A Decoding Algorithm with Restrictions for Array Codes

Christoph Haslach, *Student Member, IEEE,* and A. J. Han Vinck, *Senior Member, IEEE*

***Abstract*— We present a simple and efficient error correction scheme for array-like data structures. We assume that the channel behaves such that each row of a received array is either error-free or corrupted by many symbol errors. Provided that row error vectors are linearly independent, the proposed decoding algorithm can correct asymptotically one erroneous row per redundant row, even without having reliability information from the channel output. This efficient decoding algorithm can be used for correction of error clusters and for decoding of concatenated codes. We also derive a random access scheme that has many similarities with the Aloha system.**

***Index Terms*—Array code, block-interleaving, burst-correcting, decoding of concatenated codes, linear independency.**

I. Introduction

We consider an error correction scheme for array-like data structures. The channel is assumed to behave such that each row of a received array is either error-free or corrupted by many symbol errors. We propose an efficient and simple encoding/decoding scheme which is capable of correcting asymptotically one erroneous row per redundant row. Hereby we assume that the error vectors which disturb the rows of the array are linearly independent.

We introduce the notation and the channel model in Section I, where we also describe the encoding scheme. In Section II, we derive the principles of the decoding algorithm which is based on the detection of error-free rows without using soft information. The properties of this algorithm are being discussed and an example is given in Section III-A. In Section III-B, we refer to the problem where the assumption of linear independency is justified. We present some applications for the proposed encoding/decoding scheme: the correction of error clusters in Section IV-A; a random access scheme that has many similarities with the Aloha system in Section IV-B; the decoding of concatenated codes as shown in Section IV-C.

In the following sections matrices are referred to by bold capital letters. The rows and columns of the matrices are denoted with the corresponding lower case bold letters. For example, $\boldsymbol{c}_{i,*}$ and $\boldsymbol{c}_{*,j}$ represent the ith row and the jth column of matrix $\boldsymbol{C}$, respectively. The element of the ith row and the jth column in matrix $\boldsymbol{C}$ is denoted as $c_{i,j}$. The components are elements of the field $\mathcal{A}$. The all-0 matrix or all-0 vector

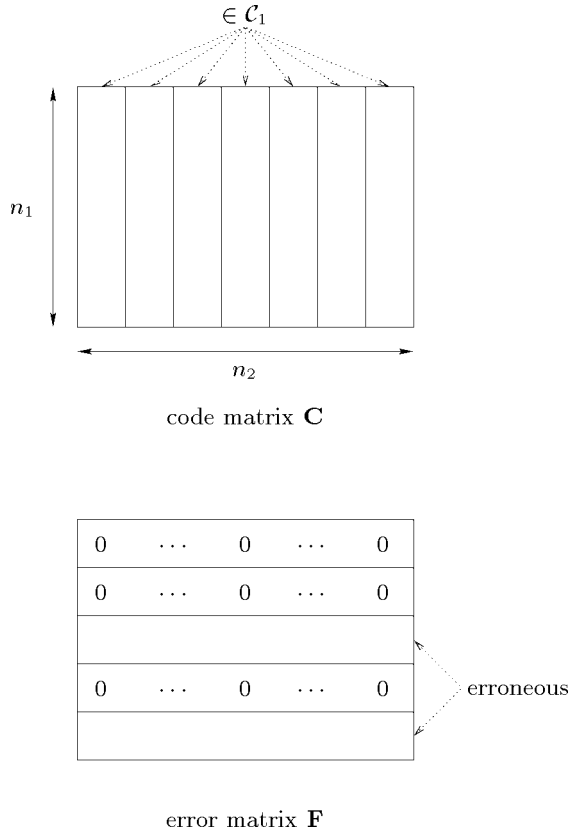

Fig. 1. Structure of code matrix $\boldsymbol{C}$ and error matrix $\boldsymbol{F}$.

are represented by $\mathbf{0}$, where the dimensions follow from the context.

We assume that the channel affects a transmitted matrix $\boldsymbol{C} \in \mathcal{A}^{n_1 \times n_2}$ such that each row of the received matrix $\boldsymbol{R} \in \mathcal{A}^{n_1 \times n_2}$ is either error-free or highly corrupted. We furthermore assume that no reliability information for the received symbols is available at the channel output. The errors inserted by the channel can be described by an additive error matrix $\boldsymbol{F} \in \mathcal{A}^{n_1 \times n_2}$ where $\boldsymbol{R} = \boldsymbol{C} + \boldsymbol{F}$. The structures of code matrix $\boldsymbol{C}$ and error matrix $\boldsymbol{F}$ are depicted in Fig. 1.

