Error control codes for parallel asymmetric channels

R. Ahlswede*and H. Aydinian

Department of Mathematics
University of Bielefeld
POB 100131
D-33501 Bielefeld, Germany
E-mail addresses:
ahlswede@mathematik.uni-bielefeld.de
ayd@mathematik.uni-bielefeld.de

Abstract

We introduce and study error correcting codes for parallel synchronous communication via asymmetric channels. Constructions for error detecting/correcting codes are presented. More generally, we consider array codes for binary asymmetric channels.

Index Terms– Asymmetric error correcting codes, parallel channel, asymmetric parallel channel, array codes

*The author was supported by the 'Finite Structures' Marie Curie Host Fellowship for the Transfer of knowledge project carried out by Alfred Renyi Institute of Mathematics, in the framework of the European Community's Structuring the European Research Area programme.

1 Introduction

In [1] the notion of "parallel error correcting codes" was introduced. A communication channel (multiple–access channel) consists of several sub–channels transmitting simultaneously and synchronously. Informally, the senders of a multiple–access channel encode their messages to the codewords c_i (of the same length over the same alphabet $\mathcal{X}$, say $\mathcal{X} = \mathbb{Z}_q$) and transmit in parallel the codewords. The errors in the channel are of the additive type and for all transmitted codewords c_i the received vectors are of the form $c_i + e$ (in the presence of noise) where e is an error vector. In particular, for two users let $\mathcal{X} = \mathbb{Z}_q$ and let $\mathcal{C} \subset \mathcal{X}^n \times \mathcal{X}^n$. $\mathcal{C}$ is called a parallel t-error correcting code of length n, if $(u, v) + (e, e) \neq (u', v') + (e', e')$ for every pair of distinct codewords $(u, v), (u', v') \in \mathcal{C}$ and any vectors $e, e' \in \mathbb{Z}_q^n$ each of Hamming weight at most t. A motivation for studying such codes is explained in [1].

In many digital systems such as fiber optical communications and optical disks the ratio between probability of errors of type 1 → 0 and 0 → 1 can be large. Practically we can assume that only one type of errors can occur in those systems. These errors are called asymmetric. Thus the binary asymmetric channel has the property that a transmitted 1 is always received correctly but a transmitted 0 may be received as a 0 or 1.

In this paper we introduce and study parallel error correcting/detecting codes for binary asymmetric channels.

We consider a parallel asymmetric channel of r senders and block length n over the binary alphabet. A message of senders $s_1, \dots, s_r$ is represented by the $r \times n$ $(0,1)$–matrix with the i-th row corresponding to the message of s_i. Thus a code $\mathcal{C}$, called $(r \times n)$–code, is viewed as a set of $r \times n$ $(0,1)$–matrices. We consider the errors of type $0 \to 1$. We say that t errors have occured in a transmitted matrix M, also called codeword, if in some t columns of M all zero entries transfered to ones. In other words, the received word M' can be considered as $M' = M \oplus E$, where the error word E is an $r \times n$ matrix with each column consisting of all-ones or all-zeros and $\oplus$ means the Boolean sum of matrices. The weight $w(E)$ is the number of all-one columns in E.

We say that an $(r \times n)$–code $\mathcal{C}$ is capable of correcting t asymmetric errors if any transmitted codeword can be uniquely reconstructed at the receiving end in a presence of t or less errors. In other words, for any two codewords M_1, M_2 and error words E_1, E_2 of weight not greater than t we have

$$M_1 \oplus E_1 \neq M_2 \oplus E_2. \tag{1.1}$$

We also say that $\mathcal{C}$ is capable of detecting t errors if there are no codewords M_1, M_2 such that $M_1 \oplus E = M_2$ with $w(E) \leq t$. Such a code is called t–error correcting/detecting asymmetric parallel code (shortly $(r \times n, t)$ AP–code).

2 Construction of error detecting/correcting AP codes.

For an $r \times n$ $(0,1)$-matrix M the columns of M can be viewed as elements of the alphabet $Q = \{0, 1, \dots, q-1\}$ $(q = 2^r)$ using arbitrary one-to-one mapping $\varphi : \{0,1\}^r \to Q$. Thus any matrix M can be represented as an n-tuple $(a_1, \ldots, a_n) \in Q^n$. A natural way is to consider each column as the binary expansion of the corresponding number from Q. Our parallel channel can be illustrated now as a q-ary asymmetric channel (called q–ary AP channel) with $q = 2^r$ shown in Figure 1.

