DIMACS Technical Report 2000-20
August 2000

A hypergraph approach to the identifying parent property: the case of multiple parents

by

Alexander Barg [1,4] Gérard Cohen[2] Sylvia Encheva[3]
Gregory Kabatiansky [4,5] Gilles Zémor[2]

[1]Bell Labs, Lucent Technologies, 600 Mountain Ave., Rm. 2C-375, Murray Hill, NJ 07974, USA, abarg@research.bell-labs.com.
[2]ENST, 46 rue Barrault, 75013 Paris, France. cohen@infres.enst.fr, zemor@infres.enst.fr.
[3]HSH, Bjørnsonsg. 45, 5528 Haugesund, Norway. sbe@hsh.no.
[4]IPPI RAN, Bol'shoj Karetnyj 19, Moscow 101447, Russia
[5]kaba@iitp.ru. Research done while visiting DIMACS Center, Rutgers University, Piscataway, NJ, in March 2000. Supported in part by the Russian Foundation for Fundamental Research, Grant No. 99-01-00828.

ABSTRACT

Let C be a code of length n over an alphabet of q letters. A codeword y is called a descendant of a set of t codewords $x^1, \dots, x^t$ if $y_i \in \{x_i^1, \dots, x_i^t\}$ for all $i = 1, \dots, n$. A code is said to have the identifiable parent property if for any n-word that is a descendant of at most t parents it is possible to identify at least one of them. We prove that for any $t \leq q-1$ there exist sequences of such codes with asymptotically nonvanishing rate.

1 Introduction

Let Q be an alphabet of size q, and let us call any subset C of Q^n an (n, M)-*code* when $|C| = M$. Elements $x = (x_1, \dots, x_n)$ of C will be called *codewords*.

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 the envelope $e(X)$ will be called *descendants* of X. Observe that $X \subseteq e(X)$ for all X, and $e(X) = X$ if $|X| = 1$.

Given a word $s \in Q^n$ (a son) which is a descendant of X we would like to identify without ambiguity at least one member of X (a parent). When this is always possible for any descendant s of an X of size 2, the code C is said to have the *identifiable parent property* [8]. More generally, we have the following definition.

Definition 1 *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 is t i.p.p. for short) if for any $s \in Q^n$, either $\mathcal{H}_t(s) = \emptyset$ or*

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

It will be convenient to view $\mathcal{H}_t(s)$ as the set of edges of a hypergraph. Its vertices are codewords of C.

Example. Let $C \subset \{0, 1, 2, 3\}^4$ be the code defined by $C = \{u, v, w, x, y, z\}$ where

$$\begin{aligned} u &= \begin{bmatrix} 0 & 1 & 2 & 3 \end{bmatrix} \\ v &= \begin{bmatrix} 1 & 2 & 3 & 0 \end{bmatrix} \\ w &= \begin{bmatrix} 2 & 3 & 0 & 1 \end{bmatrix} \\ x &= \begin{bmatrix} 3 & 0 & 1 & 2 \end{bmatrix} \\ y &= \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix} \\ z &= \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} \end{aligned}$$

The triple $\{w, y, z\}$ can produce the son $s = (2010)$. The hypergraph $\mathcal{H}_3(s)$ contains three edges, namely $X = \{v, w, x\}$, $X' = \{w, x, y\}$, and $X'' = \{w, y, z\}$. Their intersection is $X \cap X' \cap X'' = \{w\}$ and w is therefore identified as a parent of s. The code C is not

3-identifying however, it is not even 2-identifying since $\mathcal{H}_2(0101) = \{u, w\} \cup \{y, z\}$ and $\{u, w\} \cap \{y, z\} = \emptyset$.

The concept of t-identification originates with the work of Chor, Fiat and Naor on broadcast encryption [4]. It is also related to the problem of fingerprinting numerical data [3].

It is not difficult to prove that if the minimum Hamming distance of C is big enough, then C must be t-identifying: we have [4]

Theorem 1 *If C has minimum Hamming distance d satisfying*

$$d > (1 - 1/t^2)n,$$

then C is a t-identifying code.

Actually, this condition implies a stronger property, namely t-traceability, see [14].

As usual, let $R = R(C) = \log_q M/n$ denote the rate of the (n, M)-code C. Let $R_q(t) = \liminf_{n\to\infty} \max R(C_n)$, where the maximum is computed over all t-identifying codes of length n.

