Construction of uniquely decodable codes for the two-used binary adder channel

Construction of Uniquely Decodable Codes for the Two-User Binary Adder Channel

Rudolf Ahlswede and Vladimir B. Balakirsky, *Member, IEEE*

***Abstract*—A construction of uniquely decodable codes for the two-user binary adder channel is presented. The rates of the codes obtained by this construction are greater than the rates guaranteed by the Coebergh van den Braak and van Tilborg construction and these codes can be used with simple encoding and decoding procedures.**

***Index Terms*—Adder channel, coding, decoding, multiple-access channel.**

I. Introduction

We address the problem of constructing uniquely decodable codes for the two-user binary adder channel. Suppose that two independent users transmit binary codewords of the same length over the channel and the receiver gets a vector obtained by component-wise arithmetic sum of these codewords. The decoder has to decide which codeword was transmitted by each user with the error probability zero.

Systematic investigations of multiple-access channels were initiated by the papers [1], [2] where the achievable rate region for memoryless multiple-access channels under the criterion of arbitrarily small average decoding error probability was found. The boundary of this region for the two-user binary adder channel is defined by the equations

$$R_1 = 1 \qquad R_2 = 1 \qquad R_1 + R_2 = 1.5$$

where R_1 and R_2 are the code rates of the users. These equations also give an outer bound on the code rates that can be realized under the criterion of the decoding error probability zero, i.e., the rates of the pair of codes that form a *uniquely decodable code* for the adder channel. The best known lower bound on these rates was proved by Kasami, Lin, Wei, and Yamamura [3] (this bound will be referred to as the KLWY lower bound). The first constructions of specific codes for this channel were obtained by Weldon [4]. Further results in this direction were established by Khachatrian [5], Coebergh van den Braak and van Tilborg [6], and other authors. Probably, the code construction discovered in [6] gives the best known pairs (R_1, R_2) such that there exist uniquely decodable codes with these rates. This construction will be referred to as the CT-construction.

We will construct two binary codes, $\mathcal{U}$ and $\mathcal{V}$, of length tn, where t and n are fixed integers, in such a way that $(\mathcal{U}, \mathcal{V})$ is a uniquely decodable code for the two-user binary adder channel. Each codeword will be represented as a sequence of binary n-tuples having length t; these n-tuples will be regarded as subblocks. *The main point of our considerations is that we do not only prove the statement of an existence type concerning uniquely decodable codes, but build specific codes for fixed t and n in a regular way. The rates of these codes are located above the KLWY lower bound and these codes can be used in conjunction with simple encoding and decoding procedures.*

The correspondence is organized as follows. We begin with the description of codes $\mathcal{U}, \mathcal{V}$ and illustrate the definitions for specific data. Then we prove a theorem which claims that $(\mathcal{U}, \mathcal{V})$ is a uniquely decodable code and gives expressions for $|\mathcal{U}|$ and $|\mathcal{V}|$. Some numerical results and a discussion about the relationships between our construction and the CT-construction are also presented. After that we describe a simple decoding procedure. Finally, we point out to the possibility of enumerative coding which follows from the regularity of the construction.

II. Code Construction (u)–(v)

Let us fix integers $t, n \geq 1$ in such a way that t is even and construct the codes $\mathcal{U}$ and $\mathcal{V}$ using the following rules.

(u) Let $\mathcal{C}$ denote the set consisting of all binary vectors of length t and Hamming weight $t/2$, i.e.,

$$\mathcal{C} = \{c = (c_1, \cdots, c_t) \in \{0,1\}^t \colon w_H(c) = t/2\} \tag{1}$$

where w_H denotes the Hamming weight. Construct a code

$$\mathcal{U} = \bigcup_{c \in \mathcal{C}} \{(c_1^n, \cdots, c_t^n)\} \tag{2}$$

of length tn repeating n times each component of every vector $c \in \mathcal{C}$.

