On the General Defective Channel with Informed Encoder and Capacities of Some Constrained Memories

Alexander V. Kuznetsov and A. J. Han Vinck

Abstract—**From an information-theoretical point of view the write once memory (WOM), the unidirectional memory (WUM), the write isolated memory (WIM), the memory with address faults (MAF), Blackwell's broadcast channel, and some other constrained memories and channels with an informed encoder can be considered as particular cases of the general defective channel (GDC) introduced by Kuznetsov as a generalization of a memory with defects. Using the concept of the GDC we consider a unified approach to the investigation of different types of natural and artificial channels with a finite number of states known to the encoder, but unknown to the decoder. To illustrate the usefulness of this approach we derive the capacities of the above-mentioned constrained memories (WOM, WUM, WIM, MAF) as corollaries of lower and upper bounds for the number of messages transmitted over the GDC.**

Index Terms—**Memory with defects, constrained memory, capacity.**

I. Introduction

THE concepts of a defect, a channel with defects, and a channel with defects and errors were introduced in the information theory literature about 20 years ago in connection with encoding of information to be stored in a memory where some binary cells are defective [2], [3]. A binary memory cell is called defective if it has only one stable state, either 0 (a defect of type 0) or 1 (a defect of type 1), i.e., it always contains the same symbol regardless of what is written into it. In this case the process of writing, storing, and reading information can be described in information-theoretic terms as information transmission over a channel with defects and, possibly, random errors. New problems arise in situations where locations and types of defective memory cells are known during encoding (updating) of information and are unknown upon decoding (reading). A particular problem is the estimation of the maximum transmission rate $R(n, m, t)$ for the channel with defects and random errors whose multiplicities do not exceed specified numbers m and t in words of length n, respectively. Upper and lower bounds for $R(n, m, t)$ for some interesting classes of defect and error correcting codes were obtained in [2]–[5].

In addition to defects of the type described above there are also so-called conditional defects. A primitive example of the conditional defect is a binary cell that has three states: a defect of the type 0, a defect of the type 1, and a perfect state. The state of such a cell is determined by information contained in certain other cells, e.g., adjacent ones. When several conditionally defective cells are present in the word, they may influence each other. As we can readily see, the behavior of an individual conditionally defective cell, in particular, the relationship between information written into and read from it, can be defined in 3^{2^a} ways, where a is the number of "neighbors" that affect the behavior of the cell. For $a = 2$, this number is already equal to 81. Given this diversity of different types of conditionally defective cells and the complexity of describing their interaction, there was no other way then to find a general approach to the solution of similar problems that arise for different types of conditional defects. Such an approach to the investigation of different types of, in some sense, defective memories with an informed encoder was found in [1]. It is based on the concept of the general defective channel. The range of applications of the methods and results given in [1] was found to be much wider than only the study of memories with conditional defects. In fact, the notion of the GDC gives a straightforward method for the calculation of capacities of WOM's, WUM's, WIM's, MAF's, and other memories with an informed encoder, in which updating and reading cycles must satisfy some specific conditions. The models of WOM, WUM, WIM, MAF were introduced by different groups of researchers. They all use the same technique to prove the existence of "good" codes for different but, as we will see later, very similar objects (they all are particular cases of the GDC). The list of different models of constrained memories and channels with an informed encoder is growing. This is the main motivation for our return to the notion of the GDC, and for writing this paper, which can be considered as a survey of some results published in the area of special memory models in the last 10 years.

An important generalization of the GDC is considered in [1], where the output of the channel (input to the decoder) is supposed to be corrupted by some additive

Manuscript received October 5, 1993; revised September 13, 1994.

A. V. Kuznetsov is with the Institute for Problems of Information Transmission, Moscow, Russia.

A. J. H. Vinck is with the Institute for Experimental Mathematics, University of Essen, Essen, Germany.

IEEE Log Number 9406323.

Fig. 1. Block scheme of the general defective channel.

errors whose positions and values are not known neither to the encoder nor to the decoder. Therefore, these errors can be considered as random errors, and the generalized system is called a GDC with random errors. It can also be used for the analysis of different types of noisy memories with defects, or constraints on the read/write cycle, see [18].