The encoding is done such that each column of $\boldsymbol{C}$ represents a codeword of a given linear block code $\mathcal{C}_1(n_1, k_1, d_1)$ with parity-check matrix $\boldsymbol{H}$, where

$$\boldsymbol{H} \cdot \boldsymbol{c}_{*,j} = (0, 0, \cdots, 0)^T \; \forall j \in \{1, 2, \cdots, n_2\}.$$

The ith row of $\boldsymbol{R}$ or the position i will be called erroneous iff $i \in \mathcal{E} := \{l | \boldsymbol{f}_{l,*} \neq \mathbf{0}\}$. For $i \in \mathcal{E}^c := \{l | \boldsymbol{f}_{l,*} = \mathbf{0}\}$ we call this row error-free. Let $t = ||\mathcal{E}||$ be the number of erroneous rows. The row-vectors $\boldsymbol{f}_{i,*}$, $i \in \mathcal{E}$ will be referred to as error vectors.

Manuscript received October 20, 1998.

The authors are with the Institute for Experimental Mathematics, University of Essen, 45326 Essen, Germany (e-mail: {haslach, vinck}@exp-math.uni-essen.de).

Communicated by R. M. Roth, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(99)07306-X.

The arrangement of n_2 codewords of $\mathcal{C}_1$ as columns of a $n_1 \times n_2$ matrix can be interpreted as block-interleaving. For bounded minimum-distance (BMD) decoding of each column one can correct at least $\lfloor (d_1-1)/2 \rfloor$ erroneous rows. We now propose a decoding algorithm in Section II that is capable of correcting $d_1 - 2$ erroneous rows, assuming that the error vectors $\boldsymbol{f}_{i,*}$, $i \in \mathcal{E}$ are linearly independent. The assumption of linear independency of all $\boldsymbol{f}_{i,*}$, $i \in \mathcal{E}$ is always made throughout the following paragraphs. We will show in Section III-B that this assumption is correct with very high probability for many applications.

II. Decoding Principle

In this section we will define the syndrome matrix $\boldsymbol{S}$ [2]. This matrix will be used to derive an algorithm that determines error-free rows of $\boldsymbol{R}$.

For each column $\boldsymbol{r}_{*,i}$ of $\boldsymbol{R}$ one can calculate the syndrome $\boldsymbol{s}_{*,i}$ with $\boldsymbol{s}_{*,i} = \boldsymbol{H} \cdot \boldsymbol{r}_{*,i}$. Arranging all syndromes $\boldsymbol{s}_{*,i}$, $i = 1, 2, \cdots, n_2$ as columns of a matrix we get the so-called syndrome matrix $\boldsymbol{S}$. It holds that

$$\boldsymbol{S} = \boldsymbol{H} \cdot \boldsymbol{R} = \boldsymbol{H} \cdot \boldsymbol{F}. \tag{1}$$

In order to use the properties of $\boldsymbol{S}$ we will take a closer look at the syndrome matrix. It holds that

$$\boldsymbol{S} = \boldsymbol{H} \cdot \boldsymbol{F} = \boldsymbol{H}_{\text{sub}} \cdot \boldsymbol{F}_{\text{sub}} \tag{2}$$

with

$$\boldsymbol{H}_{\text{sub}} = (\boldsymbol{h}_{*,i_1}, \boldsymbol{h}_{*,i_2}, \cdots, \boldsymbol{h}_{*,i_t}) \tag{3}$$

$$\boldsymbol{F}_{\text{sub}} = \begin{pmatrix} \boldsymbol{f}_{i_1,*} \\ \boldsymbol{f}_{i_2,*} \\ \vdots \\ \boldsymbol{f}_{i_t,*} \end{pmatrix} \tag{4}$$

$$\{i_1, i_2, \cdots, i_t\} = \mathcal{E}. \tag{5}$$

Lemma 1: If $||\mathcal{E}|| \leq d_1 - 1$ and the error vectors

$$\boldsymbol{f}_{i_1,*}, \boldsymbol{f}_{i_2,*}, \cdots, \boldsymbol{f}_{i_t,*}$$

are linearly independent then the following equation holds:

$$\operatorname{rank}(\boldsymbol{S}) = ||\mathcal{E}||. \tag{6}$$

Proof: For $t \leq d_1 - 1$ any t different columns of $\boldsymbol{H}$ are linearly independent and hence $\operatorname{rank}(\boldsymbol{H}_{\text{sub}}) = t$. Furthermore, $\operatorname{rank}(\boldsymbol{F}_{\text{sub}}) = t$ because linearly independent error vectors are assumed. From [3, inequality 0.4.5] it follows that

$$\operatorname{rank}(\boldsymbol{S}) = \operatorname{rank}(\boldsymbol{H}_{\text{sub}} \cdot \boldsymbol{F}_{\text{sub}}) = t. \qquad \square$$

