Parallel Error Correcting Codes

R. Ahlswede*, B. Balkenhol† and N. Cai‡

Fakultät für Mathematik
Universität Bielefeld
Postfach 100131
33501 Bielefeld
Germany

Keywords: Error correcting codes, multiple–access channel

AMS subject classification: 94A50, 94B05, 94B25, 94B60

*email: ahlswede@mathematik.uni-bielefeld.de
†email: bernhard@mathematik.uni-bielefeld.de
‡email: cai@mathematik.uni-bielefeld.de

1 Introduction

In Information Theory we know two types of channel models for communication: the probabilistic description of transmission of letters and the combinatorial description based on counting erroneous transmission of letters.

The standard probabilistic channel is that of a discrete memoryless channel, abbreviated as DMC, which is characterized by a stochastic matrix $W : \mathcal{X} \to \mathcal{Y}$, where $\mathcal{X}, \mathcal{Y}$ are the input and output alphabets, resp. Shannon [13] found its capacity $C(W)$, that is the largest rate R achievable for arbitrary long codes for any prescribed error probability λ. Shannon [14] generalized also his 1 sender – 1 receiver channel model to certain cases of channels with several senders and receivers. Seemingly the next most important contribution in this direction is Ahlswede's [1] characterization of the capacity region for so called multiple access channels (MAC) — the first "coding theorem" for multi–user channels. This work was continued in [2].

On the combinatorial side it is assumed that for a given positive integer t at most t errors may occur when a codeword is send over the channel. An error correcting (detecting) code must be able to correct (detect) the errors. Since often algebraic tools are used in the construction of codes the subject Combinatorial Coding Theory is often called Algebraic Coding Theory ([8], [12]).

Whereas in the probabilistic setting there is a formidable area called Multi–user Information Theory (c.f. [3], [4], [10], [9]), little is done in the analog combinatorial setting.

An exception here is the adder channel, one of the simplest MAC (c.f. [11] for a survey), which has been studied for error correcting and also for error–free ($\lambda = 0$) codes.

In contrast, for 1 sender – 1 receiver channels even other code concepts like error detecting or error correcting codes with i.e. localized errors [6], [5], or feedback [7] have been considered.

In this paper we introduce a new code concept for a multi-user channel with a special error control mechanism. Let us take a look at the parallel port of a computer divice. The message from the computer to the device is transmitted in parallel over a set of lines. A magnetic influence from outside produces errors during the transmission. But the time instances of which errors occur in the different lines are related. When an error occurs in a line at time T, with a relatively high "probability" an error also occurs in its neighbour lines. Thus one can assume that the conditional probability for that an error occurs in the j-th line under the condition that an error occurs in the i-th line is a non-decreasing function of the distance between the i-th line and the j-th line. We regard the m lines connecting a computer and a user of the computer as m senders who intend to send the data from the computer to the user. Then it is modeled as a coding problem for an MAC. Its capacity region has already been determined in [1]. So we turn now to the error correcting codes.

For the simplicity of the model, we assume that an error occurs in a line iff errors occur in the other lines at the same time. (There is a certain relation to bursts insofar as

errors are linked. But this is for the senders and not in time.) As usual we assume that at most t errors occur in each line. Thus our problem is modelled as follows. The m senders encode their messages to the codewords of the same length over the same alphabet $\mathcal{X} = GF(q)$, say $\mathbf{c}_j (j = 1, 2, \ldots, m)$ and send the codewords via channels. When the codewords $\mathbf{c}_j (j = 1, 2, \ldots, m)$, are sent, then due to noise, the receiver may receive the vectors $\mathbf{c}_j + \mathbf{e}, (j = 1, 2, \ldots, m)$, for any (error) $\mathbf{e}$ with Hamming weight not larger than t. A *parallel t error correcting code* must be able to correct all errors of this type. When the m lines carry messages from the same source, the size of the code, that is the number of vectors $(\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_m)$, must not be smaller than the number of messages. So for a fixed t and the length n of the code we want the size of the code as large as possible. In this case we present a very simple construction based on a standard error correcting code and show that it is optimal if so is the error correcting code.