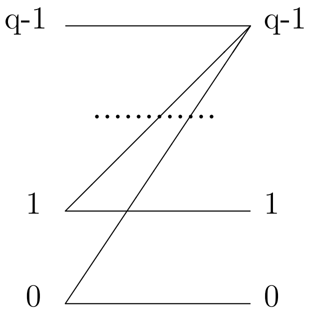

Figure 1: q–ary AP channel

Thus AP–channel is a special case of the q–ary channel, shown in Figure 1, when $q = 2^r$. Therefore in general it makes sense to study this channel for arbitrary q (for other models of q-ary asymmetric channels see [2]). The notion of t– error correcting/detecting code is extended to any q–ary AP channel in a natural way. We call such codes q–ary t–error correcting/detecting AP codes. In the sequel sometimes we will not specify q.

Let us consider now the following partial ordering on Q^n. For $a^n = (a_1, \ldots, a_n)$, $b^n = (b_1, \ldots, b_n) \in Q^n$ we say that $a^n \succeq b^n$ if either $a_i = b_i$ or $a_i = q - 1$ for $i = 1, \ldots, n$. The weight of an element $a^n \in Q^n$ is defined by $w(a^n) = |\{i : a_i = q-1\}|$. Thus Q^n is a partially ordered set ordered by $\preceq$ denoted by $S(n, q)$. In the literature $S(n, q)$ is known (see [8]) as star product. $A \subset S(n, q)$ is called an antichain if any two distinct members of A are incomparable. Let $S_i(n, q)$ be the set of all elements of $S(n, q)$ with weight i and denote $W_i = |S_i(n, q)|$.

Proposition 1 *Let $A \subset S(n, q)$. Then the following two conditions are equivalent*
(i) A is a q–ary AP code capable of detecting all errors .
(ii) A is an antichain in $S(n, q)$.

Proof. The equivalence directly follows from the definitions of antichain and error detection capability. □

Theorem 1 *Given integers $n, r \geq 1$ and $1 \leq t < n$ let $W_k = \max\{W_i : 0 \leq i \leq n\}$. Then*

(i) $S_k(n, q)$ is an optimal q–ary AP code capable of detecting all errors.

(ii) the code $\mathcal{C}$ defined by

$$\mathcal{C} = \{x \in S_i(n, q) : \ i \equiv k \mod (t+1)\} \tag{2.1}$$

is a q–ary AP code capable of detecting t errors.

Proof. Clearly $S_i(n,q)$ is an antichain. It is known also (see [8]) that the maximum size of an antichain in $S(n,q)$ is equal to $\max\{W_i : 0 \leq i \leq n\}$. This with Proposition 1 implies (i).

For (ii) it suffices to show that any $a^n \in S_i(n,q)$ and $b^n \in S_{i+t+1}(n,q)$ with $a^n \prec b^n$ satisfy the condition of t-error detection capability. This is clear since $a^n \prec b^n$ implies that there exist coordinates $i_1, \dots, i_{t+1}$ such that $a_{i_1} = \dots = a_{i_{t+1}} = q-1$ and $b_{i_1}, \dots, b_{i_{t+1}} \neq q-1$. □

Note that the size of the described code

$$|\mathcal{C}| > \frac{2^{nr}}{t+1}. \tag{2.2}$$

This follows from the unimodality of $\{W_i\}$, that is $W_0 < W_1 < ... \leq W_k \geq W_{k+1} > ... > W_n$.

Next we consider **error–correcting AP codes**. But first we define a distance d_A between elements of Q^n. To this end we define two distances d_0 and d_1 between $a^n, b^n \in Q^n$. Let $d_0(a^n, b^n) := \#\{i : a_i \neq b_i \text{ and } a_i, b_i \neq q-1\}$ and let $d_1(a^n, b^n) := \max\{\delta(a^n, b^n), \delta(b^n, a^n)\}$, where $\delta(a^n, b^n) := \#\{i : a_i \neq b_i \text{ and } a_i = q-1\}$, $\delta(b^n, a^n) := \#\{j : a_j \neq b_j \text{ and } b_j = q-1\}$.

Definition. For $a^n, b^n \in Q^n$ the distance $d_A(a^n, b^n)$ is defined by

$$d_A(a^n, b^n) = d_0(a^n, b^n) + d_1(a^n, b^n).$$

The following is easy to verify.