For $t < \min(d_1, n_1 - k_1)$ the syndrome matrix $\boldsymbol{S}$ does not have maximum rank. Consequently, $n_1 - k_1 - t$ all-0 rows can be constructed from $\boldsymbol{S}$ by performing elementary row operations according to Gaussian elimination. Let the resulting matrix with $n_1 - k_1 - t$ all-0 rows be denoted by $\boldsymbol{S}^0$. Performing on $\boldsymbol{H}$ the same row operations that were performed on $\boldsymbol{S}$ we get the matrix $\boldsymbol{H}^0$ where $\boldsymbol{H}^0 \cdot \boldsymbol{R} = \boldsymbol{S}^0$.

Let $\mathcal{W}$ denote the set of indices j with $\boldsymbol{s}^0_{j,*} = \boldsymbol{0}$. Then it follows that

$$\boldsymbol{h}^0_{j,*} \cdot \boldsymbol{F} = \sum_{l=1}^{n_1} (h^0_{j,l} \cdot \boldsymbol{f}_{l,*}) = \boldsymbol{0}, \qquad \forall j \in \mathcal{W}.$$

Since all vectors $\boldsymbol{f}_{i_s,*} \neq \boldsymbol{0}$, $s = 1, 2, \cdots, t$ are linearly independent, it holds that $\boldsymbol{f}_{l,*} = \boldsymbol{0} \forall h^0_{j,l} \neq 0$, $j \in \mathcal{W}$. This means that we can determine a set $\mathcal{D}$ of indices of error-free rows where

$$\mathcal{D} = \bigcup_{j \in \mathcal{W}} \operatorname{supp}(h^0_{j,*}). \tag{7}$$

Now we are ready to give the following algorithm for the detection of error-free rows and for the reconstruction of erroneous rows in the received matrix $\boldsymbol{R}$.

Algorithm 1:

1) Calculate syndrome matrix $\boldsymbol{S} = \boldsymbol{H} \cdot \boldsymbol{R}$.
2) Construct $n_1 - k_1 - \operatorname{rank}(\boldsymbol{S})$ all-0-rows by performing elementary row operations on $\boldsymbol{S}$.
3) Perform the same row operations on $\boldsymbol{H}$ yielding $\boldsymbol{H}^0$.
4) Determine $\mathcal{D} = \cup_{j \in \mathcal{W}} (\operatorname{supp}(h^0_{j,*}))$.
5) Output: all rows $\boldsymbol{r}_{l,*}$ of $\boldsymbol{R}$ with $l \in \mathcal{D}$ are error-free.

III. Analysis of Decoding Principle

Using Algorithm 1 we can detect error-free rows of $\boldsymbol{R}$. In Section III-A we discuss which of the error-free rows can be detected by Algorithm 1 and we derive the conditions for which the detected error-free rows uniquely determine the transmitted code matrix. In Section III-B we discuss the problem where the assumption of linear independency is justified.

A. Error Correction Capability

If the positions in $\mathcal{D}$ define the code matrix $\boldsymbol{C}$ uniquely—i.e., there exists exactly one code matrix $\boldsymbol{A}$ with $a_{i,j} = r_{i,j}$ $\forall i \in \mathcal{D}, j = 1, 2, \cdots, n_2$ and $\boldsymbol{H} \cdot \boldsymbol{A} = \boldsymbol{0}$—then we can decode $\boldsymbol{R}$ correctly. This means that there exists exactly one codeword of $\mathcal{C}_1$ for each column of $\boldsymbol{R}$ such that the column and the codeword are identical at the detected error-free positions. The following example illustrates this problem and the steps of Algorithm 1.