(v) Given an $s \in \{0, \cdots, t\}$, let

$$\mathcal{J}_s = \{J \subseteq [t] \colon |J| = s\}$$

denote the collection consisting of all s-element subsets of the set $[t] = \{1, \cdots, t\}$, and let

$$\mathcal{A}^{(s)} = \bigcup_{i=0}^{s} \{1^{in} 0^{(s-i)n}\} \tag{3}$$

where $1^0 0^{sn} = 0^{sn}$ and $1^{sn} 0^0 = 1^{sn}$. Furthermore, let us introduce an alphabet

$$\mathcal{B} = \{0,1\}^n \backslash \{0^n, 1^n\}$$

consisting of $2^n - 2$ binary vectors which differ from 0^n and 1^n. Let $j_1 < \cdots < j_s$ be the elements of the set $J \in \mathcal{J}_s$ and let $j'_1 < \cdots < j'_{t-s}$ be the elements of the set

$$J^c = [t] \backslash J.$$

For all $(a, b) \in \mathcal{A}^{(s)} \times \mathcal{B}^{t-s}$, define a vector

$$v(a, b|J) = (v_1, \cdots, v_t) \in \{0,1\}^{tn} \tag{4}$$

in such a way that

$$v_j = \begin{cases} a_k, & \text{if } j = j_k \\ b_k, & \text{if } j = j'_k \end{cases} \tag{5}$$

where $j = 1, \cdots, t$, and construct a code

$$\mathcal{V} = \bigcup_{s=0}^{t} \bigcup_{J \in \mathcal{J}_s} \bigcup_{a \in \mathcal{A}^{(s)}} \bigcup_{b \in \mathcal{B}^{t-s}} \{v(a, b|J)\}.$$

Manuscript received February 22, 1997; revised April 15, 1998. This work was supported in part by the SFB-343, Universität Bielefeld, Germany.

R. Ahlswede is with Fakultät für Mathematik, Universität Bielefeld, D-33501 Bielefeld 1, Germany.

V. B. Balakirsky was with Fakultät für Mathematik, Universität Bielefeld, D-33501 Bielefeld 1, Germany. He is now with the Electrical Engineering Department, Eindhoven University of Technology, 5600 MB Eindhoven, The Netherlands.

Communicated by K. Zeger, Associate Editor At Large.

Publisher Item Identifier S 0018-9448(99)00087-5.

Example 1: Let $t = n = 2$. Then $\mathcal{C} = \mathcal{B} = \{01, 10\}$. The code $\mathcal{U}$ consists of two codewords

$$u^{(1)} = 00 \quad 11$$
$$u^{(2)} = 11 \quad 00$$

and the code $\mathcal{V}$ consists of all binary vectors of length 4, except 0011. We construct $\mathcal{V}$ in the following way.

$s = 0$. $\mathcal{J}_s = \emptyset$, $\mathcal{A}^{(s)} = \emptyset$, $\mathcal{B}^{t-s} = \{0101, 0110, 1001, 1010\}$.

$$v^{(1)} = v(-, 0101|\emptyset) = 01 \quad 01$$
$$v^{(2)} = v(-, 0110|\emptyset) = 01 \quad 10$$
$$v^{(3)} = v(-, 1001|\emptyset) = 10 \quad 01$$
$$v^{(4)} = v(-, 1010|\emptyset) = 10 \quad 10$$

$s = 1$. $\mathcal{J}_s = \{\{1\}, \{2\}\}$, $\mathcal{A}^{(s)} = \{00, 11\}$, $\mathcal{B}^{t-s} = \{01, 10\}$.

$$v^{(5)} = v(00, 01|\{1\}) = 00 \quad 01$$
$$v^{(6)} = v(00, 10|\{1\}) = 00 \quad 10$$
$$v^{(7)} = v(11, 01|\{1\}) = 11 \quad 01$$
$$v^{(8)} = v(11, 10|\{1\}) = 11 \quad 10$$
$$v^{(9)} = v(00, 01|\{2\}) = 01 \quad 00$$
$$v^{(10)} = v(00, 10|\{2\}) = 10 \quad 00$$
$$v^{(11)} = v(11, 01|\{2\}) = 01 \quad 11$$
$$v^{(12)} = v(11, 10|\{2\}) = 10 \quad 11$$

$s = 2$. $\mathcal{J}_s = \{\{1, 2\}\}$, $\mathcal{A}^{(s)} = \{0000, 1100, 1111\}$, $\mathcal{B}^{t-s} = \emptyset$.

$$v^{(13)} = v(0000, -|\{1, 2\}) = 00 \quad 00$$
$$v^{(14)} = v(1100, -|\{1, 2\}) = 11 \quad 00$$
$$v^{(15)} = v(1111, -|\{1, 2\}) = 11 \quad 11$$