Proposition 2 *A q–ary AP-code $\mathcal{C}$ is capable of correcting t errors iff for every distinct $a^n, b^n \in \mathcal{C}$ holds*

$$d_A(a^n, b^n) \geq t+1.$$

We construct now single-error correcting AP–codes. Note that for $n \leq q+1$ (and prime power q) we can use for this purpose MDS codes (see [11], Ch.11) with the minimum Hamming distance 3 and cardinality q^{n-2}. However, one can do it better.

Proposition 3 *For arbitrary q the code $\mathcal{C} \subset Q^n$ defined by*

$$\mathcal{C} = \{(x_1, \dots, x_n) \in S_0(n,q) : \; x_n = \sum_{i=1}^{n-1} x_i \mod q-1\} \tag{2.3}$$

is a single error–correcting AP code with $|\mathcal{C}| = (q-1)^{n-1}$.

Proof. By the construction we have $|\mathcal{C}| = |S_0(n,q)| = (q-1)^{n-1}$. It is also clear that the minimum distance d_A of the code is 2. □

One can extend the construction to t-error correcting AP–codes. In view of Proposition 2 it is sufficient to construct a code $\mathcal{C}$ of length n and minimum Hamming distance $t+1$ over alphabet $Q^* = \{0, 1, \dots, q-2\}$.

Lemma 1 *For any prime power q and $n \leq q+1$ there exists a code $\mathcal{C} \subset Q^{*n}$ of minimum Hamming distance d with*

$$|\mathcal{C}| \geq \frac{(q-1)^n}{q^{d-1}}. \tag{2.4}$$

Proof. There exists an MDS code $\mathcal{C}' \subset \mathrm{GF}(q)^n$ with minimum Hamming distance d and $|\mathcal{C}'| = q^{n-d+1}$. Let now $\mathcal{C} \subset Q^{*n}$ be an optimal code with minimum distance d. We use the following known result, the idea of which is due to P. Elias (a proof can be found in [10]).

Lemma 2 (see [10]) *For any subsets $A, B \subset \mathbb{Z}_q^n$ there exists $x \in \mathbb{Z}_q^n$ such that*

$$\frac{|(x+A) \cap B|}{|A|} \geq \frac{|B|}{q^n}.$$

To obtain (2.4) we identify B with Q^* and $\mathcal{C}'$ with A. □

Clearly Lemma 1 with Proposition 2 in particular implies the following

Proposition 4 *For $n < 2^r$ one can construct an $(n \times r)$ AP code $\mathcal{C}$, capable of correcting $1 \leq t < n$ errors, with*

$$|\mathcal{C}| \geq \frac{(2^r-1)^n}{2^{rt}}.$$

It should be mentioned that the described codes can be viewed as codes correcting erasures with the erasure symbol is $q-1$ (for definition see [7]).

Next we give a construction of single error correcting $(r \times n, 1)$ AP codes for any r and n.

In [13] Varshamov and Tennengolts gave the first construction of nonlinear codes correcting asymmetric errors. Given $n \in \mathbb{N}$ and an integer a, the Varshamov–Tennengolts code (VT code) $\mathcal{C}(n, a)$ is defined by

$$\mathcal{C}(n,a) = \left\{ (x_1, \ldots, x_n) \in \{0,1\}^n : \sum_{i=1}^{n} i x_i \equiv a \mod m \right\} \tag{2.5}$$

where $m \geq n+1$ is an integer. It was shown that the code $\mathcal{C}(n,a)$ is capable of correcting any single asymmetric error. Moreover, taking $m = n+1$ there exists $a \in \{0, \ldots, n\}$ such that

$$|\mathcal{C}(n,a)| \geq \frac{2^n}{n+1}, \tag{2.6}$$

thus exceeding the Hamming upper bound for the size of a binary single symmetric error–correcting codes. Varshamov [12] showed that $|\mathcal{C}(n,0)| \geq |\mathcal{C}(n,a)|$.

VT codes can be used for construction of q–ary single error correcting PA codes.