The code has to be a cartesian product, when the messages carried by the m senders are from m independent sources. So instead of the maximum size of a code we speak of the region of achievable rates. In this case we present a construction by which one could obtain linear codes with rates in the achievable region if one would know the line codes with all possible dimensions. This reduces constructing a linear code to constructing a (classsical) error correcting code. For optimal non-linear codes and independent messages the problem is still open.

All results in this paper are for arbtrary m senders but in order to keep the notation short for the convenience of the readers we only present the proofs for two senders. The same proofs extend to general m.

The parallel codes are formally defined in the next section. The results for two senders are stated and proved in Section 3. The results for the general case are prensented in Section 4.

2 Basic definitions

In this section, we define our codes for two senders i.e., for $m = 2$, they will be generalized to m senders, for arbitrary m in Section 4. As usual for MAC, we use $\mathcal{X}$ and $\mathcal{Y}$ to stand for input alphabets for the two senders. Since we mainly consider linear codes over a finite field, we choose for a prime power $q = p^s$, $\mathcal{X}^n = \mathcal{Y}^n = GF^n(q)$ throughout this and the next section.

Definition 1. *A code $\mathcal{C} \subset \mathcal{X}^n \times \mathcal{Y}^n$ is an $(n, t, |\mathcal{C}|)$ parallel error correcting code or in short an $(n, t, |\mathcal{C}|)$ P-code over $GF^n(q)$, if there are not codewords $\mathbf{c} = (\mathbf{u}, \mathbf{v}), \mathbf{c}' = (\mathbf{u}', \mathbf{v}') \in \mathcal{C}$ where $\mathbf{u}, \mathbf{u}' \in \mathcal{X}^n, \mathbf{v}, \mathbf{v}' \in \mathcal{Y}^n$ and errors $\mathbf{e}, \mathbf{e}' \in GF^n(q)$ with Hamming weights $w_H(\mathbf{e}), w_H(\mathbf{e}') \leq t$ such that*

$$\mathbf{c} + (\mathbf{e}, \mathbf{e}) = \mathbf{c}' + (\mathbf{e}', \mathbf{e}'). \tag{2.1}$$

Definition2. *A P-code $\mathcal{C}$ is called independent, or an IP-code, if it is a cartesian product, i.e. there are $\mathcal{U} \subset \mathcal{X}^n, \mathcal{V} \subset \mathcal{Y}^n$ such that $\mathcal{C} = \mathcal{U} \times \mathcal{V}$.*

An $(n, t, |\mathcal{C}|)$ IP-code is **linear***, or an (n, t, k, l) LIP-code if $\mathcal{U}, \mathcal{V}$ are linear subspaces with $dim(\mathcal{U}) = k$ and $dim(\mathcal{V}) = l$.*

We also speak of P-codes, IP-codes and LIP-codes correcting t errors when the other parameters are clear from the context. In the context of multi–user Information Theory an IP-code is used in multiple access channel (MAC), a channel with two (or more) independent senders and one receiver, whereas a non–independent P-code is used in a parallel channel connecting one sender and one receiver.

Throughout this paper, $A(n, t)$ is the maximal cardinality of an ordinary t error correcting code of block-length n and $L(n, t)$ is the maximal dimension of the ordinary linear t error correcting code of block-length n. Let $K_n(\beta) = \{(\alpha, \alpha+\beta) : \alpha \in GF^n(q)\}$ for $\beta \in GF^n(q)$, then $\mathcal{K}_n = \{K_n(\beta) : \beta \in GF^n(q)\}$ is a partition of $\mathcal{X}^n \times \mathcal{Y}^n$.

