Separation and witnesses

G. Cohen

SEPARATION AND WITNESSES

Gérard Cohen

ENST and CNRS, Paris, France,
cohen@enst.fr

Abstract. We revisit two notions of difference between codewords, namely separation and the existence of small witnesses, and explore their links.

1 Introduction

Let Q be an alphabet of size q. A subset C of Q^n with $|C| = M$ is an $(n, M)_q$ or (n, M)-*code*. Elements $c = (c_1, \ldots, c_n)$ of C are *codewords*. Let $R = R(C) = \log_q M/n$ denote the rate of C.

Coding theory asks for codes (or sets) C such that every codeword $c \in C$ is as "different" as possible from all the others. The usual requirement is a large minimum Hamming distance between codewords; the associated question is to determine the maximum size of such a code.

We survey here two relaxations of this problem, namely, the notions of separation and witness, and their interplay.

In the first one, separation, we look for some minimum distance between disjoint *subsets* of codewords (instead of merely -singletons of- codewords).

In the second relaxation, dealing with the existence of a witness, we look for a small subset $W \subset [n]$ of coordinates such that c differs from every other codeword in W. In other words, c can be singled out from all the other codewords by observing only a small subset of coordinates.

We then establish links between some separating and witness codes and conclude with a few open problems.

2 Separation

As an introductory illustration before the general case, consider hashing, central in Computer Science and Coding, see, e.g., [12] and its references.

For a parameter $t \geq 2$ a code C is called *t-hashing* if for any t distinct codewords $c^1, \ldots, c^t \in C$ there is a coordinate $1 \leq i \leq n$ such that all values c_i^j, $1 \leq j \leq t$ are distinct.

An obvious necessary condition for the existence of a t-hashing family is $q \geq t$; it turns out to be sufficient too (see [11], [22], [23], [29] for bounds on the rate of t-hashing families of growing length).

An extension of hashing was introduced in [6].

Definition 1. *Let $2 \leq t < u$ be integers. A subset $C \subset Q^n$ is* (t,u)-hashing *if for any two subsets T, U of C such that $T \subset U$, $|T| = t$, $|U| = u$, there is some coordinate $i \in \{1, \ldots, n\}$ such that for any $x \in T$ and any $y \in U, y \neq x$, we have $x_i \neq y_i$.*

The concept of (t,u)-hashing is easily seen to generalize the standard one and some variants of separation. Indeed, when $u = t+1$, a (t,u)-hashing family is $(t+1)$-hashing; when $t = 1, u = 3$, we get $(1,2)$-separation (see later).

The main use of (t,u)-hashing codes is as a tool to show the existence of high rate parent-identifying codes ([6, 2], that we now describe.

2.1 Parent identifying codes

Let C be an (n, M)-code. Suppose $X \subseteq C$. For any coordinate i define the *projection*

$$P_i(X) = \bigcup_{x \in X} \{x_i\}.$$

Define the *envelope* $e(X)$ of X by:

$$e(X) = \{x \in Q^n : \forall i, x_i \in P_i(X)\}.$$

Elements of $e(X)$ are *descendants* of X. Observe that $X \subseteq e(X)$ and $e(X) = X$ if $|X| = 1$.

Given a descendant $s \in Q^n$, we want to identify at least one member of X (a parent). From [6, 3], we have the following definition, generalizating case $t = 2$ from [18].

Definition 2. *For any $s \in Q^n$ let $\mathcal{H}_t(s)$ be the set of subsets $X \subset C$ of size at most t such that $s \in e(X)$. We shall say that C has the* identifiable parent property of order t *(or is a t-identifying code, or has the t-IPP, for short) if for any $s \in Q^n$, either $\mathcal{H}_t(s) = \emptyset$ or*

$$\bigcap_{X \in \mathcal{H}_t(s)} X \neq \emptyset.$$

Parent identifying codes are motivated by their connection to digital fingerprinting and software piracy, see, e.g., [10], [9], [34].

