the full construction that proves Theorem 2. We could hardly qualify this construction as elementary, since it belongs to the realm of algebraic geometry, however we would like to stress that it uses nothing beyond the basic theory of linear systems on curves. So, while (partially) improving on it, it is in some way technically less demanding than [29], where the Jacobian of the curve played a key rôle. And of course it is considerably simpler than [20], where deep and sophisticated number theoretic conjectures were involved in an intricate argument. (On the other hand, this simplicity could have a price: indeed, here we improve only on the case $s = 2$ of [29]. As discussed at the very end of the text, the general case appears more difficult.)

1 Convexity and separation

Let (E, d) be a metric space. For $x, y \in E$ the segment $[x, y]$ is defined as the set of points $z \in E$ satisfying $d(x, y) = d(x, z) + d(z, y)$. A subset K of E is said convex if, whenever $x, y \in K$, then $[x, y] \subset K$. Given a finite subset $S \subset E$, we define its convex hull $\mathrm{Conv}(S)$, as the smallest convex set that contains S.

Definition 3. *Given two integers s, t, a subset $C \subset E$ is said to have the* (s,t)-separation property*, or to be* (s,t)-separated*, or* (s,t)-separating*, if for any subsets $S, T \subset C$ with $|S| \leq s$, $|T| \leq t$, and $S \cap T = \emptyset$, one has also $\mathrm{Conv}(S) \cap \mathrm{Conv}(T) = \emptyset$.*

This allows to consider (s,t)-separation in any metric space (for example, in graphs). However for some spaces these notions are quite poorly behaved. For instance it may happen that segments are not convex:



the bipartite graph $K_{3,2}$

Here, $[x, y] \subsetneq \mathrm{Conv}(x, y)$.

On the other hand, there are spaces in which these notions have very nice properties. We first describe qualitatively what we expect these desirable properties to be:

1. While in general $\mathrm{Conv}(S)$ can always be described "externally" as the intersection of *all* convex sets containing S, this may not be very manageable. One would like that this intersection could be taken over a smaller class of sets.

2. While $\mathrm{Conv}(S)$ can always be constructed "internally", starting with S, and saturating it under the operation that, to a set S', adjoins all the segments $[x, y]$ for $x, y \in S'$, in general the number of iterations in this procedure could not be bounded a priori. One would like to have such a bound (for example, linear, or better, logarithmic in $|S|$).

3. Last, one would like to have a direct or "synthetic" characterization of the individual elements of $\mathrm{Conv}(S)$ in relation to the elements of S.

These three points are best illustrated in the following well-known example.

Let E be a Euclidean space. A half-space in E is (uniquely) defined as a subset of the form

$$H_{l,\alpha} = \{x \in E \mid l(x) \leq \alpha\} = l^{-1}(]-\infty, \alpha]) \tag{16}$$

where l is a linear form on E of (dual) norm 1, and α is a real.

Then, given a finite number of points $x_1, \ldots, x_m \in E$, their convex hull $\mathrm{Conv}(x_1, \ldots, x_m)$ admits the following equivalent descriptions:

1. $\mathrm{Conv}(x_1, \ldots, x_m)$ is the intersection of the *half-spaces* that contain $x_1, \ldots, x_m$.

2. $\mathrm{Conv}(x_1) = \{x_1\}$, and for $m \geq 2$:

$$\mathrm{Conv}(x_1, \ldots, x_m) = \bigcup_{x \in \mathrm{Conv}(x_1, \ldots, x_{m-1})} [x, x_m]. \tag{17}$$

3. More directly:

$$\mathrm{Conv}(x_1, \ldots, x_m) = \left\{ \lambda_1 x_1 + \cdots + \lambda_m x_m \mid \lambda_j \geq 0, \sum \lambda_j = 1 \right\}. \tag{18}$$

We consider now another example, which is a perfect analogue of the preceding, in a discrete setting.

Let Q be a set of cardinality $|Q| = q$ (finite or infinite), and let $E = Q^n$ be the set of length n sequences over the alphabet Q. Equip E with the Hamming distance d.

Define a $\frac{q-1}{q}$-space in E to be a subset of the form

$$H_{i,\alpha} = \{x \in E \mid \pi_i(x) \neq \alpha\} = \pi_i^{-1}(Q \setminus \{\alpha\}) \tag{19}$$

where $\pi_i : E \longrightarrow Q$ is projection on the i-th coordinate ($1 \leq i \leq n$), and $\alpha \in Q$. Remark that such a subset indeed has cardinality $|H_{i,\alpha}| = (q-1)q^{n-1} = \frac{q-1}{q}|E|$. (In particular for $q = 2$ a $\frac{q-1}{q}$-space can legitimately be called a "half-space".)

Proposition 4. *Let $E = Q^n$, equipped with the Hamming distance. Then, given a finite number of points $x_1, \ldots, x_m \in E$, their convex hull $\mathrm{Conv}(x_1, \ldots, x_m)$ admits the following equivalent descriptions:*

1. $\mathrm{Conv}(x_1, \ldots, x_m)$ *is the intersection of the $\frac{q-1}{q}$-spaces that contain $x_1, \ldots, x_m$.*

2. $\mathrm{Conv}(x_1) = \{x_1\}$*, and for $m \geq 2$:*

$$\mathrm{Conv}(x_1, \ldots, x_m) = \bigcup_{x \in \mathrm{Conv}(x_1, \ldots, x_{m-1})} [x, x_m]. \tag{20}$$

3. *More directly:*

$$\mathrm{Conv}(x_1, \ldots, x_m) = \{ x \in E \mid \forall i \;\; \pi_i(x) \in \{\pi_i(x_1), \ldots, \pi_i(x_m)\} \}. \tag{21}$$

Proof. We start with the following *key observation*: for any $x, y \in E$,

$$[x, y] = \{\ z \in E \mid \forall i\ \ \pi_i(z) \in \{\pi_i(x), \pi_i(y)\}\ \}. \tag{22}$$

This was already mentionned in the introduction, and is shown by computing the contribution of each coordinate in the equality case $d(x, y) = d(x, z) + d(z, y)$ of the triangular inequality (or see [14]).