Note that for alphabet sizes $q \leq t^2$ theorem 1 does not prove that $R_q(t) > 0$ (for example because (n, M)-codes that satisfy the distance condition must have $M \leq d$, see Plotkin's bound e.g. in [11]).

In fact, non-trivial t-identifying codes do not always exist if the alphabet size q is not big enough. For example, Boneh and Shaw [3] note that if $q = 2$ then no 2-identifying code C exists with $|C| \geq 3$. To see this suppose that x, y, z are distinct codewords of C: define s by choosing s_i to be, for every coordinate i, the letter that appears most often among x_i, y_i, z_i. Then the three edges $\{x, y\}$, $\{y, z\}$, $\{z, x\}$ all belong to $\mathcal{H}_2(s)$ which has therefore empty intersection.

Hollman et al. [8] give constructions of 2-identifying codes and existence bounds on $R_q(2)$ for any alphabet size $q \geq 3$: they prove

$$R_q(2) \quad \geq \quad \log_q(q/(4q^2 - 6q + 3)^{1/3}). \tag{1}$$

The case of arbitrary t was discussed in a recent survey [14] where, in particular, it was asked whether $R_q(t) > 0$ for any $t \leq q - 1$. In this paper we shall answer this question and prove

Theorem 2 *$R_q(t) > 0$ if and only if $t \leq q - 1$.*

We shall also give a lower bound on $R_q(t)$. We shall give particular attention to the case $t = 3$ and in the case $t = 2$, $q = 3$, strengthen (1) by showing that it can be achieved by a sequence of linear ternary i.p.p. codes.

2 Decomposing the t-identifying property with the Berge-Duchet theorem

Let us call a subset of edges of a hypergraph a *star* if it has non-empty intersection. A code C is t-identifying if all the non-empty hypergraphs $\mathcal{H}_t(s)$ are stars: in this section we give necessary and sufficient conditions for $\mathcal{H}_t(s)$ to be a star.

Let us say that a family of sets, any t (or less) of which have non-empty intersection, is *t-wise* intersecting.

Recall that a family of sets has the *t-Helly property* if every t-wise intersecting finite subfamily is a star.

Let us quote a Helly-type result due to Berge and Duchet [2], see also [5]:

Theorem 3 *A hypergraph has the t-Helly property if and only if, for every set A of $t+1$ vertices, all the edges E such that $|E \cap A| \geq t$ share a common vertex.*

Let us reword this result for our purposes. Recall that a hypergraph on $t+1$ vertices whose edges are all the t-subsets is called a t-simplex, denoted $K_t(t+1)$.

Corollary 1 *The hypergraph $\mathcal{H}_t(s)$ has the t-Helly property if and only if it does not contain $K_t(t+1)$ as a subhypergraph.*

Proof : Consider any set A of size $t+1$ vertices of $\mathcal{H}_t(s)$. Let $E_1, E_2, \ldots E_m$ be all the edges of $\mathcal{H}_t(s)$ that have at least t vertices in A. Since the edges of $\mathcal{H}_t(s)$ have at most t vertices we have $|E_i| = t$ for all i and

$$|E_1 \cap E_2 ... \cap E_m| = t + 1 - m.$$

Therefore this intersection is non-empty if and only if $m < t+1$, i.e. $E_1, E_2, \ldots E_m$ do not make up the t-simplex with vertex set A. ∎

Reworded again, we get:

Corollary 2 *Suppose the hypergraph $\mathcal{H}_t(s)$ has at least $t+1$ edges. Then it is a star if and only if*

1. *any t of its edges have non-empty intersection,*
2. *it does not contain $K_t(t+1)$.*

It will be convenient to decompose all patterns of $m \leq t+1$ edges with empty intersection into "minimal forbidden configurations".

Let $\mathcal{X} = (X_1, \ldots, X_m)$ be a collection of subsets of codewords with $|X_i| \leq t$, $i = 1, \ldots, m$. We shall call $\mathcal{X}$ a *configuration* if it has empty intersection, $\cap_{i=1}^m X_i = \emptyset$, and we shall say that $\mathcal{X}$ is a *minimal configuration* if it is minimal under inclusion, i.e. if $\cap_{i\neq j} X_i \neq \emptyset$ for any $j = 1, \ldots, m$.