Let $R_q(t) := \liminf_{n \to \infty} \max R(C_n)$, where the maximum is computed over all t-identifying codes C_n of length n. In [6], answering a question of [34], the following is proved:

Theorem 1. *$R_q(t) > 0$ if and only if $t \leq q - 1$.*

The proof is based on a connection between (t,u)-hashing and t-IPP:

Lemma 1. *Let $u = \lfloor (t/2+1)^2) \rfloor$. If C is (t,u)-hashing then it is t-identifying.*

By the probabilistic method [1], one can obtain a lower bound on the rate of $(t, u = \lfloor (t/2+1)^2 \rfloor)$-hashing families, and thus of t- identifying codes:

Theorem 2. *Let $u = \lfloor (t/2+1)^2) \rfloor$. We have*

$$R_q(t) \geq \frac{1}{u-1} \log_q \frac{(q-t)!q^u}{(q-t)!q^u - q!(q-t)^{u-t}}.$$

The rate guaranteed by Theorem 2 is further improved in [2], where explicit constructions of high rate (t, u)-hashing and t- separating families are given.

2.2 Generalized separation

Interest in separating codes comes mainly from digital fingerprinting [9]. A vendor distributes digital copies of a copyrighted work, and wants to prevent the users from making illegal copies. Watermarking can be used to give every sold copy a unique ID, a digital fingerprint, identifying the buyer. If an illegal copy subsequently appears, the user guilty of copying may be identified.

An interesting combinatorial problem arises when facing coalitions of pirates. If several users collude, they may compare their copies. Every differing bit is assumed to be part of the fingerprint and these are the only ones prone to modification (by the so-called *Marking Assumption*).

The fingerprints the pirates are able to forge, based on the set X they hold, form the so-called *feasible* set or envelope previously defined.

If the set (code) of valid fingerprints still makes it possible to trace at least one guilty pirate out of a coalition of size t or less, we have the already discussed t-identifiable parent property.

If the pirates are able to forge the fingerprint of an innocent user, we say that this user is framed. Codes which prevent framing are called *frameproof codes.*

Definition 3. *A sequence $(T_1, \ldots, T_z)$ of pairwise disjoint sets of words is called a $(t_1, \ldots, t_z)$-configuration if $\#T_j = t_j$ for all j. Such a configuration is separated if there is a position i, such that for all $l \neq l'$ every word of T_l is different from every word of $T_{l'}$ on position i.*

A code is $(t_1, \ldots, t_z)$-separating if every $(t_1, \ldots, t_z)$-configuration is separated. A $\boldsymbol{t}$-separating code is also called a $\boldsymbol{t}$-SS (separating system).

A few properties are covered by our general definition of $(t_1, \ldots, t_z)$-separation: with $z = 2$ we have the (t, u)-separation; when $t_i = 1$ for each i, we recover z-hashing; when $z = t + 1$, $t_z = u - t$, and $t_i = 1$ for $i < z$, (t, u)-hashing.

In earlier works on watermarking, (t, t)-separating codes have been called t-SFP (secure frameproof) [33, 34]. The current terminology is older though [32]. The t-frameproof codes from [33, 34] are just $(t, 1)$-separating codes.

Non-binary $(2, 1)$- and $(2, 2)$-SS appear in [30].

Separating codes have also been studied in a set-theoretic framework, e.g. [24]. Reference [21] gives various problems equivalent to $(2, 1)$-separation.

2.3 A sufficient condition for separation

For any word $c = (c_1, \ldots, c_n) \in Q^n$ we define the support to be

$$\chi(c) := \{i \mid c_i \neq 0\}.$$

For any subset $S \subset V$, the support is

$$\chi(S) := \bigcup_{c \in S} \chi(c).$$

We define the weight of subsets and codewords to be the size of their support, and denote it $w(c) := \#\chi(c)$ or $w(S) := \#\chi(S)$.

