[12] W. M. Brown, "Sampling with random jitter," *J. SIAM*, vol. 11, no. 2, pp. 460–473, June 1963.
[13] W. Feller, *An Introduction to Probability Theory and Its Applications*, vol. II. New York: Wiley, 1966.
[14] P. Billingsley, *Convergence of Probability Measures.* New York: Wiley, 1968.
[15] H. E. Rowe, *Signals and Noise in Communication Systems.* Princeton, NJ: Van Nostrand, 1965.
[16] A. Papoulis, *Probability, Random Variables and Stochastic Processes.* New York: McGraw-Hill, 1965.

The Capacity of a Class of Broadcast Channels

ABBAS A. EL GAMAL, MEMBER, IEEE

Abstract—**The capacity region is established for those discrete memoryless broadcast channels $p(y,z|x)$ for which $I(X;Y) \geqslant I(X;Z)$ holds for all input distributions. The capacity region for this class of channels resembles the capacity region for degraded message sets considered by Körner and Marton.**

I. Introduction

The discrete memoryless broadcast channel $(\mathcal{X}, p(y,z|x), \mathcal{Y} \times \mathcal{Z})$ consists of three finite sets $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ and a probability transition matrix $p(y,z|x)$. Let $p_1(y|x)$ and $p_2(z|x)$ be the two marginals of $p(y,z|x)$, and let P_1 and P_2 denote the discrete memoryless channels with probability transition matrices $p_1(y|x)$ and $p_2(z|x)$, respectively. Recall the following three relations between P_1 and P_2.

Definition 1: Channel P_2 is said to be a *degraded* form of P_1 if there exists a probability transition matrix $p_3(z|y)$ such that

$$p_2(z|x) = \sum_{y \in \mathcal{Y}} p_1(y|x) p_3(z|y). \tag{1}$$

Definition 2: Channel P_1 is said to be *less noisy* than P_2 if

$$I(U;Z) \leqslant I(U;Y) \tag{2}$$

for every probability mass function of the form $p(u,x,y,z) = p(u)p(x|u)p(y,z|x)$.

Definition 3: Channel P_1 is said to be *more capable* than P_2 if

$$I(X;Z) \leqslant I(X;Y) \tag{3}$$

for all probability distributions on $\mathcal{X}$.

Manuscript received June 14, 1977; revised September 9, 1978. This work was supported in part by the National Science Foundation under Grant ENG 76-03684. This paper was presented at the IEEE International Symposium on Information Theory, Cornell University, Ithaca, NY, October 10–14, 1977.

The author was with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305. He is now with the Department of Electrical Engineering Systems, University of Southern California, University Park, Los Angeles, CA 90007.

The capacity region of the degraded broadcast channel (Definition 1) was found by Bergmans [1], Gallager [2], and Ahlswede and Körner [7] to be the set of all rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_0 + R_2 &\leqslant I(U;Z) \\ R_1 &\leqslant I(X;Y|U) \end{aligned} \tag{4}$$

where the distribution on $\mathcal{U} \times \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ is of the form $p(u)p(x|u)p(y,z|x)$.

Körner and Marton [3] introduced the "less noisy" and "more capable" concepts (Definitions 2 and 3) and showed that the "less noisy" relation is strictly weaker than the degraded relation [3, counterexample 1]. They also proved that the capacity region of the "less noisy" class of broadcast channels is given by (4).

Ahlswede gave the following example [3, counterexample 2] to show that the "more capable" relation is strictly weaker than both Definitions 1 and 2.

Example: Let $\mathcal{X}$ be the set $\mathcal{X} = \{1,2,3\}$, and let $\mathcal{Y} = \mathcal{Z} = \{1,2\}$. Consider the transition probability matrices

$$p_1\ (y|x\ ):\quad \begin{array}{c} \\ x=1 \\ x=2 \\ x=3 \end{array} \begin{array}{cc} y=1 & y=2 \\ \end{array} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

and

$$p_2\ (x|x\ ):\quad \begin{array}{c} \\ x=1 \\ x=2 \\ x=3 \end{array} \begin{array}{cc} z=1 & z=2 \\ \end{array} \begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}.$$

One easily checks that $I(X;Y) \geqslant I(X;Z)$ for every probability distribution on $\mathcal{X}$. However, for

$$U = f(X) = \begin{cases} 0, & \text{if } X=1 \text{ or } X=2 \\ 1, & \text{if } X=3 \end{cases}$$

and $p(x=1) = p(x=2) = \frac{1}{4}$, $p(x=3) = \frac{1}{2}$, we have $I(U;Y) = 0$ and $I(U;Z) > 0$.