Let $\mathcal{X}$ be a minimal configuration of size m. A set $B(\mathcal{X}) = (b^1, \ldots, b^m)$ will be called a *frame* of $\mathcal{X}$ if

$$b^j \in \bigcap_{i\neq j} X_i.$$

By minimality, frames of minimal configurations always exist. One useful property of frames gives rise to the following lemma.

Lemma 1 *Let $\mathcal{X}$ be a minimal configuration. Then*

$$|\bigcup_{i=1}^{m} X_i| \leq \sum |X_i| - m(m-2).$$

Proof : All the points b^j of a frame $B(\mathcal{X})$ are different since otherwise $\cap_i X_i \neq \emptyset$. Furthermore, by definition of $B(\mathcal{X})$ we have $(B(\mathcal{X}) \setminus b^j) \subset X_j$ for any $j = 1, \ldots, m$, and hence $m - 1 \leq t$. Then

$$\begin{aligned} |\bigcup_{i=1}^{m} X_i| &\leq \sum (|X_i \setminus (B(\mathcal{X}) \setminus b^i)|) + |B(\mathcal{X})| \\ &= \sum_{i=1}^{m} (|X_i| - (m-1)) + m. \end{aligned}$$

∎

Since $|X_i| \leq t$, we obtain $|\cup X_i| \leq m(t - m + 2)$. Note that the maximum value of m which gives a positive upper bound is $t+1$. Note also that the only minimal configurations with $m = t+1$ are t-simplexes. In particular this gives an alternative proof of corollary 2.

3 Forbidding minimal configurations

3.1 Hashing families

A subset C of Q^n is said to be t-*hashing* (or t-separating, see, e.g. [9]) if any t of its members have t distinct entries in some common coordinate $i \in [1 \ldots n]$.

Proposition 1 *$C \subset Q^n$ is $(t+1)$-hashing if and only if $\mathcal{H}_t(s)$ has the t-Helly property for every $s \in Q^n$.*

Proof : Suppose C is $(t+1)$-hashing: let A be any set of $t+1$ codewords, and let $s \in Q^n$. Since there is a coordinate where the codewords of A are all different, there exists at least one subset $X \subset A$, $|X| = t$, such that $s \notin e(X)$. Therefore $\mathcal{H}_t(s)$ cannot contain a t-simplex.

Conversely, suppose C is not $(t+1)$-hashing, so that there exists a subset A of $t+1$ codewords such that for every coordinate i, there exist at least two distinct codewords a, b of A such that $a_i = b_i$. Then define $s \in Q^n$ by choosing, for every coordinate $i \in [1 \ldots n]$, a value that occurs at least twice among the a_i, $a \in A$. Then we have $s \in e(X)$ for every subset X of size t of A, which means that $\mathcal{H}_t(s)$ contains the t-simplex with vertex set A. ∎

Remark : A consequence of proposition 1 is that when $q \leq t$, there are no q-ary t-identifying codes C of size $|C| \geq t+1$. This generalizes the argument of Boneh and Shaw quoted in the introduction.

We now have a condition on C that ensures that all the hypergraphs $\mathcal{H}_t(s)$ do not contain t-simplexes. To apply corollary 2 we now need a condition to ensure that any t edges of any $\mathcal{H}_t(s)$ have non-empty intersection.

3.2 Partially hashing families

Definition 2 *Let us say that a subset $C \subset Q^n$ is (t, u)* partially hashing *if for any two subsets T, U of C such that $T \subset U \subset C$, $|T| = t$, $|U| = u$, 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 $x_i \neq y_i$.*

Remark : If $u = t+1$ then (t, u) partial hashing is the same as $(t+1)$-hashing.

The motivation for this last definition is the following:

Proposition 2 *Let u be the maximum of $m(t-m+2)$ for $m = 1, \ldots, t$. If C is (t, u) partially hashing, then for any $s \in \mathcal{H}_t(s)$ and for any $m \leq t$, any m edges of $\mathcal{H}_t(s)$ have non-empty intersection.*

Proof : Suppose, towards a contradiction, that some collection $\mathcal{X}$ of m non-intersecting edges is contained in $\mathcal{H}_t(s)$. Let us suppose furthermore that $\mathcal{X}$ is minimal, so that by lemma 1 the set $U = \cup_{X \in \mathcal{X}} X$ satisfies $|U| \leq u$. Let T be some edge of $\mathcal{X}$. Because C is (t, u) partially hashing, there is some coordinate i satisfying the condition of definition 2 for T and U. Then $s_i = x_i$ for some $x \in T$ because $s \in e(T)$. But then the definition implies that there is only one $x \in U$ such that $s_i = x_i$. Therefore all the edges of $\mathcal{H}_t(s)$ contain x, which contradicts the assumption that $\mathcal{H}_t(s)$ has empty intersection. ∎