We write $\boldsymbol{t} = (t_1, \ldots, t_z)$. Given a $\boldsymbol{t}$-configuration $(T_1, \ldots, T_z)$, we define the separating set $\Theta(T_1, \ldots, T_z)$ to be the set of coordinate positions where $(T_1, \ldots, T_z)$ is separated. Let $\theta(T_1, \ldots, T_z) := \#\Theta(T_1, \ldots, T_z)$ be the separating weight. Clearly $\theta(T_1, \ldots, T_z) \geq 1$ is equivalent to $(T_1, \ldots, T_z)$ being separated. The minimum $\boldsymbol{t}$-separating weight $\theta_{\boldsymbol{t}(C)}$ is the least separating weight of any $\boldsymbol{t}$-configuration of C, previously studied in [32]. Clearly $\theta_{1,1}(C) = d(C)$.

Define

$$P(t_1, \ldots, t_z) := \sum_{i=1}^{z-1} \sum_{j=i+1}^{z} t_i t_j.$$

Note that if $t_j = 1$ for all j, then

$$P(t_1, \ldots, t_z) = \binom{z}{2},$$

and if $z = 2$, then $P(t_1, t_2) = t_1 t_2$. The following sufficient condition on minimum distance for separability from [14] generalizes various results on separating codes and perfect hashing families. Write $(n, M, d)_q$ for a q-ary code of minimum distance d.

Proposition 1. *An $(n, M, d)_q$ code Γ is $\boldsymbol{t}$-separating if*

$$\frac{d}{n} > 1 - \frac{1}{P(\boldsymbol{t})}.$$

Proof. Consider any $\boldsymbol{t}$-configuration $(T_1, \ldots, T_z)$ from Γ, and define the sum

$$\Sigma := \sum_{i=1}^{z-1} \sum_{j=i+1}^{z} \sum_{(x,y) \in T_i \times T_j} d(x, y).$$

This is the sum of $P(t_1, \ldots, t_z)$ distances in the code, so

$$\Sigma \geq P(t_1, \ldots, t_z) d. \tag{1}$$

Each coordinate can contribute at most $P(t_1, \ldots, t_z)$ to the sum Σ; if any coordinate does contribute that much, then it separates. Hence we get that

$$\Sigma \leq n(P(\boldsymbol{t}) - 1) + \theta_{\boldsymbol{t}}. \tag{2}$$

The proposition follows by combining the upper and lower bounds (1) and (2).

For sufficiently large alphabets, good separating codes are constructible from, e.g., algebraic geometry (AG).

Theorem 3 (The AG Codes). *[35] For any $\alpha > 0$ there are constructible, infinite families of codes $A(N)$ with parameters $[N, NR, N\delta]_q$ for $N \geq N_0(\alpha)$ and*

$$R + \delta \geq 1 - (\sqrt{q} - 1)^{-1} - \alpha.$$

2.4 Concatenation

For small alphabets, we can resort to concatenation to build infinite families of separating codes. Though this construction is well-known in various special cases from the literature, we give a general statement below for the sake of completeness. The outer codes used in concatenation will often be AG codes.

Definition 4 (Concatenation). *Let C_1 be an $(n_1, Q)_q$ (the inner code) and let C_2 be an $(n_2, M)_Q$ code (the outer code). Then the concatenated code $C_1 \circ C_2$ is the $(n_1 n_2, M)_q$ code obtained by taking the words of C_2 and mapping every symbol on a word from C_1.*

Proposition 2. *Let Γ_1 be a $(n_1, M)_{M'}$ code with minimum $\boldsymbol{t}$-separating weight $\theta_{\boldsymbol{t}^{(1)}}$, and let Γ_2 be a $(n_2, M')_q$ code with separating weight $\theta_{\boldsymbol{t}^{(1)}}$. Then the concatenated code $\Gamma := \Gamma_2 \circ \Gamma_1$ has minimum separating weight $\theta_{\boldsymbol{t}} = \theta_{\boldsymbol{t}^{(1)}} \cdot \theta_{\boldsymbol{t}^{(2)}}$.*

