An Elementary Proof of the Strong Converse Theorem for the Multiple-access Channel

RUDOLF AHLSWEDE

Fakultät für Mathematik Universität Bielefeld Universitätsstraße 1
4800 Bielefeld 1, West Germany

1. Introduction

In [1] we determined the capacity region of the multiple-access channel (MAC) by proving a coding theorem and its weak converse. Recently Dueck [2] proved a strong converse theorem in the sense of Wolfowitz [3]. His proof uses the Ahlswede-Gács-Körner [4] method of "blowing up decoding sets" in conjunction with a new "wringing technique". This technique makes it now possible to prove strong converses, if the average error probability criterion is genuinely used (as is the case in the results for the MAC mentioned above, c.f. [5]).

In this paper we prove Dueck's result without using the method of "blowing up decoding sets", which is based on non-elementary combinatorial work of Margulis [6].

Our proof follows our old approach of [7] to derive upper bounds on the length of maximal error codes. In [7] we considered the TWC, the MAC can be treated in essentially the same way. In conjunction with a suitable "wringing technique" (Lemma 3) this approach becomes applicable also to average error codes. The heart of the matter is the fact that codes for the MAC have subcodes with a certain independence structure. Actually even this fact can be understood from a more basic simple principle concerning the comparison of two probability distributions on a product space (Lemma 4). This general principle makes the combinatorial or probabilistic nature of Dueck's technique and our improvement thereof (Lemma 3) fully transparent. It also leads to a somewhat sharper result on coding: Strong converse with \( \sqrt{n} \log n \) deviation.

The paper is self-contained and all ideas are explained in detail.

2. The Strong Converse Theorem for the MAC

\( \mathcal{X}, \mathcal{Y} \) are the (finite) input alphabets and \( \mathcal{Z} \) is the (finite) output alphabet of a MAC with transmission matrix \( w \). For words of length \( n \) the
transmission probabilities are

\[
W(z_n \mid x^n y^n) = \prod_{i=1}^{n} w(z_i \mid x_i y_i) \quad \text{for} \quad x^n = (x_1, \ldots, x_n) \in \mathcal{X}^n = \prod_{i=1}^{n} \mathcal{X},
\]

\[
y^n \in \mathcal{Y}^n, z^n \in \mathcal{Z}^n
\]

A code \( (n, M, N, \bar{\lambda}) \) for the MAC is a system \( \{(u_i, v_j, D_{ij}) : 1 \leq i \leq M, 1 \leq j \leq N \} \) with

(a) \( u_i \in \mathcal{X}^n, v_j \in \mathcal{Y}^n, D_{ij} \subseteq \mathcal{Z}^n \) for \( 1 \leq i \leq M, 1 \leq j \leq N \)

(b) \( D_{ij} \cap D_{i'j'} = \emptyset \) for \( (i, j) \neq (i', j') \)

(c) \[
\frac{1}{MN} \sum_{i=1}^{N} \sum_{j=1}^{M} W(D_{ij} \mid u_i v_j) \geq 1 - \bar{\lambda}
\]

A pair of non-negative reals \( (R_1, R_2) \) is an achievable pair of rates for \( \bar{\lambda} \in (0, 1) \), if for all sufficiently large \( n \) there exist codes \( (n, [\exp R_1 n], [\exp R_2 n], \bar{\lambda}) \). \( \mathcal{R}(\bar{\lambda}) \) denotes the set of those pairs and \( \mathcal{R} = \bigcap_{\bar{\lambda} \in (0, 1)} \mathcal{R}(\bar{\lambda}) \)

is called the capacity region. The characterization found in [9], which is somewhat different from the original one in [1], is

\[
(2.2) \quad \mathcal{R} = \text{conv} \{(R_1, R_2) : R_1 \leq I(X \land Z \mid Y), R_2 \leq I(Y \land Z \mid X),
R_1 + R_2 \leq I(XX \land Z) \quad \text{for some indep. } X, Y, \}
\]

where \( X, Y \) are input variables, \( Z \) is the corresponding output variable, \( I(X \land Z) \), \( I(X \land Z \mid Y) \) etc. denote mutual resp. conditional mutual information, and "conv" stands for the convex hull operation.

Dueck's strong converse theorem states

\[
(2.3) \quad \mathcal{R}(\bar{\lambda}) \subseteq \mathcal{R} \quad \text{(and hence } \mathcal{R} = \mathcal{R}(\bar{\lambda}) \text{ for } \bar{\lambda} \in (0, 1).)
\]

We prove the

**THEOREM.** For every \( n \) and every \( (n, M, N, \bar{\lambda}) \) code:

\[
(n \log M, n \log N) \in (n + o(n \log n))(\mathcal{R})
\]

The approach of [7] makes use of Augustin's [11] strong converse estimate for one-way channels. Wolfowitz gave in [12] a general lemma for proving strong converses, which he credited as follows: "It is a formalization and slight generalization of methods used by Kemperman, Yoshihara, and the author". We formulate and prove here a slight extension thereof, called packing lemma, which yields also the result of [11]. This way one has one key tool for proving strong converses and also, the paper becomes self-contained.

3. **THE PACKING LEMMA AND A BOUND ON CODES FOR THE MAC**

Let \( \mathcal{K} \) and \( \mathcal{L} \) be finite sets and let \( P \) be a \(|\mathcal{K}| \times |\mathcal{L}|\)-stochastic matrix.

