Reprinted from INFORMATION AND CONTROL
Vol. 19, No. 2, September 1971
Printed in Belgium

Bounds on Algebraic Code Capacities for Noisy Channels. II

R. AHLSWEDE* AND J. GEMMA

Ohio State University, Columbus, Ohio 43210

and

Battelle Memorial Institute, Columbus Laboratories

SUMMARY

It was proved by Ahlswede (1971) that codes whose codewords form a group or even a linear space do not achieve Shannon's capacity for discrete memoryless channels even if the decoding procedure is arbitrary. Sharper results were obtained in Part I of this paper. For practical purposes, one is interested not only in codes which allow a short encoding procedure but also an efficient decoding procedure. Linear codes—the codewords form a linear space and the decoding is done by coset leader decoding—have a fairly efficient decoding procedure. But in order to achieve high rates the following slight generalization turns out to be very useful: We allow the encoder to use a coset of a linear space as a set of codewords. We call these codes shifted linear codes or coset codes. They were implicitly used by Dobrushin (1963). This new code concept has all the advantages of the previous one with respect to encoding and decoding efficiency and enables us to achieve positive rate on discrete memoryless channels whenever Shannon's channel capacity is positive and the length of the alphabet is less or equal to 5 (Theorem 3.1.1). (The result holds very likely also for all alphabets with a length $a = p^s$, p prime, s positive integer). A disadvantage of the concepts of linear codes and of shifted linear codes is that they can be defined only for alphabets whose length is a prime power. In order to overcome this difficulty, we introduce generalized shifted linear codes. With these codes we can achieve a positive rate on arbitrary discrete memoryless channels if Shannon's capacity is positive (Theorem 3.2.1).

* Research of this author was supported by the National Science Foundation under Grant Contract No. GP-9464 to The Ohio State University.

All these results are obtained for average error. Estimates for the linear code capacity for maximal error are given for binary channels (Theorem 3.3.1). This capacity can be zero even if Shannon's capacity is positive. We continue using definitions and notations as given in Part I and we procede with the numbering of the chapters and paragraphs.

III. Relations between Shannon's Capacity and Algebraic Code Capacities

1. *Shifted Linear Codes*

In this and the following paragraph we deal with average error only. We are interested in the quantity $\bar{C}_{sl}^{-}$—which was defined in Part I, 1.4.3—as function of the channel matrix w. In order to have a convenient notation, we write T for $\bar{C}_{sl}^{-}$. Optimization over all possible field structures in X and Y leads to the quantity T^*. Frequently, we shall use notations as $T(w)$, $C_g(w)$, $C(w)$ to indicate the dependence on w.

Theorem 3.1.1. *Let* $X = Y = \mathrm{GF}(a)$, $a \leqslant 5$, *and let* $\mathscr{P}$ *be a* d.m.c. *given by* w. *Then* $T^*(w) > 0$ *if and only if* (*Shannon's capacity*) $C(w) > 0$.

Proof. Suppose first that $a = 2$. Let

$$w = w_1 = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix},$$

and define w_2 by

$$w_2(i \mid j) = w_1(i + 1 \mid j + 1), \qquad i, j \in \mathrm{GF}(2).$$

Thus,

$$w_2 = \begin{pmatrix} a_{11} & a_{10} \\ a_{01} & a_{00} \end{pmatrix}.$$

Let

$$w^* = \tfrac{1}{2}(w_1 + w_2) = \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix},$$

where $\alpha = \frac{1}{2}(a_{00} + a_{11})$ and $\beta = \frac{1}{2}(a_{01} + a_{10})$. $C(w) = 0$ if and only if w has equal rows (Wolfowitz, 1964). Therefore, $C(w) = 0$ implies $C(w^*) = 0$. On the other hand, $C(w^*) = 0$ implies $\alpha = \beta$, which implies that $a_{00} = a_{10}$ and hence $C(w) = 0$.