0018-9448/79/0300-0166$00.75 ©1979 IEEE

In this paper the capacity of the class of "more capable" broadcast channels [4, open problem XXIII] is determined. First we show that achievability follows from Körner and Marton's proof of the coding theorem for the general broadcast channels with degraded message sets [5]. We then prove in detail a weak converse to establish that the achievable rate region is actually the capacity region.

II. Definitions and Statement of the Result

Before stating our result we recall the following standard definitions. The nth *extension* of the broadcast channel $(X, P(y,z|x), \mathcal{Y}\times\mathcal{Z})$ is the broadcast channel $(\mathcal{X}^n, P(\mathbf{y},\mathbf{z}|\mathbf{x}), \mathcal{Y}^n\times\mathcal{Z}^n)$, where

$$p(\mathbf{y},\mathbf{z}|\mathbf{x})=\prod_{i=1}^{n} p(y_i,z_i|x_i). \tag{5}$$

An $((M_0,M_1,M_2),n)$ *code* for a broadcast channel consists of three sets of integers

$$\mathfrak{M}_0=\{1,\cdots,M_0\},$$
$$\mathfrak{M}_1=\{1,\cdots,M_1\}, \tag{6}$$

and

$$\mathfrak{M}_2=\{1,\cdots,M_2\},$$

an encoding function

$$X:\quad \mathfrak{M}_0\times\mathfrak{M}_1\times\mathfrak{M}_2\to X^n, \tag{7}$$

and two decoding functions

$$g_1:\quad \mathcal{Y}^n\to\mathfrak{M}_0\times\mathfrak{M}_1; \qquad g_1(\mathbf{Y})=(\hat{W}_0,\hat{W}_1)$$
$$g_2:\quad \mathcal{Z}^n\to\mathfrak{M}_0\times\mathfrak{M}_2; \qquad g_2(\mathbf{Z})=\left(\hat{\hat{W}}_0,\hat{W}_2\right). \tag{8}$$

The set $\{\mathbf{x}(w_0,w_1,w_2)\colon (w_0,w_1,w_2)\in\mathfrak{M}_0\times\mathfrak{M}_1\times\mathfrak{M}_2\}$ is called the *set of codewords*. The integer w_0 has the interpretation of the *common part* of the message, while the integers w_1, w_2 are called the *independent part* of the message. Assuming a uniform distribution on the set of messages $\mathfrak{M}_0\times\mathfrak{M}_1\times\mathfrak{M}_2$, define

$$P_{e_1}^n=\frac{1}{M_0M_1M_2}\cdot\sum_{w_0,w_1,w_2\in\mathfrak{M}_0\times\mathfrak{M}_1\times\mathfrak{M}_2} P\{g_1(\mathbf{Y})\neq(w_0,w_1)|(w_0,w_1,w_2)\text{ sent}\}$$

$$P_{e_2}^n=\frac{1}{M_0M_1M_2}\cdot\sum_{w_0,w_1,w_2\in\mathfrak{M}_0\times\mathfrak{M}_1\times\mathfrak{M}_2} P\{g_2(\mathbf{Z})\neq(w_0,w_2)|(w_0,w_1,w_2)\text{ sent}\} \tag{9}$$

to be the *average probabilities of error* of the decoders g_1 and g_2, respectively.