Temporarily define alternative "convex hulls" $\widetilde{\mathrm{Conv}}_1$ $\widetilde{\mathrm{Conv}}_2$ $\widetilde{\mathrm{Conv}}_3$ as given by descriptions 1. 2. 3. respectively (while "Conv" still denotes the original one).

First we prove

$$\widetilde{\mathrm{Conv}}_2(x_1, \ldots, x_m) \subset \mathrm{Conv}(x_1, \ldots, x_m) \tag{23}$$

by induction on m. It clearly holds for $m = 1$, so let $m \geq 2$ and suppose it holds for $m-1$: $\widetilde{\mathrm{Conv}}_2(x_1, \ldots, x_{m-1}) \subset \mathrm{Conv}(x_1, \ldots, x_{m-1})$. Then $\mathrm{Conv}(x_1, \ldots, x_m)$ being convex contains all the segments $[x, x_m]$ for $x \in \widetilde{\mathrm{Conv}}_2(x_1, \ldots, x_{m-1})$, hence it contains $\widetilde{\mathrm{Conv}}_2(x_1, \ldots, x_m)$ as claimed.

Now, in order to show

$$\mathrm{Conv}(x_1, \ldots, x_m) \subset \widetilde{\mathrm{Conv}}_3(x_1, \ldots, x_m) \tag{24}$$

it suffices to show that $\widetilde{\mathrm{Conv}}_3(x_1, \ldots, x_m)$ is convex. This will follow from our *key observation* at the beginning of this proof: if $x, y \in \widetilde{\mathrm{Conv}}_3(x_1, \ldots, x_m)$ and $z \in [x, y]$, then for any i, one has $\pi_i(z) \in \{\pi_i(x), \pi_i(y)\} \subset \{\pi_i(x_1), \ldots, \pi_i(x_m)\}$ hence $z \in \widetilde{\mathrm{Conv}}_3(x_1, \ldots, x_m)$, which is what we wanted.

Now we prove

$$\widetilde{\mathrm{Conv}}_3(x_1, \ldots, x_m) \subset \widetilde{\mathrm{Conv}}_2(x_1, \ldots, x_m) \tag{25}$$

by induction on m. It clearly holds for $m = 1$, so let $m \geq 2$ and suppose it holds for $m - 1$. Pick any $z \in \widetilde{\mathrm{Conv}}_3(x_1, \ldots, x_m)$ and define some $x \in \widetilde{\mathrm{Conv}}_3(x_1, \ldots, x_{m-1})$ coordinate by coordinate as follows:

$$\pi_i(x) = \begin{cases} \pi_i(z) & \text{if } \pi_i(z) \in \{\pi_i(x_1), \ldots, \pi_i(x_{m-1})\} \\ \pi_i(x_1) & \text{if } \pi_i(z) = \pi_i(x_m) \notin \{\pi_i(x_1), \ldots, \pi_i(x_{m-1})\}. \end{cases} \tag{26}$$

Then for all i, $\pi_i(z) \in \{\pi_i(x), \pi_i(x_m)\}$, hence (key observation) $z \in [x, x_m]$, so $z \in \widetilde{\mathrm{Conv}}_2(x_1, \ldots, x_m)$ and the conclusion follows.

Thus we have $\mathrm{Conv} = \widetilde{\mathrm{Conv}}_2 = \widetilde{\mathrm{Conv}}_3$, and to conclude, write for any $S \subset E$:

$$\begin{aligned} \widetilde{\mathrm{Conv}}_1(S) &= \bigcap_{1 \leq i \leq n} \ \bigcap_{\alpha \notin \pi_i(S)} \pi_i^{-1}(Q \setminus \{\alpha\}) \\ &= \bigcap_{1 \leq i \leq n} \pi_i^{-1}(\pi_i(S)) \ = \ \widetilde{\mathrm{Conv}}_3(S) \end{aligned} \tag{27}$$

as wished. □

Drawing the parallel with the Euclidean case, it may be convenient to see 1. as a *discrete Hahn-Banach theorem*: given any (Hamming-)convex set $K \subset Q^n$ and any $x \notin K$, there is a coordinate i that separates x from K, in the sense that $\pi_i(x) \notin \pi_i(K)$.

Remark that when $m = 2$, description 2. asserts that segments are convex.[5] Thus we retrieve the condition asked in Problem A: a code $C \subset Q^n$ is $(2,1)$-separating if for any $x, y, z \in C$ with $z \neq x, y$, one has $z \notin [x, y]$.