Construction

Let $\mathcal{C}(n,a)$ be a VT code and let $v \in \mathcal{C}(n,a)$ be a codeword of weight $n-k$. Suppose w.l.o.g. $v = (0, \ldots, 0, 1, \ldots, 1)$. Let also $D(k, 2)$ be a code of length k and minimum Hamming distance 2 over $Q^* = \{0, 1, \ldots, q-2\}$ $(q = 2^r)$. In particular given $\alpha \in Q^*$ let $D_\alpha(k, 2)$ be the code defined by

$$D_\alpha(k,2) = \{(x_1, \ldots, x_k) \in Q^{*k} : \ x_k = \sum_{i=1}^{k-1} x_i + \alpha \mod (q-1)\}. \tag{2.7}$$

We define now

$$\mathcal{S}_v(n,a,\alpha) = \{(a_1, \ldots, a_k, q-1, \ldots, q-1) \in Q^n : (a_1, \ldots, a_k) \in D_\alpha(k,2) \tag{2.8}$$

Similarly for every $x \in \mathcal{C}(n,a)$ define $\mathcal{S}_x(n,a,\alpha)$. Clearly $\mathcal{S}_x(n,a,\alpha)$ is a single error correcting AP–code. Observe also that for distinct x and y and every $v^n \in \mathcal{S}_x(n,a,\alpha)$ and $u^n \in \mathcal{S}_y(n,a,\alpha)$ the minimum distance $d_A(u^n, v^n) \geq 2$. Thus $\mathcal{S}(n,a,\alpha) := \bigcup_{x \in \mathcal{C}(n,a)} \mathcal{S}_x(n,a,\alpha)$ is q–ary AP–code capable of correcting all single errors.

Let $A_0(n,a), A_1(n,a), \ldots, A_n(n,a)$ be the weight distribution of $C(n,a)$ (that is $A_i(n,a) :=$ $\#$ {codewords of weight i}). Then it can be easily seen that $|\mathcal{S}(n,a,\alpha)| = \sum_{i=1}^n A_i(n,a) \cdot (q-1)^{n-i-1}$. Thus we have proved the following

Theorem 2 *For integers $q, n \geq 2$; $0 \leq a \leq n$ and $0 \leq \alpha \leq q$, the code $\mathcal{S}(n,a,\alpha)$ is q–ary single error correcting AP code with $|\mathcal{S}(n,a,\alpha)| = \sum_{i=1}^n A_i(n,a) \cdot (q-1)^{n-i-1}$.*

Note that $\{\mathcal{S}(n,a,\alpha)\}$, $a = 0, \ldots, n$; $\alpha = 0, \ldots, q-2$ is a partition of Q^n into $(n+1)(q-1)$ single error correcting AP–codes. Therefore $\max\limits_{a,\alpha} |\mathcal{S}(n,a,\alpha)| \geq q^n/(n+1)(q-1)$.

Corollary 1 *For integers $n, r \geq 2$ there exists a single error correcting $(n \times r, 1)$ AP code S^* (described above) with*

$$|S^*| \geq \frac{2^{nr}}{(n+1)(2^r-1)}. \tag{2.9}$$

Example. $n = 8$, $r = 2$ $(q = 4)$.
Let A_i be the number of codewords of weight i in the VT code $\mathcal{C}(8,0)$. We have $A_0 = A_8 = 1$, $A_2 = A_6 = 4$, $A_3 = A_4 = A_5 = 6$. Then the construction above gives us a single error-correcting $(2 \times 8, 1)$ AP code of size $A_0 \cdot 3^7 + A_2 \cdot 3^5 + A_3 \cdot 3^4 + A_4 \cdot 3^3 + A_5 \cdot 3^7 + A_6 \cdot 3 + A_8 = 3874$. Note that the size of a single symmetric error correcting code of length 8 (over an alphabet of size 4) is upper bounded (by the Hamming bound) by $2^{16}/(3 \cdot 8 + 1) = 2621$.

3 Array codes for binary asymmetric channels

In general, a binary array code $\mathcal{C}$ is a set of $r \times n$ (0,1)–matrices, intended for correction/detection of erroneous bits which can for instance occur only in t rows or only in t columns or in both, in t rows and t columns.

Array codes for binary symmetric channels are well studied (see [5] for a good survey).

It seems that array codes for asymmetric channels also deserve (from both theoretical and practical points of view) to study. Here we consider the case when errors can occur in t or less columns.