If $C(w^*) > 0$, then it follows from Theorem 2.1 (Part I) that $\bar{C}_l(w^*) = C(w^*) > 0$. Let $\mathscr{P}^*$ denote the d.m.c. given by w^*. Then

$$P_n^*(A \mid u) = \sum_{v \in A} \prod_{t=1}^{n} w^*(v^t \mid u^t), \qquad \text{for} \quad u = (u^1, \ldots, u^n) \in X_n,$$

$$v = (v^1, \ldots, v^n) \in Y_n, \qquad A \subset Y_n.$$

We give now another description for $P_n^*(\cdot \mid \cdot)$. Let

$$S = \{1, 2\}, \qquad S_n = \prod_{1}^{n} S \qquad \text{and} \qquad P_{s_n}(A \mid u) = \sum_{v \in A} \prod_{t=1}^{n} w_{s^t}(v^t \mid u^t),$$

where $s_n = (s^1, \ldots, s^n) \in S_n$. Furthermore, let q be a probability distribution on S_n such that

$$q(s_n) = \frac{1}{2^n} \qquad \text{for all} \quad s_n \in S_n.$$

Then we have

$$P_n^*(A \mid u) = \sum_{s_n} q(s_n) P_{s_n}(A \mid u) \qquad \text{for} \quad u \in X_n, \quad A \subset Y_n.$$

A code $(n, N, \bar{\lambda})$ for $\mathscr{P}^*$ satisfies

$$\frac{1}{N} \sum_{i=1}^{N} \sum_{s_n} q(s_n) P_{s_n}(A_i \mid u_i) \geqslant 1 - \bar{\lambda}$$

which implies that there exists an s_n^* such that

$$\frac{1}{N} \sum_{i=1}^{N} P_{s_n}^*(A_i \mid u_i) \geqslant 1 - \bar{\lambda}. \tag{3.1.1}$$

Let $i_1, \ldots, i_k$ be the components where a 2 occurs in channel sequence s_n^*. Let $x_n \in X_n$ be the vector with 1's in $i_1, \ldots, i_k$ and 0's elsewhere. Then by the definition of w_2 and (3.1.1),

$$\{(u_i + x_n, A_i + x_n) \mid i = 1, \ldots, N\}$$

is an $(n, N, \bar{\lambda})$ shifted linear code for $\mathscr{P}$. Hence we have $T^*(w) \geqslant T(w) \geqslant C(w^*) > 0$.

Consider now the case $a = 3$. In order to indicate the field structures choosen in X and Y we adopt now—and similarly in later cases—the following notation:

$$w = \begin{array}{c} \\ 0 \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & 1 & 2 \end{array} \\ \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix} \end{array}.$$

Let $w = w_1$. "Shift" by 1, 2 to obtain w_2, w_3:

$$w_2 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & 1 & 2 \end{array} \\ \begin{pmatrix} a_{11} & a_{12} & a_{10} \\ a_{21} & a_{22} & a_{20} \\ a_{01} & a_{02} & a_{00} \end{pmatrix} \end{array},$$

$$w_3 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & 1 & 2 \end{array} \\ \begin{pmatrix} a_{22} & a_{20} & a_{21} \\ a_{02} & a_{00} & a_{01} \\ a_{12} & a_{10} & a_{11} \end{pmatrix} \end{array}.$$

Let $w^* = \frac{1}{3}(w_1 + w_2 + w_3)$. Then

$$w^* = \begin{array}{c} \\ 0 \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & 1 & 2 \end{array} \\ \begin{pmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{pmatrix} \end{array},$$

where

$$\alpha = \tfrac{1}{3}(a_{00} + a_{11} + a_{22}),$$
$$\beta = \tfrac{1}{3}(a_{01} + a_{12} + a_{20}),$$
$$\gamma = \tfrac{1}{3}(a_{02} + a_{10} + a_{21}).$$

$C(w^*) = 0$ if and only if

$$a_{00} + a_{11} + a_{22} = a_{01} + a_{12} + a_{20} = a_{02} + a_{10} + a_{21}. \qquad (3.1.2)$$

Now we use different field structures and define

$$w_1' = \begin{array}{c} \\ 0 \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 0 & 2 \end{array} \\ \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix} \end{array}.$$

Rearranging the columns, we get

$$w_1' = \begin{array}{c} \\ 0 \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & 1 & 2 \end{array} \\ \begin{pmatrix} a_{01} & a_{00} & a_{02} \\ a_{11} & a_{10} & a_{12} \\ a_{21} & a_{20} & a_{22} \end{pmatrix} \end{array},$$

$$w_1' = \begin{array}{c} \\ 0 \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & 1 & 2 \end{array} \\ \begin{pmatrix} c_{00} & c_{01} & c_{02} \\ c_{10} & c_{11} & c_{12} \\ c_{20} & c_{21} & c_{22} \end{pmatrix} \end{array}.$$