Assume $\mathcal{C}_1$ to be a binary $(n_1 = 6, k_1 = 2, d_1 = 4)$-code with generator matrix

$$\boldsymbol{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix} \tag{8}$$

and with parity-check matrix

$$\boldsymbol{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{9}$$

Let $n_2 = 8$ and assume that we transmit the all-0 matrix. The first two rows are received in error such that

$$\boldsymbol{R} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{10}$$

According to (1)

$$\boldsymbol{S} = \boldsymbol{H} \cdot \boldsymbol{R} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}. \tag{11}$$

Performing Gaussian elimination on $\boldsymbol{S}$ we get

$$\boldsymbol{S}^0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \tag{12}$$

and applying the same row operations on $\boldsymbol{H}$ we obtain

$$\boldsymbol{H}^0 = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{13}$$

Hence, $\mathcal{W} = \{1, 2\}$, $\boldsymbol{h}^0_{1,*} = (001010)$, $\boldsymbol{h}^0_{2,*} = (000111)$, and $\mathcal{D} = \operatorname{supp}(\boldsymbol{h}^0_{1,*}) \cup \operatorname{supp}(\boldsymbol{h}^0_{2,*}) = \{3, 4, 5, 6\}$. In order to reconstruct the transmitted codeword we need $k_1 = 2$ linearly independent columns of $\boldsymbol{G}$ that correspond to the elements of $\mathcal{D}$, e.g., positions 4 and 6. These two positions can be considered as information positions of the code $\mathcal{C}_1$. The corresponding columns of $\boldsymbol{G}$ are unity vectors and so we can reconstruct $\boldsymbol{C}$ by

$$\boldsymbol{C} = \boldsymbol{G}^T \cdot \begin{pmatrix} \boldsymbol{r}_{4,*} \\ \boldsymbol{r}_{6,*} \end{pmatrix} = \boldsymbol{0}. \tag{14}$$

The problem remains to determine the general conditions under which the transmitted codeword can be correctly reconstructed. Therefore, we now analyze which of the correctly received rows are detected by Algorithm 1.

Assume that the uth row of $\boldsymbol{R}$ is error-free. A necessary condition for Algorithm 1 to find row u to be error-free is the existence of a parity-check vector $\boldsymbol{h}^0$ for code $\mathcal{C}_1$ such that

1) $\operatorname{supp}\left(\boldsymbol{h}^0\right) \cap \mathcal{E} = \{\}$
2) $u \in \operatorname{supp}\left(\boldsymbol{h}^0\right)$.

These conditions follow from (7). For $t \leq d_1 - 1$ the columns $\boldsymbol{h}_{*,i_1}, \boldsymbol{h}_{*,i_2}, \cdots, \boldsymbol{h}_{*,i_t}$ of $\boldsymbol{H}$, $\{i_1, i_2, \cdots, i_t\} = \mathcal{E}$ form a set of linearly independent column vectors. It follows that there exists an equivalent parity-check matrix $\boldsymbol{H'}$ such that the columns $\boldsymbol{h}'_{*,i_1}, \boldsymbol{h}'_{*,i_2}, \cdots, \boldsymbol{h}'_{*,i_t}$ of $\boldsymbol{H'}$ are all unity vectors with $\operatorname{supp}(\boldsymbol{h}'_{i_s,*}) = \{s\}$. Now it is easy to see that all parity-check vectors, generated by

$$(v_1, v_2, \cdots, v_{n_1-k_1}) \cdot \boldsymbol{H'}, \qquad \text{with } v_1 = v_2 = \cdots = v_t = 0 \tag{15}$$

fulfill condition 1). Hence, there is a total of $\|\mathcal{A}\|^{n_1-k_1-t}$ parity-check vectors that meet condition 1). Since all $\boldsymbol{h}^0_{j,*}$, $j \in \mathcal{W}$ are linearly independent we can construct $\|\mathcal{A}\|^{\|\mathcal{W}\|} = \|\mathcal{A}\|^{n_1-k_1-t}$ different linear combinations of these vectors. It is easy to see that all these linear combinations fulfill condition 1). Thus the vectors $\boldsymbol{h}^0_{j,*}$, $j \in \mathcal{W}$ are a linear basis for all parity-check vectors of $\mathcal{C}_1$ that fulfill condition 1).