Let $\mathcal{M}(r \times n)$ be the set of all $r \times n$ $(0,1)$–matrices. We say that $\mathcal{C} \subset \mathcal{M}(r \times n)$ is a t–error correcting/detecting array code (shortly t–AEC/AED array code) if $\mathcal{C}$ is capable of correcting all asymmetric errors in t or less columns. Note that any t–AEC/AED array code $\mathcal{C} \subset \mathcal{M}(r \times n)$ is also a t–error correcting/detecting AP code.

We discuss first the error detection problem. For two binary sequences $a^k = (a_1, \dots, a_k)$ and $b^k = (b_1, \dots, b_k)$ we say that a^k covers b^k and write $a^k \geq b^k$ iff $a_i \geq b_i$ for $i = 1, \dots, n$. Let us also define a partial ordering on $\mathcal{M}(r \times n)$. For $A, B \in \mathcal{M}(r \times n)$, let $h_1, \dots, h_n$ and $g_1, \dots, g_n$ be the columns of A and B, respectively.

We say that $A \preceq_{\mathcal{M}} B$ iff $h_i \leq g_i$ for $i = 1, \dots, n$. $\mathcal{A} \subset \mathcal{M}(r \times n)$ is called an antichain iff any two members of $\mathcal{A}$ are incomparable. By definition of asymmetric error detection condition for array codes we have

Proposition 5 *$\mathcal{A} \subset \mathcal{M}(r \times n)$ is a code detecting all asymmetric errors iff $\mathcal{A}$ is an antichain.*

By the classical Sperner theorem (see [8]) it follows that the maximal size of an antichain in $\mathcal{M}(r \times n)$ (with respect to ordering defined above) is $\binom{nr}{\lfloor nr/2 \rfloor}$. Thus the problem of constructing an optimal array code detecting all asymmetric errors is easy. We just take the set of all matrices $\mathcal{A} \subset \mathcal{M}(r \times n)$ with the Hamming weight $wt_H(\mathcal{A}) = \lfloor nr/2 \rfloor$, i.e. having $\lfloor nr/2 \rfloor$ ones.

However, the problem of construction of optimal t-AED codes (given parameters n, r, t) seems to be not so easy. In particular, one can observe that for $t = 1$ the problem is equivalent to (a special case) of a problem known (in Extremal Set Theory) as n–part Sperner problem. However the latter problem is solved only for $n = 2$ (see [3] or [8]).

The following lower bound for the size of a t–AED code can be easily verified.

Proposition 6 *Given integers $1 \leq t \leq n$, $1 \leq r$ let*

$$\mathcal{A} = \{A \in \mathcal{M}(r \times n) : wt_H(A) \equiv \lfloor nr/2 \rfloor \mod (tr + 1)\} \tag{3.1}$$

then $\mathcal{A}$ is a t–AED array code.

The lower bound (3,1) appears to be tight for $r = 1$, that is for usual t–AED codes. This was observed in Borden [6]. However, this is not the case in general. Let for example $r = n = 3$, $t = 1$. Then the size of the code $\mathcal{A}$ defined by (3.1) $|\mathcal{A}| = \binom{9}{0} + \binom{9}{4} + \binom{9}{8} = 136$.

Let now $B(w_1, w_2, w_3)$ be the set all $X \in \mathcal{E}(3 \times 3)$ with the i–th column $(i = 1, 2, 3)$ having the Hamming weight w_i. It is easy to observe that the union of the sets below denoted by $\mathcal{B}$ is a 1–AED array code of size $|\mathcal{B}|= 144$:

$B(1,0,3),\ B(1,1,2),\ B(1,2,1),\ B(1,3,0), B(2,0,0),\ B(2,1,1),\ B(2,2,2),\ B(2,3,3)$

$B(0,0,1),\ B(0,1,0),\ B(0,2,3),\ B(0,3,2),\ B(3,2,0), B(3,1,3),\ B(3,2,0),\ B(3,3,1).$

Let us consider now the error correcting problem for the simplest case $t = 1$.

Every matrix $B \subset \mathcal{M}(r \times n)$, with columns denoted by $\bar{b}_1, \ldots, \bar{b}_n$, is associated with the sequence $(b_1, \ldots, b_n)$ where $\bar{b}_i$ $(i = 1, \ldots, n)$ is the binary representation of b_i. For a subset $\mathcal{S} \subset Q^n$, $(Q = \{0, \ldots, q-1 = 2^r - 1\})$ we denote by $\mathcal{S}(r \times n) \subset \mathcal{M}$ the set of all matrices corresponding to $\mathcal{S}$.