Form w^{**} by shifting w_1' by 1, 2 to obtain w_2', w_3' and then setting $w^{**} = \frac{1}{3}(w_1' + w_2' + w_3')$. Then we obtain $C(w^{**}) = 0$ if and only if

$$c_{00} + c_{11} + c_{22} = c_{01} + c_{12} + c_{20} = c_{02} + c_{10} + c_{21},$$

i.e.,

$$a_{01} + a_{10} + a_{22} = a_{00} + a_{12} + a_{21} = a_{02} + a_{11} + a_{20}. \qquad (3.1.3)$$

Therefore, $C(w^*)$ and $C(w^{**}) = 0$ imply (3.1.2), (3.1.3). If we can show in this case that $C(w) = 0$, then we have $C(w) > 0$ if and only if $C(w^*)$ or $C(w^{**}) > 0$.

Using Theorem 2.2 of Part I and essentially the same argument as in the case $a = 2$, we can conclude that

$$T^*(w) \geqslant \max(C(w^*), C(w^{**})).$$

We now show that $C(w^*) = C(w^{**}) = 0$ indeed implies $C(w) = 0$ and thus complete the proof of the theorem.

We have, in addition to (3.1.2), (3.1.3), and (3.1.4),

$$a_{00} + a_{01} + a_{02} = 1,$$
$$a_{10} + a_{11} + a_{12} = 1,$$
$$a_{20} + a_{21} + a_{22} = 1.$$

In total, we have 7 equations in 9 unknowns.

The homogeneous system associated with Eqs. (3.1.2), (3.1.3), (3.1.4) has 7 linearly independent equations as can be seen by direct calculation. The set of solutions of the inhomogeneous system is therefore a translate of a space of dimension 2.

But

$$\begin{pmatrix}1&0&0\\1&0&0\\1&0&0\end{pmatrix}, \begin{pmatrix}0&1&0\\0&1&0\\0&1&0\end{pmatrix}, \begin{pmatrix}0&0&1\\0&0&1\\0&0&1\end{pmatrix} \tag{3.1.5}$$

are solutions of (3.1.2), (3.1.3), (3.1.4).

$$\begin{pmatrix}1&0&-1\\1&0&-1\\1&0&-1\end{pmatrix}, \begin{pmatrix}0&1&-1\\0&1&-1\\0&1&-1\end{pmatrix}$$

are linearly independent and therefore span the 2-dimensional space of solutions of the homogeneous system. Therefore, the set of all solutions of the inhomogeneous system is the set of matrices

$$\left\{\begin{pmatrix}a&b&c\\a&b&c\\a&b&c\end{pmatrix}\middle|\, a, b \text{ arbitrary; } c = 1-a-b\right\}$$

and contains among the stochastic matrices precisely those with equal rows. So if w satisfies (3.1.2), (3.1.3), and (3.1.4), then $C(w) = 0$. This proves the result for $a = 3$. Let now p be a prime and let

$$w_1 = \begin{array}{c} \\ 0 \\ 1 \\ \vdots \\ p-1 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & & p-1 \end{array} \\ \begin{pmatrix} a_{00} & a_{01} & \cdots & a_{0(p-1)} \\ a_{10} & a_{11} & \cdots & a_{1(p-1)} \\ \vdots & \vdots & & \vdots \\ a_{(p-1)0} & a_{(p-1)1} & \cdots & a_{(p-1)(p-1)} \end{pmatrix} \end{array}.$$

Shift by $1, 2, \ldots, p-1$ and obtain

$$w_2 = \begin{array}{c} \\ 0 \\ 1 \\ \vdots \\ p-1 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & & p-1 \end{array} \\ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{10} \\ a_{21} & a_{22} & \cdots & a_{20} \\ \vdots & \vdots & & \vdots \\ a_{01} & a_{02} & \cdots & a_{00} \end{pmatrix} \end{array}.$$