For $\mathcal{C} \subset \mathcal{X}^n \times \mathcal{Y}^n$ we write $\mathcal{C}(\beta) = \mathcal{C} \cap K_n(\beta), \beta \in GF^n(q)$. That is $(\mathbf{u}, \mathbf{v}) \in \mathcal{C}(\beta)$, iff $(\mathbf{u}, \mathbf{v}) \in \mathcal{C}$ and $\mathbf{v} - \mathbf{u} = \beta$. Let $Q(\mathcal{C}, \beta) = \{\alpha : (\alpha, \alpha + \beta) \in \mathcal{C}(\beta)\}$. Thus $\mathcal{C}(\beta)$ is determined by a subset $Q(\mathcal{C}, \beta) \in GF^n(q)$ as follows

$$\mathcal{C}(\beta) = \{(\alpha, \alpha + \beta) : \alpha \in Q(\mathcal{C}, \beta)\}.$$

Clearly, $\mathcal{C}(\beta)$ and thus also $Q(\mathcal{C}, \beta)$ may be empty.

3 The two sender model

Lemma 1. *$\mathcal{C} \subset \mathcal{X}^n \times \mathcal{Y}^n$ is an $(n, t, |\mathcal{C}|)$ P-code iff for all $\beta \in GF^n(q)$, $Q(\mathcal{C}, \beta)$ is a t error correcting code.*

Proof: Suppose that $Q(\mathcal{C}, \beta)$ is not a t error correcting code. Then there exist $\alpha, \alpha' \in Q(\mathcal{C}, \beta)$ (i.e., $(\alpha, \alpha + \beta), (\alpha', \alpha' + \beta) \in \mathcal{C}$) $\mathbf{e}, \mathbf{e}' \in GF^n(q)$ with $w_H(\mathbf{e}), w_H(\mathbf{e}') \leq t$ with $\alpha + \mathbf{e} = \alpha' + \mathbf{e}'$. This implies that $\alpha + \beta + \mathbf{e} = \alpha' + \beta + \mathbf{e}'$ and hence $(\alpha + \mathbf{e}, \alpha + \beta + \mathbf{e}) = (\alpha' + \mathbf{e}', \alpha' + \beta + \mathbf{e}')$, i.e. (2.1) holds. This means that $\mathcal{C}$ is not an $(n, t, |\mathcal{C}|)$ code.

Conversely, if $Q(\mathcal{C}, \beta)$ are t error correcting for all $\beta \in GF^n(q)$, but there exist $\mathbf{c} = (\mathbf{u}, \mathbf{v}), \mathbf{c}' = (\mathbf{u}', \mathbf{v}') \in \mathcal{C}$ and $\mathbf{e}, \mathbf{e}' \in GF^n(q)$ with Hamming weights $w_H(\mathbf{e}), w_H(\mathbf{e}') \leq t$ such that $\mathbf{c} \neq \mathbf{c}'$ and (2.1) holds i.e.,

$$(\mathbf{u} + \mathbf{e}, \mathbf{v} + \mathbf{e}) = (\mathbf{u}' + \mathbf{e}', \mathbf{v}' + \mathbf{e}').$$

Write $\mathbf{v} = \mathbf{u} + \beta, \mathbf{v}' = \mathbf{u}' + \beta'$ and observe that

$$(\mathbf{u} + \mathbf{e}, \mathbf{u} + \beta + \mathbf{e}) = (\mathbf{u}' + \mathbf{e}', \mathbf{u}' + \beta' + \mathbf{e}')$$

implies $\mathbf{u} + \mathbf{e} = \mathbf{u}' + \mathbf{e}'$ and $\mathbf{u} + \beta + \mathbf{e} = \mathbf{u}' + \beta' + \mathbf{e}'$ and thus $\beta = \beta'$. In other words $\mathbf{u}, \mathbf{u}' \in Q(\mathcal{C}, \beta)$ and $\mathbf{u} + \mathbf{e} = \mathbf{u}' + \mathbf{e}', w_H(\mathbf{e}), w_H(\mathbf{e}') \leq t$ contradict that $Q(\mathcal{C}, \beta)$ is t error correcting since $\mathbf{c} \neq \mathbf{c}'$, $\mathbf{v} = \mathbf{u} + \beta$, $\mathbf{v}' = \mathbf{u}' + \beta'$ and $\beta = \beta'$ imply that $\mathbf{u} \neq \mathbf{u}'$.