If also $\boldsymbol{h}_{*,u}, \boldsymbol{h}_{*,i_1}, \boldsymbol{h}_{*,i_2}, \cdots, \boldsymbol{h}_{*,i_t}$ form a set of linearly independent column vectors then there exists an equivalent parity-check matrix $\boldsymbol{H''}$ such that the columns $\boldsymbol{h}''_{*,u}, \boldsymbol{h}''_{*,i_1} = \boldsymbol{h}'_{*,i_1}, \boldsymbol{h}''_{*,i_2} = \boldsymbol{h}'_{*,i_2}, \cdots, \boldsymbol{h}''_{*,i_t} = \boldsymbol{h}'_{*,i_t}$ of $\boldsymbol{H''}$ are all unity vectors with

$$\operatorname{supp}(\boldsymbol{h}''_{i_s,*}) = \{s\}$$

and

$$\operatorname{supp}(\boldsymbol{h}''_{*,u}) = \{t+1\}.$$

All $\|\mathcal{A}\|^{n_1-k_1-t-1} \cdot (\|\mathcal{A}\| - 1)$ vectors generated by

$$(v_1, v_2, \cdots, v_{n_1-k_1}) \cdot H', \qquad \text{with } v_1 = v_2 = \cdots = v_t = 0,\ v_{t+1} \neq 0 \tag{16}$$

fulfill conditions 1) and 2). Applying the preceding considerations for the case of arbitrary t we get the following lemma.

Lemma 2: An error-free row $\boldsymbol{r}_{u,*}$ of $\boldsymbol{R}$ is detected by Algorithm 1 iff

$$\operatorname{rank}(\boldsymbol{h}_{*,u}|\boldsymbol{h}_{*,i_1}|\boldsymbol{h}_{*,i_2}|\cdots|\boldsymbol{h}_{*,i_t}) - 1 = \operatorname{rank}(\boldsymbol{h}_{*,i_1}|\boldsymbol{h}_{*,i_2}|\cdots|\boldsymbol{h}_{*,i_t}) =: t^{\perp}.$$

Consequently, we can determine error-free rows (not necessarily all) as long as $t^{\perp} < n_1 - k_1$ holds. The question that now remains is whether the positions that were found to be error-free determine the transmitted codeword uniquely.

Lemma 3: Let $\|\mathcal{E}\| = t \leq d_1 - 2$ then Algorithm 1 gives a correct decision.

Proof: From $t \leq d_1 - 2$ and the Singleton bound it follows that $t < n_1 - k_1$. Then rank of any t columns of the parity-check matrix is t and rank of any $t+1$ columns is $t+1$. It follows from Lemma 2 that $n_1 - d_1 + 2$ error-free rows will be detected by Algorithm 1. $n_1 - d_1 + 2$ error-free positions are enough to reconstruct a codeword by the vertical code. □

B. The Linear Independency

The assumption that error vectors are linearly independent is essential for the proposed decoding algorithm. In practical situations the validity of this assumption heavily depends on the channel characteristics and on the chosen parameters n_1 and n_2. We address this problem for two cases which enables us to derive a general guideline for the choice of the code parameters.

In the first case we assume that all error vectors are equally likely. Let $\mathcal{S}$ be a set of j linearly independent error vectors. They can be considered as a basis of a linear space containing $\|\mathcal{A}\|^j$ different vectors. An arbitrary random vector $\boldsymbol{v}$ is linearly dependent of the j vectors if $\boldsymbol{v}$ is an element

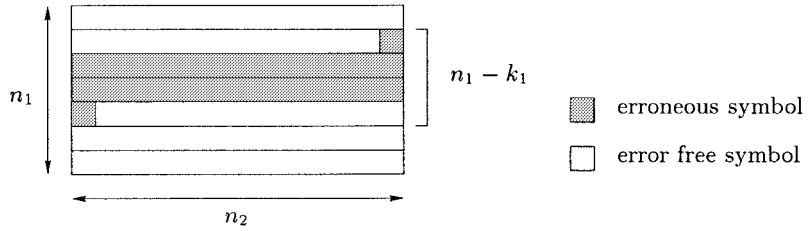

Fig. 2. Shortest error burst that can corrupt $n_1 - k_1$ rows.

of the linear space spanned by the j vectors. As there are a total of $||\mathcal{A}||^{n_2}$ different vectors of length n_2 the probability that $\boldsymbol{v}$ is linearly dependent on the j vectors is then equal to $||\mathcal{A}||^{-(n_2-j)}$. So, we can derive an upper bound for the probability P_d that s vectors are linearly dependent

$$P_d \leq \sum_{j=1}^{s-1} ||\mathcal{A}||^{-(n_2-j)} \leq 2 \cdot ||\mathcal{A}||^{-(n_2-s+1)}. \tag{17}$$

As the decoding algorithm corrects up to $d_1 - 2$ error vectors we must choose n_2 large enough compared with $s = d_1 - 2$ in order to achieve a sufficiently small P_d. Another more general bound for the probability of linear independency can be found in [4, Lemma 14].

