Electronics Research Laboratory
University of California
Berkeley, California

ON CHANNEL CAPACITY

by

E. Eisenberg

The research reported herein is made possible through support received from the Departments of Army, Navy, and Air Force under grant AF-AFOSR-139-63.

November 4, 1963

ON CHANNEL CAPACITY*

by E. Eisenberg†

Summary— Necessary and sufficient conditions are given for a set of input probabilities to achieve capacity in a memoryless, discrete, constant channel. These conditions are then applied to show that optimal output probabilities are unique and all positive. With respect to the problem of calculating the capacity of a channel, two approaches are discussed; the first method considers the dual of the given problem, and in that case the solution may be obtained by standard convex programming techniques. The second computational method is heuristic and is known to converge (in a finite number of steps) only when the number of output symbols is two, yet there is strong evidence to believe that with some modifications it can be made convergent in all cases with finite output (and input) alphabets.

*The research reported herein is made possible through support received from the Departments of Army, Navy, and Air Force under grant AF-AFOSR-139-63.

†College of Engineering, University of California, Berkeley, California.

The problem of computing the capacity of a discrete, constant channel is the following: given an $m \times n$ matrix $P = [p_{ij}]$, where each row of P represents a probability distribution, to

find $\quad y = (y_1, \ldots, y_m)$ which

maximizes $\quad F(y) = \sum_{i,j} y_i p_{ij} \log \left[\frac{p_{ij}}{\sum_s y_s p_{sj}} \right] \quad (1)$

subject to $\quad y \geq 0, \; \sum_{i=1}^{m} y_i = 1.$

In order to avoid inessential arguments we assume that each column of P has at lease one positive entry. It should also be noted that the logarithm is taken with respect to an arbitrary fixed basis $b > 1$. We shall find it convenient to use the following abbreviation:

$$r_i = \sum_{j=1}^{n} p_{ij} \log p_{ij} \, . \tag{2}$$

In these terms, the function F may be expressed by:

$$F(y) = \sum_{i=1}^{m} y_i r_i - \sum_{j=1}^{n} \left[\sum_{i=1}^{m} y_i p_{ij} \right] \log \left[\sum_{s=1}^{m} y_s p_{sj} \right] . \tag{3}$$

That the problem described by (1) is nontrivial in general can be seen from the fact that in Ref. 4, p. 136 it is stated incorrectly that y is a solution of (1) if, and only if,

$$C = r_i - \sum_{j=1}^{n} p_{ij} \log\left[\sum_{s=1}^{m} y_s p_{sj}\right] \qquad \text{for } i=1,\ldots, m$$

and (4)

$$y \geq 0, \quad \sum_{i=1}^{m} y_i = 1.$$

That (4) need not hold for any optimizing y can be seen by taking

$$P = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{3} & \frac{2}{3} \\ \frac{3}{8} & \frac{5}{8} \end{bmatrix} .$$

It is readily checked that in this case $y = (1753)^{-1}(1163, 590, 0)$ is the only optimal y and the first condition in (4) is violated when $i = 3$. Furthermore, a procedure advocated in Ref. 4, p. 139 for finding a solution of (1), and based on (4), may yield an incorrect answer. The procedure in question is this: solve (4) without requiring $y \geq 0$, (it is not clear that a solution will always exist); if it turns out that $y \geq 0$, then we have a desired y. The difficulty arises in case some y_i turn out negative. It is then suggested in Ref. 4 that one solve the m problems generated by (4) when letting one $y_i = 0$ at a time. If any of the y's thus obtained satisfies $y \geq 0$ then the one with largest $F(y)$ is accepted as a solution to (1), otherwise set two of the y_i's equal to zero, etc. It is not clear whether the first relation in (4), for that y_i which is zero, is retained or not. If it is retained one is certainly going to be in trouble as can be seen from the example cited above. If the particular relation is omitted one may get into difficulties too in case two of the y_i's must be zero at an optimum. This will be the case when:

$$P = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{3} & \frac{2}{3} \\ \frac{3}{8} & \frac{5}{8} \\ \frac{3}{8} & \frac{5}{8} \end{bmatrix} .$$