Theorem 1. *The following two statements hold:*

(i) For an (n, t, M) P-code

$$M \leq A(n,t)q^n. \tag{3.1}$$

(ii) For $M = A(n,t)q^n$ exists an (n, t, M) P-code.

Proof: (i) is an immediate consequence of Lemma 1.

We derive (ii) by the following

Construction I: Choose any t error correcting code of size $A(n,t)$, say $\mathcal{C}_0$ and set $\mathcal{C} = \mathcal{C}_0 \times GF^n(q)$. It is clearly $|\mathcal{C}| = A(n,t)q^n$. For $\mathbf{c} = (\mathbf{u}, \mathbf{v}) \neq \mathbf{c}' = (\mathbf{u}', \mathbf{v}')$ in $\mathcal{C}$

$$(\mathbf{u} + \mathbf{e}, \mathbf{v} + \mathbf{e}) = (\mathbf{u}' + \mathbf{e}', \mathbf{v}' + \mathbf{e}')$$

is impossible, because for $\mathbf{u} \neq \mathbf{u}'$ $\mathbf{u} + \mathbf{e} \neq \mathbf{u}' + \mathbf{e}'$ since $\mathcal{C}_0$ is a t error correcting code and $\mathbf{u} = \mathbf{u}'$ yields that $\mathbf{v} = \mathbf{v}' + (\mathbf{e}' - \mathbf{e}) = \mathbf{v}' + (\mathbf{u} - \mathbf{u}') = \mathbf{v}'$ i.e., $\mathbf{c} = \mathbf{c}'$.

3.1 LIP-codes

In Theorem 1 we have obtained an optimal P-code in the sense of total rate. However, since the sources accessed by the two senders are assumed to be independent, we are concerned as usual for MAC about their achievable pairs of rates instead about their sums. The following theorem completely characterizes LIP-codes.

Theorem 2. *For two linear subspaces $\mathcal{U}$ and $\mathcal{V}$ of $GF^n(q)$, $\mathcal{C} = \mathcal{U} \times \mathcal{V}$ is an LIP-code correcting t errors iff $\mathcal{U} \cap \mathcal{V}$ is a linear t error correcting code.*

Proof: Suppose $\mathcal{U}$ and $\mathcal{V}$ are two linear subspaces such that $\mathcal{C}_0 = \mathcal{U} \cap \mathcal{V}$ is a t error correcting code.

Assume $\mathcal{C}$ is not an LIP-code, namely there exist $\mathbf{e}, \mathbf{e}' \in GF^n(q)$ with $w_H(\mathbf{e}), w_H(\mathbf{e}') \leq t$ and $\mathbf{c} = (\mathbf{u}, \mathbf{v}), \mathbf{c}' = (\mathbf{u}', \mathbf{v}')$ such that (2.1) holds. Let $\alpha^\star = \mathbf{e}' - \mathbf{e}$. Then by (2.1) $\mathbf{u} - \mathbf{u}' = \mathbf{v} - \mathbf{v}' = \alpha^\star$. Thus by linearity $\alpha^\star \in \mathcal{U}, \alpha^\star \in \mathcal{V}$ and therefore $\alpha^\star \in \mathcal{U} \cap \mathcal{V}$. However $(0, \ldots, 0) = \mathbf{0} \in \mathcal{C}_0$ and $\mathbf{0} + \mathbf{e}' = \alpha^\star + \mathbf{e}$ with $w_H(\mathbf{e}), w_H(\mathbf{e}') \leq t$, which is a contradiction to the assumption, that $\mathcal{C}_0$ is a t error correcting code.