Proof. Consider a $\boldsymbol{t}$-configuration $(T_1, \ldots, T_z)$ in Γ. Then there is a corresponding configuration in Γ_1, $(T_1'', \ldots, T_z'')$ which is separated on a set I of at least $\theta_{\boldsymbol{t}^{(1)}}$ positions by assumption. Considering only the positions of Γ corresponding to a particular position $i \in I$ in Γ_2, we get a $\boldsymbol{t}'$-configuration $(T_1', \ldots, T_z')$ in Γ_1 where $1 \leq t_j' \leq t_j$ for all j. Clearly, $(T_1', \ldots, T_z')$ must be separated on at least $\theta_{\boldsymbol{t}^{(2)}}$ positions, and consequently $\theta(T_1, \ldots, T_z) \geq \theta_{\boldsymbol{t}^{(1)}} \theta_{\boldsymbol{t}^{(2)}}$.

2.5 A variation on the tetracode

The ternary construction of [14] makes use of three ingredient codes, and applies twice the concatenation method. It gives an asymptotic family of codes which are $(2,2)$-, $(3,1)$-, and $(1,1,1)$-separating.

The first seed is the $(4, 3^2, 3)_3$ tetracode T, a simplex (all codewords are at distance 3 apart). It follows that T is 3-hashing and $(3,1)$-separating from Proposition 1. The tetracode was first proved 3-hashing in [23]; combined with the $(2,2)$-separation property, this yields the 2-IPP property ([18]).

Let R_1 be the $(9, (3^2)^3, 7)_{3^2}$ Reed-Solomon code, which is both $(2,2)$- and $(1,3)$-separating, and 3-hashing, again by Proposition 1. The concatenated code $T \circ R_1$ has parameters $(36, 3^6)_3$, and by Proposition 2, it is $(2,2)$- and $(1,3)$-separating, and 3-hashing. Concatenating it with $A(N)$ over $GF(3^6)$ results in $T \circ R_1 \circ A(N)$, an infinite family of ternary $(3,1)$- and $(2,2)$-separating and 3-hashing codes with rate $R'/6 \approx 0.0352$.

3 Witness

We now move to the second extension on the notion of minimum distance. We consider only the binary case in this section and follow [13].

For $x \in \{0,1\}^n$, and $W \subset [n]$, define the projection π_W

$$\begin{aligned} \pi_W \ : \{0,1\}^{[n]} &\to \{0,1\}^W \\ x &\mapsto (x_i)_{i \in W} \end{aligned}$$

and say that W is a *witness set* (or a witness for short) for $c \in C$ if $\pi_W(c) \neq \pi_W(c')$ for every $c' \in C$, $c \neq c'$. Codes for which every codeword has a small witness set arise in a variety of contexts, in particular in machine learning theory [4, 7, 17] where a witness set is also called a specifying set or a discriminant: see [19, Ch. 12] for a short survey of known results and also [5, 25] and references therein for a more recent discussion.

A code has the w-witness property, or is a *w-witness code*, if every one of its codewords has a witness set of size w. Our concern in [13] was to study the maximum possible cardinality $f(n,w)$ of a w-witness code of length n.

3.1 Easy facts

Let C be the set of all n vectors of length n and weight 1. Then every codeword of C has a witness of size 1, namely its support. Note the dramatic change for the slightly different code $C \cup \{\mathbf{0}\}$. Now the all-zero vector $\mathbf{0}$ has no witness set of size less than n. Bondy [7] shows however that if $|C| \leq n$, then C is a w-witness code with $w \leq |C|-1$ and furthermore C is a *uniform* w-witness code, meaning that there exists a single subset of $[n]$ of size w that is a witness set for *all* codewords.

A trivial lower bound on $f(n,w)$ is based on a construction.

Proposition 3. *We have:* $f(n,w) \geq \binom{n}{w}$.

Proof. Let $C = \binom{[n]}{w}$ be the set of all vectors of weight w. Notice that for all $c \in C$, $W(c) = \mathit{support}(c)$ is a witness set of c.