With respect to (4) the correct statement is:

Theorem 1: The vector y is a solution of (1) if, and only if,

$$y \geq 0, \quad \sum_{i=1}^{m} y_i = 1 \tag{5a}$$

$$\sum_{i=1}^{m} y_i p_{ij} > 0 \quad , \quad \text{all } j = 1, \ldots, n \tag{5b}$$

$$F(y) \geq r_i - \sum_{j=1}^{n} p_{ij} \log \left[\sum_{s=1}^{m} y_s p_{sj} \right], \text{ all } i = 1, \ldots, m. \tag{5c}$$

A proof of Theorem 1 will be found in the appendix.

In order to relate conditions (4) (which are sufficient, but not always necessary, for capacity) with Theorem 1 we observe that if one multiplies (5c) by y_i and then sums over all i one obtains

$F(y) \geq F(y)$, thus equality must hold in (5c) whenever $y_i > 0$, but the crucial point is that when $y_i = 0$ (5c) must still hold, though it may turn out to be a strict inequality.

A fundamental tool needed to establish Theorem 1, as well as other pertinent results, is the following well-known

Lemma 1: Let a_j, b_j $(j = 1, \ldots, n)$ be given (real) numbers which satisfy $a_j \geq 0$, $b_j > 0$, all j, and $\Sigma_{j=1}^{n} a_j > 0$. Then,

$$\sum_{j=1}^{n} a_j \log \left[\frac{b_j}{\sum_{k=1}^{n} b_k} \right] \leq \sum_{j=1}^{n} a_j \log \left[\frac{a_j}{\sum_{k=1}^{n} a_k} \right] . \qquad (6)$$

Furthermore, equality holds in (6) if, and only if, there exists a number λ such that $a_j = \lambda b_j$ for all $j = 1, \ldots, n$.*

One of the important consequences of Theorem 1 and Lemma 1 is that if y and y' both solve (1), then, even though y need not equal y', we must have:

Theorem 2: (Uniqueness of optimal output probabilities): If the vectors y and y' both satisfy (1) and if we let

$$q_j = \sum_{i=1}^{m} y_i p_{ij}, \quad q'_j = \sum_{i=1}^{m} y'_i p_{ij}, \quad \text{for all } j = 1, \ldots, n,$$

then

$$q_j = q'_j \quad \text{for all } j.$$

The proof is immediate: by Theorem 1 we know that

---

*For details the reader may refer to Lemma 1 on page 13 and remark 2.i on page 20 in Ref. 5.

$$F(y) = F(y') \geqq \sum_{i=1}^{m} y_i r_i - \sum_{j=1}^{n} \sum_{i=1}^{m} y_i p_{ij} \log q'_j$$

$$\geqq \sum_{i=1}^{n} y_i r_i - \sum_{j=1}^{n} q_j \log q_j = F(y),$$

by Lemma 1. Thus, again by Lemma 1, there exists a scalar λ such that $q_j = \lambda q'_j$ for all $j = 1, \ldots, n$. But $\Sigma_{j=1}^{n} q_j = \Sigma_{j=1}^{n} q'_j = 1$, and thus $\lambda = 1$, as required.

It should be re-emphasized here that the optimal input probabilities, i.e., the y satisfying (1), need not be unique; this can be illustrated by the almost trivial example when each p_{ij} is independent of i (or equivalently, when the capacity of the given channel is zero), and consequently any y satisfying $y \geqq o$, $\Sigma_{i=1}^{m} y_i = 1$ will solve (1).