More generally, from description 1. (or 3.) in the Proposition, a code $C \subset Q^n$ is (s,t)-separating if for any subsets $S, T \subset C$ with $|S| \leq s$, $|T| \leq t$, and $S \cap T = \emptyset$, there is a coordinate i such that $\pi_i(S) \cap \pi_i(T) = \emptyset$. In this situation we then say that i is a *separating coordinate* for S and T, or equivalently, that the codewords in S and T are *separated* at i. Whether the code itself should be called "separating" or "separated" is a matter of taste; this ambiguity is caused by some "duality" introduced in the shift of point of view from the original notion of separating systems (as it arose from [22]) to the one used in our context.

Remark 5. In fact the Hahn-Banach-like description of convexity in our "nice" spaces allows to define higher notions of separation:

- Given k subsets $S_1, \ldots, S_k$ in Q^n, we say that a coordinate i separates $S_1, \ldots, S_k$ if $\pi_i(S_1), \ldots, \pi_i(S_k)$ are pairwise disjoint. Then, given integers $s_1, \ldots, s_k$ and u, we say that a code $C \subset Q^n$ is u-$(s_1, \ldots, s_k)$-separating, if any pairwise disjoint $S_1, \ldots, S_k \subset C$ with $|S_1| \leq s_1, \ldots, |S_k| \leq s_k$ admit at least u separating coordinates.

- Analogously, if $S_1, \ldots, S_k$ are subsets of a Euclidean space E, we say that a linear form l on E separates $S_1, \ldots, S_k$ if there exist pairwise disjoint intervals $[\alpha_1, \beta_1], \ldots, [\alpha_k, \beta_k] \subset \mathbb{R}$ with $l(S_1) \subset [\alpha_1, \beta_1], \ldots, l(S_k) \subset [\alpha_k, \beta_k]$. Denote by Σ the unit sphere in the dual $E^\vee$, and equip Σ with its natural measure μ, normalized so that it has total mass $\mu(\Sigma) = 1$. Then, given integers $s_1, \ldots, s_k$ and a real $u \in [0,1]$, we say that a subset $C \subset E$ is u-$(s_1, \ldots, s_k)$-separating, if any pairwise disjoint $S_1, \ldots, S_k \subset C$ with $|S_1| \leq s_1, \ldots, |S_k| \leq s_k$ are separated by all linear forms in some subset $\Lambda \subset \Sigma$ of measure $\mu(\Lambda) \geq u$.

Then a code $C \subset Q^n$ (resp. a finite subset $C \subset E$) is (s,t)-separating if and only if it is 1-(s,t)-separating (resp. ϵ-(s,t)-separating for some $\epsilon > 0$).

In the literature one also finds the terminology *s-frameproof* ([3])[6] for $(s,1)$-

[5] More generally, both for Euclidean space and for Hamming space, a slight modification of our proof shows that if S is a finite set, written as a union $S = T \cup T'$, then

$$\mathrm{Conv}(S) = \bigcup_{x \in \mathrm{Conv}(T), x' \in \mathrm{Conv}(T')} [x, x']. \tag{28}$$

As a consequence, if one defines $S_0 = S$ and inductively $S_{i+1} = \bigcup_{x,x' \in S_i} [x, x']$, then $\mathrm{Conv}(S) = S_{\lceil \log_2 |S| \rceil}$.

[6] In fact the original definition of frameproof codes in [3] differed slightly, but it was subsequently modified by the community so as to coincide with the one given here.

separating codes, and *s-secure-frameproof* ([26]) for (s,s)-separating codes. This terminology is mainly used in the context of traitor tracing. Our convex hull $\mathrm{Conv}(S)$ is then called the *feasible set* or the *set of descendants* of S, with description 3. in the Proposition taken as its definition.

Also it is easily shown that a *linear* code is $(s,1)$-separating if and only if the supports of any s non-zero codewords have non-empty intersection (indeed, this amounts to say that the zero codeword is not in their convex hull). In particular, a $(2,1)$-separating linear code is the same thing as a *linear (self-)intersecting code* ([17]).

2 Algebraic geometry codes and the intersecting support property

Here we recall some material from [29], and start to develop from it.

Let K be a field (in the next section we will also suppose K perfect, and actually the reader may assume K is a finite field).

Suppose Y is any scheme over K, and L is an invertible sheaf on Y. For any point $P \in Y(K)$, the fiber $P^*L = L|_P = L_P/\mathfrak{m}_P L_P$ is a one-dimensional K-vector space, so can be (non-canonically) identified with K. Thus, given a finite set of points $G = \{P_1, \ldots, P_n\}$ in $Y(K)$, one can choose (arbitrarily) for each i an isomorphism $L|_{P_i} \simeq K$, and define the generalized Goppa evaluation code $C(G,L)$ as the image of the morphism

$$\phi_{G,L} : \Gamma(Y,L) \longrightarrow \bigoplus_{i=1}^{n} L|_{P_i} \simeq K^n \tag{29}$$

whose components are the natural restriction (or evaluation) morphisms.

This definition depends on the choices made (ordering of the P_i and isomorphisms $L|_{P_i} \simeq K$), but in fact other choices would only modify $\phi_{G,L}$ by composing it with a generalized permutation matrix. So in the end the *equivalence class* of $C(G,L)$ only depends on G and L.

This construction is fairly general, but we will be interested only in the following particular case, which can be described in more elementary terms.

Instead of a general scheme Y, we consider an algebraic curve[7] X over K, of genus g, and $L = \mathcal{O}(D)$ is the invertible sheaf associated with a divisor[8] D on X. We will denote by $\mathcal{L}(D) = \Gamma(X, \mathcal{O}(D))$ its space of global sections, and $l(D) = \dim_K \mathcal{L}(D)$ the dimension of the latter.