II. A General Defective Channel with an Informed Encoder

Let S, X, and Y be some finite sets of elements, which we call the set of states, the input alphabet and the output alphabet of the channel, respectively. We suppose that for any element (state) $s \in S$ there is a deterministic function φ_s defined on some subset $X_s \subset X$, such that $\varphi_s(x) \in Y$ for any $x \in X_s$. In other words, the channel transforms an input symbol x to an output symbol y according to its state s. In fact, it is a set of deterministic mappings $\Phi = \{\varphi_s, s \in S\}$. Let

$$Y_s = \{y = \varphi_s(x) | x \in X_s, s \in S\}. \tag{1}$$

This is the set of symbols (elements) that are available at the output of the channel in state s (a symbol $y \in Y$ is available at the output of the channel in state s, if there is an input symbol $x \in X$ that gives this symbol y at the output of the channel, i.e., $\varphi_s(x) = y$).

Consider the model of communication for the storage system shown in Fig. 1. It consists of a channel Φ as described above, an encoder, and a decoder, which are used for the transmission of some number M of messages u from a source to a recipient. Without any loss of generality, we may use integers from the set $U = \{1, 2, \cdots, M\}$ as M possible values of the message u. In the sequel we always assume that the encoder knows the state s of the channel, and hence the set Y_s of available output sequences, but the decoder does not have this side information. This means that an encoding f and a decoding g are functions such that

$$f(u, s): \{1, 2, \cdots, M\} \times S \to X \tag{2}$$

$$g(y): Y \to \{1, 2, \cdots, M\}. \tag{3}$$

The encoder generates a code symbol $x = f(u, s) \in X$ for the message $u \in U = \{1, 2, \cdots, M\}$ and the state of the channel $s \in S$. The channel converts this code symbol to the output symbol $y = \varphi_s[f(u, s)] \in Y_s$. On the basis of this output symbol the decoder makes a decision regarding the original message: output is the symbol $\hat{u} = g(y) \in \{1, 2, \cdots, M\}$. The system of relations above, which establishes the relationship between the message u at the encoder input and the estimate $\hat{u}$ of this message at the decoder output, is called a general defective channel with an informed encoder. For simplicity we call it the GDC. We say that M messages can be transmitted over the GDC if there exist an encoding function $f(u, s)$, $u \in U$, $s \in S$, and a decoding function $g(y)$, $y \in Y$, such that

$$\hat{u} = g(\varphi_s[f(u, s)]) = u \tag{4}$$

for any $u \in U$ and $s \in S$.

An important parameter of the described system is the maximum number M_ϕ of messages that can be transmitted over the GDC. The maximum transmission rate, defined by the expression $R_\phi = n^{-1} \log_2 M_\phi$, can be used to characterize the GDC whose output symbols are sequences of length n with components from some other smaller alphabet. It would be naive to expect that exact values of M_ϕ or R_ϕ can be found for an arbitrary GDC.

Lower and upper bounds for M_ϕ and R_ϕ are given below, and in all particular cases considered below they give exact asymptotic values of R_Φ as $N \to \infty$. Let

$$N_\Phi = \min_{s \in S} |Y_s| \tag{5}$$

where $|Y_s|$ is the cardinality of the set Y_s, i.e., the number of symbols available at the output of the channel in state s. Let N'_Φ be the maximum integer such that

$$N'_\Phi \ln (N'_\Phi |S|) \le N_\Phi. \tag{6}$$

Theorem 1: For any arbitrary GDC

$$M_\Phi \le N_\Phi \tag{7}$$

where N_Φ is defined by (5).

Proof: Let s be the state from S for which the number of available output symbols $|Y_s|$ is minimal. It is obvious that for any encoding $f(u, s)$, which enables the transmission of M messages, all output symbols $\varphi_s[f(1, s)], \varphi_s[f(2, s)], \cdots, \varphi_s[f(M, s)]$ must be distinct. Since they are elements of Y_s, we have $M \le |Y_s| = N_\Phi$. This gives the upper bound (7).

Theorem 2: For an arbitrary GDC with an informed encoder

$$N'_\Phi \le M_\Phi \tag{8}$$

where N'_Φ, is defined by (6).

The proof of Theorem 2 is given in Appendix A. Note that $N_\Phi / \ln (N_\Phi |S|) \le N'_\Phi$. From this inequality and Theorem 2 we have the following lower bound.

Corollary to Theorem 2: For an arbitrary GDC

$$N_\Phi / \ln (N_\Phi |S|) \le M_\Phi. \tag{9}$$

This corollary can be used to get the capacities of different constrained memories. First let us consider the principle of additive coding that can be used in GDC's with output alphabets that consist of sequences of some fixed length n [1].