The pair $(\mathcal{U}, \mathcal{V})$ is optimal in the following sense: any codes $\mathcal{U}$ and $\mathcal{V}$ such that $(\mathcal{U}, \mathcal{V})$ is a uniquely decodable code for the binary adder channel may contain at most one common codeword; thus

$$|\mathcal{U}| + |\mathcal{V}| \le 2^{tn} + 1.$$

In our case,

$$|\mathcal{U}| + |\mathcal{V}| = 17 = 2^{tn} + 1.$$

III. Properties of Codes Constructed by (u)–(v)

Theorem: The code $(\mathcal{U}, \mathcal{V})$ of length tn defined in (u)–(v) is a uniquely decodable code for the two-user binary adder channel and

$$|\mathcal{U}| = \binom{t}{t/2} \tag{6}$$
$$|\mathcal{V}| = (2^n - 1)^t \left[\frac{t}{2^n - 1} + 1\right]. \tag{7}$$

Hence

$$R_1 = \frac{1}{n} - \frac{1}{tn} \log \left[2^t \binom{t}{t/2}^{-1}\right]$$
$$R_2 = \frac{1}{n} \log(2^n - 1) + \frac{1}{tn} \log \left[\frac{t}{2^n - 1} + 1\right].$$

Proof: Equation (6) directly follows from (1) and (2). Given an $s \in \{0, \cdots, t\}$, the set $\mathcal{J}_s$ consists of $\binom{t}{s}$ elements. For each $J \in \mathcal{J}_s$ there are $s + 1$ possibilities for the vector $a \in \mathcal{A}^{(s)}$ and $(2^n - 2)^{t-s}$ possibilities for the vector $b \in \mathcal{B}^{t-s}$. Therefore,

$$|\mathcal{V}| = \sum_{s=0}^{t} \binom{t}{s} (s + 1) (2^n - 2)^{t-s}.$$

It is easy to check that this equation can be expressed as (7).

The proof is complete if we show that $(\mathcal{U}, \mathcal{V})$ is a uniquely decodable code. Let us introduce an alphabet $\mathcal{B}^*$ consisting of the $2^n - 2$ elements of $\mathcal{B}$ and an element specified as "$*$," i.e.,

$$\mathcal{B}^* = \mathcal{B} \bigcup \{*\}. \tag{8}$$

Let $(\mathcal{B}^*)^t$ denote the tth extension of $\mathcal{B}^*$. For all $b^* \in (\mathcal{B}^*)^t$, we introduce the set

$$\begin{aligned} \mathcal{V}(b^*) = \{v = (v_1, \cdots, v_t) \in \{0, 1\}^{tn}: \\ v_j = b_j^*, \text{ if } b_j^* \ne *, \text{ and} \\ v_j \in \{0^n, 1^n\}, \text{ if } b_j^* = *; \\ \text{for all } j = 1, \cdots, t\}. \end{aligned} \tag{9}$$

Note that $\{\mathcal{V}(b^*), b^* \in (\mathcal{B}^*)^t\}$ is a collection of pairwise disjoint sets and get the following proposition.

Proposition 1: Suppose that, for all $b^* \in (\mathcal{B}^*)^t$, there are subsets $\hat{\mathcal{V}}(b^*) \subseteq \mathcal{V}(b^*)$ satisfying the following condition:

$$(\mathcal{U} + v) \bigcap (\mathcal{U} + v') = \emptyset, \qquad \text{for all } v, v' \in \hat{\mathcal{V}}(b^*).$$

Then $(\mathcal{U}, \cup_{b^* \in (\mathcal{B}^*)^t} \hat{\mathcal{V}}(b^*))$ is a uniquely decodable code.

Furthermore, using (1), (2) and (8), (9) we obtain

Proposition 2: Given $b^* \in (\mathcal{B}^*)^t$ and $v, v' \in \mathcal{V}(b^*)$, the following two statements are equivalent:

1) There exist $u, u' \in \mathcal{U}$ such that

$$u + v = u' + v'.$$

2) There exist $c, c' \in \mathcal{C}$ such that

$$\begin{aligned} v_j = v_j' &\Longrightarrow c_j = c_j' \\ (v_j, v_j') = (0^n, 1^n) &\Longrightarrow (c_j, c_j') = (1, 0) \\ (v_j, v_j') = (1^n, 0^n) &\Longrightarrow (c_j, c_j') = (0, 1), \qquad \text{for all } j = 1, \cdots, t. \end{aligned} \tag{10}$$

Let us fix $b^* \in (\mathcal{B}^*)^t$ and, for all $v, v' \in \mathcal{V}(b^*)$, define

$$\begin{aligned} t_{01}(v, v') &= \sum_{j=1}^{t} \chi\{(v_j, v_j') = (0^n, 1^n)\} \\ t_{10}(v, v') &= \sum_{j=1}^{t} \chi\{(v_j, v_j') = (1^n, 0^n)\}. \end{aligned} \tag{11}$$

Hereafter, χ stands for the indicator function: $\chi\{S\} = 1$ if the statement S is true and $\chi\{S\} = 0$ otherwise.