Recall X admits a so called *canonical divisor* Ω, which may be taken to be the divisor of any (rational) differential form on X. It has degree $\deg(\Omega) = 2g-2$ and dimension $l(\Omega) = g$. The Riemann-Roch theorem asserts that

$$l(D) = \deg(D) + 1 - g + l(\Omega - D). \tag{30}$$

[7] a smooth, projective, absolutely irreducible 1-dimensional scheme

[8] in this text "divisor" will always mean "K-rational divisor"; likewise, "points" will be "K-points", etc.

In particular $l(D) \geq \deg(D) + 1 - g$, with equality when $\deg(D) \geq 2g - 1$.

Suppose given a divisor G on X that can be written as a sum of distinct K-points, each with multiplicity 1. Let $n = \deg(G) \leq |X(K)|$ be its degree, and choose an ordering $P_1, \ldots, P_n$ of the points in its support, so

$$G = P_1 + \cdots + P_n. \tag{31}$$

Also, for each i, choose a local parameter t_i at P_i. Then, if D is any divisor on X, the section $t_i^{-v_{P_i}(D)}$ is a trivialization for $L = \mathcal{O}(D)$ at P_i. Restricting to the fiber, this trivialization then gives an identification $\mathcal{O}(D)|_{P_i} \simeq K$, and this is the particular choice we will make in (29). Thus, writing $C(G, D)$ for $C(G, \mathcal{O}(D))$ and $\phi_{G,D}$ for $\phi_{G,\mathcal{O}(D)}$, this can be restated as:

Definition 6. *For any divisor D on X, the generalized Goppa evaluation code $C(G, D)$ is the image of the morphism*

$$\begin{array}{cccc} \phi_{G,D}: & \mathcal{L}(D) & \longrightarrow & K^n \\ & f & \mapsto & ((t_1^{v_1} f)(P_1), \ldots, (t_n^{v_n} f)(P_n)) \end{array} \tag{32}$$

where for each i we let $v_i = v_{P_i}(D)$.

The kernel of $\phi_{G,D}$ is $\mathcal{L}(D-G)$. Hence, if $l(D-G) = 0$, then $\dim C(G, D) = l(D)$. This occurs for example when $\deg(D) < n$.

As noted by Xing, this construction generalizes Goppa's evaluation codes, while allowing the supports of G and D to overlap (in fact Xing's original definition also asked D to be positive, but this condition is clearly unnecessary).

A virtue of this description is that the ordering of the P_i and the choice of the t_i are made once and for all, independently of D. This gives some coherence in the choice of our identifications of the fibers $\mathcal{O}(D)|_{P_i} \simeq K$ as D varies, which in turn makes the system of our evaluation maps $\phi_{G,D}$ compatible, in the sense that, given two divisors D and D', the following diagram is commutative:

$$\begin{array}{ccc} \mathcal{L}(D) \times \mathcal{L}(D') & \xrightarrow{\phi_{G,D} \times \phi_{G,D'}} & K^n \times K^n \\ \downarrow & & \downarrow \\ \mathcal{L}(D + D') & \xrightarrow{\phi_{G,D+D'}} & K^n \end{array} \tag{33}$$

where the first vertical map is multiplication in the function field $K(X)$, and the second vertical map is termwise multiplication in K^n. Indeed, both paths in the diagram send $(f, f') \in \mathcal{L}(D) \times \mathcal{L}(D')$ to $((t_1^{v_1+v'_1} ff')(P_1), \ldots, (t_n^{v_n+v'_n} ff')(P_n))$ in K^n.

Said otherwise, the collection of maps $\phi_{G,D}$ define a morphism of K-*algebras*

$$\phi_G : \bigoplus_{D \in \mathrm{Div}(X)} \mathcal{L}(D) \longrightarrow K^n \tag{34}$$

where the multiplication law in K^n is termwise multiplication.

We now recall:

Theorem 7 (Xing's criterion, [29] Th. 3.5, with $s = 2$)**.** *With the preceding notations, suppose* $\deg(D) < n$ *and*

$$l(2D - G) = 0. \tag{35}$$

Then $C(G, D)$ *has dimension* $l(D)$ *and is a linear (self-)intersecting code.*

In fact it is possible to say slightly more.

Two linear codes $C, C' \subset K^n$ are said mutually intersecting if any non-zero codewords $c \in C$ and $c' \in C'$ have intersecting supports. Then:

Proposition 8. *Suppose* D, D' *are divisors on* X *with* $\deg(D) < n$*,* $\deg(D') < n$*, and*

$$l(D + D' - G) = 0. \tag{36}$$

Then $C = C(G, D)$ *and* $C' = C(G, D')$ *have dimension* $l(D) \geq \deg(D) + 1 - g$ *and* $l(D') \geq \deg(D') + 1 - g$ *respectively, and are mutually intersecting.*

Proof. Let $c \in C$ and $c' \in C'$ and suppose the termwise product cc' is zero in K^n. Write $c = \phi_{G,D}(f)$ and $c' = \phi_{G,D'}(f')$ for $f \in \mathcal{L}(D)$ and $f' \in \mathcal{L}(D')$. Then $0 = cc' = \phi_{G,D+D'}(ff')$ so $ff' \in \ker \phi_{G,D+D'} = \mathcal{L}(D + D' - G) = \{0\}$, hence $f = 0$ or $f' = 0$, that is $c = 0$ or $c' = 0$. This proves the intersection property, and then the lower bound on the dimensions follows from Riemann-Roch. □

Remark that this Proposition includes Theorem 7 as a particular case (namely when $D = D'$). In fact the proof given here is essentially the same as Xing's.