Vol. 7, No. 3 (1982)
A (\(M, \lambda\))-code is a system \((u_i, D_i) : 1 \leq i \leq M\) with
- \(u_i \subset \mathcal{K}, D_i \subset \mathcal{L}\) for \(1 \leq i \leq M\)
- \(D_i \cap D_j = \emptyset\) for all \(i \neq j \leq M\)
- \(P(D_i \mid u_i) \geq 1 - \lambda\) for all \(1 \leq i \leq M\)

For a probability distribution \((P_D)_{i \in \mathcal{L}}\) and a number \(\theta > 0\) define
- \(P(D_i \mid u_i) \geq 1 - \lambda\) for \(1 \leq i \leq M\)

For a probability distribution \((P_D)_{i \in \mathcal{L}}\) and a number \(\theta > 0\) define

\[
\beta_{\theta}(D_l, r) = \sum_{i \in \mathcal{I}} P(D_i \mid u_i) < \theta,
\]

\[
\alpha_{\theta}(D_l, r) = \frac{1}{M} \sum_{i \in \mathcal{I}} \theta_i < \theta
\]

Lemma 1. Suppose that a (\(M, \lambda\))-code \((u_i, D_i) : 1 \leq i \leq M\) there exists a PDR on \(\mathcal{L}\) and positive numbers \(\theta_1, \ldots, \theta_M\) such that

Lemma 2. Suppose that an (\(M, \lambda\))-code \((u_i, D_i) : 1 \leq i \leq M\) there exists a PDR on \(\mathcal{L}\) and positive numbers \(\theta_1, \ldots, \theta_M\) such that

\[
\max_{l \in \mathcal{L}} \sum_{1 \leq i \leq M} P(l \mid u_i) < \kappa,
\]

\[
M < (1 - \lambda - \kappa)^{-1} \exp \left( \frac{1}{M} \sum_{i=1}^M \theta_i \right).
\]

The case \(\theta_i = \theta\) for \(1 \leq i \leq M\) is the result of [12].

Proof. Consider the code \((u_i, D_i) : 1 \leq i \leq M\) and define for \(1 \leq i \leq M\)

\[
\theta_i = \frac{P(l \mid u_i)}{r(l)} < \theta
\]

Then for \(l \in A_i\), \(P(A_i < r(l) \mid u_i) < \theta\) and hence \(u_i \geq 1 - \lambda - \kappa\).

It follows that \(e^{\theta_i(r(A_i) - r(l))} > P(A_i \mid u_i) > P(D_i \mid u_i)\) for all \(1 \leq i \leq M\) and hence \(e^{\theta_i} > 1 - \lambda - \kappa\).

It follows that \(\theta_i \geq \log \frac{1 - \lambda - \kappa}{r(A_i)} \geq \log \frac{1 - \lambda - \kappa}{r(D_i)}\)

and also that

\[
\sum_{i=1}^M \frac{1}{M} \log \frac{1 - \lambda - \kappa}{r(A_i)} \geq \log \frac{1 - \lambda - \kappa}{r(D_i)}
\]

This implies

\[
M \leq (1 - \lambda - \kappa)^{-1} \exp \left( \frac{1}{M} \sum_{i=1}^M \theta_i \right).
\]

Q.E.D.

Remark 1. The lemma can be further generalized for average error codes. We did not present this more general form, because we have no genuine applications for it. The lemma can be further generalized to average error codes.

Remark 2. We did not present this more general form, because we have no genuine applications for it. Theorem naturally has to involve non-stationary DMC's, which are defined.

Theorem naturally has to involve non-stationary DMC's, which are defined.

Jr. Comb., Inf. & Syst. Sc.
by a sequence \((w_i)^n_{i=1}\) of \(|\mathcal{X}| \times |\mathcal{Z}|\)-stochastic matrices and

\[
W(z^n | x^n) = \prod_{i=1}^{n} w_i(z_i | x_i) \quad \text{for every } n = 1, 2, \ldots; \quad \text{every } x^n \in \mathcal{X}^n; \quad \text{and every } z^n \in \mathcal{Z}^n
\]

as transmission probabilities for words. We show next how to prove the familiar strong converse for non-stationary DMC’s via Lemma 1. In applying this lemma one has some freedom in the choice of \(r\). Kemperman [10] used \(r^{**} = r^*_r x_r \ldots x_r^n\), where \(r^*_r\) is the maximizing output distribution for \(w_i\), that is,

\[
R(p^*_r, w_i) = \sum_{x,z} p^*_r(x) w_i(z | x) \log \frac{w_i(z | x)}{r^*_r(z)} = \max_{X_i} I(X_i \wedge Z_i) = C_i.
\]

For a given \((n, M, \lambda)\)-code \(\{(u_i, D_i) : 1 \leq i \leq M\}\) Augustin [11] used \(r^n = r_1 x \ldots x_r^n\), where

\[
r_r(z) = \frac{1}{M} \sum_{i=1}^{M} w_i(z | u_i) \quad \text{for } u_i = (u_{i1}, \ldots, u_{in}).
\]

In order to understand this choice let us choose first \(r\) as

\[
r(z^n) = \frac{1}{M} \sum_{i=1}^{M} W(z^n | u_i),
\]

that is the output distribution corresponding to the “Fano-distribution”:

\[
\frac{1}{M} \text{ probability on each code word } u_i.
\]

With \(\theta_i = c \sum_{z} W(z^n | u_i) \log \frac{W(z^n | u_i)}{r(z^n)}\), \(c\) a constant, we get that \(\theta = \frac{1}{M} \sum_{i=1}^{M} \theta_i\) is a mutual information up to a constant \(c\). By a suitable choice of \(c\) one can derive the weak converse by using Lemma 1. One does not get the strong converse, because \(\log \frac{W(\cdot | u_i)}{r(\cdot)}\) is not a sum of independent RV’s and therefore the variance is too big. \(r^n\) is the output distribution obtained by choosing as input distribution

\[
p^n = \prod_{i=1}^{n} p, p(x) = \frac{1}{M} \delta(u_i, x), \quad x \in \mathcal{X}, \quad 1 \leq t \leq n,
\]

that is the product of 1-dimensional marginal distributions of the “Fano-distribution” and may therefore be called Fano*-distribution. This way one achieves both, the independence property and the “matching” of an information quantity. \(r^n\) reflects structural properties of the set of code words, which \(r^{**}\) doesn’t.

Now with the choices \(\mathcal{K} = \mathcal{X}^n, \mathcal{L} = \mathcal{Z}^n, r = r^n, P = W, \gamma = \frac{1 - \lambda}{2}\), and
for $i = 1, \ldots, M$

$$\theta_i = \mathbb{E}_{\mathcal{W}(\cdot | u_i)} \log \frac{W(\cdot | u_i)}{r^n(\cdot)} + \left( \frac{2}{1 - \lambda} \text{Var}_{\mathcal{W}(\cdot | u_i)} \log \frac{W(\cdot | u_i)}{r^n(\cdot)} \right)^{1/2}.$$ 

By Chebyshev's inequality

(3.7) \quad W(B_u(\theta_i, r^n) | u_i) \leq \frac{1 - \lambda}{2} \quad \text{for } 1 \leq i \leq M

and hence Lemma 1 yields

(3.8) \quad M < \frac{2}{1 - \lambda} \exp \left\{ \frac{1}{M} \sum_{i=1}^{M} \theta_i \right\}.