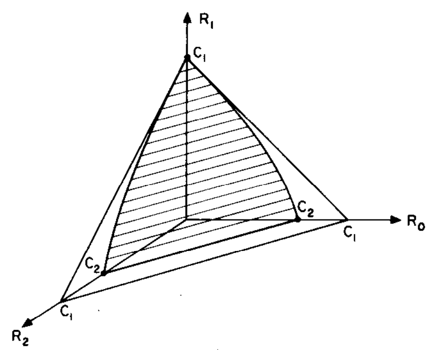

Fig. 1. Capacity region: $C_1=\max_{p(x)} I(X;Y)$; $C_2=\max_{p(x)} I(X;Z)$.

Also define the rate triple (R_0,R_1,R_2) of an $((M_0,M_1,M_2),n)$ code by

$$R_0=\frac{1}{n}\log M_0$$
$$R_1=\frac{1}{n}\log M_1$$
$$R_2=\frac{1}{n}\log M_2. \tag{10}$$

The rate (R_0,R_1,R_2) is said to be *achievable* by a broadcast channel if, for any $\epsilon>0$, there exists for all sufficiently large n, $((M_0,M_1,M_2),n)$ code with

$$M_0\geqslant 2^{nR_0}\qquad M_1\geqslant 2^{nR_1}\qquad M_2\geqslant 2^{nR_2} \tag{11}$$

such that

$$\max\{P_{e_1}^n,P_{e_2}^n\}<\epsilon.$$

The *capacity region* C for the broadcast channel is the set of all achievable rates (R_0,R_1,R_2). (see Fig. 1.)

The main result of the paper can now be stated.

Theorem 1 (Capacity Region): Let $(\mathcal{X}, P(y,z|x), \mathcal{Y}\times\mathcal{Z})$ be the broadcast channel defined above, and let U be an arbitrary random variable with cardinality $\|U\|\leqslant\|X\|+2$. If condition (3) holds then the capacity region C is given by

$$C=\{(R_0,R_1,R_2)\colon\quad R_0+R_1+R_2\leqslant I(X;Y),$$
$$R_0+R_1+R_2\leqslant I(X;Y|U)+I(U;Z),$$
$$R_0+R_2\leqslant I(U;Z),\ P\in\mathcal{P}\} \tag{12}$$

where $\mathcal{P}$ is the set of all probability mass functions of the form

$$p(u,x,y,z)=p(u)p(x|u)p(y,z|x). \tag{13}$$

It is easily seen that

1) the region is symmetric in R_0 and R_2,
2) the plane region (R_1,R_0) coincides with the degraded message sets region given in [5],
3) the plane region (R_0,R_2) is defined by
$$R_0+R_2\leqslant I(X;Z) \tag{14}$$
and also coincides with the region in [5] when condition (3) is imposed, and
4) for any fixed $R_1=r$ the plane region (R_0,R_2) is a triangle.

It is important to note that C is convex (see Appendix). Thus the usual convexification of the union of information regions is unnecessary.

III. The Achievability of C

First notice that because of the symmetry of C in R_0, R_2 it suffices to show that any $(R_0, R_1, 0)$ or $(0, R_1, R_2) \in C$ is achievable. It follows from 4) that, by time-sharing, any other rate triple in C can be achieved.

Theorem 2: Any $(R_0, R_1, 0) \in C$ is achievable.

Proof: It has been proved by Körner and Marton [5] that

$$(R_0, R_1, 0) \in C, \qquad \text{if and only if } R_0 \leqslant I(U;Z), \quad R_1 \leqslant I(X;Y|U), \; R_0 + R_1 \leqslant I(X;Y)$$

under the same conditions as in Theorem 1. Now clearly

$$(R_0, R_1, 0) \in C, \qquad \text{if and only if } (R_0 - t, R_1 + t, 0) \in C$$

for any $0 \leqslant t \leqslant R_0$, i.e., the common rate can be made partly or entirely private. This proves that the region of Körner and Marton can be written into the form

$$R_0 \leqslant I(U;Z)$$
$$R_0 + R_1 \leqslant I(X,Y|U) + I(U;Z)$$
$$R_0 + R_1 \leqslant I(X,Y).$$

Hence Theorem 2 follows. □

IV. The Converse

We now show the optimality of the achievable rate region C by proving a weak converse.