$w_3, \ldots,$ and

$$w_p = \begin{array}{c} \\ 0 \\ 1 \\ \vdots \\ p-1 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & & p-1 \end{array} \\ \begin{pmatrix} a_{(p-1)(p-1)} & \cdots & a_{(p-1)(p-2)} \\ a_{0(p-1)} & \cdots & a_{0(p-2)} \\ \vdots & & \vdots \\ a_{(p-2)(p-1)} & \cdots & a_{(p-2)(p-2)} \end{pmatrix} \end{array}.$$

Let $w^* = 1/p(w_1 + w_2 + \cdots + w_p)$; then

$$w^* = \begin{array}{c} \\ 0 \\ 1 \\ \vdots \\ p-1 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & & p-1 \end{array} \\ \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_p \\ \alpha_p & \alpha_1 & \cdots & \alpha_{p-1} \\ \vdots & \vdots & & \vdots \\ \alpha_2 & \alpha_3 & \cdots & \alpha_1 \end{pmatrix} \end{array},$$

where

$$\alpha_1 = \frac{1}{p}(a_{00} + a_{11} + \cdots + a_{(p-1)(p-1)}),$$
$$\alpha_2 = \frac{1}{p}(a_{01} + a_{12} + \cdots + a_{(p-1)0}),$$
$$\cdots$$
$$\alpha_p = \frac{1}{p}(a_{0(p-1)} + a_{10} + \cdots + a_{(p-1)(p-2)}).$$

$C(w^*) = 0$ if and only if

$$\begin{aligned} (1)\quad & a_{00} + a_{11} + \cdots + a_{(p-1)(p-1)} \\ & = a_{01} + a_{12} + \cdots + a_{(p-1)0} \\ & = \cdots = a_{0(p-1)} + a_{10} + \cdots + a_{(p-1)(p-2)}\,. \end{aligned}$$

Define

$$w_1^{(1)} = \begin{array}{c} \\ 0 \\ 1 \\ \\ (p-1) \end{array} \begin{array}{c} \begin{array}{ccccccc} 1 & 0 & 2 & 3 & \cdots & (p-1) \end{array} \\ \begin{pmatrix} a_{00} & a_{01} & a_{02} & \cdot & \cdots & a_{0(p-1)} \\ & & & & & \\ \vdots & \vdots & & & & \vdots \\ a_{(p-1)0} & & \cdot & \cdot & \cdots & a_{(p-1)(p-1)} \end{pmatrix} \end{array},$$

produce by shifting $w_2^{(1)}, \ldots, w_p^{(1)}$, and define

$$w^{2*} = \frac{1}{p}(w_1^{(1)} + w_2^{(1)} + \cdots + w_p^{(1)}),$$

and obtain $C(w^{2*}) = 0$ if and only if

$$\begin{aligned} (2)\quad & a_{01} + a_{10} + a_{22} + \cdots + a_{(p-1)(p-1)} \\ & = a_{00} + a_{12} + \cdots + a_{(p-1)1} \\ & = \cdot \quad \cdot \quad \cdot \\ & \vdots \\ & = a_{0(p-1} + a_{11} + \cdots + a_{(p-1)(p-2)}\,. \end{aligned}$$

Proceeding in this manner, we get Eqs. (3), (4),..., $(p-2)$, and, finally,

$$(p-1)\quad a_{0(p-2)} + a_{11} + \cdots + a_{(p-2)0} + a_{(p-1)(p-1)} = a_{01} + a_{12} + \cdots + a_{(p-3)0} + a_{(p-2)(p-1)} + a_{(p-1)(p-2)} \\ \vdots \\ = a_{0(p-1)} + a_{1(p-2)} + a_{21} + \cdots + a_{(p-1)0}\,.$$

In addition, we have

$$(p)\quad a_{00} + a_{01} + \cdots + a_{0(p-1)} = 1 \\ \vdots \\ a_{(p-1)0} + a_{(p-1)} + \cdots + a_{(p-1)(p-1)} = 1.$$

Systems (1), (2),..., (p) yield $p^2 - (p-1)$ equations in p^2 unknowns.

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & 1 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

are solutions of Eqs. (1),..., (p). Hence, the set of solutions contains all stochastic matrices with equal rows. If the $p^2 - (p-1)$ equations are linearly independent, these are the only solutions. Then we could conclude $C > 0$ implies $T^*(w) \geqslant \max(C(w^*), \ldots, C(w^{(p^*)})) > 0$. We have been unable to establish the linear independence for general primes p. For $p = 5$, the linear independence can be proved by straightforward calculation. Thus the theorem holds for $p = 5$.