We say that there exists a k–factorization of $\mathbb{Z}_m^*$ ($\mathbb{Z}_m^* := \mathbb{Z}_m \setminus \{0\}$) if there exists a subset $A \subset \mathbb{Z}_m^*$ such that each element of $\mathbb{Z}_m^*$ can be uniquely represented as a product $i \cdot a$ where $i \in \{1, \ldots, k\}$ and $a \in A$.

Theorem 3 *Given integers $n, r \geq 2$ let $m := n(q-1) + 1$ $(q = 2^r)$. Let also there exists a $(q-1)$–factorization of $\mathbb{Z}_m^*$ by a subset $A = \{a_1, \ldots, a_n\}$. For $a \in \mathbb{Z}_m$ let $\mathcal{B} \in Q^n$ be defined by*

$$\mathcal{B} = \{(x_1, \ldots, x_n) \in Q^n : \sum_{i=1}^{n} a_i x_i \equiv a \mod m\} \tag{3.2}$$

then $\mathcal{B}(r \times n)$ is a single error–correcting array code with

$$|\mathcal{B}(r \times n)| \geq \frac{q^n}{n(q-1)+1}. \tag{3.3}$$

Proof. Assume the opposite. Then there exist two codewords B and C with columns $\bar{b}_1, \ldots, \bar{b}_n$ and $\bar{c}_1, \ldots, \bar{c}_n$, such that $\bar{b}_i > \bar{c}_i$, $\bar{c}_j > \bar{b}_j$ for some $i, j \in \{1, \ldots, n\}$, and $\bar{b}_k = \bar{c}_k$ for all indices $k \neq i, j$. This clearly means that $b_i > c_i$, $c_j > b_j$ and $b_k = c_k$ (for all $k \neq i, j$) for the corresponding sequences $(b_1, \ldots, b_n)$ and $(c_1, \ldots, c_n)$. The latter with (3.2) implies that $a_i(b_i - c_i) \equiv a_j(c_j - b_j) \mod m$. However this is a contradiction with the $(q-1)$–factorization of Z_m^* by $A = \{a_1, \ldots, a_n\}$. The lower bound (3.3) is clear. □

Example. Let $n = 12$ and $r = 2$ $(q = 4)$, thus $n(q-1) + 1 = 37$. One can check that there exists 3–factorization of $\mathbb{Z}_{37}^*$ by the set $\{2, 9, 12, 15, 16, 17, 20, 21, 22, 25, 28, 35\}$. Therefore, the code $\mathcal{B}(2 \times 12)$ defined by (3.2) has cardinality $|\mathcal{B}(2 \times 12)| \geq 4^{12}/37$ exceeding the Hamming bound for a quaternary single symmetric error–correcting code of length 12.

We give now a construction of single-error correcting array codes with a very simple decoding algorithm.

Construction

For integers $1 < r \leq n$ let $\mathcal{E}(r \times n)$ denote the set of all $r \times n$ $(0,1)$-matrices with even row weights. Thus $|\mathcal{E}| = 2^{(n-1)r}$. For an $r \times n$ $(0,1)$-matrix M let $h_i(M)$ be the Hamming weight of its i-th column. Let also p be the smallest prime such that $p \geq n + 1$. We define now the code $\mathcal{C}(r \times n)$ as follows.

$$\mathcal{C}(r \times n) = \{M \subset \mathcal{E} : \sum_{i=1}^{n} i h_i(M) \equiv a \mod p\}. \tag{3.4}$$

Theorem 4 *(i) $\mathcal{C}(r \times n)$ is capable of correcting all asymmetric errors in a single column.*

(ii) There exists $0 \leq a \leq p-1$ *such that*

$$|\mathcal{C}(r \times n)| \geq \frac{2^{(n-1)r}}{p}. \tag{3.5}$$

Proof. Only part (i) is needed to argue. Let M' be a received word and let $(\varepsilon_1, \ldots, \varepsilon_r)^T$ be the sum of all columns of M' where ε_i is taken modulo 2, that is, $(\varepsilon_1, \ldots, \varepsilon_r)$ is the parity check of the rows of M'. Then the nonzero coordinates $\varepsilon_{i_1}, \ldots, \varepsilon_{i_t}$ indicate that the errors occur in the rows $i_1, \ldots, i_t$. Suppose now there are two codewords M_1, M_2 such that the addition of $(\varepsilon_1, \ldots, \varepsilon_r)^T$ to the i-th column of M_1 and j-th column of M_2 ($i \neq j$) results in M'. Then in view of (3.4) we have

$$\sum_{i=1}^{n} ih_i(M' - M_1) \equiv \sum_{i=1}^{n} ih_i(M' - M_2) \mod p$$

which implies that $it \equiv jt \mod p$. However this is a contradiction since $t, i, j < p$. Therefore $M_1 = M_2$ concluding the proof. □