Proposition 3: If $v, v' \in \mathcal{V}(b^*)$ and

$$t_{01}(v, v') \ne t_{10}(v, v') \tag{12}$$

then there are no $c, c' \in \mathcal{C}$ such that statement (10) is true.

TABLE I
THE RATES (R_1, R_2) OF SOME UNIQUELY DECODABLE CODES DEFINED BY (u)–(v), THE SUM RATS $R_1' + R_2'$ FOR THE CODES WHOSE EXISTENCE IS GUARANTEED BY THE CT-CONSTRUCTION, AND THE DIFFERENCES BETWEEN R_2 AND THE VALUES $\hat{R}_2$ DEFINED BY THE KLWY LOWER BOUND ON THE MAXIMAL RATE OF UNIQUELY DECODABLE CODES

tn	t	R_1	R_2	$R_1 + R_2$	$R_1' + R_2'$	$R_2 - \hat{R}_2$
28	14	0.419458	0.881856	1.301315	1.299426	0.008833
32	16	0.426616	0.875699	1.302315	1.301048	0.009834
36	18	0.432480	0.870463	1.302943	1.302071	0.010462
40	20	0.437382	0.865946	1.303328	1.302714	0.010847
44	22	0.441549	0.862002	1.303550	1.303109	0.011069
48	24	0.445141	0.858521	1.303662	1.303339	0.011181
52	**26**	**0.448272**	**0.855424**	**1.303696**	**1.303457**	**0.011215**
56	28	0.451030	0.852646	1.303676	1.303497	0.011195
60	30	0.453480	0.850138	1.303618	1.303482	0.011137
64	32	0.455672	0.847861	1.303533	1.303428	0.011052
68	34	0.457646	0.845783	1.303428	1.303347	0.010947
72	36	0.459434	0.843876	1.303311	1.303248	0.010829
76	38	0.461063	0.842121	1.303184	1.303134	0.010702
80	40	0.462553	0.840498	1.303051	1.303012	0.010570

Proof: Since all vectors $c, c' \in \mathcal{C}$ have the same Hamming weight, we obtain

$$\sum_{j=1}^{t} \chi\{(c_j, c_j') = (0,1)\} = \sum_{j=1}^{t} \chi\{(c_j, c_j') = (1,0)\}. \tag{13}$$

If these vectors satisfy (10) given $v, v' \in \mathcal{V}(b^*)$, then using (9), (11), and (13), we conclude that $t_{01}(v, v') = t_{10}(v, v')$, but this equation contradicts (12). □

Let us fix $b^* \in (\mathcal{B}^*)^t$, denote

$$J = \{j \in [t]: b_j^* = *\}, \qquad s = |J|,$$

and suppose that $j_1 < \cdots < j_s$ and $j_1' < \cdots < j_{t-s}'$ are the elements of the sets J and J^c. Assign

$$\hat{\mathcal{V}}(b^*) = \{v \in \mathcal{V}(b^*): (v_{j_1}, \cdots, v_{j_s}) \in \mathcal{A}^{(s)}\}$$

where the set $\mathcal{A}^{(s)}$ is defined in (3). Then, for all $v, v' \in \hat{\mathcal{V}}(b^*)$, $v \neq v'$, either $t_{01}(v, v') > 0$ and $t_{10}(v, v') = 0$, or $t_{01}(v, v') = 0$ and $t_{10}(v, v') > 0$. Therefore, based on Proposition 3, we conclude that, for all $v, v' \in \hat{\mathcal{V}}(b^*)$, there are no $c, c' \in \mathcal{C}$ such that statement (10) is true, and using Proposition 2 obtain that the sets $\mathcal{U} + v$, $v \in \hat{\mathcal{V}}(b^*)$, are pairwise disjoint. Finally, Proposition 1 says that $(\mathcal{U}, \cup_{b^* \in (\mathcal{B}^*)^t} \hat{\mathcal{V}}(b^*))$ is a uniquely decodable code and, as is easy to see,