Note that the problem is essentially solved for $w \geq n/2$; since $f(n,w)$ is increasing with w, we then have:

$2^n \geq f(n,w) \geq f(n,n/2) \geq \binom{n}{n/2} \geq 2^n/(2n)^{1/2}$.

Thus, only the case $w \leq n/2$ is considered here.

3.2 Upper bounds

In [13], an upper bound is obtained which comes close to the lower bound of Proposition 3; the key result there is the following.

Theorem 4. *Let $g(n,w) = f(n,w)/\binom{n}{w}$. Then, for fixed w, $g(n,w)$ is a decreasing function of n. That is:*

$$n \geq v \geq w \qquad \Rightarrow \qquad g(n,w) \leq g(v,w).$$

Theorem 4 has a number of consequences.

Corollary 1. *For fixed w, the limit*

$$\lim_{n\to\infty} g(n,w) = \frac{f(n,w)}{\binom{n}{w}}$$

exists.

Corollary 2. *For $w \leq n/2$, we have the upper bound:*

$$f(n,w) \leq 2w^{1/2}\binom{n}{w}.$$

Set $w = \omega n$ and denote by $h(x)$ the binary entropy function

$$h(x) = -x\log_2 x - (1-x)\log_2(1-x).$$

Corollary 2 together with Proposition 3 yield:

Corollary 3. *We have*

$$\lim_{n\to\infty} \tfrac{1}{n}\log_2 f(n,\omega n) = h(\omega) \qquad \text{for } 0 \leq \omega \leq 1/2.$$

4 Links betwen (1, 2)-separation and witnesses

We first summarize the known facts here. Denote by $R = R_2$ in this section the largest possible rate of a $(1,2)$- separating code. A lower bound on R is easily provided by the non-constructive approach (see, e.g., [16]), yielding $R \geq 1 - (1/2)\log 3$.

For constructions,we use the fact pointed out in [26] that shortened Kerdock codes $K'(m)$ for $m \geq 4$ are $(2,1)$-SS and concatenate them with the following ones (with $t = 2$) from [36].

Theorem 5. *Suppose that $q = p^{2r}$ with p prime, and that s is an integer such that $2 \leq t \leq \sqrt{q}-1$. Then there is an asymptotic family of $(t,1)$-separating codes with rate*

$$R_t = \frac{1}{t} - \frac{1}{\sqrt{q}-1} + \frac{1-2\log_q t}{t(\sqrt{q}-1)}.$$

Corollary 4. *There is a constructive asymptotic family of $(2,1)$-SS with $R = 0.2033$.*

Proof. Take an arbitary subcode of size 11^2 in $K'(4)$ which is a $(15, 2^7)$ $(2,1)$-SS. Concatenate with a code of Theorem 5 code ($t = 2$) over $GF(11^2)$, with $R \approx 0.4355$.

Let us now rephrase the classical proof of the upper bound, to emphasize the relationship with witnesses. Consider *any* partition of $[n]$ into two parts P_1, P_2. Then, for *any* $c \in C$, P_1 or P_2 is a witness for c. Indeed, otherwise, c would be matched by some c^i on $P_i, i = 1, 2$ and c^1 and c^2 together would frame c. Denoting by U_i the subcode of C with witness $P_i, i = 1, 2$ and making the two parts (almost) equal, we get $|C| \leq |U_1| + |U_2| \leq 2.2^{\lceil n/2 \rceil}$. Summarizing:

Proposition 4. *The rate of the largest* $(1,2)$*-separating code satisfies:*
$1 - (1/2)\log 3 \approx 0.207518 \leq R \leq 1/2$.

The gap between the lower and upper bounds is annoyingly wide, and narrowing it seems a difficult problem. Let us nevertheless explore a possible approach to improve the upperbound.