Decoding algorithm: For a received word M'

1. Determine the column vector $(\varepsilon_1, \ldots, \varepsilon_r)^T := M' \cdot (1, \ldots, n)^T \mod 2$.
Let $w_H(\varepsilon_1, \ldots, \varepsilon_r) = t$.
If $t = 0$ then M' is a codeword, otherwise

2. Compute $b := \sum ih_i(M') \mod p$.

3. Compute $i := \frac{b-a}{t} \mod p$.

4. Subtract from the i-th column of M' the column vector
$(\varepsilon_1, \ldots, \varepsilon_r)^T$, obtaining the transmitted codeword.

4 Concluding remarks

We have considered two models of multiple–access parallel asymmetric channels giving constructions of error– detecting/correcting codes for that channels.

Many problems remain open in this direction:
1. What is the size of an optimal t–error detecting AP–code?
Is the code defined by (2.1) is an optimal t–error detecting AP–code?

2. What is the size of an optimal t–AED array code?

3. Costruction of good t–error correcting AP codes and t–AED array codes.

4. Nontrivial upper bounds for the size of both classes of codes.

We considered array codes for detecting/correcting t column errors. Several natural and interesting models can be considered here.

Consider array codes for correction/detection of t_1 column and t_2 row errors.

It would be also interesting to consider the case when the number of errors in each column (row) is limited.

The study of array codes for unidirectional type of errors (see [4] for a collection of papers on error control codes for uniderectional errors) is also seems to be natural.

References

[1] R. Ahlswede and N. Cai, Parallel error correcting codes, *IEEE Trans. Inform. Theory* 46, No.4,959–962,2002.

[2] R. Ahlswede, H. Aydinian , L.H. Khachatrian and L.M.G.M. Tolhuizen, On q–ary codes coorecting all undirectional errors of a limited magnitude , in *Proceedings of Ninth International workshop on Algebraic and Combinatorial Coding Theory*, 19–25 June, Kranevo, Bulgaria, 20–26, 2004.

[3] I. Anderson, *Combinatorics of Finite Sets*, Clarendon Press, Oxford, 1987.

[4] M. Blaum (ed.), *Codes for detecting and correcting unidirectional errors*, IEEE Computer Society Press Reprint Collections, IEEE Computer Society Press, Los Alamitos, CA, 1993.

[5] M. Blaum, P. G. Farrell and H. C. A. van Tilborg, Array codes, *Handbook of coding theory*, Vol. II, pp 1855–1909, (V.S. Pless, W.C. Huffman and R.A. Brualdi (eds), North-Holland, Amsterdam) 1998.

[6] J.M. Borden, Optimal asymmetric error detecting codes, *Information and Control* 53, No. 1–2, 66–73, 1982.

[7] P. Elias, The noisy channel coding theorem for erasure channels, *Amer. Math. Monthly* 81, 853-862, 1974.

[8] K. Engel, *Sperner Theory,* Cambridge University Press, 1997.

[9] T. Kløve, Error correcting codes for the assymetric channel, Report, Dept. of Math. Univ. of Bergen, 1981 (with updated bibliography in 1995).

[10] J.H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, Berlin, 1999.

[11] F.J. MacWilliams and N.J. Sloane, *The Theory of Error-Correcting Codes*, New York: North-Holland, 1988.

[12] R.R. Varshamov, On the theory of assymmetric codes (in Russian), *Doklady Akademii Nauk USSR*, Vol. 164, 757–760, 1965. (transl: Soviet Physics-Doklady 10, 185–187, 1965).

[13] R.R. Varshamov and G.M. Tennengolts, A code which corrects single asymmetric errors (in Russian) *Avtomat. Telemeh.* 26, 282–292, 1965. (transl: Automation and Remote Contr., 286–290, 1965).