Let $\mathcal{C} = \mathcal{U} \times \mathcal{V}$ be an LIP-code correcting t errors. We have to show $\mathcal{C}_0 = \mathcal{U} \cap \mathcal{V}$ is a linear t error correcting code. Indeed, if it is not so i.e., there are $\alpha^\star \in \mathcal{C}_0 = \mathcal{U} \cap \mathcal{V}$ and $\mathbf{e}, \mathbf{e}' \in GF^n(q)$ with $w_H(e), w_H(e') \leq t$ such that $\mathbf{0} + \mathbf{e} = \alpha^\star + \mathbf{e}'$, then $\mathbf{c} = (\mathbf{0}, \mathbf{0})$ and $\mathbf{c}' = (\alpha^\star, \alpha^\star) \in \mathcal{C} = \mathcal{U} \times \mathcal{V}$ and (2.1) holds. This is a contradiction. □

Theorem 3. *For given positive integers n, t and non-negative integers k_1 and k_2, there exists an (n, t, k_1, k_2) LIP-code iff $k_1, k_2 \leq n$ and*

$$k_1 + k_2 \leq L(n,t) + n. \tag{3.2}$$

Proof: Suppose that we are given an (n, t, k_1, k_2) LIP-code. Recalling its definition we have that $K_n(\mathbf{0})$ is a linear subspace of $GF^{2n}(q)$ and $\mathcal{K}_n$ actually is the set of its

cosets. Notice an LIP-code $\mathcal{C}$ is a linear subspace of $GF^{2n}(q)$. Then for a LIP-code $\mathcal{C}$, $\mathcal{C}(\mathbf{0}) = \mathcal{C} \cap K_n(\mathbf{0})$ is a linear subspace of $GF^{2n}(q)$, $\mathcal{C}(\beta), \beta \in GF^n(q)$ are its cosets, and therefore $|\mathcal{C}(\beta)| = |\mathcal{C}(\mathbf{0})|$. By Lemma 1 $Q(\mathcal{C}, \mathbf{0})$ is a t error correcting code if $\mathcal{C}(\beta)$ is an LIP-code correcting t errors. Finally $Q(\mathcal{C}, \mathbf{0})$ is obviously a linear space with $|Q(\mathcal{C}, \mathbf{0})| = |C(\mathbf{0})|$. Thus we have $|\mathcal{C}(\beta)| = |Q(\mathcal{C}, \mathbf{0})| \leq q^{L(n,t)}$ for all $\beta \in GF^n(q)$. Therefore $|\mathcal{C}| \leq q^{L(n,t)+n}$.

Conversely, without loss of generality we can assume

$$k_1 + k_2 = L(n,t) + n \tag{3.3}$$

since we can obtain a new LIP-code from an LIP code $\mathcal{C} = \mathcal{U} \times \mathcal{V}$ by replacing $\mathcal{U}$ and/or $\mathcal{V}$ with any of their subspaces $\mathcal{U}'$ and $\mathcal{V}'$. Under this assumption we have

$$L(n,t) \leq k_1, k_2 \leq n. \tag{3.4}$$

Let $\mathcal{C}_0$ be a linear t error correcting code of length n and $dim(\mathcal{C}_0) = k$. In particular, to show the "if" part, we choose it as a linear error correcting code achieving $dim(\mathcal{C}_0) = k = L(n,t)$. Then the proof follows from the following construction.

Construction II: Let $\mathcal{C}_0$ be a k–dimensional t error correcting code of length n and let $\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_k}$ be any basis. We extend the basis to a basis of $GF^n(q)$, $\mathbf{u_1}, \mathbf{u_2}$, $\mathbf{u_k}, \mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_{n-k}}$, in an arbitrary way and divide $\{1, 2, \ldots, n-k\}$ into two parts I_1 and I_2 with cardinalities $k_1 - k$ and $k_2 - k$ respectively (notice $k = L(n,t)$ in (3.3), hence $(k_1 - k) + (k_2 - k) = n - k$). Let $\mathcal{U}$ and $\mathcal{V}$ be the linear subspaces spanned by $\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_k}, \mathbf{v_i}$ $(i \in I_1)$ and $\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_k}, \mathbf{v_j}$ $(j \in I_2)$ respectively and $\mathcal{C} = \mathcal{U} \times \mathcal{V}$.

Then it is clear that $\dim(\mathcal{U}) = k_1$, $\dim(\mathcal{V}) = k_2$ and $\mathcal{C}_0 = \mathcal{U} \cap \mathcal{V}$. So by Theorem 2 $\mathcal{U} \times \mathcal{V}$ is the desired code.