III. Additive Coding for the GDC

Let q be some given positive integer and $E = \{0, 1, 2, \cdots, q-1\}$. An additive code $B = \{B_1, B_2, \cdots, B_M\}$ for the

transmission of $M = q^k$ messages through the GDC with output alphabet E^n is defined by

1) a set C of $L \le q^{n-k}$ words $c = (c_1, c_2) \in E^n$ with distinct prefixes c_1 of length $l = n - k$;

2) a set $\underline{U}$ of M "shifts" $\underline{u} = (\underline{0}, \underline{u}') \in E^n$, where $\underline{0}$ is the zero prefix of length l (l zeros), and $\underline{u}'$ is a q-ary representation of the message $u = 1, 2, \cdots, q^k$.

The additive code B has the following structure:

$$B_u = \{c \oplus \underline{u} | c \in C, \underline{u} \in \underline{U}\}. \tag{10}$$

Using (10), it is not difficult to see that

$$B_i \cap B_j = \phi, \qquad 1 \le i \ne j \le M. \tag{11}$$

Lemma 1: For an arbitrary GDC with output alphabet E^n and any integer k such that

$$q^k \ln (q^k |S|) \le N_\Phi = \min_{s \in S} |Y_s| \tag{12}$$

there exists a set C with $L = q^{n-k}$ words such that for any $u \in U$ and $s \in S$

$$B_u \cap Y_s \ne \phi. \tag{13}$$

The proof of Lemma 1 is given in Appendix B.

For an additive code B with a masking set C from Lemma 1 it is possible to define an encoding function $f(u,s)$ and a decoding function $g(y)$ in such a way that $M = q^k$ messages can be transmitted through the GDC. For example, it can be done in the following way.

Encoding Procedure: According to Lemma 1, $B_u \cap Y_s \ne \phi$ for any $\underline{u} \in \underline{U}$ and $s \in S$. Therefore, for any message u and any state s we can find the word $y(u, s) \in B_u \cap Y_s$. Let $f(u, s)$ be any element $x \in X_s$ such that $\varphi_s(x) = y(u, s)$. Since $y(u, s) \in Y_s$ an encoding function $f(u, s)$ can thus be defined in this way for any $\underline{u} \in \underline{U}$ and $s \in S$.

Decoding Procedure: For each pair $\underline{u} \in \underline{U}$ and $y \in \bigcup B_u$ let $g(y) = \underline{u}$ (for $y \notin \bigcup_{\underline{u} \in \underline{U}} B_u$ a decoding function $g(y)$ is not defined). Since an additive code B has property (11), this definition of $g(y)$ is correct. As a result, we have the following theorem.

Theorem 3: For an arbitrary GDC with $|S|$ states and a minimum number of available output words N_Φ there exists an additive code by which $M = q^k$ messages, where k is an arbitrary integer satisfying (12), can be transmitted through the GDC.

Corollary to Theorem 3: For an arbitrary GDC with $|S|$ states and a minimum number of available output words N_Φ there exists an additive code by which $M = q^k$ messages, where

$$N_\Phi / \ln (N_\Phi |S|) \le q^k = M_\Phi. \tag{14}$$

can be transmitted through the GDC.

IV. Capacity of a Write Once Memory

Rivest and Shamir considered updating punchcards, punchtapes, and other storage media which degrade from one updating to another one [7]–[11]. In this section we show how to get the capacity of the punchcard and other similar degrading memories by additive coding using the notion of the GDC, Theorems 1–3 given in the previous two sections and an approach described in [12].

In order to be able to use a punchcard at least twice we must restrict the number of holes punched at the first use of a new punchcard by some number a, $0 < a < n$. Under this restriction there are

$$M_1 = \sum_{i=0}^{a} \binom{n}{i} \tag{15}$$

different ways to punch a new card. Therefore M_1 messages can be represented in this way, and during the first use of the punchcard we store $k_1 = \log_2 M_1$ bits. The configuration of holes on the punchcard can be represented by the binary vector $s = (s_1, s_2, \cdots, s_n)$, where $s_i = 1$ if the ith position of the card is punched (a hole), and $s_i = 0$ otherwise ($1 \le i \le n$). At the second use of the punchcard the existing configuration of holes (for example, represented by the vector s) can be considered as the state of the GDC with an input alphabet X, an output alphabet Y, a state set S, and a set Y_s of output vectors available at state s, i.e.,

$$\begin{aligned} X = Y = E^n, \quad E = \{0, 1\} \\ S = \{s \in E^n | w(s) \le a\} \\ X_s = Y_s = \{y \in E^n | y \ge s\} \\ \varphi_s(x) = x \qquad \text{for } x \in X_s,\ s \in S \end{aligned} \tag{16}$$