Now consider the second case where we have a set of $v \ll ||\mathcal{A}||^{n_2-s}$ typical error vectors all having the same probability of occurrence. Error vectors that occur in the system are with high probability members of this set. We assume that the probability that j different vectors from this set are linearly dependent is roughly equal to the probability that j arbitrary random vectors are linearly dependent.

Suppose that j linearly independent typical error vectors are given. Then the probability that a new typical error vector $\boldsymbol{v}$ is linearly dependent on the j given vectors is dominated by the probability that $\boldsymbol{v}$ is identical with one of the given j vectors. The probability is equal to $j \cdot v^{-1}$. Hence, the probability P'_d that s of the typical error vectors are linearly dependent can be approximated by the following equation:

$$P'_d \approx \sum_{j=1}^{s-1} \frac{j}{v} = \frac{s \cdot (s-1)}{2 \cdot v}. \tag{18}$$

Hence, we must assure that the number of typical error vectors is large enough in order to achieve a sufficiently small P'_d.

IV. Applications

A. Decoding of Error Clusters

The number of errors per erroneous row is not important for the decoding algorithm as long as the error vectors are linearly independent. Hence, this algorithm is suited for the correction of error bursts. In order to achieve a good error correction capability it is very attractive to use a Reed–Solomon (RS) code as a column-code because RS codes reach the Singleton bound. They can be used for M-ary transmission as well as for binary transmission. For binary transmission an RS code over GF (2^m) is used where m adjacent bits of a row are considered as one symbol of the GF (2^m). The number of bits per row must be a multiple of m in this case.

Using an RS code $\mathcal{C}_1(n_1, k_1, d_1 = n_1 - k_1 + 1)$ we can correct $n_1 - k_1 - 1$ erroneous rows. Having row-wise transmission the shortest error burst that can affect more than $n_1 - k_1 - 1$ rows has a length of $n_2 \cdot (n_1 - k_1 - 2) + 2$ symbols, as shown in Fig. 2. Hence, we are capable of correcting all error bursts of length $n_2 \cdot (n_1 - k_1 - 2) + 1$ symbols provided that the error vectors are linearly independent. A redundancy of $n_2 \cdot (n_1 - k_1)$ symbols is required. For the case that u error bursts occur in one received array, we are capable of correcting error bursts with a total length of $n_2 \cdot (n_1 - k_1 - 2u) + 2u - 1$ symbols. Consequently, for $(n_1 - k_1) \to \infty$ the ratio between the number of correctable errors and redundancy goes to 1. This seems to be contradicting the Reiger bound, which states that a redundancy of at least $2 \cdot L$ symbols is needed to correct all error bursts of length L. However, our result is only valid if the error vectors are linearly independent. We do not correct all error bursts with the given parameters and thus the Reiger bound is not appropriate.

B. Aloha-Like Random-Access Scheme Without Feedback

The Aloha system [1] is a simple and well-known random-access scheme. Nevertheless, it requires collision detection and feedback from the receiver or channel to the transmitters. We will now use the proposed decoding algorithm to construct a random-access scheme that requires no feedback. No collision detection is required because our decoding algorithm performs this collision detection inherently by searching for error-free rows. Consequently, we do not need redundancy in the rows for error detection.

Assume that we have U independent users that have access to Z parallel and independent transmission channels. Each user encodes his data as described in Section I. Let $\mathcal{C}_1$ be a Reed–Solomon code $\mathcal{R}(n_1, k_1, d_1 = n_1 - k_1 + 1)$ with code symbols from GF (M). In addition every user possesses a signature sequence $(s(1), s(2), \cdots, s(n_1))$ of integers $s(i)$, with $1 \leq s(i) \leq n_1$. The $s(i)$, $1 \leq i \leq n_1$ are chosen with

$$\text{prob}\,(s(i) = j,\ 1 \leq j \leq Z) = 1/Z.$$

The signature connected with each user is known at the receiver site. At time interval i the transmitter selects channel $s(i)$ for the transmission of the ith code row. Furthermore, the users are assumed to be row-synchronized. If two or more users use the same channel at the same time, we assume that the received row is erroneous. Hence, we have exactly the same situation as is required for the proposed decoding