Corollary 9. *Suppose*[9] $n > g$*. Let* m *be an integer with* $g \leq m < n$ *and let* D *be a divisor on* X *of degree* $\deg(D) = m$*. Then there exists a divisor* D' *on* X*, with* $\deg(D') = n + g - 1 - m$*, such that* $C = C(G, D)$ *and* $C' = C(G, D')$ *have dimension*

$$\dim C \geq m + 1 - g \tag{37}$$

and

$$\dim C' \geq n - m \tag{38}$$

respectively, and are mutually intersecting.

Proof. For $0 \leq i \leq g$ we construct divisors D'_i such that

$$\deg(D'_i) = n + i - 1 - m \qquad \text{and} \qquad l(D + D'_i - G) = 0 \tag{39}$$

iteratively as follows:

- Start with any divisor D'_0 of degree $n - 1 - m$, hence $\deg(D + D'_0 - G) < 0$ and $l(D + D'_0 - G) = 0$ as asked.
- Suppose up to some $i < g$, we have a divisor D'_i satisfying (39). The divisor $A = D + D'_i - G$ has then degree $\deg(A) = i - 1$ and $l(A) = 0$, and since $|X(K)| > g$, we can apply Lemma 10 below to find P such that $l(A + P) = 0$. Then we set $D'_{i+1} = D'_i + P$, so D'_{i+1} satisfies (39).

[9] note that this implies $|X(K)| > g$, hence in some way "X has many rational points"

- This ends when $i = g$, and we set $D' = D'_g$.

With this choice of D', the conditions in Proposition 8 are satisfied, hence C and C' are mutually intersecting. Moreover, $\dim C' = l(D') \geq \deg(D')+1-g = n-m$ as claimed. □

Lemma 10. *Let X be a curve over K of genus g, and let A be a divisor on X with $\deg(A) \leq g-2$ and*

$$l(A) = 0. \tag{40}$$

Then for all points $P \in X(K)$ except perhaps for at most g of them, we have

$$l(A+P) = 0. \tag{41}$$

Proof (adapted from [25], ch. I, claim (6.8)). By contradiction, suppose there are $g+1$ distinct points $P_1, \dots, P_{g+1} \in X(K)$ for which (41) fails, hence for each $1 \leq i \leq g+1$ we can find a function $f_i \in \mathcal{L}(A+P_i) \setminus \mathcal{L}(A)$. Let also

$$A' = A + P_1 + \cdots + P_{g+1}. \tag{42}$$

Then we also have $f_i \in \mathcal{L}(A') \setminus \mathcal{L}(A'-P_i)$, which means that the quotient space $\mathcal{L}(A')/\mathcal{L}(A'-P_i)$ has dimension 1 and admits f_i as a generator. On the other hand, for $j \neq i$, we have $f_i \in \mathcal{L}(A'-P_j)$, hence f_i maps to 0 in $\mathcal{L}(A')/\mathcal{L}(A'-P_j)$. This implies that the natural map

$$\mathcal{L}(A') \longrightarrow \bigoplus_{i=1}^{g+1} \mathcal{L}(A')/\mathcal{L}(A'-P_i) \tag{43}$$

is onto, hence by the rank theorem,

$$l(A') \geq g+1. \tag{44}$$

But at the same time

$$\deg(A') = \deg(A) + g + 1 \leq 2g-1 \tag{45}$$

which contradicts Riemann-Roch. □

Let q be a prime power. Say that a sequence of curves X_i over the finite field $\mathbb{F}_q$ form an ∞-sequence if the genus g_i of X_i tends to infinity as i goes to infinity.

Let $A(q)$ be the *largest* real number such that there exists an ∞-sequence of curves X_i over $\mathbb{F}_q$ with

$$\frac{|X_i(\mathbb{F}_q)|}{g_i} \underset{i\to\infty}{\longrightarrow} A(q). \tag{46}$$

An ∞-sequence of curves for which this limit is attained is then said *optimal*.

It is known ([7]) that $A(q) \leq q^{1/2}-1$, with equality when q is a square ([11][28]).

Corollary 11. *Suppose $A(q) > 1$. Let r and r' be two positive real numbers such that*

$$r + r' \leq 1 - \frac{1}{A(q)}. \tag{47}$$

Then there exists a sequence of pairs of mutually intersecting codes (C, C') over $\mathbb{F}_q$, of length going to infinity, and of rates at least asymptotically (r, r').

Proof. Let X_i be curves forming an optimal sequence over $\mathbb{F}_q$. Let $G_i = \sum_{P \in X_i(\mathbb{F}_q)} P$ be the sum of all rational points in X_i. Since $A(q) > 1$, one has $n_i = \deg(G_i) = |X_i(\mathbb{F}_q)| > g_i$ for i big enough. Let m_i be a sequence of integers such that $\frac{m_i}{n_i} \longrightarrow r + \frac{1}{A(q)}$ as i goes to infinity (hence $g_i \leq m_i < n_i$ if i is big enough). Let D_i be an arbitrary divisor of degree m_i on X_i, and apply the preceding Corollary 9. This gives mutually intersecting codes (C_i, C_i'), where the rate of C_i is at least

$$\frac{m_i + 1 - g_i}{n_i} \underset{i \to \infty}{\longrightarrow} r + \frac{1}{A(q)} - \frac{1}{A(q)} = r \tag{48}$$

and the rate of C_i' is at least

$$\frac{n_i - m_i}{n_i} \underset{i \to \infty}{\longrightarrow} 1 - r - \frac{1}{A(q)} \geq r' \tag{49}$$

as claimed. □

Remark that for $r = r'$, this last Corollary gives a family of mutually intersecting codes (C, C') of asymptotic rate $\frac{1}{2} - \frac{1}{2A(q)}$. This can be seen as a weak version of Theorem 2, which asserts that this can be done with $C = C'$ (but with more restrictive conditions on q).