Consider a $(1,2)$- separating code $C(n, \lfloor 2^{Rn} \rfloor)$. Let c and c' be two codewords at distance w; thus $|\chi(c + c')| = w$. Then, by the preceeding discussion, $P_1 := \chi(c + c')$ is a witness for c and for c'. The idea is now to expurgate C from its pairs of close-by codewords to end up with a subcode of increased minimum distance, while preserving the rate. More precisely:

Definition 5. *Denote by* $f(n, w, \geq d)$ *the maximal size of a* w*-witness code with minimum distance* d*. Let's go asymptotics and set*
$\limsup_{n\to\infty} \frac{1}{n} \log_2 f(n, \omega n, \geq \delta n) := \phi(\omega, \delta)$.
Finally, set $\phi(\delta, \delta) := \phi(\delta)$.

From Corollary 3, we know that for $0 \leq \delta \leq 1/2$, $\phi(\delta) \leq h(\delta)$. As long as $\phi(\delta) < R$, we keep expurgating. Note that there are at most $f(n, i, \geq i)$ pairs of codewords in C at distance i apart. This process results in a code with distance $\lfloor \delta n \rfloor$ retaining the original rate.

Define $\epsilon_\delta \geq 0$ by setting $\phi(\delta) := h(\delta - \epsilon_\delta)$; or equivalently:
$\delta = h^{-1}(R) + \epsilon_\delta$.
We get the following "win-win" result:

Proposition 5. *If* $\epsilon_\delta > 0$*, then i) or ii) hold:*
i) $R = 1/2$ *and the expurgated code satifies* $\delta = h^{-1}(R) + \epsilon_\delta > h^{-1}(1 - R)$*, i.e. lies* **above** *the Varshamov-Gilbert bound!*
ii) $R < 1/2$.

5 Open problems

The size of optimal w-witness codes is asymptotically known. A few issues remain open, among which:

- When is the sphere $S_w(\mathbf{0})$ the/an optimal w-witness code?

– Do we have $f(n,w) = \binom{n}{w}$ for $w \leq n/2$?
– In the asymptotic case, can Corollary 3 be improved for $\delta \leq \omega \leq 1/2$ to $\phi(\omega,\delta) < h(\omega)$?
– A conjecture of [31] says that R_2 obtained in Theorem 5 could be improved to $R_2 = (1/2) - (2(q^{1/2}-1))^{-1}$. This would give, with $q = 11^2$ like in Corollary 4, $R_2 = 0.45$ and through concatenation a constructive rate of $R = (3/50)\log_2 11 \approx 0.207565$, thus beating the non-constructive bound (by an incredibly small quantity, though)!

References

1. N. Alon and J.Spencer, *The probabilistic method*, Wiley-Interscience 2000.
2. N. Alon, G. Cohen, M. Krivelevitch and S. Litsyn, "Generalized hashing and parent-identifying codes", *J. Combin. Theory Ser. A* 104 (2003) 207-215.
3. N. Alon, E. Fischer and M. Szegedy, "Parent-identifying codes", *J. Combin. Theory Ser. A* **95** 2001, pp. 349–359.
4. M. Anthony, G. Brightwell, D. Cohen, J. Shawe-Taylor, "On exact specification by examples", *5th Workshop on Computational learning theory* 311-318, 1992.
5. M. Anthony and P. Hammer, "A Boolean Measure of Similarity", *Discrete Applied Mathematics* Volume 154, Number 16, 2242 - 2246, 2006.
6. A. Barg, G. Cohen, S. Encheva, G. Kabatiansky and G. Zémor, "A hypergraph approach to the identifying parent property", *SIAM J. Disc. Math.*, **14** 2001, pp. 423-432.
7. J.A. Bondy, "Induced subsets", *J. Combin. Theory* (B) 12, 201-202, 1972.
8. D. Boneh and M. Franklin, "An efficient public-key traitor-tracing scheme", *Crypto'99*, LNCS 1666 (1999), pp. 338–353.
9. D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data", *IEEE Trans. Inf. Theory*, **44** (1998)480–491.
10. B. Chor, A. Fiat and M. Naor, "Tracing traitors", *Crypto'94* LNCS 839 (1994), pp. 257–270.
11. M. Fredman and J. Komlós, "On the size of separating systems and perfect hash functions", *SIAM J. Algebraic and Disc. Meth*, **5** (1983), pp. 61–68.
12. T. H. Cormen, C. E. Leiserson, and R. L. Rivest, *Introduction to Algorithms*, MIT Press, 1990, Chapter 12.
13. G. Cohen, H. Randriam and G. Zémor, "Witness sets", *Springer LNCS* 5228 (2008) 37-45.
14. G. Cohen and H.G. Schaathun, "Upper bounds on separating codes", http://personal.cs.surrey.ac.uk/personal/st/H.Schaathun/research/reports.html
15. G. Cohen and H.G. Schaathun, "Upper bounds on separating codes", *IEEE Trans. Inf. Theory* 50 (2004) 1291 - 1294.
16. G. Cohen and G. Zémor, "Intersecting codes and independent families", *IEEE Trans. Inf. Theory* 40 (1994) 1872-1881.
17. S.A. Goldman, M.J. Kearns, "On the complexity of teaching", *4th Workshop on Computational learning theory* 303-315, 1991.
18. H. D. L. Hollmann, J. H. van Lint, J.-P. Linnartz and L. M. G. M. Tolhuizen, "On codes with the identifiable parent property", *J. Combin. Theory Ser. A*, **82** (1998) 121–133.
19. S. Jukna, *Extremal Combinatorics*, Springer Texts in Theoretical Computer Science (2001).