$$\bigcup_{b^* \in (\mathcal{B}^*)^t} \hat{\mathcal{V}}(b^*) = \mathcal{V}$$

where $\mathcal{V}$ is defined in (4) and (5). □

The rates (R_1, R_2) of some uniquely decodable code are given in Table I. For $R_1 \in (1/3, 1/2)$, the pair

$$\left(R_1, \hat{R}_2 = \frac{\log 6}{2} - R_1\right)$$

belongs to the KLWY lower bound. We show the difference $R_2 - \hat{R}_2$ and the values of the sum rates $R_1' + R_2'$ of the codes $(\mathcal{U}', \mathcal{V}')$ whose existence is guaranteed if we use the CT-construction with given t and n. The sum rates of all codes presented in Table I are greater than $R_1' + R_2'$ and the points (R_1, R_2) are located above the curve obtained using the KLWY lower bound.

Remark (on the CT-Construction): The authors of [6] described a rather general construction which "almost" contains our construction (u)–(v) when $t \geq 4$, meaning that we fix the Hamming weight of each element of the set $\mathcal{C}$, while this weight should be divisible by $t/2$ in the CT-construction (if we consider the case $q = 2, r = 0$ [6, p. 8]). Then the expressions for the cardinalities of the codes given in Theorem 2 are reduced (in our notations) to

$$|\mathcal{U}'| = 2 + \binom{t}{t/2}$$

$$|\mathcal{V}'| = (2^n - 1)^t \left[\frac{t}{2} - \sum_{i=0}^{t/2-2} \binom{t}{i}(t/2 - i - 1)\pi^i(1-\pi)^{t-i} + \sum_{i=0}^{t/2-2} \binom{t}{i}(t/2 - i - 1)\pi^{t-i}(1-\pi)^i\right]$$

where $\pi = 1/(2^n - 1)$ and t is even. The difference in the code rate between $\mathcal{U}$ and $\mathcal{U}'$ vanishes when t is not very small. However, our change makes it impossible to apply Lemma 5 one-to-one (the statement: "(6) is equivalent to ...," fails to be true), and we can improve the result for $|\mathcal{V}'|$. For example, consider the case $t = 4$ and set (in the notations of [6])

$$n = s = 2 \quad D^{(0)} = \{00\} \quad D^{(1)} = \{11\} \quad E = \{01, 10\}$$
$$\boldsymbol{y} = (00, 00, 01, 01) \quad \boldsymbol{d} = (00, 00) \quad \boldsymbol{d}' = (11, 11).$$

Then (see [6, p. 5]),

$$w^*(\boldsymbol{d}) = w^*(\boldsymbol{d}') = \gamma(\boldsymbol{d}, \boldsymbol{d}') = 0$$

and the vectors $(00, 00, 01, 01)$, $(11, 11, 01, 01)$ cannot simultaneously belong to $\mathcal{V}'$. Nevertheless, this is possible for the code $\mathcal{V}$.

IV. DECODING ALGORITHM

The codes derived in (u)–(v) can be used with a simple decoding procedure. Let $z = (z_1, \cdots, z_t) \in \{0,1,2\}^{tn}$ denote the received vector, where $z_j \in \{0,1,2\}^n$ for all $j = 1, \cdots, t$. We will write $0 \in z_j$ and $2 \in z_j$ if the received subblock z_j has 0 and 2 as one of components, respectively.

Since $u_j \in \{0^n, 1^n\}$ for all $j = 1, \cdots, t$, each received subblock cannot contain both 0 and 2 symbols. Thus the decoder knows u_j if z_j contains either 0 or 2. The number of subbocks 1^n in u corresponding to the received subblocks 1^n can be found using the fact that the total Hamming weight of u is fixed to be $tn/2$. These remaining subblocks can be discovered based on the structure of the sets $\mathcal{A}^{(0)}, \cdots, \mathcal{A}^{(t)}$. A formal description of the decoding algorithm is given below.