Theorem 3 (Weak Converse): If $(R_0, R_1, R_2) \notin C$, then there exists $\epsilon > 0$ such that

$$\max\{P_{e,1}^n, P_{e,2}^n\} \geqslant \epsilon, \qquad \text{for all } n.$$

Proof: Fano's inequality yields

$$H(W_0, W_1|\mathbf{Y}) \leqslant n(R_0 + R_1)P_{e,1}^n + h(P_{e,1}^n) \triangleq n\lambda_{1n} \tag{15a}$$

$$H(W_0, W_2|\mathbf{Z}) \leqslant n(R_0 + R_2)P_{e,2}^n + h(P_{e,2}^n) \triangleq n\lambda_{2n}. \tag{15b}$$

First consider

$$\begin{aligned} n(R_0 + R_1 + R_2) &\triangleq H(W_0, W_1, W_2) = H(W_0) + H(W_1) + H(W_2) \\ &= H(W_0, W_1) + H(W_0, W_2) - H(W_0) \\ &= I(W_0, W_1; \mathbf{Y}) + I(W_0, W_2; \mathbf{Z}) - I(W_0; \mathbf{Z}) \\ &\quad + H(W_0, W_1|\mathbf{Y}) + H(W_0, W_2|\mathbf{Z}) - H(W_0|\mathbf{Z}). \end{aligned}$$

Substituting from (15) we obtain

$$n(R_0 + R_1 + R_2) \leqslant I(W_2; \mathbf{Z}|W_0) + I(W_0, W_1; \mathbf{Y}) + n(\lambda_{1n} + \lambda_{2n}). \tag{16}$$

Similarly

$$n(R_0 + R_1 + R_2) \leqslant I(W_1; \mathbf{Y}|W_0) + I(W_0, W_2; \mathbf{Z}) + n(\lambda_{1n} + \lambda_{2n}), \tag{17}$$

and

$$n(R_0 + R_2) \triangleq H(W_0, W_2) \leqslant I(W_0, W_2; \mathbf{Z}) + n\lambda_{2n}. \tag{18}$$

Next we bound the right sides of (16), (17), and (18).

Lemma: Given any probability mass function on $W_0, W_1, W_2, \mathbf{X}, \mathbf{Y}, \mathbf{Z}$ of the form

$$p(w_0, w_1, w_2, \mathbf{x}, \mathbf{y}, \mathbf{z}) = p(w_0)p(w_1)p(w_2)p(\mathbf{x}|w_0, w_1, w_2) \cdot \prod_{i=1}^{n} p(y_i, z_i|x_i), \tag{19}$$

then

$$\text{1)} \quad I(W_2; \mathbf{Z}|W_0) + I(W_0, W_1; \mathbf{Y}) \leqslant \sum_{i=1}^{n} I(X_i; Y_i) \tag{20}$$

$$\text{2)} \quad I(W_1; \mathbf{Y}|W_0) + I(W_0, W_2; \mathbf{Z}) \leqslant \sum_{i=1}^{n} I(X_i; Y_i|U_i) + I(U_i; Z_i) \tag{21}$$

$$\text{3)} \quad I(W_0, W_2; \mathbf{Z}) \leqslant \sum_{i=1}^{n} I(U_i; Z_i) \tag{22}$$

where

$$U_i = (W_0, W_2, \mathbf{Y}_{i-1}, \mathbf{Z}^{i+1}),$$
$$\mathbf{Y}_{i-1} = (Y_1, \cdots, Y_{i-1}),$$

and

$$\mathbf{Z}^{i+1} = (Z_{i+1}, \cdots, Z_n), \qquad \text{for all } 1 \leqslant i \leqslant n. \tag{23}$$

Proof: First consider:

$$\begin{aligned} I(W_0, W_2; \mathbf{Z}) &= \sum_{i=1}^{n} I(W_0, W_2; Z_i|\mathbf{Z}^{i+1}) \\ &\leqslant \sum_{i=1}^{n} I(W_0, W_2, \mathbf{Z}^{i+1}; Z_i) \\ &\leqslant \sum_{i=1}^{n} I(U_i; Z_i). \end{aligned}$$