In order to bound the right-side expression set

$$T_1 = \frac{1}{M} \sum_{i=1}^{M} \mathbb{E}_{\mathcal{W}(\cdot | u_i)} \log \frac{W(\cdot | u_i)}{r^n(\cdot)},$$

$$T_2 = \frac{1}{M} \sum_{i=1}^{M} \left( \text{Var}_{\mathcal{W}(\cdot | u_i)} \log \frac{W(\cdot | u_i)}{r^n(\cdot)} \right)^{1/2}.$$

Clearly,

$$T_1 = \sum_{i=1}^{M} \sum_{z} \frac{1}{M} W(z^n | u_i) \log \frac{W(z^n | u_i)}{r^n(z)}$$

$$= \sum_{i=1}^{n} \sum_{z} \sum_{x} \frac{1}{M} \delta(u_{it}, x) w_i(z | x) \log \frac{w_i(z | x)}{r_i(z)}$$

(3.9) \quad = \sum_{i=1}^{n} I(X_i \land Z_i), \text{ where } \Pr(X_i = x) = p_i(x)

and $Z_i$ is the corresponding output distribution.

$T_2$ was bounded in [11] as follows:

By the convexity of the square root function

$$T_2 \leq \left( \sum_{i=1}^{M} \frac{1}{M} \text{Var}_{\mathcal{W}(\cdot | u_i)} \log \frac{W(\cdot | u_i)}{r^n(\cdot)} \right)^{1/2}$$

and

$$\sum_{i=1}^{M} \frac{1}{M} \text{Var}_{\mathcal{W}(\cdot | u_i)} \log \frac{w_i(\cdot | u_i)}{r^n(\cdot)} = \sum_{i=1}^{n} \sum_{z} \frac{1}{M} \text{Var}_{\mathcal{W}(\cdot | u_i)} \log \frac{w_i(z | x)}{r_i(z)}$$

$$= \sum_{i=1}^{n} \sum_{z} \sum_{x} p_i(x) w_i(z | x) \left( \log \frac{w_i(z | x)}{r_i(z)} - \mathbb{E}_{\mathcal{W}(\cdot | x)} \log \frac{w_i(\cdot | x)}{r_i(\cdot)} \right)^2.$$ 

Since for any RV $F$ and any constant $a$ a $\text{Var} F \leq \mathbb{E}(F + a)^2$, the last quantity can be upperbounded by

$$ \sum_{i=1}^{n} \sum_{z} \sum_{x} p_i(x) w_i(z | x) \left( \log \frac{w_i(z | x)}{r_i(z)} + \log p_i(x) \right)^2$$

$$= \sum_{i=1}^{n} \sum_{z} \sum_{x} r_i(z) p_i(x) w_i(z | x) \left( \log \frac{w_i(z | x) p_i(x)}{r_i(z)} \right)^2.$$ 

Since for a probability vector \((a_1, \ldots, a_c)\)
\[
\sum_{i=1}^{c} a_i \log^2 a_i \leq \max (\log^2 3, \log^2 c),
\]
also
\[
\sum_{x} \frac{p_i(x) w_i(z \mid x)}{r_i(z)} \left( \log \frac{p_i(x) w_i(z \mid x)}{r_i(z)} \right)^2 \leq \max (\log^2 3, \log^2 |\mathcal{X}|) \leq 3 |\mathcal{X}|.
\]
Thus
\[
(3.10) \quad T_2 \leq (3 |\mathcal{X}| n)^{1/2}.
\]
Thus, (3.9) and (3.8) yield
\[
\log M \leq \sum_{i=1}^{n} I(X_i \wedge Z_i) + \left( \frac{2}{1 - \lambda} |\mathcal{X}| n \right)^{1/2} + \log \frac{2}{1 - \lambda}
\]
and hence the

**Corollary 1 (Augustin [11]):** For an \((n, M, \lambda)\) code \(\{u_i, D_i\}: 1 \leq i \leq M\)
for the non-stationary DMC \(\left(\omega_i\right)_{i=1}^{\infty}
\]
\[
(3.11) \quad \log M \leq \sum_{i=1}^{n} I(X_i \wedge Z_i) + \frac{3}{1 - \lambda} |\mathcal{X}| n^{1/2}, \quad 0 < \lambda < 1,
\]
where the distributions of the RV's are (as usual) determined by the Fano-distribution on the code words.

Already in [7] we showed how to use Fano-distributions to derive upper bounds on the lengths of codes for the restricted TWC in case of maximal errors. We apply this approach now to \((n, M, N)\) codes \(\{(u_i, v_j, D_{ij}) : 1 \leq i \leq M, 1 \leq j \leq N\}\) for the MAC with average error \(\bar{\lambda}\), that is,

\[
(3.12) \quad \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} W(D_{ij} \mid u_i, v_j) = 1 - \bar{\lambda}.
\]

\[
(3.13) \quad \mathcal{A} = \left\{ (i, j) : W(D_{ij} \mid u_i, v_j) \geq \frac{1 - \bar{\lambda}}{2} \geq 1 - \lambda, 1 \leq i \leq M, \right. \\
\left. \quad \quad \quad \quad 1 \leq j \leq N \right\}
\]

\[
(3.14) \quad \mathcal{C}(i) = \{(i, j) : (i, j) \in \mathcal{A}, 1 \leq j \leq N\},
\quad \quad \mathcal{B}(j) = \{(i, j) : (i, j) \in \mathcal{A}, 1 \leq i \leq M\}.
\]

Consider the subcode \(\{(u_i, v_j, D_{ij}) : (i, j) \in \mathcal{A}\}\) and define its Fano-distribution RV's \(X^n, Y^n\)
\[
(3.15) \quad \Pr((X^n, Y^n) = (u_i, v_j)) = |\mathcal{A}|^{-1}, \text{ if } (i, j) \in \mathcal{A}.
\]
It follows from Corollary 1 that

\[
(3.16) \quad \log |\mathcal{B}(j)| \leq \sum_{i=1}^{n} I(X_i \wedge Z_i \mid Y_i = v_j) + \frac{3}{1 - \lambda} |\mathcal{X}| n^{1/2},
\]