where $w(s)$ is the Hamming weight of the vector s, and $y = (y_1, y_2, \cdots, y_n) \ge (s_1, s_2, \cdots, s_n) = s$, if and only if $y_i \ge s_i$ for all $1 \le i \le n$ (y_i and s_i are compared as ordinary integers). For a given GDC we must first find or estimate the number N_Φ of sequences available at the output of the channel in the worst state (when N_Φ is minimal). In our case this is a simple problem:

$$N_\Phi = \min_{s \in S} |Y_s| = 2^{n-a} \tag{17}$$

for $w(s) = a$. From (16) and (17) using Theorem 1 and the Corollary to Theorem 3 we have the following lower and upper bounds for the number M_2 of messages that can be transmitted through the GDC by additive coding (stored on the punchcard at its second use):

$$2^{n-a} \ge M_2 \ge 2^{n-a} / (n + k_1 - a) \ln 2. \tag{18}$$

Let $k = k_1 + k_2$, where $k_2 = \log M_2$, be the total amount of bits stored on the punchcard when it is used twice. For $n \to \infty$ and $a = pn$, $0 \le p = \text{const} \le 1/2$, using (15), (18), and standard estimates for binomial coefficients, we have

$$R = k/n \ge H(p) + 1 - p + o_1(n) \tag{19}$$

where $H(p) = -p \log_2 p - (1 - p) \log_2 (1 - p)$, and $o_1(n) \to 0$ when $n \to \infty$. The right-hand side of (19) has a maximum for $p = 1/3$. This gives the following lower bound:

$$R \ge 1.58496 + o_1(n). \tag{20}$$

In fact, this lower bound is the capacity of the punchcard used twice. We should note that additive coding can be

used at the second updating of the punchcard. In this case it is not difficult to check that the Corollary to Theorem 3 also gives the capacity of the punchcard.

When the punchcard is used T, $T \geq 2$, times, the number of holes punched on the card at its ith use must be restricted by some integer a_i, such that $a_1 \leq a_2 \leq \cdots \leq a_{T-1}$. Therefore, at the ith use the punchcard can be considered as a GDC with

$$N_\Phi \geq \binom{n - a_{i-1}}{a_i - a_{i-1}}, \qquad 1 \leq i \leq T-1, \quad \text{and}$$

$$N_\Phi \geq 2^{n - a_{T-1}}, \qquad \text{for } i = T.$$

Using these inequalities and Theorem 2, we can get lower bounds for the number of messages stored on the punchcard at each time moment $i = 1, 2, \cdots, T$. After optimization with respect to the parameters $a_1, a_2, \cdots, a_T$ these bounds give the capacity region of the punchcard used T times. Finally, we should note that in the same way we can get lower bounds (in fact, the capacity region) for WOM's with memory cells described by an arbitrary state transition graph.

V. Capacity of the Write Unidirectional Memory

In this section we derive the capacity of WUM's using the concept of the GDC and Theorems 1–3. We consider only WUM's with binary memory cells that are error free and absolutely reliable. The WUM with random errors at the input of the decoder were considered in [18].

Let E^n be the set of all binary sequences of length n with components 0 and 1, and $s_i \in E^n$, $i = 1, 2, \cdots$, be the state of n binary memory cells at time $i = 0, 1, 2, \cdots$. The updating at the moment $i = 1, 2, \cdots$ can be described by one of the following two operations:

$$s_i = s_{i-1} \,\&\, x_i, \qquad \text{for AND cycles} \tag{21}$$

$$s_i = s_{i-1} \vee x_i, \qquad \text{for OR cycles} \tag{22}$$

where & and V are componentwise logical multiplication (AND) and logical addition (OR) in E^n, respectively, and $x_i \in E^n$ is the output of the encoder at the time i; x_i is the value of the encoding function $f_i(s_{i-1}, u_i)$ of the previous state s_{i-1} and ith message $u_i = 1, 2, \cdots, M$. The decoding can be described as follows:

$$g_i(s_i): E^n \to \{1, 2, \cdots, M\}. \tag{23}$$

Let $\hat{u}_i = g_i(s_i)$ be an estimate of the message u_i, $i = 1, 2, \cdots$. The rate $R = (\log_2 M)/n$ is achievable for the WUM, if for all $i = 1, 2, \cdots$, and $u_i = 1, 2, \cdots, M$,

$$\hat{u}_i = g_i(s_i) = u_i. \tag{24}$$

The maximum achievable rate is called the capacity of the WUM. To get a lower bound for the capacity, we use AND cycles for the updating of the memory at even time moments $i = 2, 4, \cdots$, and OR cycles at odd time moments $i = 1, 3, \cdots$. In fact, we will also do the encoding under the following restriction:

$$s_i \in \begin{cases} S_0, & \text{if } i \text{ even} \\ S_1, & \text{if } i \text{ odd} \end{cases} \tag{25}$$

where $S_0 = \{s | s \in E^n, w(s) = a\}$, $S_1 = \{s | s \in E^n, w(s) = n - a\}$, $w(s)$ is Hamming weight of the word s, and $0 \leq a \leq n/2$ is an integer, which will be chosen later to maximize the achievable rate. Under these conditions at each updating the WUM can be considered as a GDC with an input X, an output Y, a state set S, and a set Y_s of output vectors available in state s, given below:

$$X = Y = E^n$$

$$S = \begin{cases} S_0, & \text{if } i \text{ odd} \\ S_1, & \text{if } i \text{ even} \end{cases}$$

$$X_s = Y_s = \begin{cases} \{y \in E^n | y \geq s, y \in S_1\}, & \text{for odd } i \\ \{y \in E^n | y \leq s, y \in S_0\}, & \text{for even } i \end{cases}$$

$$\varphi_s(x) = x, \qquad \text{for } x \in X_s, s \in S. \tag{26}$$

For a given GDC we must first find or estimate the number N_Φ of sequences available at the output of the channel in the worst state (when N_Φ is minimal). In our case

$$N_\Phi = \min_{s \in S} |Y_s| = \binom{n - a}{a}. \tag{27}$$

From (25)–(27), Theorem 1 and the Corollary to Theorem 2 we have the following lower and upper bounds for the number M of messages that can be transmitted through the GDC:

$$\binom{n - a}{a} \geq M_2 \geq \binom{n - a}{a} \Big/ \ln\left[\binom{n}{a}\binom{n - a}{a}\right]. \tag{28}$$

For $n \to \infty$ and $a = pn$, $0 \leq p = \text{const} \leq 1/2$, using (28) and standard estimates for binomial coefficients, we have

$$R = \log_2 M/n \geq (1 - p) H[p/(1 - p)] + o_2(n) \tag{29}$$

where $o_2(n) \to 0$ when $n \to \infty$. The right-hand side of (29) is maximized for $p = (\sqrt{5} - 1)/2\sqrt{5}$. This gives the following lower bound:

$$R \geq \log_2 ((1 + \sqrt{5})/2) + o_2(n). \tag{30}$$

In fact, this lower bound is the capacity of the WUM. It is not difficult to see from Theorem 3 (or its corollary) that additive coding also gives the capacity. In the same way we can get lower bounds (on the capacity region) for WUM's with q-ary memory cells as well.

VI. Capacity of the Write Isolated Memory

Let E^n be the set of all binary sequences of length n with components 0 and 1, and $s_i \in E^n$, $i = 1, 2, \cdots$, be the state of n binary memory cells at time $i = 0, 1, 2, \cdots$. The updating at the moment i can be described by the operation

$$s_i = s_{i-1} \oplus x_i \tag{31}$$

where $\oplus$ is componentwise modulo 2 addition in E^n, and $x_i \in E^n$ is a vector of transitions at the time i; x_i is the value of an encoding function $f(s_{i-1}, u_i)$ of the previous state s_{i-1}, and the ith message $u_i = 1, 2, \cdots, M$. A write isolated memory (WIM) is an ordered set of n binary memory cells with updatings satisfying the following constraint: no change of states in two consecutive cells is allowed, or in other words, any two consecutive 1's in the transition vectors x_i are separated by at least one zero [19]. Here we will consider the more general so called (d, k)-constraint, usually used in magnetic and optical recording: any two consecutive 1's in the transition vector x_i are separated by at least d but not more than k zeros (d and k are some given positive integers, $d \le k$).

The decoding can be formulated as

$$g_i(s_i): E^n \to \{1, 2, \cdots, M\} \tag{32}$$

and $\hat{u}_i = g_i(s_i)$ is an estimate of the message u_i, $i = 1, 2, \cdots$. The rate $R = (\log M)/n$ is achievable in the WIM, if for all $i = 1, 2, \cdots$, and $u_i = 1, 2, \cdots, M$

$$\hat{u}_i = g_i(s_i) = u_i. \tag{33}$$

The maximum achievable rate is called the capacity of the WIM, and can be found as follows. At the ith updating of the WIM, its previous state s_{i-1} can be considered as the state of the GDC with an input alphabet X, an output alphabet Y, a state set S, and a set Y_s of output vectors available at state s given below:

$$\begin{aligned} X = Y = S = E^n \\ Y_s = \{s \oplus x | x \in E^n(d, k)\} \\ \varphi_s(x) = s \oplus x, \qquad \text{for } x \in E^n(d, k),\ s \in S \end{aligned} \tag{34}$$

where $E^n(d, k)$ is a subset of E^n consisting of sequences satisfying the following (d, k)-constraint: the number of zeros between any two consecutive ones is not less than d, and is not greater than k. For a given GDC we must first find or estimate the number N_Φ of sequences available at the output of the channel in the worst state. Here,

$$N_\Phi = \min_{s \in S} |Y_s| = |E^n(d, k)|. \tag{35}$$

From (33)–(35), Theorem 1 and the Corollary to Theorem 2 we have the following lower and upper bounds for the number M of messages that can be transmitted through the GDC (stored at each updating of the WIM):

$$|E^n(d, k)| \ge M \ge |E^n(d, k)|/\ln(2^n \cdot |E^n(d, k)|). \tag{36}$$

For $n \to \infty$

$$R = \frac{\log_2 M}{n} = C(d, k) + o_3(n) \tag{37}$$

where $C(d, k)$ is the capacity of the (d,k)-constrained channel considered by C. Shannon [20], and $o_3(n) \to 0$ when $n \to \infty$. In particular, $C(1, \infty) = \log_2(1 + \sqrt{5})/2$ for the particular WIM considered in [19]. Capacities $C(d, k)$ for different values of d and k are given in [21].

VII. The Memory with Address Defects

For some semiconductor memories, the most common type of memory defects is the coupling fault: reading and/or writing data in one location of memory affects the contents of another location [22]. In [1] such defects were called conditional defects. In this section we consider a model of memory with deterministic coupling faults described in [23] and it is called a memory with address faults (MAF).

Let $x = (x_1, x_2, \cdots, x_n) \in E^n$ and $\varphi(x) \in E^n$ be the words written into and read back from the memory. In [23] a MAF is defined as a set Φ of mappings $\varphi: E^n \to E^n$, of the following type

$$\varphi(x_1, x_2, \cdots, x_n) = (x_{i_1}, x_{i_2}, \cdots, x_{i_n}) \tag{38}$$

where $i_j \in \{1, 2, \cdots, n\}$ for all $j = 1, 2, \cdots, n$. For a given mapping φ of the type (38) let $k(\varphi)$ be the number of different indexes i_j in the right-hand side of (38). Note that there are n^n distinct mappings of this type, and therefore for all MAF

$$|\Phi| \le n^n. \tag{39}$$

Encoding and decoding for a MAF are defined exactly as for the GDC by (2) and (3), respectively. The definition of the maximum rate of the code $x = f(u, \varphi)$ correcting address faults from Φ is similar to the definition of the maximum transmission rate of a GDC with the set Φ of input–output mappings.

One special class of MAF (with t holes, t is an integer parameter, $0 \le t \le n$) was considered in [23]. For a MAF with t holes we have by definition $\min_{\varphi \in \Phi} k(\varphi) = n - t$, and therefore

$$N_\Phi = 2^{n-t}. \tag{40}$$

From (39), (40), Theorem 1 and the Corollary to Theorem 3 we have the following lower and upper bounds for the number M of messages that can be transmitted through a GDC by additive coding (stored in a MAF with t holes):

$$2^{n-t} \ge M \ge 2^{n-t}/(n \ln n + (n - t)\ln 2). \tag{41}$$

For $n \to \infty$ and $t = np$, $0 \le p = \text{const} \le 1$, we have

$$R = \frac{\log_2 M}{n} = 1 - p + o_4(n) \tag{42}$$

where $o_4(n) \to 0$ when $n \to \infty$.

Appendix I

Proof of Theorem 2: Without loss of generality, let $Y = \{1, \cdots, N\}$ where $N = |Y|$. In this case the sets Y_s, $s \in S$, are subsets of the set $\{1, 2, \cdots, N\}$. The proof of Theorem 2 is based on the following lemma, which first appeared in [1].

Lemma 2: For an arbitrary positive integer $M \le N'_\Phi$ there exists a binary matrix $A = \|a_{ij}\|$, $i = 1, 2, \cdots, M$, $j = 1, 2, \cdots, N$, such that for any $u \in U = \{1, 2, \cdots, M\}$ and any $s \in S$ it has a column with the number $j(u, s) \in Y_s$ and $a_{u, j(u,s)} = 1$, $a_{v, j(u,s)} = 0$ for $1 \le v \ne u \le M$.