3 The construction

From now on K is assumed to be a *perfect* field.

The main technical tool in the proof of Theorem 2 will be the following "higher version" of Lemma 10:

Lemma 12. *Let X be a curve over K of genus g, and let A be a divisor on X with* $\deg(A) \leq g - 3$ *and*

$$l(A) = 0. \tag{50}$$

Then for all points $P \in X(K)$ except perhaps for at most $4g$ of them, we have

$$l(A + 2P) = 0. \tag{51}$$

Proof. We can assume $|X(K)| > 4g \geq g$, otherwise there is nothing to prove. Then, thanks to Lemma 10, successively adding points to A, we can find a divisor $A' \geq A$ with $\deg(A') = g - 3$ and $l(A') = 0$. Then for any $P \in X(K)$ with $l(A + 2P) > 0$, we also have $l(A' + 2P) > 0$. So we can replace A with A', that is, it suffices to prove Lemma 12 with $\deg(A) = g-3$. In turn, by Riemann-Roch, setting $B = \Omega - A$ where Ω is a canonical divisor on X, this is equivalent to the following statement:

If B is a divisor on X with $\deg(B) = g+1$ and $l(B) = 2$, then there are at most $4g$ points $P \in X(K)$ with $l(B-2P) > 0$.

Replacing B by a linearly equivalent divisor, we can suppose $B \geq 0$. Let then $\{1, f\}$ be a basis of $\mathcal{L}(B)$. We will conclude by a degree argument on the differential form df.

First we claim that df is non-zero. If $\operatorname{char} K = 0$ this is true because f is non-constant. If $\operatorname{char} K = p > 0$ then, since K is assumed perfect, $df = 0$ means $f = h^p$ for some $h \in K(X)$. But then $h \in \mathcal{L}(\frac{1}{p}B) \subset \mathcal{L}(B)$ and $\{1, h, f\}$ are linearly independent in $\mathcal{L}(B)$, contradicting our hypothesis $l(B) = 2$.

Let $\mathcal{S} = \{\, P \in X(K) \mid l(B-2P) > 0 \,\}$. We have to show $|\mathcal{S}| \leq 4g$.

Now if P is a closed point (of arbitrary degree) in X, we are in one of these four mutually exclusive situations:

(i) $P \notin \mathcal{S} \cup \operatorname{Supp}(B)$. Then $v_P(f) \geq 0$, and $v_P(df) \geq 0$.

(ii) $P \in \operatorname{Supp}(B) \setminus \mathcal{S}$. Then $v_P(B) \geq 1$, and $v_P(df) \geq v_P(f) - 1 \geq -v_P(B) - 1$ hence

$$v_P(df) \geq -2v_P(B). \tag{52}$$

(iii) $P \in \mathcal{S} \setminus \operatorname{Supp}(B)$. Consider the inclusions $\mathcal{L}(B-2P) \subset \mathcal{L}(B-P) \subset \mathcal{L}(B)$. By hypothesis $l(B) = 2$ and $l(B-2P) > 0$, and since $1 \in \mathcal{L}(B) \setminus \mathcal{L}(B-P)$, necessarily $\mathcal{L}(B-P) = \mathcal{L}(B-2P)$.

Now let $\alpha = f(P)$. Then $f - \alpha \in \mathcal{L}(B-P) = \mathcal{L}(B-2P)$, so $v_P(f-\alpha) \geq 2$, hence $v_P(d(f-\alpha)) \geq 1$. But since $df = d(f-\alpha)$ we conclude:

$$v_P(df) \geq 1. \tag{53}$$

(iv) $P \in \mathcal{S} \cap \operatorname{Supp}(B)$. By hyposthesis $v_P(f) \geq -v_P(B)$ and $v_P(B) \geq 1$. We claim it is impossible to have simultaneously $v_P(f) = -v_P(B)$ and $v_P(B) = 1$.

For if it were the case, then $f \in \mathcal{L}(B) \setminus \mathcal{L}(B-P)$ and $1 \in \mathcal{L}(B-P) \setminus \mathcal{L}(B-2P)$, so all inclusions $\mathcal{L}(B-2P) \subset \mathcal{L}(B-P) \subset \mathcal{L}(B)$ would be strict, contradicting $l(B) = 2$ and $l(B-2P) > 0$.