Because of the structure of Galois fields, the case $a = 4$ is somewhat different. By shifting the matrix

$$w = w_1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix} \end{array}$$

by 1, 2, 3 and proceeding as before, we obtain

$$w^* = \tfrac{1}{4}(w_1 + w_2 + w_3 + w_4)$$

which gives

$$w^* = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \alpha & \delta & \gamma \\ \gamma & \delta & \alpha & \beta \\ \delta & \gamma & \beta & \alpha \end{pmatrix},$$

where

$$\begin{aligned} \alpha &= \tfrac{1}{4}(a_{00} + a_{11} + a_{22} + a_{33}), \\ \beta &= \tfrac{1}{4}(a_{01} + a_{10} + a_{22} + a_{32}), \\ \gamma &= \tfrac{1}{4}(a_{02} + a_{13} + a_{20} + a_{31}), \\ \delta &= \tfrac{1}{4}(a_{30} + a_{12} + a_{21} + a_{30}). \end{aligned}$$

$C(w^*) = 0$ if and only if $\alpha = \beta = \gamma = \delta$. To obtain channels w^{2*}, w^{3*}, w^{4*} we use

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 0 & 2 & 3 \end{array} \\ \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ a_{30} & \cdot & \cdot & a_{33} \end{pmatrix} \end{array}, \quad \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 2 & 1 & 0 & 3 \end{array} \\ \begin{pmatrix} a_{00} & \cdot & \cdot & a_{03} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ a_{30} & \cdot & \cdot & a_{33} \end{pmatrix} \end{array}, \quad \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 3 & 1 & 2 & 0 \end{array} \\ \begin{pmatrix} a_{00} & \cdot & \cdot & a_{03} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ a_{30} & \cdot & \cdot & a_{33} \end{pmatrix} \end{array}.$$

Note that we interchange 0 with 3, whereas this is not necessary in the case of p prime. It is necessary here in order to obtain sufficiently many linearly independent equations. Besides the equations we obtain from $C(w^*) = 0$, $C(w^{2*}) = 0$, $C(w^{3*}) = 0$, $C(w^{4*}) = 0$, we use the equations

$$\begin{aligned} a_{00} + a_{01} + a_{02} + a_{03} &= 1, \\ &\cdots \\ a_{30} + a_{31} + a_{32} + a_{33} &= 1. \end{aligned}$$

Checking, we find that w with equal rows is a solution of all these equations and that 13 equations in 16 unknowns are linearly independent. Hence, as before, matrices with equal rows form the only solutions, so we can conclude $C > 0$ implies

$$T^*(w) \geqslant \max(C(w^*), \ldots, C(w^{4*})) > 0.$$

Again, it seems very likely that this result holds in general for $a = p^k$, p prime, k positive integer.

2. *Generalized Shifted Linear Codes*

Now suppose $\mathscr{P}$ is a d.m.c. given by w, where X and Y are finite sets, not necessarily of equal size. We define generalized shifted linear codes as follows:

Let GF(a) be a Galois field, where $a \leqslant \min(|X|, |Y|)$. Let X' be a subset of X, $|X'| = a$, and let φ be a $1:1$ mapping of X' onto GF(a), and let ψ be a mapping of Y onto GF(a). This gives rise to a new d.m.c. $P_{X',\varphi,\psi}$ with input and output alphabets equal to GF(a). We denote the transition matrix by $w_{X',\varphi,\psi}$. The transition probabilities are given by

$$w_{X',\varphi,\psi}(c \mid b) = \sum_{y \in \psi^{-1}(c)} w(y \mid \varphi^{-1}(b))c, \; b \in \mathrm{GF}(a). \tag{3.2.1}$$

We call a shifted linear code for $P_{X',\varphi,\psi}$ a generalized shifted linear code for $\mathscr{P}$. The use of those codes on P requires an additional mapping φ in the encoding and φ^{-1} in the decoding procedure. Define $T(w_{X',\varphi,\psi})$ as usual and let

$$G = \max_{\substack{X' \subset X \\ p^s = |X'| \leqslant |Y|}} \left(\max_{\varphi,\psi} T(w_{X',\varphi,\psi})\right) \tag{3.2.2}$$

G is a lower bound on the achievable rate for generalized shifted linear codes on $\mathscr{P}$.