Propositions 1 and 2 imply:

Corollary 3 *Let $u = \lfloor (t/2+1)^2) \rfloor$. If C is (t, u) partially hashing then C is a t-identifying code.*

The (t, u) hashing property is easier to handle than t-identification, in particular it will give us a lower bound on $R_q(t)$ through the probabilistic method.

3.3 A lower bound on $R_q(t)$

Fix t and let $u = \lfloor (t/2+1)^2) \rfloor$. We apply the probabilistic method with expurgation (see e.g. [1]) to (t,u) partially hashing codes. This means that we take a random (n,M)-code C and compute the expectation $\mathbf{E}$ of the number of pairs of subsets T, U, $T \subset U \subset C$, $|T| = t$, $|U| = u$ that contradict the (t,u) partially hashing property. Whenever $\mathbf{E} \leq M/2$ then $(n, M/2)$-codes with the (t,u) partially hashing property exist. By corollary 3 these codes are also t-identifying.

The probability that a given T and U violate the partially hashing property is

$$P_{t,u,n} = \left(1 - \frac{q(q-1)\cdots(q-t+1)(q-t)^{u-t}}{q^u}\right)^n = \left(1 - \frac{q!(q-t)^{u-t}}{(q-t)!q^u}\right)^n.$$

The expectation of the number of pairs T, U that violate the partially hashing property is

$$\mathbf{E} = \binom{M}{u}\binom{u}{t} P_{t,u,n}.$$

Writing $M = q^{Rn}$ and letting n go to infinity we get that infinite sequences of (t,u) partially hashing codes exist for all rates R such that $\log_q \mathbf{E} < Rn$, i.e. such that

$$uR + \frac{1}{n}\log_q P_{t,u,n} < R.$$

Hence:

Theorem 4 *Let $u = \lfloor (t/2+1)^2) \rfloor$. We have*

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

In particular we see that $R_q(t) > 0$ for $q \geq t+1$ which proves Theorem 2.

4 Small t

The (t,u) partial hashing property is only a sufficient condition for a code to be t-identifying. In the case of small t we can obtain precise necessary and sufficient conditions. A code C is t-identifying if and only if, for every s such that $\mathcal{H}_t(s) \neq \emptyset$, the hypergraph $\mathcal{H}_t(s)$ has the t-Helly property and any m edges of $\mathcal{H}_t(s)$ have non-empty intersection, for any m, $2 \leq m \leq t$. Proposition 1 tells us therefore that C is t-identifying if and only if it is $(t+1)$-hashing and any m edges of $\mathcal{H}_t(s)$ have non-empty intersection, for any m, $2 \leq m \leq t$, and for any $s \in Q^n$. For $t = 2$, the latter property means that $\mathcal{H}_2(s)$ does not contain disjoint edges: equivalently, for any $X = \{a,b\}$, $Y = \{c,d\}$, with a,b,c,d distinct codewords, $e(X) \cap e(Y) = \emptyset$. Equivalently again, this means that there exists a coordinate i such that

$$\{a_i, b_i\} \cap \{c_i, d_i\} = \emptyset. \tag{2}$$

This property of C was named IPP2 by Hollman et al. in [8]: in other contexts it has often been called $(2,2)$-separation and has been investigated by a number of authors, among which [7, 6, 10, 12, 13]. The 3-hashing property was called IPP1 in [8].

Let us now characterize the 3 i.p.p. property.

4.1 The case $t = 3$

This time proposition 1 tells us that C is 3-identifying if and only if

(i) it is 4-hashing

(ii) for any $s \in Q^n$, any two edges of $\mathcal{H}_3(s)$ have non-empty intersection and any three edges of $\mathcal{H}_3(s)$ have non-empty intersection.

Condition (ii) is equivalent to saying that $\mathcal{H}_3(s)$ does not contain minimal configurations of size $m = 2$ and of size $m = 3$.