Thus necessarily $v_P(f) \geq -v_P(B) + 1$ or $v_P(B) \geq 2$. In any case, since $v_P(df) \geq v_P(f) - 1$, this gives

$$v_P(df) \geq -2v_P(B) + 1. \tag{54}$$

Now summing these inequalities we find

$$2g - 2 = \deg(\operatorname{div} df) = \sum_P v_P(df) \deg(P) \geq -2\deg(B) + |\mathcal{S}| \tag{55}$$

and since $\deg(B) = g+1$ this gives $|\mathcal{S}| \leq 4g$ as claimed. □

Proposition 13. *Let X be a curve over K of genus g, and suppose*

$$|X(K)| > 4g. \tag{56}$$

Let G be a divisor on X, of degree $n = \deg(G) \in \mathbb{Z}$. Then there exists a divisor D on X of degree $\deg(D) = \lfloor \frac{n+g-1}{2} \rfloor$ (or equivalently: $g-2 \leq \deg(2D-G) < g$), such that

$$l(2D - G) = 0. \tag{57}$$

Proof. For $0 \leq i \leq N = \lfloor \frac{n+g-1}{2} \rfloor - \lfloor \frac{n-1}{2} \rfloor$ we construct divisors D_i such that

$$\deg(D_i) = i + \left\lfloor \frac{n-1}{2} \right\rfloor \qquad \text{and} \qquad l(2D_i - G) = 0 \tag{58}$$

iteratively as follows:

- Start with any[10] divisor D_0 of degree $\lfloor \frac{n-1}{2} \rfloor$, hence $\deg(2D_0 - G) < 0$ and $l(2D_0 - G) = 0$ as asked.
- Suppose up to some $i < N$, we have a divisor D_i satisfying (58). The divisor $A = 2D_i - G$ then satisfies $-2 \leq \deg(A) < g - 2$ and $l(A) = 0$, so by (56) and Lemma 12 we can find $P \in X(K)$ such that $l(A + 2P) = 0$. Then we set $D_{i+1} = D_i + P$, and D_{i+1} satisfies (58).
- This ends when $i = N$, and we can set $D = D_N$.

□

Remark that the construction given in the proof involves roughly $g/2$ iterations, and each step requires testing at most $4g + 1$ points. So, as soon as a curve of genus g, as well as sufficiently many of its rational points, and the various Riemann-Roch spaces $\mathcal{L}(A)$, can be computed in time polynomial in g, then the overall construction will be polynomial in g.

Corollary 14. *Let X be a curve over K of genus g, such that $|X(K)| > 4g$. Let n be an integer such that $g < n \leq |X(K)|$. Then there exists a linear intersecting code C over K, of length n and dimension*

$$\dim C \ \geq \ \left\lfloor \frac{n+g-1}{2} \right\rfloor + 1 - g \ \geq \ \frac{n-g}{2}. \tag{59}$$

Proof. Let $G = P_1 + \cdots + P_n$ for pairwise distinct $P_i \in X(K)$. The Proposition gives a divisor D on X of degree $\deg(D) = \lfloor \frac{n+g-1}{2} \rfloor < n$ with $l(2D - G) = 0$. The conclusion then follows from Theorem 7, with $C = C(G, D)$. □

We can now proceed with:

[10] For example take $P_0 \in X(K)$ and set $D_0 = \lfloor \frac{n-1}{2} \rfloor P_0$. Remark that $X(K)$ is non-empty, because of (56).

Proof of Theorem 2. Let X_i be curves forming an optimal sequence over $\mathbb{F}_q$, let g_i be the genus of X_i, and let G_i be the sum of all points in $X_i(\mathbb{F}_q)$, so $n_i = \deg(G_i) = |X_i(\mathbb{F}_q)|$. By definition we have $g_i \to \infty$ and $n_i/g_i \to A(q) > 4$, so $n_i > 4g_i$ if i is big enough. The preceding corollary then gives a linear intersecting code C_i over $\mathbb{F}_q$ of rate at least

$$\frac{1 - g_i/n_i}{2} \underset{i\to\infty}{\longrightarrow} \frac{1}{2} - \frac{1}{2A(q)} \tag{60}$$

as asked.

If $q \geq 25$ is a square, then $A(q) = q^{1/2} - 1$, and the conclusion follows, except perhaps for $q = 25$, $A(q) = 4$. But in this last particular case, we know that the sequence of modular curves $X_0(11\ell)$, for $\ell \geq 13$ prime, has genus $g_\ell = \ell$ and number of points $|X_0(11\ell)(\mathbb{F}_{25})| \geq 4\ell + 4 > 4g_\ell$, and we conclude in the same way. □

As regards constructiveness issues in this last proof, note that when q is a square, such optimal sequences are known explicitly (see for example [9]), and all computations in the Proposition can be made in polynomial time, hence the overall construction can be made in polynomial time (although perhaps with constants and exponents too big to be really useful in practice).

Remark 15. We finish by noting two possible improvements on Theorem 2.

(i) In fact the hypothesis $A(q) > 4$ (or $q = 25$, $A(q) = 4$) in Theorem 2 is not optimal. This constant 4 comes from Lemma 12, and it turns out that the estimation in this lemma (as well as the one in Lemma 10, by the way) can be slightly improved, as done in [21] (the proof is more technically involved).

From this stronger version of the lemma one can show that the conclusion in Theorem 2 holds already when $A(q) \geq 4 - \frac{12q^2-4}{q^4+2q^2-1}$ (see [21] for more details).

Clearly this improvement is small, not to say unimpressive, and for the application to Theorem 1, we only need the case $q = 121$, $A(q) = 10$, so we can leave such refinements apart. Nevertheless, further relaxing of the condition on q in Theorem 2 could have interest by itself.