THEOREM 3.2.1. *$G > 0$ if and only if $C > 0$.*

Proof. If $C > 0$, then there exist two rows in w, say the i-th and the j-th, which are unequal. Let $X' = \{i, j\}$ and let $\varphi(i) = 0$, $\varphi(j) = 1 \in \mathrm{GF}(2)$. Partition Y into sets Y_1 and Y_2 such that $P(Y_1 \mid i) \neq P(Y_1 \mid j)$ and let

$$\psi(y) = \begin{cases} 0 & \text{for } y \in Y_1 \\ 1 & \text{for } y \in Y_2 . \end{cases}$$

Then $\mathscr{P}_{X',\varphi,\psi}$ is a binary d.m.c. with alphabets equal to GF(2). $w_{X',\varphi,\psi}$ has unequal rows. By Theorem 3.1.1, $T^*(w_{X',\varphi,\psi}) > 0$ and hence $G > 0$.

Remark. It follows from Example 1 of Ahlswede (1971) that we sometimes can achieve higher rates for generalized shifted linear codes than for shifted linear codes.

3. *On The Linear Code Capacity For Maximal Errors For Binary Channels*

Let w be a 2×2-stochastic matrix. Let $1 = (x_1, y_1)$ denote the first and let $2 = (x_2, y_2)$ denote the second row vector. We represent these vectors

as points in the euclidean space E^2. Let α represent the vector $(\frac{1}{2}, \frac{1}{2})$. Then we have either

Case I. 1 and 2 are unequal to α and on different sides of α, or

Case II. 1 and 2 are on the same side of α.

In Case I we say that vector i is closer to α than vector j, if $d(i, \alpha) \leqslant d(j, \alpha)$, where $d(\cdot \mid \cdot)$ is the 2-dimensional euclidean metric. Define in this case

$$w^* = \begin{cases} \begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix} & \text{if 1 is closer to } \alpha \\ \begin{pmatrix} y_2 & x_2 \\ x_2 & y_2 \end{pmatrix} & \text{if 2 is closer to } \alpha. \end{cases} \tag{3.3.1}$$

We call w^* the underlying symmetric matrix for w.

In Case II we say that there is no underlying symmetric matrix for w. We need the following lemma, which was proved by Ahlswede and Wolfowitz (1970). Suppose that w and w' are 2×2-stochastic matrices. Denote the row vectors of w by 1, 2 and the row vectors of w' by 1′, 2′. Suppose w and w' are given by one of the figures:

(3.3.2)

LEMMA 3.3.1. *Suppose* $\{(u_i, A_i)\ (i = 1,\ldots, N)$ *is an* s.m.l.c. *for the* d.m.c. $\mathscr{P}^*$ *given by* w^*. *Then* $\{(u_i, A_i \mid i = 1,\ldots, N)$ *is an* (n, N, λ) *code for the* d.m.c. $\mathscr{P}$ *given by* w.

Now we can state

THEOREM 3.3.1. *Let* $\mathscr{P}$ *be a binary* d.m.c. *given by* w. *If there exists an underlying symmetric matrix* w^* *for* w, *then* $C_l^*(w) \geqslant C_l(w^*) > 0$. *Otherwise* $C_l^*(w) = 0$.

Proof. First assume that there exists an underlying matrix w^* for w. According to Theorem 2.1 of Part I, $C_l(w^*) = C(w^*) > 0$. Choose a field structure $\mathrm{GF}(2) = \{0, 1\}$ in X, Y such that $w^*(0 \mid 0)$, $w^*(1 \mid 1) > \frac{1}{2}$. Let

$\{u_i, A_i) \mid i = 1,..., N\}$ be an (n, N, λ) linear code for $\mathscr{P}^*$, $\lambda < \frac{1}{2}$, where the coset leaders have minimal weight. Furthermore, let

$$B_i = \{y_n \mid P_n^*(y_n \mid u_i) > \max_{j \neq i} P_n^*(y_n \mid u_j)\}.$$

Then $B_i \subset A_i$, $i = 1,..., N$ and $\{(u_i, B_i) \mid i = 1,..., N\}$ is a s.m.l.c. with respect to $\mathscr{P}^*$. From Lemma 4 (Ahlswede, 1971) we have that $\{(u_i, B_i) \mid i = 1,..., N\}$ is an $(n, N, 2\lambda)$ code with respect to $\mathscr{P}^*$. Then from Lemma 3.3.1, it follows that $\{(u_i, B_i)\, i = 1,..., N\}$ is an $(n, N, 2\lambda)$ code for the d.m.c. and hence so is $\{(u_i, A_i) \mid i = 1,..., N\}$. Hence $C_l^*(w) \geqslant C_l(w^*) > 0$.