Remark: Obviously by Theorem 2 all LIP-codes can be constructed by Construction II.

In this way one would construct all (n, t, k_1, k_2) LIP-codes if one could find all $(n, k_1 + k_2, t)$ linear error correcting codes.

3.2 The decoding algorithms

In this subsection we present decoding algorithms for our LIP-codes. First of all we notice that it is sufficient for us to find a decoding algorithm for the codes in Construction II since they cover all LIP-codes. However, because of their simple configuration, the codes in Construction I can be easily decoded as follows.

Assume $\mathcal{C}_0$ is a t error correcting code of length n, $\mathcal{C} = \mathcal{C}_0 \times GF^n(q)$, $(\mathbf{u}, \mathbf{v}) \in \mathcal{C}$ has been sent and $(\mathbf{u}', \mathbf{v}')$ for $\mathbf{u}' = \mathbf{u} + \mathbf{e}$, $\mathbf{v}' = \mathbf{v} + \mathbf{e}$, $w_H(\mathbf{e}) \leq t$ is received by the decoder. Then

Decoding Algorithm I:

1. Use a decoding algorithm for code $\mathcal{C}_0$ to find $\mathbf{u}$ and $\mathbf{e}$ from $\mathbf{u}'$.

2. Let $\mathbf{v} = \mathbf{v}' - \mathbf{e}$.

We now turn to the decoding algorithm for codes in Construction II. Let $\mathcal{C} = \mathcal{U} \times \mathcal{V}$ be such a code, let $(\mathbf{u}, \mathbf{v}) \in \mathcal{C}$ be sent and $\mathcal{C}_0 = \mathcal{U} \cap \mathcal{V}$. Assume $(\mathbf{u}', \mathbf{v}')$ is received by the decoder with $\mathbf{u}' = \mathbf{u} + \mathbf{e}$, $\mathbf{v}' = \mathbf{v} + \mathbf{e}$. Let $\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_k}, \mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_{n-k}}$, I_1 and I_2 be as in Construction II and let G_0, G_1 and G_2 be the matrices whose rows are $\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_k}$; $\mathbf{v_i}$ $(i \in I_1)$; and $\mathbf{v_j}$ $(j \in I_2)$ respectively. Let $G = \begin{pmatrix} G_0 \\ G_1 \\ G_2 \end{pmatrix}$ and then G is a full rank matrix.

Decoding Algorithm II:

1. Calculate $\mathbf{y} = (y_1, y_2, \ldots, y_{n-k_2+1}, \ldots, y_n) = (\mathbf{v}' - \mathbf{u}')G^{-1}$, and let $\overline{\mathbf{y}} = (y_{n-k_2+1}, \ldots, y_n)G_2$.

2. Find the parity check matrix H_0, syndromes of cosets and the leaders $\boldsymbol{\ell_i}$, $i = 1, 2, \ldots, q^{n-k} - 1$ of cosets of code $\mathcal{C}_0$.

3. Calculate the syndrome of $\mathbf{v}' - \overline{\mathbf{y}}$ (for code $\mathcal{C}_0$) and find the leader $\boldsymbol{\ell_j}$ of the coset of $\mathcal{C}_0$ in which $\mathbf{v}' - \overline{\mathbf{y}}$ is contained by comparing the resulting syndrome and the syndromes in step 2.

4. Decoding of $(\mathbf{u}', \mathbf{v}')$ to $(\hat{\boldsymbol{u}}, \hat{\boldsymbol{v}}) = (\mathbf{u}' - \boldsymbol{\ell_j}, \mathbf{v}' - \boldsymbol{\ell_j})$.