1) Set

$$J_1 = \{j \in [t]: z_j = 1^n\}, \qquad J_1^c = [t] \backslash J_1.$$

2) For all $j \in J_1^c$, set

$$u_j = \begin{cases} 0^n, & \text{if } 0 \in z_j \\ 1^n, & \text{if } 2 \in z_j, \end{cases}$$

and

$$w' = |\{j \in J_1^c: 2 \in z_j\}|.$$

3) Set

$$w = t/2 - w'$$

and represent the elements of J_1 in the increasing order, i.e.,

$$|J_1| = k, j_1, \cdots, j_k \in J_1 \Longrightarrow j_1 < \cdots < j_k.$$

Set

$$u_j = \begin{cases} 0^n, & \text{if } j \in \{j_1, \cdots, j_{k-w}\} \\ 1^n, & \text{if } j \in \{j_{k-w+1}, \cdots, j_k\}. \end{cases}$$

4) Set

$$v = (z_1, \cdots, z_t) - (u_1, \cdots, u_t).$$

Example 2: Let $t = n = 2$ (see Example 1). If the first received subblock contains 0 then the codeword $u^{(1)}$ was sent by the first sender, and if it contains 2 then this codeword was $u^{(2)}$. Similarly, if the second received subblock contains 0 or 2 then the decoder makes a decision $u^{(2)}$ or $u^{(1)}$. The codeword $v \in \mathcal{V}$ is discovered in these cases after the decoder subtracts u from the received vector. At last, if the received vector consists of all 1's then there are two possibilities: $(u, v) = (u^{(1)}, 1100)$ and $(u, v) = (u^{(2)}, 0011)$. However, $0011 \notin \mathcal{V}$, and the decoder selects the first possibility.

V. Enumerative Coding

Enumerative procedures were developed in source coding to make the storage of a code book unnecessary at both sides of the communication link and essentially reduce computational efforts [7]–[9]. In this case, the encoder having received a message calculates the corresponding codeword, and the decoder calculates the inverse function. Our decoder does not use the code book to decode transmitted codewords, and an enumerative algorithm for messages completely escapes the storage of code books. We present this algorithm below.

First, we construct one-to-one mappings

$$\begin{aligned} f(m) &\to \mathcal{U} \\ f_1^{(s)}(m_J) &\to \mathcal{J}_s \\ f_2^{(s)}(m_a) &\to \mathcal{A}^{(s)} \\ f_3^{(s)}(m_b) &\to \mathcal{B}^{t-s} \end{aligned}$$

where m, m_J, m_a, and m_b are integers taking values in the corresponding sets: $m \in \{1, \cdots, |\mathcal{U}|\}$, $m_J \in \{1, \cdots, |\mathcal{J}_s|\}$, $m_a \in \{1, \cdots, |\mathcal{A}^{(s)}|\}$, $m_b \in \{1, \cdots, |\mathcal{B}^{t-s}|\}$, and $s = 0, \cdots, t$. The structure of the possible mappings $f_2^{(s)}(m_a)$ and $f_3^{(s)}(m_b)$ is evident; the mappings $f(m)$ and $f_1^{(s)}(m_J)$ are based on the enumeration procedures for binary vectors having a fixed Hamming weight [7]–[9].

Let (m, m') be the message to be transmitted over the binary adder channel, where $m \in \{1, \cdots, |\mathcal{U}|\}$ and $m' \in \{1, \cdots, |\mathcal{V}|\}$. Encoding and decoding of the message m are obvious: we assign

$$f(m) = u \qquad f^{-1}(u) = m.$$

Let us consider encoding and decoding of the message m'. Denote

$$K_0 = 0$$

$$K_{s+1} = K_s + \binom{t}{s}(s+1)\,(2^n - 2)^{t-s}, \qquad s = 0, \cdots, t-1$$

and

$$M_a^{(s)} = s + 1 \qquad M_b^{(s)} = (2^n - 2)^{t-s}$$

for all $s = 0, \cdots, t$. Furthermore, for all integers $q \geq 0$ and $Q \geq 1$, introduce the function

$$\Delta(q, Q) = q - Q\lfloor q/Q \rfloor.$$

The enumerative encoding procedure is given below.

1) Find the maximal value of $s \in \{0, \cdots, t-1\}$ such that $m' > K_s$, denote $m_s = m' - K_s - 1$, and set

$$\begin{aligned} m_J &= \lfloor m_s/(M_a^{(s)} M_b^{(s)}) \rfloor + 1 \\ m_a &= \lfloor \Delta(m_s, M_a^{(s)} M_b^{(s)})/M_b^{(s)} \rfloor + 1 \\ m_b &= \Delta(\Delta(m_s, M_a^{(s)} M_b^{(s)}), M_b^{(s)}) + 1. \end{aligned}$$

2) Set

$$J = f_1^{(s)}(m_J) \qquad a = f_2^{(s)}(m_a) \qquad b = f_3^{(s)}(m_b).$$

3) Construct the vector $v(a, b|J)$ in accordance with (4) and (5).