We now prove the second statement of the theorem. We show first that $C_l^*(w) = 0$ for $w = \left(\begin{smallmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{smallmatrix}\right)$. The cases $\left(\begin{smallmatrix} 0 & 1 \\ \frac{1}{2} & \frac{1}{2} \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & 0 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 1 \end{smallmatrix}\right)$ can be treated in the same way for symmetry reasons.

We have to consider the cases

$$\text{(a)}\ \begin{array}{c} \\ 0 \\ 1 \end{array}\!\!\begin{array}{c} \begin{array}{cc} 0 & 1 \end{array} \\ \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \end{array} \qquad \text{(b)}\ \begin{array}{c} \\ 0 \\ 1 \end{array}\!\!\begin{array}{c} \begin{array}{cc} 1 & 0 \end{array} \\ \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \end{array} \qquad \text{(c)}\ \begin{array}{c} \\ 1 \\ 0 \end{array}\!\!\begin{array}{c} \begin{array}{cc} 1 & 0 \end{array} \\ \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \end{array} \qquad \text{(d)}\ \begin{array}{c} \\ 1 \\ 0 \end{array}\!\!\begin{array}{c} \begin{array}{cc} 0 & 1 \end{array} \\ \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \end{array}$$

Let $\{u_1,..., u_N\}$ be the codewords—u_1 being the zero codeword—and let $A_1 = \{l_1,..., l_L\}$. Then in cases (a), (b)

$$P(u_i + l_j \mid u_i) = P(l_j \mid u_i) \qquad \text{for} \quad i = 1,..., N, \quad j = 1,..., L. \tag{3.3.3}$$

Hence $P(A_1 \mid u_i) = P(A_i \mid u_i)$ for $i = 1,..., N$.

Then, since $P(A_1 \mid u_i) + P(A_i \mid u_i) \leqslant 1$, we have $P(A_i \mid u_i) \leqslant \frac{1}{2}$ for $i = 2,..., N$. So for $\lambda < \frac{1}{2}$, $N(n, \lambda) = 1$ and hence $C_l(w) = 0$. In cases (c), (d), we have for $\lambda < \frac{1}{2}$ that $P(A_i \mid u_i) > \frac{1}{2}$ $(i = 1,..., N)$ implies $\mid A_1 \mid > 2^{n-1}$ so that $A_1 = Y_n$ and hence again $N(n, \lambda) = 1$. This proves the result for these special matrices. The result for general matrices which have no underlying symmetric matrix follows now from Lemma 4 of Ahlswede (1971) and Lemma 3.3.1.

Remark 1. In cases (a) and (b) the result can be proved in the same way for average errors.

RECEIVED: June 22, 1970

REFERENCES

AHLSWEDE, R. (1971), Group codes do not achieve Shannon's channel capacity for general discrete channels, *Ann. Math. Stat.* 42, No. 1, 224–240.

AHLSWEDE, R., AND J. GEMMA (1971), Bounds on algebraic code capacities for noisy channels, I, *Information and Control*, to appear.

AHLSWEDE, R., AND J. WOLFOWITZ (1970), The capacity of a channel with arbitrarily varying channel probability functions and binary output alphabet, *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **15**, 186–194.

DOBRUSHIN, R. L. (1963), Asymptotic optimality of group and systematic codes for some channels, *Theor. Probability Appl.* **8**, 47–59.

ELIAS, P. (1955), Coding for noisy channels, *IRE Convention Record*, Part 4, pp. 37–46.

WOLFOWITZ, J. (1964), "Coding Theorems of Information Theory," 2nd ed., Springer-Verlag, Berlin/New York.

Printed in Belgium by the St. Catherine Press Ltd., Tempelhof 37, Bruges