We now turn our attention to the problem of finding a solution of (1), or of (5), in practice. It is known that the function $F(y)$, in (1) is a concave function, thus (1), its constraints being linear, is a convex programming problem, and may be treated by standard methods (Ref 2). However, we may wish to make use of a convex programming method which requires that all functions in question possess gradients, and clearly F is not necessarily differentiable at points where some $y_i = 0$. It is possible, though, to state a convex programming problem which is, in a sense, equivalent to (1) and which enjoys the property that all its functions are differentiable. The problem is:

find α and $\omega = (\omega_1, \ldots, \omega_n)$

which minimize α, subject to

$$\alpha \geq r_i - \sum_{j=1}^{n} \omega_j p_{ij}, \quad i=1, \ldots, m \qquad (7)$$

$$\sum_{j=1}^{n} e^{\omega_j} \leq 1.$$

The correspondence between (1) and (7) is: If y solves (1), then $\alpha = F(y)$, $\omega_j = \log \left(\Sigma_{s=1}^{m} y_s p_{sj}\right)$ solve (7). If α, ω solve (7), then let $x_j = e^{\omega_j}\left[\Sigma_{k=1}^{n} e^{\omega_k}\right]^{-1}$ and any solution y of

$$y = (y_1, \ldots, y_m) \geq 0 \tag{8}$$
$$\sum_{i=1}^{m} y_i p_{ij} = y_j, \quad j = 1, \ldots, n$$

will then be a solution of (1). The important point is that, providing α, ω solve (6), there will always exist a solution of (8). The proof of the above described equivalence between (1) and (7) is not difficult, it may be established by using duality results for convex-homogeneous programming (Ref. 1); in the appendix a direct proof of this equivalence is provided. The interest of (7) lies, among other things,* in the fact that in order to solve it one may apply any convex programming technique which requires that all functions entering the problem be differentiable, a convenient description of some pertinent methods may be found in Ref. 6. These methods, being quite general, only guarantee that a solution is obtained as a limit of a convergent process. Providing the convergence rate is reasonable such methods are quite satisfactory from the practical point of view. At the same time it would be of interest, both theoretical and practical, to have a method which yields a solution to (1) in a finite number of steps. We will now describe such a method, which is

*In the appendix we use another form of (7) to prove Theorem 1; in fact, it appears, and the reasons are not quite clear, that the most direct way to prove Theorem 1 is to consider (7) rather than (1).

known to yield a solution after a finite number of steps when n, the number of output symbols, is two; it also may, with some slight modifications, do the same for any n; this last is still an open question, and one of the purposes of this note is to draw attention to this problem.

The algorithm is as follows: take any $x = (x_1, \ldots, x_n)$ such that $x_j > 0$ all j, and $\Sigma_{j=1}^{n} x_j = 1$. Next calculate

$$M = \min_{i=1,\ldots,m} \left[-r_i + \sum_{j=1}^{n} p_{ij} \log x_j \right],$$

$$I = \left\{ i \,\middle|\, M = -\sum_{j=1}^{n} p_{ij} \log \left(\frac{p_{ij}}{x_j} \right) \right\}. \tag{9}$$

The next step is to solve the following linear programming problem:

find $y = (y_1, \ldots, y_m)$

which maximizes $\sum_{i=1}^{n} y_i$, subject to (10)

$$y \geq 0, \quad \sum_{i=1}^{m} y_i p_{ij} \leq x_j \quad \text{all } j = 1, \ldots, n, \quad y_i = 0 \text{ if } i \notin I.$$

Problem (10) always has a solution with $y \neq 0$ and $0 \leq \Sigma_{i=1}^{m} y_i < 1$. If $\Sigma_{i=1}^{m} y_i = 1$, then $yP = x$ and we have a solution to (1). Otherwise, $\mu = \Sigma_{i=1}^{m} y_i$ is strictly between 0 and 1, and $\Sigma_{i=1}^{m} y_i p_{ij} < x_j$ for some j.