The enumerative decoding procedure goes in the opposite direction.

1) Find J, a, and b from v. Denote $s = |J|$.
2) Set

$$m_J = (f_1^{(s)})^{-1}(J) \quad m_a = (f_2^{(s)})^{-1}(a) \quad m_b = (f_3^{(s)})^{-1}(b).$$

3) Set

$$\begin{aligned} m' = K_s &+ (m_J - 1) M_a^{(s)} M_b^{(s)} + (m_a - 1) M_b^{(s)} \\ &+ (m_b - 1) + 1. \end{aligned} \tag{14}$$

Example 3: Let $t = n = 2$ (see Example 1). Then

$$\begin{aligned} K_0 &= 0 \\ K_1 &= 0 + \binom{2}{0}(0+1)2^{2-0} = 4 \\ K_2 &= 4 + \binom{2}{1}(1+1)2^{2-1} = 12. \end{aligned}$$

Let $m' = 11$. Then $s = 1$ since $11 > K_1$ and $11 \leq K_2$. Therefore,

$$\begin{aligned} m_1 &= 11 - 4 - 1 = 6 \\ m_J &= \lfloor 6/(2 \cdot 2) \rfloor + 1 = 2 \\ m_a &= \lfloor \Delta(6, 4)/2 \rfloor + 1 = 2 \\ m_b &= \Delta(\Delta(6, 4), 2) + 1 = 1 \end{aligned}$$

since $M_a^{(s)} = M_b^{(s)} = 2$ and

$$\begin{aligned} \Delta(6, 4) &= 6 - 4\lfloor 6/4 \rfloor = 2 \\ \Delta(2, 2) &= 2 - 2\lfloor 2/2 \rfloor = 0. \end{aligned}$$

Suppose that

$$\begin{aligned} f_1^{(1)}&: \ (1,2) \to (\{1\}, \{2\}) \\ f_2^{(1)}&: \ (1,2) \to ((00), (11)) \\ f_3^{(1)}&: \ (1,2) \to ((01), (10)). \end{aligned} \tag{15}$$

Then we assign

$$\begin{aligned} J &= f_1^{(1)}(2) = \{2\} \\ a &= f_2^{(1)}(2) = (11) \\ b &= f_3^{(1)}(1) = (01) \end{aligned}$$

and construct the codeword using (4)and (5)

$$v(a, b|J) = (01, 11).$$

Let us consider decoding of the message m' when $v = (11, 10)$. We discover that

$$J = \{1\} \qquad a = (11) \qquad b = (10).$$

Hence, $s = |J| = 1$ and

$$m_J = (f_1^{(1)})^{-1}(\{1\}) = 1$$
$$m_a = (f_2^{(1)})^{-1}((11)) = 2$$
$$m_b = (f_3^{(1)})^{-1}((10)) = 2$$
$$m' = 4 + (1-1)\cdot 2 \cdot 2 + (2-1)\cdot 2 + (2-1) + 1 = 8$$

where (14) and (15) were used.

REFERENCES

[1] R. Ahlswede, "Multi-way communication channels," in *2nd Int. Symp. Information Theory* (Tsahkadzor, Armenian SSR, 1971). Budapest, Hungary: Publishing House of the Hungarian Academy of Sciences, 1973, pp. 23–52.

[2] ____, "The capacity region of a channel with two senders and two receivers," *Ann. Probab*., vol. 2, no. 5, pp. 805–814, 1974.

[3] T. Kasami, S. Lin, V. K. Wei, and S. Yamamura, "Graph theoretic approaches to the code construction for the two-user multiple-access binary adder channel," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 114–130, Jan. 1983.

[4] E. J. Weldon, "Coding for a multiple-access channel," *Inform. Contr.*, vol. 36, pp. 256–274, Mar. 1978.

[5] G. G. Khachatrian, "On the construction of codes for noiseless synchronized 2-user channel," *Probl. Contr. Inform. Theory*, vol. 11, no. 4, pp. 319–324, 1982.

[6] P. A. B. M. Coebergh van den Braak and H. C. A. van Tilborg, "A family of good uniquely decodable code pairs for the two-access binary adder channel," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 3–9, Jan. 1985.