(ii) Theorem 2 is concerned only in improving the case $s = 2$ of Xing's bound ([29], we will keep his notations), since this is all we need for Theorem 1 again. However, following [20], it is natural to conjecture that, for any s, and maybe under suitable conditions on q,

$$R_q(s) \geq \frac{1}{s} - \frac{1}{A(q)} + \frac{1}{sA(q)}. \tag{61}$$

If one tries to prove (61) with a method similar to the one given here, one will construct inductively some divisors A of controlled degree and dimension $l(A) = 0$, and the main point will be to show that, given sufficiently many points, there is one of them, say P, such that $l(A+sP) = 0$ (of which Lemma 10 is the case $s = 1$ and Lemma 12 the case $s = 2$). Equivalently (see e.g. [16] or [27]) one has to prove that $B = \Omega - A$ has order sequence at P starting with $\epsilon_0(P) = 0, \ldots, \epsilon_{s-1}(P) = s - 1$. A necessary condition for this to be possible, is that B has *generic* order sequence starting with $\epsilon_0 = 0, \ldots, \epsilon_{s-1} = s - 1$. If this holds, the existence of P can be derived from a Plücker formula ([16], Theorem 9).

For $s = 2$, it is known that any complete linear system has generic order sequence starting with $\epsilon_0 = 0$ and $\epsilon_1 = 1$. In our situation, this is equivalent to the non-vanishing of df established during the proof of Lemma 12 — and then the proof of Lemma 12 proceeds with a variant of the Plücker formulas suitable for our particular case (classically, this relies on Wronskians; in the proof given here, the Wronskian is just df).

Unfortunately, for $s \geq 3$, not all divisors B have generic order sequence starting with $\epsilon_0 = 0, \ldots, \epsilon_{s-1} = s - 1$. While this is known to hold for "most" divisors ([19]), it might be difficult to ensure that it is so for the particular divisors constructed in an inductive procedure such as ours.

References

[1] N. Alon and J. H. Spencer, *The probabilistic method, 2nd ed.*, Wiley-Interscience, 2000.

[2] S. R. Blackburn, *Frameproof codes*, SIAM J. Discrete Math. **16** (2003) 499–510.

[3] D. Boneh and J. Shaw, *Collusion-secure fingerprinting for digital data*, IEEE Trans. Inform. Theory **44** (1998) 1897–1905.

[4] G. Cohen and A. Lempel, *Linear intersecting codes*, Discr. Math. **56** (1985) 35–43.

[5] G. Cohen and H. G. Schaathun, *Asymptotic overview on separating codes*, Reports in Informatics **248**, Univ. Bergen, 2003.

[6] G. Cohen and G. Zémor, *Intersecting codes and independent families*, IEEE Trans. Inform. Theory **40** (1994) 1872–1881.

[7] V. G. Drinfeld and S. G. Vladut, *Number of points of an algebraic curve*, Funct. Anal. **17** (1983) 53–54.

[8] A. D. Friedman, R. L. Graham, and J. D. Ullman, *Universal single transition time asynchronous state assignments*, IEEE Trans. Comput. **18** (1969) 541–547.

[9] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121** (1995) 211–222.

[10] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Math. **52**, Springer-Verlag, 1977.

[11] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981) 721–724.

[12] G. Katona and J. Srivastava, *Minimal* 2*-coverings of a finite affine space based on* $GF(2)$, J. Statist. Plann. Inference **8** (1983) 375–388.

[13] J. Komlós, unpublished, cited in [18].

[14] J. Körner, *On the extremal combinatorics of the Hamming space*, J. Combin. Theory Ser. A **71** (1995) 112–126.

[15] A. Krasnopeev and Yu. L. Sagalovich, "The Kerdock codes and separating systems", in: *ACCT-8, Tsarskoe Selo (St Petersbourg) 2002*, 165–167.

[16] D. Laksov, *Wronskians and Plücker formulas for linear systems on curves*, Ann. Sci. École Norm. Sup. **17** (1984) 45–56.

[17] A. Lempel and S. Winograd, *A new approach to error-correcting codes*, IEEE Trans. Inform. Theory **23** (1977) 503–508.

[18] D. Miklós, *Linear binary codes with intersection properties*, Discr. Appl. Math. **9** (1984) 187–196.

[19] A. Neeman, *Weierstrass points in characteristic* p, Invent. Math. **75** (1984) 359–376.

[20] H. Randriam, "Hecke operators with odd determinant and binary frameproof codes beyond the probabilistic bound?", in *Proceedings of 2010 IEEE Information Theory Workshop (ITW 2010 Dublin)*, to appear.

[21] H. Randriambololona, *Diviseurs de la forme* $2D - G$ *sans sections et rang de la multiplication dans les corps finis*, preprint, available online at: `http://arxiv.org/abs/1103.4335`

[22] A. Rényi, *On random generating elements of a finite Boolean algebra*, Acta Sci. Math. Szeged **22** (1961) 75–81.

[23] Yu. L. Sagalovich, *Cascade codes of automata states*, Probl. Peredachi Inf. **14** (1978) 77–85.

[24] Yu. L. Sagalovich and A. G. Chilingarjan, *Separating systems and new scopes of its application*, Information Processes **9** (2009) 225–248.

[25] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, 1993.

[26] D. R. Stinson and R. Wei, *Combinatorial properties and constructions of traceability schemes and frameproof codes*, SIAM J. Discr. Math. **11** (1998) 41–53.

[27] K.-O. Stöhr and F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. **52** (1986) 1–19.

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

[29] C. Xing, *Asymptotic bounds on frameproof codes*, IEEE Trans. Inform. Theory **48** (2002) 2991–2995.