Analysis: We have to show $\hat{\boldsymbol{u}} = \mathbf{u}$ and $\hat{\boldsymbol{v}} = \mathbf{v}$ for $(\hat{\boldsymbol{u}}, \hat{\boldsymbol{v}})$ in the last step, if $w_H(\mathbf{e}) \leq t$. For this it is sufficient to show $\boldsymbol{\ell_j} = \mathbf{e}$ for $\boldsymbol{\ell_j}$ obtained in step 3. By Construction II we know that there exist unique vectors $(c_1, \ldots, c_k;\ a_i\ (i \in I_1))$ and $(c'_1, \ldots, c'_k;\ b_{i'}, (i' \in I_2))$ such that $\mathbf{u} = \sum_{\ell=1}^{k} c_\ell\ \boldsymbol{u_\ell} + \sum_{i \in I_1} a_i \mathbf{v_i}$ and $\mathbf{v} = \sum_{\ell'=1}^{k} c'_{\ell'}\ \boldsymbol{u_{\ell'}} + \sum_{i' \in I_2} b_{i'} \mathbf{v_{i'}}$ (of course the vectors are unknown by the decoder until the decoding procedure is finished). Then

$\mathbf{v} - \mathbf{u} = \mathbf{v}' - \mathbf{u}' = \sum_{\ell=1}^{k} (c'_\ell - c_\ell)\ \boldsymbol{u_\ell} - \sum_{i \in I_1} a_i \mathbf{v_i} + \sum_{i' \in I_2} b_{i'} \mathbf{v_{i'}} = (c'_1 - c_1, c'_2 - c_2, \ldots, c'_k - c_k, -a_{i_1}, \ldots, a_{i_{|I_1|}}, b_{i'_1}, \ldots, b_{i'_{|I_2|}})G$, where $\{i_1, \ldots, i_{|I_1|}\} = I_1$ and $\{i'_1, \ldots, i'_{|I_2|}\} = I_2$.

By comparing this, $\mathbf{y}$ and $\overline{\mathbf{y}}$, we conclude that $(y_{n-k_2+1}, \ldots, y_n) = (b_{i'_1}, \ldots, b_{i'_{|I_2|}})$ and therefore $\overline{\mathbf{y}} = \sum_{i' \in I_2} b_{i'} \mathbf{v_{i'}}$. Hence $\mathbf{v}' - \overline{\mathbf{y}} = (\mathbf{v} - \overline{\mathbf{y}}) + \mathbf{e} = \sum_{\ell'=1}^{k} c'_{\ell'}\ \boldsymbol{u'_\ell} + \mathbf{e}$. Consequently $\boldsymbol{\ell_j} = \mathbf{e}$ since $\sum_{\ell'=1}^{k} c'_{\ell'}\ \boldsymbol{u_{\ell'}} \in \mathcal{C}_0$ and $\mathcal{C}_0$ is able to correct t errors.

4 A general model

Finally we remark that all results above can be directly extended to the case that there are more than two senders without changing the proofs. The following are our model and results.

For $m \geq 2$ define an $(n, m, t, |\mathcal{C}|)$ P-code over $GF^n(q)$ as a subset

$$\mathcal{C} \subset \underbrace{GF^n(q) \times \cdots \times GF^n(q)}_{m \text{ times}}$$

such that there do not exist $\mathbf{c} = (\mathbf{c}_1, \ldots, \mathbf{c}_m), \mathbf{c}' = (\mathbf{c}'_1, \ldots, \mathbf{c}'_m) \in \mathcal{C}$, (where $\mathbf{c}_i, \mathbf{c}'_j \in GF^n(q)$) and $\mathbf{e}, \mathbf{e}' \in GF^n(q)$ with $w_H(\mathbf{e}), w_H(\mathbf{e}') \leq t$ such that

$$(\mathbf{c}_1 + \mathbf{e}, \ldots, \mathbf{c}_m + \mathbf{e}) = (\mathbf{c}'_1 + \mathbf{e}', \ldots, \mathbf{c}'_m + \mathbf{e}').$$

Again such a code is independent or an IP-code if there are $\mathcal{C}_j \in GF^n(q)$, $1 \leq j \leq m$ such that $\mathcal{C} = \prod_{j=1}^{m} \mathcal{C}_j$, and an $(n, m, t, k_1, \ldots, k_m)$ LIP-code if $\mathcal{C}_j$ is a linear subspaces of $GF^n(q)$ with dimension k_j for all $1 \leq j \leq m$. Then our theorems 1–3 can be immediately extended to

Theorem 4. *(i) If there exists an (n, m, t, M) P-code, then*

$$M \leq A(n, t)q^{(m-1)n}.$$

(ii) Let $M = A(n, t)q^{(m-1)n}$, then there exists an (n, m, t, M) P-code.