Vol. 7, No. 3 (1982)
\begin{align}
(3.17) \quad \log |\mathcal{C}(i)| \leq \sum_{i=1}^{n} I(Y_i \wedge Z_i \mid X_i = u_i) + \frac{3}{1 - \lambda} |\mathcal{X}| n^{1/2},
\end{align}
and
\begin{align}
(3.18) \quad \log |\mathcal{A}| \leq \sum_{i=1}^{n} I(X_i,Y_i \wedge Z_i) + \frac{3}{1 - \lambda} |X| n^{1/2}.
\end{align}

Since \(\text{Prob} \ (Y_i = y) = |\mathcal{A}^{-1} \sum_{(i,j) \in \mathcal{A}} \delta(v_{ij}, y)|\), it follows from (3.16) that
\begin{align}
(3.19) \quad \log |\mathcal{B}(j)| 
\leq |\mathcal{A}^{-1} \sum_{(i,j) \in \mathcal{A}} \sum_{i=1}^{n} I(X_i \wedge Z_i \mid Y_i = v_{ij}) \sum_{y} \delta(v_{ij}, y) + \frac{3}{1 - \lambda} |\mathcal{X}| n^{1/2}
\end{align}
\begin{align}
= |\sum_{i=1}^{n} I(X_i \wedge Z_i \mid Y_i) + \frac{3}{1 - \lambda} |\mathcal{X}| n^{1/2}.
\end{align}

Since \(|\mathcal{A}| + \frac{1 - \lambda}{2} (MN - |\mathcal{A}|) \geq (1 - \lambda)MN\), we get
\begin{align}
(3.20) \quad |\mathcal{A}| \geq \frac{1 - \lambda}{1 + \lambda} MN = \left(1 - \frac{2\lambda}{1 + \lambda}\right) MN = (1 - \lambda^*) MN.
\end{align}

Furthermore,
\begin{align}
|\mathcal{A}^{-1} \sum_{(i,j) \in \mathcal{A}} \log |\mathcal{B}(j)| = |\mathcal{A}^{-1} \sum_{j=1}^{\mathcal{A}} |\mathcal{B}(j)| \log |\mathcal{B}(j)|
\geq |\mathcal{A}^{-1} \sum_{j: |\mathcal{B}(j)| > \frac{1 - \lambda^*}{n} M} |\mathcal{B}(j)| \log |\mathcal{B}(j)|
\geq |\mathcal{A}^{-1} \left(|\mathcal{A} - \frac{1}{n} |\mathcal{A}|\right) \log \frac{1 - \lambda^*}{n} M
\end{align}
\begin{align}
= \left(1 - \frac{1}{n}\right) \log \frac{1 - \lambda^*}{n} M,
\end{align}
and therefore by (3.19)
\begin{align}
\log M \leq \left(1 + \frac{2}{n}\right) \left(\sum_{i=1}^{n} I(X_i \wedge Z_i \mid Y_i) + \frac{3}{1 - \lambda} |\mathcal{X}| n^{1/2}\right) - \log (1 - \lambda^*)
+ \log n
\leq \sum_{i=1}^{n} I(X_i \wedge Z_i \mid Y_i) + c_1(\lambda)n^{1/2}.
\end{align}

Analogously,
\begin{align}
\log N \leq \sum_{i=1}^{n} I(Y_i \wedge Z_i \mid X_i) + c_2(\lambda)n^{1/2}
\end{align}
and by (3.18), (3.20) also
\begin{align}
\log MN \leq \sum_{i=1}^{n} I(Y_i \wedge Z_i \mid X_i) + c_3(\lambda)n^{1/2}.
\end{align}

Thus we have proved

\textit{Jr. Comb., Inf. & Syst. Sci.}
LEMMA 2. An \((n, M, N, \tilde{\lambda})\) code \(\{(u_i, v_j, D_{ij}) : 1 \leq i \leq M, 1 \leq j \leq N\}\) for the MAC satisfies for \(0 \leq \tilde{\lambda} < 1\) and \(c(\tilde{\lambda})\) suitable
\[
\log M \leq \sum_{i=1}^{n} I(X_i \wedge Z_i \mid Y_i) + c(\tilde{\lambda})n^{1/2},
\]
\[
\log N \leq \sum_{i=1}^{n} I(Y_i \wedge Z_i \mid X_i) + c(\tilde{\lambda})n^{1/2},
\]
\[
\log NM \leq \sum_{i=1}^{n} I(X_iY_i \wedge Z_i) + c(\tilde{\lambda})n^{1/2},
\]
where the distributions of the RV's are determined by the Fano-distribution on the code words \(\{(u_i, v_j) : (i, j) \in \mathcal{A}\}\). \(\mathcal{A}\) is defined in (3.13).

REMARK 2. This does not yet prove the Theorem, because \(X_i\) and \(Y_i\) are not necessarily independent.

4. WRINGING TECHNIQUES

To fix some ideas let us quickly recall the attempt of [7], which may be considered as the first "wringing idea". In order to gain the independence of \(X^n, Y^n\) mentioned in Remark 2 it would suffice to find for an \((n, M, N, \lambda)\) code a maximal error subcode of essentially the same rates, that is, a set \(\mathcal{A}^* = \mathcal{B}^* \times \mathcal{C}^*\) with \(\mathcal{B}^* \subset \{1, \ldots, M\}\), \(\mathcal{C}^* \subset \{1, \ldots, N\}\) such that

\[
W(D_{ij} \mid u_i, v_j) > \epsilon \quad \text{for} \quad (i, j) \in \mathcal{A}^*
\]

and

\[
|\mathcal{B}^*| \geq M \exp\{-o(n)\}, \quad |\mathcal{C}^*| \geq N \exp\{-o(n)\}.
\]

Abstractly the problem can be stated as follows:

Given \(\mathcal{A} \subset \{1, \ldots, M\} \times \{1, \ldots, N\}\), \(|\mathcal{A}| \geq 8MN\), \(M = \exp\{R_1n\}\), \(N = \exp\{R_2n\}\), does there exist an \(\mathcal{A}^* = \mathcal{B}^* \times \mathcal{C}^* \subset \mathcal{A}\) satisfying (4.2)?