We first complete the proof of Theorem 2. Using the matrix A from lemma 2 we can easily construct an encoding and a

decoding rule for the transmission of $M \le N'_\Phi$ messages over the GDC. At first, for each pair (u, s), $u \in \{1, 2, \cdots, M\}$, $s \in S$, we must find an input symbol $x \in X$, such that $\varphi_s(x) = j(u, s)$. Since $j(u, s) \in Y_s$, such an element x always exists. Let $f(u, s) = x$. The encoding is defined. After that, for each $j \in \{1, 2, \cdots, N\}$ we search the jth column of the matrix A for the nonzero element. If such an element is found, let $g(j)$ be the number of the row that contains this nonzero element. It is not difficult to check that for such encoding and decoding, based on matrix A, equality (4) is true for any $u \in \{1, 2, \cdots, M\}$ and $s \in S$. If $M = N'_\Phi$, we get the lower bound (8). Therefore, Theorem 2 has been proven if we can prove Lemma 2. □

Proof of Lemma 2: Let us consider an ensemble $\{A\}$ of random matrices A of size $M \times N$ with independent columns containing exactly one 1, with probability $1/M$ for each possibility. Let $P_{u,s}$ be the probability that there is no column in the matrix A with the number $j \in Y_s$, such that $a_{u,j} = 1$ and $a_{v,j} = 0$ for all v, $v \ne u$, $1 \le v \le M$. It is obvious that for any fixed $u \in U$ and $s \in S$

$$P_{u,s} = \left(1 - \frac{1}{M}\right)^{|Y_s|}. \tag{A1}$$

Since the probability of the union of events is not greater than the sum of probabilities of particular events, the probability P that the random matrix A does not satisfy the conditions of Lemma 2, can be upper bounded as follows:

$$P \le M|S| \max_{u \in U,\, s \in S} P_{u,s}. \tag{A2}$$

Since N_Φ is the minimum of $|Y_s|$ over $s \in S$, then from (A1) and (A2) we have

$$P \le M|S|\left(1 - \frac{1}{M}\right)^{N_\Phi}. \tag{A3}$$

Using (A3) and the inequality: $\ln x < x - 1$, $0 \le x \ne 1 < \infty$, it is not difficult to check that $P < 1$ for all $M < N'_\Phi$. This means that in the ensemble $\{A\}$ there exists a matrix A that has the property as indicated in Lemma 2. Therefore, Lemma 2 is proven. □

Appendix B

Proof of Lemma 1: Let us consider an additive code with a random masking set C consisting of $L = q^l$, $l = n - k$, words $c = (c', c'')$ concatenated from a nonrandom prefix c' of length l and a random subblock c'' of length k. Suppose that all kL components of subblocks c'' are independent random variables that take values $0, 1, 2, \cdots, q - 1$ with equal probability. Let us estimate the probability P that such a random set C does not satisfy condition (13). It is obvious that

$$P \le \sum_{s \in S,\, 1 \le u \le M} P_{s,u} \tag{B1}$$

where $P_{s,u} = \Pr\{Y_s \cap B_u = \phi\}$. Let $Y_{s,u} = \{y - \underline{u} | y \in Y_s\}$, where $-$ is the componentwise subtraction modulo q, $\underline{u} = (\underline{0}, \underline{u}') \in E^n$, $\underline{0}$ is the zero prefix of length l (l zeros), and $\underline{u}'$ is a q-ary representation of the message $u = 1, 2, \cdots, q^k$. The set $Y_{s,u}$ can be represented in the following way:

$$Y_{s,u} = \bigcup_{a \in E^l} Y_{s,u}(a)$$

where $Y_{s,u}(a)$ is a subset of $Y_{s,u}$ consisting of words that have the prefix $a \in E^l$. It is not difficult to check that

$$P_{s,u} = P\{C \cap Y_{s,u} = \phi\} = \prod_{a \in E^l} \Pr\{c(a) \notin Y_{s,u}(a)\}$$
$$= \prod_{a \in E^l} [1 - (|Y_{s,u}(a)|/q^k)] \tag{B2}$$

where $c(a)$ is the word from C that has the prefix a, $a \in E^l$, and Π denotes the product (like Σ denotes the sum). Since $\ln x < x - 1$, $1 < x \ne 1 < \infty$, and $|Y_{s,u}| = |Y_s|$ for $u = 1, 2, \cdots, M$, then from (B2) we have

$$\ln P_{s,u} < -q^{-k} \sum_{a \in E^l} |Y_{s,u}(a)| = -q^{-k}|Y_{s,u}| = -q^{-k}|Y_s|. \tag{B3}$$