Theorem 5. *Let $\mathcal{C}_1, \ldots, \mathcal{C}_m$ be linear subspaces of $GF^n(q)$. $\mathcal{C} = \prod_{j=1}^{m} \mathcal{C}_j$ is a LIP-code correcting t errors iff $\mathcal{C}_0 = \bigcap_{j=1}^{m} \mathcal{C}_j$ is a linear t error correcting code.*

Theorem 6. *For given positive integers n, m, t and non-negative integers $k_1, \ldots, k_m$ there exists an $(n, m, t, k_1, \ldots, k_m)$ LIP-code iff $k_j \leq n$ for all $1 \leq j \leq m$ and*

$$\sum_{j=1}^{m} k_j \leq L(n, t) + (m - 1)n.$$

Moreover, the Decoding Algorithms I and II can be easily extended to m senders. We leave all these extensions for readers as exercises.

References

[1] R. Ahlswede, Multi–way communication channels, in: 2nd Int. Symp. Inform. Theory, 23–52, Publishing House of the Hungarian Academy of Sciences, Tsahkadzor, Armenian SSR, 1973.

[2] R. Ahlswede, The capacity region of a channel with two senders and two receivers, Ann. Prob., 2(5), 805–814, 1974.

[3] R. Ahlswede, Coloring hypergraphs: A new approach to multi–user source coding, Journ. of Combinatorics, Information and System Sciences, 4(1), 76–115, 1979.

[4] R. Ahlswede, Coloring hypergraphs: A new approach to multi–user source coding, part ii, Journ. of Combinatorics, Information and System Sciences, 5(3), 220–268, 1980.

[5] R. Ahlswede, L.A. Bassalygo and M.S. Pinsker, On the Hamming bound for nonbinary localized–error–correcting codes, Preprint 99–077, SFB 343, Diskrete Strukturen in der Mathematik, Universität Bielefeld, Problemy Per. Informatsii, Vol. 35, No. 2, 29–37, Probl. of Inf. Transmission, Vol. 35, No. 2, 117–124, 1999.

[6] L.A. Bassalygo, S.I. Gelfand, and M.S. Pinsker, Coding for channels with localized errors, Proc. 4–th Soviet–Swedish Workshop in Information Theory, Gotland, Sweden, 95–99, 1989.

[7] E.R. Berlekamp, Block coding for the binary symmetric channel with noiseless, delayless feedback, in H.B. Mann, "Error Correcting Codes", Wiley, 61–85, 1968.

[8] E.R. Berlekamp, Algebraic Coding Theory, New York McGraw–Hill, 1968 (Series in Systems science).

[9] T.M. Cover and J.A. Thomas, Elements of Information Theory, Wiley Series in Telecommunication, City College of New York, 1991.

[10] I. Csiszár and J. Körner, Information Theory: Coding Theorems for Discrete Memoryless Systems, Academic Press, New York, 1981.

[11] G.H. Khachatrian, A survey of coding methods for the adder channel, I. Althöfer, N. Cai, G. Dueck, L. Khachatrian, M. Pinsker, A. Sárközy, I. Wegener and Z. Zhang (eds.), Numbers, Information and Complexity, (Festschrift in honour of Rudolf Ahlswede's 60th birthday), 181–196, 1999.

[12] F.J. McWilliams and N.J.A. Sloane, The theory of error correcting codes, Amsterdam, North–Holland, 1986.

[13] C.E. Shannon, A mathematical theory of communication, Bell. Syst. Techn. J. 27, 379–423, 623–656, 1948.

[14] C.E. Shannon, Two–way communication channels, Proc. 4th Berkeley Symp. Math. Statist. and Prob., Univ. of Calif. Press, Berkeley, Vol. 1, 611–644, 1961.