This is exactly the problem of Zarankiewicz [13] for certain values of the parameters (there exists an extensive literature on this problem for \(|\mathcal{B}^*|, \quad |\mathcal{C}^*|\) small). In [17] we showed that the question has in general a negative answer and Dueck [5] proved that also the reduction to a maximal error subcode is in general impossible, because average and maximal error capacity regions can be different.

Next observe that the existence of subcodes with weaker properties suffices. It is enough that \(X^n\) and \(Y^n\) are almost independent. As a possible approach one might try to achieve this by considering a Quasi-Zarankiewicz problem in which the condition \(\mathcal{A}^* = \mathcal{B}^* \times \mathcal{C}^* \subset \mathcal{A}\) is replaced by

\[
|\mathcal{A}^* \cap \mathcal{B}(j)| \geq (1 - \eta)|\mathcal{B}^*|, \quad |\mathcal{A}^* \cap \mathcal{C}(j)| \geq (1 - \eta)|\mathcal{C}^*|
\]

for \(j \in \mathcal{C}^*, \; i \in \mathcal{B}^*\) and \(\eta\) close to 1.
Selecting $\mathcal{A}$ at random it is readily verified that this is in general again not possible for the parameters specified above.

However, in order to prove the strong converse via Lemma 2 it suffices to find subcodes, whose associated component variables $X_i, Y_i$ are almost independent for $i = 1, 2, \ldots, n$. The answer is given by Lemma 3 below.

Dueck's original solution is based on a wringing technique, which is slightly weaker (see Remark 3). He doesn't need to produce a sub-code, because he uses instead of Lemma 2 the method of blowing up decoding sets [4] in conjunction with Fano's Lemma.

**Lemma 3.** Let $X^n, Y^n$ be RV's with values in $\mathcal{X}^n, \mathcal{Y}^n$ resp. and assume that

$$\mathcal{I}(X^n \wedge Y^n) \leq \sigma.$$

Then for any $0 < \delta < \sigma$ there exist $t_1, \ldots, t_k \subseteq \{1, \ldots, n\}$, where $0 \leq k < \frac{2\delta}{\sigma}$, such that for some $\bar{x}_{t_1}, \bar{y}_{t_1}, \bar{x}_{t_2}, \bar{y}_{t_2}, \ldots, \bar{x}_{t_k}, \bar{y}_{t_k}$

$$\mathcal{I}(X_{t_1} \wedge Y_{t_1} | X_{t_2} = \bar{x}_{t_2}, Y_{t_2} = \bar{y}_{t_2}, \ldots, X_{t_k} = \bar{x}_{t_k}, Y_{t_k} = \bar{y}_{t_k}) \leq \delta$$

for $t = 1, 2, \ldots, n$, and

$$\Pr(X_{t_1} = \bar{x}_{t_1}, Y_{t_1} = \bar{y}_{t_1}, \ldots, X_{t_k} = \bar{x}_{t_k}, Y_{t_k} = \bar{y}_{t_k}) \geq \left(\frac{\delta}{|\mathcal{X}|^k|\mathcal{Y}|(2\sigma - \delta)}\right)^k.$$

**Proof.** If (4.1) does not hold already for $k = 0$, then for some $t_1$

$$\mathcal{I}(X_{t_1} \wedge Y_{t_1}) > \delta.$$

Since

$$\sigma \geq \mathcal{I}(X^n \wedge Y^n) \geq \mathcal{I}(X^n \wedge Y^n | X_{t_1}, Y_{t_1}) + \mathcal{I}(X_{t_1} \wedge Y_{t_1}),$$

we obtain

$$\mathcal{I}(X^n \wedge Y^n | X_{t_1}, Y_{t_1}) < \sigma - \delta.$$

Set

$$\sigma_1 = \sigma, \epsilon_1 = \frac{\delta}{2\sigma_1 - \delta}$$

and

$$A_n(\epsilon_1) = \{(x_i, y_i) : \Pr(X_i = x_i, Y_i = y_i) \geq \frac{\epsilon_1}{|\mathcal{X}|^2|\mathcal{Y}|}\}.$$

Then

$$\sigma_1 - \delta \geq \sum_{(x_{t_1}, y_{t_1}) \in A_n(\epsilon_1)} \mathcal{I}(X^n \wedge Y^n | X_{t_1} = x_{t_1}, Y_{t_1} = y_{t_1}) \Pr(X_{t_1} = x_{t_1}, Y_{t_1} = y_{t_1})$$

and since

$$\Pr((X_{t_1}, Y_{t_1}) \in A_n(\epsilon_1)) \leq \epsilon$$

there exists an $(\bar{x}_{t_1}, \bar{y}_{t_1}) \in A_n(\epsilon_1)$ such that

$$\sigma_1 - \delta \geq \mathcal{I}(X^n \wedge Y^n | X_{t_1} = \bar{x}_{t_1}, Y_{t_1} = \bar{y}_{t_1})(1 - \epsilon).$$

*Jr. Comb., Inf. & Syst. Sci.*
Using \((a_1 - \delta)(1 - \varepsilon_1)^{-1} = a_1 - \frac{\delta}{2}\) we get therefore

\[(4.3) \quad a_1 - \frac{\delta}{2} \geq I(X^n \wedge Y^n \mid X_{t_2} = \overline{x}_{t_2}, Y_{t_2} = \overline{y}_{t_2})\]

and

\[(4.4) \quad \Pr (X_{t_2} = \overline{x}_{t_2}, Y_{t_2} = \overline{y}_{t_2}) \geq \frac{\varepsilon_1}{|\mathcal{X}| |\mathcal{Y}|}.
\]

We repeat now the argument with the choices \(a_2 = a_1 - \frac{\delta}{2}, \varepsilon_2 = \frac{\delta}{2a_2 - \delta}\).