Next, using the independence of W_0, W_1, W_2, note that

$$I(W_1; \mathbf{Y}|W_0) \leqslant I(W_1; \mathbf{Y}|W_0, W_2),$$
$$I(W_2; \mathbf{Z}|W_0) \leqslant I(W_2; \mathbf{Z}|W_0, W_1). \tag{24}$$

Now consider 2):

$$\begin{aligned} I(W_1; \mathbf{Y}|W_0) &+ I(W_0, W_2; \mathbf{Z}) \\ &\leqslant \sum_{i=1}^{n} \left[I(W_1; Y_i|W_0, W_2 \mathbf{Y}_{i-1}) + I(W_0, W_2; Z_i|\mathbf{Z}^{i+1}) \right] \\ &\leqslant \sum_{i=1}^{n} \left[I(W_1; Y_i|W_0, W_2, \mathbf{Y}_{i-1}, \mathbf{Z}^{i+1}) \right. \\ &\quad + I(\mathbf{Z}^{i+1}; Y_i|W_0, W_2, \mathbf{Y}_{i-1}) + I(W_0, W_2, \mathbf{Z}^{i+1}, \mathbf{Y}_{i-1}; Z_i) \\ &\quad \left. - I(\mathbf{Y}_{i-1}; Z_i|W_0, W_2, \mathbf{Z}^{i+1}) \right]. \end{aligned}$$

It can be shown [6, lemma 7] that a summation by parts yields

$$\sum_{i=1}^{n} I(\mathbf{Z}^{i+1}; Y_i | W_0, W_2, \mathbf{Y}_{i-1}) = \sum_{i=1}^{n} I(\mathbf{Y}_{i-1}; Z_i | W_0, W_2, \mathbf{Z}^{i+1}). \quad (25)$$

Hence two terms cancel in (24), and

$$\begin{aligned} I(W_1; \mathbf{Y} | W_0) + I(W_0, W_2; \mathbf{Z}) &\leqslant \sum_{i=1}^{n} I(W_1; Y_i | U_i) + I(U_i; Z_i) \\ &\leqslant \sum_{i=1}^{n} [I(X_i; Y_i | U_i) + I(U_i; Z_i)] \end{aligned}$$

since $W_1 U_i \rightarrow X_i \rightarrow (Y_i, Z_i)$ form a Markov chain in this order for all $1 \leqslant i \leqslant n$. Similarly consider 1):

$$\begin{aligned} &I(W_2; \mathbf{Z} | W_0) + I(W_0, W_1; \mathbf{Y}) \\ &\leqslant \sum_{i=1}^{n} [I(W_2; Z_i | W_0, W_1, \mathbf{Z}^{i+1}) + I(W_0, W_1; Y_i | \mathbf{Y}_{i-1})] \\ &\leqslant \sum_{i=1}^{n} [I(W_2; Z_i | W_0, W_1, \mathbf{Z}^{i+1}, \mathbf{Y}_{i-1}) \\ &\quad + I(\mathbf{Y}_{i-1}; Z_i | W_0, W_1, \mathbf{Z}^{i+1}) \\ &\quad + I(W_0, W_1, \mathbf{Z}^{i+1}, \mathbf{Y}_{i-1}; Y_i) \\ &\quad - I(\mathbf{Z}^{i+1}; Y_i | W_0, W_1, \mathbf{Y}_{i-1})]. \end{aligned} \quad (26)$$

Replacing W_2 by W_1 in (25) and substituting in (26) gives

$$\begin{aligned} I(W_2; \mathbf{Z} | W_0) + I(W_0, W_1; \mathbf{Y}) &\leqslant \sum_{i=1}^{n} [I(W_2; Z_i | U_i') + I(U_i'; Y_i)] \\ &\leqslant \sum_{i=1}^{n} [I(X_i; Z_i | U_i') + I(U_i'; Y_i)] \end{aligned}$$

where $U_i' \triangleq (W_0, W_1, \mathbf{Y}_{i-1}, \mathbf{Z}^{i+1})$ and $W_2 U_i' \rightarrow X_i \rightarrow (Y_i, Z_i)$ form a Markov chain in this order for all $1 \leqslant i \leqslant n$.