From (B1)–(B3) we have

$$\ln P < \ln(q^k|S|) - \min_{s \in S} |Y_s| q^{-k}.$$

Using assumption (12), it is not difficult to check that the right-hand side of the last inequality is negative and, therefore, $P < 1$. This means that there exists a set C that satisfies the condition (13), and Lemma 1 is proven. □

References

[1] A. V. Kuznetsov, "Universal decoding for a class of deterministic channels," *Problemy Peredachi Informatsii*, vol. 19, no. 4, pp. 97–100, Oct.–Dec. 1983.

[2] A. V. Kuznetsov and B. S. Tsybakov, "Coding in a memory with defective cells," *Problemy Peredachi Informatsii*, vol. 10, no. 2, pp. 52–60, Apr.–June 1974.

[3] B. S. Tsybakov, "Defect and error correction," *Problemy Peredachi Informatsii*, vol. 11, no. 3, pp. 21–30, July–Sept. 1975.

[4] A. Kuznetsov, T. Kasami, and S. Yamamura, "An error correcting scheme for defective memory," *IEEE Trans. Inform. Theory*, vol. 4, pp. 712–718, Nov. 1978.

[5] L. A. Bassalygo and M. S. Pinsker, "Correction of errors in the channel with defects," *Rep. USSR Acad. Sci.*, vol. 243, no. 6, pp. 1361–1365, 1978.

[6] A. V. Kuznetsov, "Coding in a channel with generalized defects and random errors," *Problemy Peredachi Informatsii*, vol. 21 no. 1 pp. 28–34, Jan.–Mar. 1985.

[7] R. L. Rivest and A. Shamir, "How to reuse the write once memory," *Inform. Control*, vol. 55, pp. 1–19, Oct.–Dec. 1982.

[8] J. K. Wolf, A. D. Wyner, J. Ziv, and J. Korner, "Coding for write once memory," *AT&T Bell Lab. Tech. J.*, vol. 63, no. 6, pp. 1089–1112, 1984.

[9] S. I. Gelfand and M. S. Pinsker, "Coding for channel with random parameters," *Prob. Control Inform. Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[10] C. Heegard and A. El Gamal, "On the capacity of computer memory with defects," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 731–739, Sept. 1983.

[11] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 439–441, May 1983.

[12] A. V. Kuznetsov, "WOM as a memory with artificial defects," presented at 2nd Soviet–Swedish Workshop Inform Theory, Granna, Sweden, 1985.

[13] J. M. Borden, "Coding for write–unidirectional memories," preprint, *IEEE Trans. Inform. Theory*, manuscript, 1986.

[14] F. M. J. Willems and A. J. Vinck, "Repeated recording for an optical disk," in *Proc. 7th Symp. Inform Theory, Benelux*, Delft Univ., pp. 49–59, 1986.

[15] G. Cohen, "On the capacity of write-unidirectional memories," *Bull. Instit. Mathemat. Academia Sinica*, vol. 16, no. 4, pp. 285–293, Dec. 1988.

[16] G. Simonyi, "On write–unidirectional memories," *IEEE Trans. Inform. Theory*, vol. 35, pp. 663–667, May 1989.

[17] W. M. C. J. van Overveld, "The four classes of write–unidirectional memory codes over arbitrary alphabets," *IEEE Trans. Inform. Theory*, vol. 37, pp. 872–877, May 1991.

[18] A. V. Kuznetsov, "A lower bound on the capacity of write-unidirectional memory in the presence of random errors," *IEEE Symp. Inform. Theory, Abstr. Papers*, Kyoto, Japan, June 19–24, 1988.

[19] G. Cohen and G. Zemor, "Write–isolated memories," private communication, 1988.

[20] C. E. Shannon, "A mathematical theory of communication," *Bell System Tech. J.*, vol. 27, pp. 379–423, 1948.

[21] K. A. Schouhamer Immink, *Coding Techniques for Digital Recorders*. Englewood Cliffs, NJ: Prentice Hall, 1991.

[22] M.-F. Chang, W. K. Fuchs, and J. H. Patel, "Diagnosis and repair of memory with coupling faults," *IEEE Trans. Comput.*, vol. C-38, pp. 493–500, Apr. 1989.

[23] T. Fuja, "Coding for memories with address defects," in *Proc. 1990 Conf. Inform. Sci., Syst.*, Mar. 21–23, 1990, Princeton, NJ.