We are either done or there exists a \(t_2\) with

\[I(X_{t_2} \wedge Y_{t_2} \mid X_{t_2} = \overline{x}_{t_2}, Y_{t_2} = \overline{y}_{t_2}) > \delta.\]

Then

\[a_2 \geq I(X^n \wedge Y^n \mid X_{t_2} = \overline{x}_{t_2}, Y_{t_2} = \overline{y}_{t_2})\]

\[\geq I(X^n \wedge Y^n \mid X_{t_2} = \overline{x}_{t_2}, Y_{t_2} = \overline{y}_{t_2}, X_{t_2}, Y_{t_2})\]

\[+ I(X_{t_2} \wedge Y_{t_2} \mid X_{t_2} = \overline{x}_{t_2}, Y_{t_2} = \overline{y}_{t_2})\]

and there exists a pair \((\overline{x}_{t_2}, \overline{y}_{t_2})\) with

\[(4.5) \quad a_2 - \frac{\delta}{2} \geq I(X^n \wedge Y^n \mid X_{t_2} = \overline{x}_{t_2}, Y_{t_2} = \overline{y}_{t_2}, X_{t_2} = \overline{x}_{t_2}, Y_{t_2} = \overline{y}_{t_2}).\]

and with

\[(4.6) \quad \Pr (X_{t_2} = \overline{x}_{t_2}, Y_{t_2} = \overline{y}_{t_2} \mid X_{t_2} = \overline{x}_{t_2}, Y_{t_2} = \overline{y}_{t_2}) \geq \frac{\varepsilon_2}{|\mathcal{X}| |\mathcal{Y}|}.
\]

Iterating the argument with the choices \(a_i = a_{i-1} - \frac{\delta}{2}, \varepsilon_i = \frac{\delta}{2a_i - \delta} (i = 3, 4, \ldots)\) we obtain either for some \(i = k < \frac{2\sigma - \delta}{\delta}\),

\[I(X_t \wedge Y_t \mid X_t = \overline{x}_t, Y_t = \overline{y}_t, \ldots, X_{t_k} = \overline{x}_{t_k}, Y_{t_k} = \overline{y}_{t_k}) \leq \delta\]

or for \(k = \left\lfloor \frac{2\sigma}{\delta} \right\rfloor, a_k = a\left(\frac{2\sigma}{\delta} - 1\right)\frac{\delta}{2} \leq \delta,\) and hence again

\[\delta \geq a_k \geq I(X^n \wedge Y^n \mid X_t = \overline{x}_t, Y_t = \overline{y}_t, \ldots, X_{t_k} = \overline{x}_{t_k}, Y_{t_k} = \overline{y}_{t_k})\]

\[\geq I(X_t \wedge Y_t \mid X_t = \overline{x}_t, Y_t = \overline{y}_t, \ldots, X_{t_k} = \overline{x}_{t_k}, Y_{t_k} = \overline{y}_{t_k})\]

for \(t = 1, \ldots, n\).

In any case also

\[\Pr (X_{t_1} = \overline{x}_{t_1}, Y_{t_1} = \overline{y}_{t_1}, \ldots, X_{t_k} = \overline{x}_{t_k}, Y_{t_k} = \overline{y}_{t_k})\]

\[\geq \prod_{i=1}^{k} \frac{\varepsilon_i}{|\mathcal{X}| |\mathcal{Y}|} = \prod_{i=1}^{k} \frac{\delta}{|\mathcal{X}| |\mathcal{Y}| (2\sigma_i - \delta)} \geq \left(\frac{\delta}{|\mathcal{X}| |\mathcal{Y}| (2\sigma - \delta)}\right)^{k}.\]

Q.E.D.

Vol. 7, No. 3 (1982)
Remark 3. Dueck's result is that under the assumption of the Lemma $I(X_t \wedge Y_t | X_{t_1}Y_{t_1}, \ldots, X_{t_k}Y_{t_k}) \leq \delta$ for $i = 1, 2, \ldots, n$

and some $t_1, \ldots, t_k; k < \frac{\sigma}{\delta}$.

In the following it is convenient to adopt the notation:

For a RV $X^n = (X_1, \ldots, X_n)$ with values in $\mathcal{X}^n$ and distribution $P$ we define

$$P(x^n) = \Pr (X^n = x^n)$$

and

$$P(x_{s_1}, \ldots, x_{s_l}, x_{t_1}, \ldots, x_{t_m}) = \Pr (X_{s_1} = x_{s_1}, \ldots, X_{s_l} = x_{s_l}, X_{t_1} = x_{t_1}, \ldots, X_{t_m} = x_{t_m})$$

for any not necessarily distinct

$s_1, \ldots, s_l, t_1, \ldots, t_m \in \{1, \ldots, n\}$.

Lemma 4. Let $P$ and $Q$ be probability distributions on $\mathcal{X}^n$ such that for a positive constant $c$

$$(4.7) \quad P(x^n) = (1 + c)Q(x^n) \text{ for all } x^n \in \mathcal{X}^n,$$

then for any $0 < \gamma < c$, $0 \leq \epsilon < 1$ there exist $t_1, \ldots, t_k \in \{1, \ldots, n\}$, where

$0 \leq k \leq \frac{c}{\gamma}$, such that for some $\bar{x}_{t_1}, \ldots, \bar{x}_{t_k}$

$$(4.8) \quad P(x_{t_1} \mid \bar{x}_{t_1}, \ldots, \bar{x}_{t_k}) \leq \max \left((1 + \gamma)Q(x_{t_1} \mid \bar{x}_{t_1}, \ldots, \bar{x}_{t_k}), \epsilon\right)$$

for all $x_t \in \mathcal{X}$ and all $t = 1, 2, \ldots, n$

and

$$(4.9) \quad P(\bar{x}_{t_1}, \ldots, \bar{x}_{t_k}) \geq \epsilon^k.$$

Proof. If (4.8) does not hold already for $k = 0$, then for some $t_1$ and some $\bar{x}_{t_1}$

$$P(\bar{x}_{t_1}) > \max \left((1 + \gamma)Q(\bar{x}_{t_1}), \epsilon\right)$$

and we derive from (4.7)

$$(1 + c)Q(\bar{x}_{t_1}) \geq P(\bar{x}_{t_1}) > \max \left((1 + \gamma)Q(\bar{x}_{t_1}), \epsilon\right).$$