That $\mathcal{H}_3(s)$ does not contain minimal configurations of size 2 is equivalent to saying that for any $X = \{a,b,c\}$, $\{d,e,f\}$, with a,b,c,d,e,f distinct codewords, $e(X) \cap e(Y) = \emptyset$, which means that there exists a coordinate i such that

$$\{a_i, b_i, c_i\} \cap \{d_i, e_i, f_i\} = \emptyset. \tag{3}$$

Property (3) is usually called $(3,3)$-separation [7, 6, 10].

There remains to characterize the condition that $\mathcal{H}_3(s)$ does not contain a minimal configuration of 3 edges, i.e. $\mathcal{X} = (X, Y, Z)$ such that $X \cap Y \cap Z = \emptyset$ but any two edges of $\mathcal{X}$ intersect. Clearly, the only cases that we need consider are when $|X| = |Y| = |Z| = 3$. We have two situations to forbid, namely:

(a) for any $X, Y, Z \subset \binom{C}{3}$ such that $X \cap Y \cap Z = \emptyset$ and $|X \cap Y| = |Y \cap Z| = |Z \cap X| = 1$,

(b) for any $X, Y, Z \subset \binom{C}{3}$ such that $X \cap Y \cap Z = \emptyset$ and $|X \cap Y| = 2$ and $|Y \cap Z| = |Z \cap X| = 1$.

Forbidding these configurations means that we must have, in each case,

$$e(X) \cap e(Y) \cap e(Z) = \emptyset.$$

Those two cases involve respectively 6 and 5 codewords. After a straightforward examination we finally obtain:

Proposition 3 *C is 3-identifying if and only if the four following conditions hold:*

1. *C is 4-hashing*
2. *C is $(3,3)$-separating*

3. for any 6 *distinct codewords* a, b, c, d, e, f *there exists a coordinate* i *such that*

- a_i, b_i, c_i *are all different,*
- $d_i \neq a_i$, $e_i \neq b_i$, $f_i \neq c_i$,
- d_i, e_i, f_i *are not all equal.*

4. for any 5 *distinct codewords* a, b, c, d, e *there exists a coordinate* i *such that*

- $c_i \neq e_i$ *and* $\{a_i, b_i\} \cap \{c_i, e_i\} = \emptyset$.
- $d_i \neq a_i$ *and* $d_i \neq b_i$.

Example: q=4. By applying repeatedly the probabilistic expurgation method, we get lower bounds on the rate of codes satisfying the previous four conditions. Namely

$$\begin{aligned} R_1 &\geq \frac{1}{3}\log_4(32/29), \\ R_2 &\geq \frac{1}{5}\log_4(2^{10}/919), \\ R_3 &\geq \frac{1}{5}\log_4(256/217), \\ R_4 &\geq \frac{1}{4}\log_4(256/226). \end{aligned}$$

Taking the smallest of the R_i's gives a 3- identifying quaternary code with rate R_2, showing that

$$R_4(3) \geq \frac{1}{5}\log_4(1024/919) \approx 0.0156.$$

4.2 Linear i.p.p. codes

Bound (1) for $q = 3$ implies that $R_3(2) \geq (1/3)\log_3(9/7)$. We strengthen this result in the following way.

Theorem 5 *There exists a sequence of linear ternary* 3*-identifying codes* C_n *with* $R(C_n) \geq (1/3)\log_3(9/7)$.

The result in [8] implies only the existence of unrestricted codes with the same rate.

We again apply the probabilistic method and prove theorem 5 by averaging this time over the ensemble of linear ternary codes. Let C be a linear subspace of F_3^n. The code C is i.p.p. if any triple of vectors in it is 3-hashing and any quadruple satisfies the separation condition (2).

Linear $(2, 2)$-separating codes were first studied in [12], were most of the calculations below were essentially carried out. We include them here for completeness.

Consider condition (2). Suppose that $\dim C = k$ and let G be a generator matrix of C, i.e., a $k \times n$ matrix whose rows form a basis of C as an F_3-linear space. Let $g^1, g^2, \dots, g^n$ be the columns of G. Any vector $c \in C$ has the form aG for some $a \in F_3^k$. Let $c^1, \dots c^4$ be some vectors in C. Since the i.p.p. property is translation invariant, suppose that $c^4 = 0$. Suppose that $c^i = a^i G$ for $i = 1, 2, 3$.