It can be shown that (3) implies

$$I(X; Z | U) \leqslant I(X; Y | U) \quad (27)$$

for all $U \rightarrow X \rightarrow (Y, Z)$. Thus

$$\begin{aligned} I(W_2; \mathbf{Z} | W_0) + I(W_0, W_1; \mathbf{Y}) &\leqslant \sum_{i=1}^{n} [I(X_i; Y_i | U_i') + I(U_i'; Y_i)] \\ &= \sum_{i=1}^{n} I(X_i; Y_i), \end{aligned}$$

and the proof of the lemma is completed. □

Combining the lemma and (16), (17), and (18), it is easy to show that there exists an auxiliary random variable U such that

$$p(u,x,y,z) = p(u)p(x|u)p(y,z|x), \quad (28)$$

and the rate triple (R_0, R_1, R_2) satisfies the inequalities in (12).

To complete the proof of the converse we have to show that there exists a random variable U^* with $\|U^*\| \leqslant \|X\| + 2$ that yields the same mutual information quantities as U. This proof uses standard techniques (e.g., see [7]) and will not be repeated here. □

A Final Remark: Janos Körner pointed out to the author that Theorem 1 is intuitively clear since by the alternative definition of the "more capable," relation (3), every ϵ-code for channel P_2 is an ϵ-code for P_1. Therefore the private information to Z can always be incorporated as common information to both Y and Z.

Acknowledgment

The author would like to thank Prof. Thomas Cover and Dr. Janos Körner for invaluable comments during the preparation of this paper.

Appendix

C is Convex: Let (U_i, X_i, Y_i, Z_i), $i = 1, 2$, be two collections of random variables with probability mass functions in $\mathcal{P}$, and let T be a random variable taking on values 1, 2 with probabilities α and $\bar{\alpha}$, respectively. For $T = i$ define $U_T = U_i$, $X = X_i$, $Y = Y_i$, and $Z = Z_i$. Then $(T, U_T) \rightarrow X \rightarrow (Y, Z)$ form a Markov chain in this order. Now consider

$$\begin{aligned} \alpha I(X_1; Y_1) + \bar{\alpha} I(X_2; Y_2) &= \alpha I(X_1; Y_1 | U_1) + \alpha I(U_1; Y_1) \\ &\quad + \bar{\alpha} I(X_2; Y_2 | U_2) + \bar{\alpha} I(U_2; Y_2) \\ &= I(U_T; Y | T) + I(X; U_T, T) \\ &\leqslant I(U_T, T; Y) + I(X; Y | U_T, T) \\ &= I(X; Y). \end{aligned}$$

Next

$$\begin{aligned} &\alpha I(X_1; Y_1 | U_1) + \alpha I(U_1; Z_1) + \bar{\alpha} I(X_2; Y_2 | U_2) + \alpha I(U_2; Z_2) \\ &= I(X; Y | U_T, T) + I(U_T; Z | T) \\ &\leqslant I(X; Y | U_T, T) + I(U_T, T; Z), \end{aligned}$$

and

$$\alpha I(U_1; Z_1) + \bar{\alpha} I(U_2; Z_2) = I(U_T; Z | T) \leqslant I(U_T, T; Z).$$

References

[1] P. Bergmans, "Coding theorem for broadcast channels with degraded components," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 197–207, Mar. 1973.

[2] R. G. Gallager, "Capacity and coding for degraded broadcast channels," *Probl. Peredac. Inform.*, vol. 10, no. 3, pp. 3–14, 1974.

[3] J. Körner and K. Marton, "A source network problem involving the comparison of two channels II," in *Trans. Colloquium Inform. Theory*, Keszthely, Hungary, Aug. 1975.

[4] E. van der Meulen, "A survey of multi-way channels in information theory," *IEEE Trans. Inform. Theory*, vol. IT-23, no. 1, pp. 1–37, Jan. 1977.

[5] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. Inform. Theory*, vol. IT-23, no. 1, pp. 60–64, Jan. 1977.

[6] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[7] R. F. Ahlswede and J. Körner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Inform. Theory*, vol. IT-21, no. 6, pp. 629–637, Nov. 1975.