This insures (4.9) for $k = 1$ and $P(\bar{x}_{t_1}) > (1 + \gamma)Q(\bar{x}_{t_1}) > 0$. From (4.7) we can derive therefore

$$(4.10) \quad P(x^n \mid \bar{x}_{t_1}) \leq \frac{1 + c}{1 + \gamma} Q(x^n \mid \bar{x}_{t_1}) \text{ for all } x^n \in \mathcal{X}^n.$$
with
\[
\frac{1 + c}{1 + \gamma} Q(\vec{x}_n | \vec{x}_n) \geq P(\vec{x}_n | \vec{x}_n) > \max ((1 + \gamma)Q(\vec{x}_n | \vec{x}_n), \epsilon).
\]
This yields (4.9) for \(k = 2\) and implies with (4.10)
\[
P(x^n | \vec{x}_n, \vec{x}_n) \leq \frac{1 + c}{(1 + \gamma)^2} Q(x^n | \vec{x}_n, \vec{x}_n).
\]
Clearly, after \(k\) steps (without the procedure having ended before) (4.9) holds and
\[
P(x^n | \vec{x}_n, \vec{x}_n, \ldots, \vec{x}_n) \leq \frac{1 + c}{(1 + \gamma)^k} Q(x^n | \vec{x}_n, \ldots, \vec{x}_n),
\]
which implies
\[
P(x_t | \vec{x}_t, \vec{x}_t, \ldots, \vec{x}_t) \leq \frac{1 + c}{(1 + \gamma)^t} Q(x_t | \vec{x}_t, \ldots, \vec{x}_t)
\]
for all \(x_t \in \mathcal{X}, 1 \leq t \leq n.

Now for \(k + 1 \geq \frac{c}{\gamma} > \frac{\log (1 + c)}{\log (1 + \gamma)} : \frac{1 + c}{(1 + \gamma)^k} \leq 1 + \gamma. \text{ Q.E.D.}

**Corollary 2.** Let \(\mathcal{A} \subset \{1, \ldots, M\} \times \{1, \ldots, M\}, |\mathcal{A}| \geq (1 - \lambda^*)MN,\) and let \((u_i, v_i, D_{ij}) : (i, j) \in \mathcal{A}\) be a code for the MAC with maximal error probability \(\lambda^*\).

Then for any \(0 < \gamma < c = \frac{\lambda^*}{1 - \lambda^*}, 0 \leq \epsilon < 1\) there exist \(t_1, \ldots, t_k \in \{1, \ldots, n\},\) where \(k \leq \frac{\lambda^*}{\gamma(1 - \lambda^*)}\), and some \((\vec{x}_n, \vec{y}_n), \ldots, (\vec{x}_n, \vec{y}_n)\) such that
\[
\text{(4.12)} \quad \{(u_i, v_j, D_{ij}) : (i, j) \in \mathcal{A}\} \leq \mathcal{A} \cup \mathcal{A} : u_{tl} = \vec{x}_n, v_{jl} = \vec{y}_n, \text{ for } 1 \leq l \leq k\}
\]
is a subcode with maximal error \(\lambda\) and

(a) \(|\mathcal{A}| \geq e^k |\mathcal{A}|, \vec{M} = |\{u_i : (i,j) \in \mathcal{A}\}| \geq e^k M,\)

(b) \((1 + \gamma) \Pr (\vec{X}_t = x) \Pr (\vec{Y}_t = y) - \gamma - |\mathcal{X}| |\mathcal{Y}| e\)

\[
\leq \Pr (\vec{X}_t = x, \vec{Y}_t = y) \leq \max ((1 + \gamma) \Pr (\vec{X}_t = x) \Pr (\vec{Y}_t = y), \epsilon)
\]
for all \(x \in \mathcal{X}, y \in \mathcal{Y}, 1 \leq t \leq n.\)

\(\bar{X}_n = (\vec{X}_1, \ldots, \vec{X}_n), \bar{Y}_n = (\vec{Y}_1, \ldots, \vec{Y}_n)\) are distributed according to the Fano-distribution of the subcode.

**Proof.** Apply Lemma 4 with \(P\) as Fano-distribution of the code, that
is,
\[ P(x^n, y^n) = \Pr (X^n = x^n, Y^n = y^n) = \frac{1}{|\mathcal{A}|}, \]  
if \((x^n, y^n) = (u_i, v_j)\) for \((i, j) \in \mathcal{A}\)
and \(Q\) defined by
\[ Q(x^n, y^n) = \Pr (X^n = x^n) \Pr (Y^n = y^n), (x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n. \]

\(\mathcal{X}^n \times \mathcal{Y}^n\) takes the role of \(\mathcal{X}^n\) in the Lemma.

Now \(Q(x^n, y^n) = 0\) implies \(P(x^n, y^n) = 0\), \(Q(x^n, y^n) = \frac{1}{|\mathcal{A}|}\) implies
\(P(x^n, y^n) = \frac{1}{MN}\), and by our assumption on \(\mathcal{A}\), \(\frac{1}{|\mathcal{A}|} \leq \frac{1}{1 - \lambda^*} MN\).

Therefore (4.7) holds with \(c = \frac{1}{1 - \lambda^*} - 1 = \frac{\lambda^*}{1 - \lambda^*}\) and the Lemma
yields immediately (a) and the right side inequality in (b). This inequality
implies
\[
\Pr (\tilde{X}_i = x, \tilde{Y}_i = y) = 1 - \sum_{(x', y') \in (x, y)} \Pr (\tilde{X}_i = x', \tilde{Y}_i = y') \\
\geq 1 - \sum_{(x', y') \in (x, y)} \max ((1 + \gamma) \Pr (\tilde{X}_i = x', \tilde{Y}_i = y'), \epsilon) \\
\geq 1 - \|\mathcal{X}\| \|\mathcal{Y}\| \epsilon - (1 + \gamma)(1 - \Pr (\tilde{X}_i = x, \tilde{Y}_i = y)) \\
= (1 + \gamma) \Pr (\tilde{X}_i = x, \tilde{Y}_i = y) - \gamma - \|\mathcal{X}\| \|\mathcal{Y}\| \epsilon. \]

Q.E.D.

5. PROOF OF THE THEOREM

We simply have to combine Lemma 2 and Corollary 2.