Case (a). a^1, a^2, a^3 are linearly independent. Choose a basis $f_1, \dots f_k$ in F_3^k such that $a^i \cdot f_j = \delta_{ij}$ for $i = 1, 2, 3$; $j = 1, \dots, k$. (Complement a^1, a^2, a^3 to a basis and take the dual basis.) Observe that $\{c_i^1, c_i^2\} \cap \{c_i^3, c_i^4\} = \emptyset$ if and only if the first three coordinates of the column g^i in the basis (f) have one of the following forms:

$$\begin{matrix} \pm 1 & \pm 1 & 0 \\ -1 & -1 & 1 \\ 1 & 1 & -1 \end{matrix}\ .$$

Hence the total number of favorable choices is 6 out of 27. This implies that the probability for a matrix G to be bad for a given linearly independent triple is $(21/27)^n = (7/9)^n$. The number of triples is less than 3^{3k}, so the probability that a given matrix spans a quadruple of vectors that violate condition (2) is bounded above by $3^{3k}(7/9)^n$. Hence if $R = (1/3)\log_3(9/7) - \epsilon$, for any $\epsilon > 0$, there exists a favorable choice.

Case (b). Some of the vectors a^1, a^2, a^3 are linearly dependent. For instance, suppose that a^1 is spanned by a^2, a^3, and these two are not collinear. Take the basis dual to a basis that includes a^2, a^3. As above, we count the number of unfavorable choices for the column g^i. Good choices for (g_1^i, g_2^i) are $(\pm 1, \pm 1)$. Hence the number of bad choices of G is at most $3^{2k}(5/9)^n$, and this is less than $3^{3k}(7/9)^n$. Other cases of dependence are dealt with analogously; none accounts for a fraction of bad matrices larger than in case (a).

The proof is completed by lower bounding the achievable rate for linear i.p.p. codes by the minimum of the achievable rates for random linear 3-hashing functions and for random linear codes satisfying (2).

References

[1] L. A. Bassalygo, S. I. Gelfand, and M. S. Pinsker, "Simple methods for obtaining lower bounds in coding theory", *Probl. Inform. Trans.* **27** (1991), no. 4, pp. 3–8.

[2] C. Berge and P. Duchet, "A generalisation of Gilmore's theorem", *Recent Advances in Graph Theory*, ed. M. Fiedler (Acad. Praha) (1975), pp. 49-55.

[3] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data", *IEEE Trans. on Inf. Theory*, **44** (1998), pp. 480–491.

[4] B. Chor, A. Fiat and M. Naor, "Tracing traitors", *Crypto'94* LNCS 839 (1994), pp. 257–270.

[5] P. Duchet, “Hypergraphs”, in Handbook of Combinatorics, (Graham, Grötschel and Lovász , Eds.) North-Holland 1995.

[6] M.L. Fredman and J. Komlós, “On the size of separating systems and families of perfect hash functions”, SIAM J. of Algebraic and Discrete Methods, **5**, No 1 (1984) pp. 61–68.

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

[8] H.D. Hollmann, J.H. van Lint, J.-P. Linnartz and L.M. Tolhuizen, “On codes with the identifiable parent property”, *J. Combinatorial Theory*, Series A, **82** (1998) pp. 121–133.

[9] J. Körner and A. Orlitski, “Zero-error information theory”, *IEEE Trans. Information Theory*, **44** (1998), pp. 2207–2229.

[10] J. Körner and G. Simonyi, “Separating partition systems and locally different sequences”, SIAM J. of Discrete Math., **1** No 3 (1988) pp. 355–359.

[11] J. H. van Lint, *Introduction to Coding Theory*, Grad. Texts in Math. 86, Springer-Verlag 1982.

[12] M. S. Pinsker and Yu. L. Sagalovich “Lower bound for the power of an automaton state code,” Probl. Inform. Trans. **8**, No. 3 (1972), pp. 224–230.

[13] Yu. L. Sagalovich, “Separating systems”, Probl. Inform. Trans. **30** No 2 (1994) pp. 105–123.

[14] J. N. Staddon, D. R. Stinson, and R. Wei, “Combinatorial properties of frameproof and traceability codes”,
available from `http://cacr.math.uwaterloo.ca/~dstinson`.

[15] D.R. Stinson, Tran van Trung and R. Wei, “Secure Frameproof Codes, Key Distribution Patterns, Group Testing Algorithms and Related Structures”, *J. Stat. Planning and Inference*, **86** (2) (2000), pp. 595-617.

[16] 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.