[7] V. F. Babkin, "A universal encoding method with nonexponential work expediture for a source of independent messages," *Probl. Pered. Inform.*, vol. 7, no. 4, pp. 13–21, Oct.–Dec. 1971. English translation: *Probl. Inform. Transm.*, pp. 288–294.

[8] J. P. M. Schalkwijk, "An algorithm for source coding," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 395–399, May 1972.

[9] T. M. Cover, "Enumerative source coding," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 73–77, Jan. 1973.

Hierarchical Guessing with a Fidelity Criterion

Neri Merhav, *Senior Member, IEEE*, Ron M. Roth, *Senior Member, IEEE*, and Erdal Arikan, *Senior Member, IEEE*

***Abstract*— In an earlier paper, we studied the problem of guessing a random vector $\boldsymbol{X}$ within distortion D, and characterized the best attainable exponent $E(D, \rho)$ of the ρth moment of the number of required guesses $G(\boldsymbol{X})$ until the guessing error falls below D. In this correspondence, we extend these results to a multistage, hierarchical guessing model, which allows for a faster search for a codeword vector at the encoder of a rate-distortion codebook. In the two-stage case of this model, if the target distortion level is D_2, the guesser first makes guesses with respect to (a higher) distortion level D_1, and then, upon his/her first success, directs the subsequent guesses to distortion D_2. As in the above-mentioned earlier paper, we provide a single-letter characterization of the best attainable guessing exponent, which relies heavily on well-known results on the successive refinement problem. We also relate this guessing exponent function to the source-coding error exponent function of the two-step coding process.**

***Index Terms*— Guessing, rate-distortion theory, source-coding error exponent, successive refinement.**

I. INTRODUCTION

In [1], we studied the basic problem of guessing a random vector with respect to (w.r.t.) a fidelity criterion. In particular, for a given information source, a distortion measure d, and distortion level D, this problem is defined as follows. The source generates a sample vector $\boldsymbol{x} = (x_1, \cdots, x_N)$ of a random N-vector $\boldsymbol{X} = (X_1, \cdots, X_N)$. Then, the guesser, who does not have access to $\boldsymbol{x}$, provides a sequence of N-vectors (guesses) $\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots$ until the first success of guessing $\boldsymbol{x}$ within per-letter distortion D, namely, $d(\boldsymbol{x}, \boldsymbol{y}_i) \le ND$ for some positive integer i. Clearly, for a given list of guesses, this number of guesses i is solely a function of $\boldsymbol{x}$, denoted by $G_N(\boldsymbol{x})$. The objective of [1] was to characterize the best achievable asymptotic performance and to devise good guessing strategies in the sense of minimizing moments of $G_N(\boldsymbol{X})$. It has been shown in [1], that for a finite-alphabet, memoryless source P and an additive distortion measure d, the smallest attainable asymptotic exponential growth rate of $\boldsymbol{E}\{G_N(\boldsymbol{X})^\rho\}$ $(\rho > 0)$ with N, is given by

$$E(D, \rho) = \max_{P'}[\rho R(D, P') - \mathcal{D}(P'||P)] \tag{1}$$

where the maximum w.r.t. P' is over the set of all memoryless sources with the same alphabet as P, $R(D, P')$ is the rate-distortion function of P' w.r.t. distortion measure d at level D, and $\mathcal{D}(P'||P)$ is the relative entropy, or the Kullback–Leibler information divergence, between P' and P, i.e., the expectation of $\ln [P'(X)/P(X)]$ w.r.t. P'.

Manuscript received December 1, 1996. The work of N. Merhav was supported in part by the Israel Science Foundation founded by the Israel Academy of Sciences and Humanities.

N. Merhav was with Hewlett-Packard Laboratories, Palo Alto, CA 94304 USA. He is now with the Department of Electrical Engineering, Technion–Israel Institute of Technology, Haifa 32000, Israel (e-mail: merhav@ee.technion.ac.il).

R. M. Roth was with Hewlett-Packard Laboratories, Palo Alto, CA 94304 USA. He is now with the Department of Computer Science, Technion–Israel Institute of Technology, Haifa 32000, Israel (e-mail: ronny@cs.technion.ac.il).

E. Arikan is with the Electrical-Electronics Engineering Department, Bilkent University, 06533 Ankara, Turkey (e-mail: arikan@ee.bilkent.edu.tr).

Communicated by R. Laroia, Associate Editor for Source Coding.

Publisher Item Identifier S 0018-9448(99)00067-X.