algorithm. We manage to decode the received matrix correctly if not more than $n_1 - k_1 - 1$ code rows are corrupted by the other users and if the error vectors that result from the collisions are linearly independent. Whether the second condition is fulfilled depends on how the channel reacts in the case of a collision. We consider the case where a collision as channel output is a random sequence. Hence, all error vectors are equally likely. This case is discussed in Section III-B and we can assume linear independency for $n_2 \gg (n_1 - k_1 - 1)$. The probability p_e that a row is received as a collision is given by

$$p_e = 1 - \left(\frac{Z-1}{Z}\right)^{(U-1)}. \tag{19}$$

According to [1], we can expect correct decoding with an arbitrary small decoding error probability for $n_1 \to \infty$ and $k_1/n_1 =$ constant if $n_1 \cdot p_e < d_1 - 2 = n_1 - k_1 - 1$ or

$$p_e < 1 - r, \qquad \text{with} \quad r = \frac{k_1}{n_1}. \tag{20}$$

The transmission of one code matrix per user requires a total of $Z \cdot n_1 \cdot n_2$ symbol slots. The total transmitted, uncoded information is $U \cdot k_1 \cdot n_2 = U \cdot n_1 \cdot n_2 \cdot r$ symbols. Substituting $r = 1 - p_e$ we get the following expression for the efficiency η of this random access scheme:

$$\eta = \frac{U \cdot n_1 \cdot n_2 \cdot \left(\left(\frac{Z-1}{Z}\right)^{(U-1)}\right)}{Z \cdot n_1 \cdot n_2} = \frac{U \cdot \left(\frac{Z-1}{Z}\right)^{(U-1)}}{Z}. \tag{21}$$

For $U \to \infty$ and $Z \to \infty$ we get

$$\eta = G \cdot e^{-G}, \qquad \text{with} \quad G = \frac{U}{Z}. \tag{22}$$

The efficiency of the proposed system has the same performance as the efficiency of the Aloha system. The maximum efficiency is equal to e^{-1}.

C. Decoding of Concatenated Codes

We now consider the decoding of concatenated codes. The encoding is carried out in two steps. At first, every column of a $k_1 \times k_2$ matrix of information symbols is encoded with a linear block code $\mathcal{C}_1(n_1, k_1, d_1)$. Then, each row of the resulting $n_1 \times k_2$ matrix is encoded with a linear block code $\mathcal{C}_2(n_2, k_2, d_2)$. We obtain an $n_1 \times n_2$ matrix $\boldsymbol{C}$ where every column is a codeword of $\mathcal{C}_1$ and every row is a codeword of $\mathcal{C}_2$. The concatenated code has length $n_1 \cdot n_2$, dimension $k_1 \cdot k_2$, and minimum distance $d_1 \cdot d_2$. After transmission over a noisy channel we first decode the rows corresponding the code $\mathcal{C}_2$. A row is decoded incorrectly if at least $\lfloor \frac{d_2+1}{2} \rfloor$ errors have occurred in this row. After decoding the rows we obtain an $n_1 \times n_2$ matrix $\boldsymbol{R}$ where each row is either error-free or erroneous. Hence, we can apply the proposed decoding algorithm to decode $\boldsymbol{R}$.

As the proposed decoding algorithm is capable of correcting up to $d_1 - 2$ erroneous rows, we can decode at least $\lfloor \frac{d_2+1}{2} \rfloor \cdot (d_1 - 2)$ errors with the codes $\mathcal{C}_1$ and $\mathcal{C}_2$, provided that the error vectors after decoding of $\mathcal{C}_2$ are linearly independent. A simple BMD decoding of rows and columns can correct at least $\lfloor \frac{d_2+1}{2} \rfloor \cdot \lfloor \frac{d_1-1}{2} \rfloor$ errors. In order to design the parameters of the concatenated code several aspects have to be considered.