20. G. L. Katsman, M. A. Tsfasman and S. G. Vlăduţ, "Modular curves and codes with a polynomial construction", *IEEE Trans. Inform. Theory,* 30 (1984), 353–355.
21. J. Körner, "On the extremal combinatorics of the Hamming space", *J. Combin. Theory Ser. A* 71 (1) (1995) 112-126.
22. J. Körner, "Fredman-Komlós bounds and information theory", *SIAM J. Algebraic and Disc. Methods*, **7** 1986, pp. 560–570.
23. J. Körner and K. Marton, "New bounds for perfect hashing via information theory", *Europ. J. Combinatorics*, **9** 1988, pp. 523–530.
24. J. Körner and G. Simonyi, "separating partition systems and locally different sequences", *SIAM J. Discrete Math.* 1 (1998) 355-359.
25. E. Kushilevitz, N. Linial, Y. Rabinovitch and M. Saks, "Witness sets for families of binary vectors", *J. Combin. Theory* (A) 73, 376-380, 1996.
26. A. Krasnopeev and Yu Sagalovitch, "The Kerdock codes and separating systems", *Eight International Workshop on Algebraic and Combinatorial Theory*, 8-14 Sept. 2002,pp. 165-167.
27. R. Kumar, S. Rajagopalan and A. Sahai, "Coding constructions for blacklisting problems without computational assumptions", Crypto'99 *LNCS* 1666 (1999) 609-623.
28. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, (1977).
29. A. Nilli, "Perfect hashing and probability", *Combinatorics, Probability and Computing*, **3** 1994, pp. 407–409.
30. M. Pinsker and Yu. Sagalovitch, "A lower bound on the size of automata state codes", *Problems Inform. Transmission*, 8 (3) (1972) 59-66.
31. H. Randriam, personal communication.
32. Yu.L. Sagalovich, "Separating systems", *Problems of Information Transmission*, Vol. 30 (2) (1994), pp. 105-123.
33. D.R. Stinson and R. Wei, "Combinatorial properties and constructions of traceability schemes and frameproof codes", *SIAM J. Discrete Math.*, 11 (1998), pp. 41-53.
34. J. N. Staddon, D. R. Stinson and R. Wei, "Combinatorial properties of frameproof and traceability codes", *IEEE Trans. Information Theory*, **47** 2001, pp. 1042–1049.
35. M. A. Tsfasman, S. G. Vlăduţ and Th. Zink, "Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound", *Math. Nachr.,* 109 (1982), 21–28.
36. Chaoping Xing, "Asymptotic bounds on frameproof codes", *IEEE Trans. Inform. Th.* 40 (2002) 2991-2995.