For an \((n, M, N, \bar{\lambda})\) code \(\{u_i, v_j, D_{ij}\} : 1 \leq i \leq M, 1 \leq j \leq N\) define \(\mathcal{A}\)
as in (3.13). Then \(|\mathcal{A}| \geq (1 - \lambda^*) MN\) for \(\lambda^* = \frac{2\bar{\lambda}}{1 + \bar{\lambda}}\). Apply corollary
2 with the parameters
\((5.1)\) \(\gamma = n^{-1/2}, \epsilon = n^{-1}\).

Thus for some \(k \leq \frac{\lambda^*}{1 - \lambda^*} n^{1/2}\)
\((5.2)\) \(|\mathcal{A}| \geq \epsilon^k |\mathcal{A}| \geq n^{-\lambda^* n^{1/2}} (1 - \lambda^*) (1 - \lambda^*) M, \tilde{N} \geq n^{-\lambda^* n^{1/2}} (1 - \lambda^*)
 Application of Lemma 2 to this subcode yields
\[
\log M \leq \frac{\lambda^*}{1 - \lambda^*} n^{1/2} \log n + \log \bar{M} \\
\leq \sum_{i=1}^n I(\tilde{X}_i \wedge \tilde{Z}_i \mid \tilde{Y}_i) + C(\lambda)n^{1/2} \log n \\
\log N \leq \sum_{i=1}^n I(\tilde{Y}_i \wedge \tilde{Z}_i \mid \tilde{X}_i) + C(\lambda)n^{1/2} \log n
\]

\[ \log MN \leq \sum_{i=1}^{n} I(\tilde{X}_i, \tilde{Y}_i, \tilde{Z}_i) + C(\lambda) n^{1/2} \log n \]

with \[ C(\lambda) = c(\lambda) + \frac{\lambda^*}{1 - \lambda^*} - \log (1 - \lambda^*). \]

Since
\[ I(\tilde{X}_i, \tilde{Y}_i, \tilde{Z}_i) = H(\tilde{X}_i, \tilde{Y}_i) + H(\tilde{Z}_i) - H(\tilde{X}_i, \tilde{Y}_i, \tilde{Z}_i), \]
\[ I(\tilde{X}_i, \tilde{Z}_i | \tilde{Y}_i) = I(\tilde{X}_i, \tilde{Y}_i, \tilde{Z}_i) - I(\tilde{X}_i, \tilde{Z}_i) = H(\tilde{X}_i, \tilde{Y}_i) - H(\tilde{X}_i, \tilde{Y}_i, \tilde{Z}_i) - H(\tilde{X}_i) + H(\tilde{X}_i, \tilde{Z}_i), \]

etc., using (b) we complete the proof by showing that for \( n^{-1/2} \geq |\mathcal{X}|/|\mathcal{Q}|n^{-1} \)
\[ |H(\tilde{X}_i, \tilde{Y}_i) - H(\tilde{X}_i, \tilde{Y}_j)| \leq \text{const. } n^{-1/2} \log n \text{ etc.,} \]

where \( \Pr(\tilde{X}_i = x, \tilde{Y}_i = y) = \Pr(\tilde{X}_i = x) \Pr(\tilde{Y}_i = y). \)

Clearly,
\[ (1 + n^{-1/2}) \Pr(\tilde{X}_i = x) \Pr(\tilde{Y}_i = y) - 2n^{-1/2} \leq \Pr(\tilde{X}_i = x, \tilde{Y}_i = y) \leq (1 + n^{-1/2}) \Pr(\tilde{X}_i = x) \Pr(\tilde{Y}_i = y) + n^{-1} \]

and hence
\[ |\Pr(\tilde{X}_i = x) \Pr(\tilde{Y}_i = y) - \Pr(\tilde{X}_i = x, \tilde{Y}_i = y)| \leq 2n^{-1/2}. \]

This implies with
\[ \Pr(\tilde{Z}_i = z | \tilde{X}_i = x, \tilde{Y}_i = y) = w(z | xy) = \Pr(\tilde{Z}_i = z | \tilde{X}_i = x, \tilde{Y}_i = y) \]
\[ |\Pr(\tilde{X}_i = x, \tilde{Y}_i = y, \tilde{Z}_i = z) - \Pr(\tilde{X}_i = x, \tilde{Y}_i = y, \tilde{Z}_i = z)| \leq 2n^{-1/2} \]
for \( x \in \mathcal{X}, y \in \mathcal{Q}, z \in \mathcal{Z}. \)

For \( 0 \leq a \leq b \leq a + \text{const. } n^{-1/2} \leq 1 \) obviously
\[ |a \log a - b \log b| \leq \text{const. } n^{-1/2} \log n. \]

This and (5.5) imply (5.3). Q.E.D.

**Remark 4.** Using Lemma 3 instead of Lemma 4, one can proceed as follows:

1. One shows that for \( X^n, Y^n \) associated with the code \( I(X^n | Y^n) \leq \delta = f(\lambda). \)

2. Application of Lemma 3 and the analogue of Corollary 3 gives a subcode with the usual desired properties and \( I(X_i | Y_i) \leq \delta \) for \( 1 \leq i \leq n. \)

Since \( I(X_i, Y_i) \) is an \( I \)-divergence Pinsker's inequality implies
\[ \sum_{x,y} |\Pr(\tilde{X}_i = x, \tilde{Y}_i = y) - \Pr(\tilde{X}_i = x) \Pr(\tilde{Y}_i = y)| \leq 2\delta^{1/2}. \]

For \( \delta = n^{-1/2} \) this approach yields a strong converse with the weaker \( n^{3/4} \log n \)-deviation.

**Remark 5.** The fact that our question concerning the Quasi-Zarankiewicz problem has a negative answer has also the consequence that the
conclusion in Lemma 4 cannot be replaced by

\[(4.8^*) \quad P(x^n | \bar{x}_{n1}, \ldots, \bar{x}_{nt}) \leq \max ((1 + \gamma)Q(x^n | \bar{x}_{n1}, \ldots, \bar{x}_{nt}), \epsilon)\]

for all $x^n \in \mathcal{X}^n$ and $\bar{x}_{n1}, \ldots, \bar{x}_{nt}$ suitable

and (4.9)

if for instance $\epsilon \geq 1/n$.

REFERENCES


[Received : August 1980]