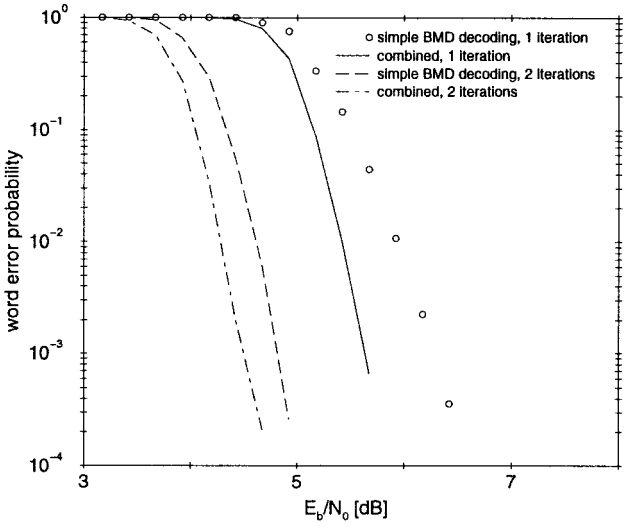

Fig. 3. Decoding of concatenated BCH-codes: $\mathcal{C}_1(63, 45, 7)$, $\mathcal{C}_2(63, 45, 7)$.

1) The error vectors after the first decoding step are codewords of $\mathcal{C}_2$ if no decoding failure occurs. Hence, not all error vectors are equally likely. Assuming that mainly codewords with small Hamming weight occur as error vectors, $\mathcal{C}_2$ must be chosen such that there is a sufficiently large number of codewords with small Hamming weight. This is necessary in order to get a sufficient amount of linearly independent error vectors (see Section III-B).

2) The decoding of the concatenated code will only yield good results if the first decoding step has a sufficiently small decoding error probability. Hence, it is obvious that $\mathcal{C}_2$ should have a higher error correcting capability than $\mathcal{C}_1$.

3) Assume that $\mathcal{C}_1$ and $\mathcal{C}_2$ are maximum-distance separable (MDS) codes with dimension k_1 and k_2, respectively. The total distance $d_1 \cdot d_2 = (n_1 - k_1 + 1) \cdot (n_2 - k_2 + 1)$ is maximized for fixed $k_1 \cdot k_2$ if $\frac{k_1}{n_1+1} = \frac{k_2}{n_2+1}$. This aim is concurring to point 2).

An alternative to the proposed algorithm is simple BMD decoding of rows and columns. The advantage of this method is that it can be repeated several times. We will call it simple BMD decoding with i iterations where i counts how often BMD decoding of rows and columns is repeated. Simple BMD decoding can also be combined with our algorithm and we will call it combined decoding with i iterations. For this we first perform simple BMD decoding with $i-1$ iterations. Then we apply BMD decoding of the rows and our proposed algorithm. In Fig. 3, simulations are presented for these algorithms for the memoryless AWGN channel. It can be seen that the proposed decoding algorithm performs better for high E_b/N_0 than simple BMD decoding with one iteration. If BMD decoding of rows and columns is repeated twice, we get much better results than for simple BMD decoding with one iteration. This can be explained by the fact that the number of symbol errors per erroneously decoded row is usually significantly smaller than n_2. Hence, it is quite likely that there are columns with less than $\lfloor \frac{d_1-1}{2} \rfloor$ symbol errors after decoding the rows although

more than $\lfloor \frac{d_1-1}{2} \rfloor$ rows were decoded erroneously. So, the number of errors can be further reduced by BMD decoding of the columns and one can expect that some of the erroneously decoded rows can be corrected when these rows are decoded again after the decoding of columns. Again, the combined algorithm outperforms simple BMD decoding when the same number of iterations are carried out.

V. Conclusions

We have presented a new decoding algorithm for block interleaved linear block codes that can be considered as a simple class of array codes. It turns out that RS codes are well suited for the column-wise encoding. They can be used for M-ary transmission as well as for binary transmission. Using RS codes we are capable of correcting asymptotically one erroneous row per redundant row. The assumption that the error vectors affecting the rows of the code matrix are linearly independent is essential for the decoding algorithm. We derived examples that show that this assumption is valid for a variety of applications: for the decoding of error clusters; for random-access schemes, and for the decoding of concatenated codes.

Acknowledgment

The authors wish to thank the Associate Editor R. M. Roth and the reviewers for their constructive comments and suggestions that helped to improve the paper.

References

[1] N. Abramson, "The throughput of packet broadcasting channels," *IEEE Trans. Commun.*, vol. COM-25, pp. 117–128, Jan. 1977.
[2] M. Breitbach, M. Bossert, V. Zyablov, and V. Sidorenko, "Array codes correcting a two dimensional cluster of errors," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2025–2031, Sept. 1998.
[3] R. A. Horn and C. R. Johnson, *Matrix Analysis.* Cambridge, U.K.: Cambridge Univ. Press, 1985, p. 13.
[4] R. M. Roth, "Probabilistic crisscross error correction," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1425–1438, Sept. 1997.