Let

$$J = \left\{ j \;\middle|\; \sum_{i=1}^{m} y_i p_{ij} = x_j \right\}$$

$$\theta = \sum_{j \in J} x_j, \quad \sigma_i = \sum_{j \in J} p_{ij}$$

$$\lambda_1 = \max_{j \notin J} \frac{1}{x_j} \sum_{i=1}^{m} y_i p_{ij}$$

$$\lambda_2 = \max_{\substack{i \in I,\ s \notin I \\ \sigma_s < \sigma_i}} \left[\exp \frac{M - d_s}{\sigma_i - \sigma_s} \right]$$

$$\lambda = \max(\lambda_1, \lambda_2)$$

where

$$d_i = - \sum_{j=1}^{n} p_{ij} \log \left(\frac{p_{ij}}{x_j} \right) .$$

We now modify x according to the formula

$$x_j' = \begin{cases} x_j \left[\lambda + (1 - \lambda)\theta\right]^{-1} & \text{if } j \in J \\ x_j \lambda \left[\lambda + (1 - \lambda)\theta\right]^{-1} & \text{if } j \notin J \end{cases} .$$

Next one recalculates M with the new x', then proceeds to (9), (10), etc. This process will yield the answer [i. e., a maximum of 1 in (10)] in a finite number of steps providing $n = 2$.

APPENDIX

In order to prove Theorem 1 and to establish the correspondence between (1) and (7) we require:

Lemma 2: Consider the following problem: find, if possible, the minimum of the set

$$S = \left\{ \mu \;\middle|\; \exists q = (q_1, \dots, q_n) > 0 \text{ with } \sum_{j=1}^{n} q_j \leqq 1 \text{ and } \mu \geqq r_i - \sum_{j=1}^{n} p_{ij} \log q_j, \text{ all } i=1,\dots,m \right\}.$$

We conclude that S always has a minimum μ_o and, furthermore, if $q^{(o)} = (q_1^{(o)} \dots, q_n^{(o)})$ are the corresponding quantities given by the definition of S then there exists a vector $y = (y_1, \dots, y_m)$ such that

$$y \geqq 0, \sum_{i=1}^{m} y_i = 1$$

$$F(y) = \mu_o \quad \text{and} \tag{11}$$

$$q_j^{(o)} = \sum_{i=1}^{m} y_i p_{ij} > 0, \text{ all } j=1, \dots, n.$$

Proof: We first show the existence of a minimum. Let μ_o be the infimum of S, μ_o is well defined because S is nonempty and bounded below; there must then exist sequences

μ_k and $q^{(k)} = (q_1^{(k)}, \ldots, q_n^{(k)})$, for $k = 1, 2, \ldots$ satisfying

$$\left.\begin{aligned} & q^{(k)} > 0 , \quad \sum_{j=1}^{n} q_j^{(k)} \leqq 1 \\ & \mu_k \geqq r_i - \sum_{j=1}^{n} p_{ij} \log q_j^{(k)} , \quad \text{all } i \end{aligned}\right\} \quad k = 1, 2, \ldots \tag{12}$$

$$\lim_{k \to \infty} \mu_k = \mu_o \ .$$

It is clear that every limit point of the sequence $\{q^{(k)}\}_{k=1}^{\infty}$ must be strictly positive, because otherwise we would have $\mu_o = \infty$; taking $q^{(o)}$ to be any limit point of the sequence in question it follows that (12) holds for $k = 0$ as well, which establishes the existence of a minimum for S.

We next consider the system of inequalities in μ and $q = (q_1, \ldots, q_n)$:

$$\begin{aligned} & q_j > 0 , \quad j=1, \ldots, n \\ & 1 - \sum_{j=1}^{n} q_j > 0 \\ & \mu - r_i + \sum_{j=1}^{n} p_{ij} \log q_j > 0, \quad \text{all } i=1, \ldots, m \\ & \mu_o - \mu > 0. \end{aligned} \tag{13}$$

Since μ_o is the minimum of S, the system (13) cannot have a solution μ, q. Applying the fundamental theorem of Fan, Glicksberg, and Hoffman, on the solvability of convex inequalities (Ref. 3), it follows that there must exist scalars λ_1, λ_2 and a vector $\beta = (\beta_1, \ldots, \beta_m)$ satisfying

$$\lambda_1,\ \lambda_2,\ \beta_i \geqq 0,\ \lambda_1 + \lambda_2 + \sum_{i=1}^{m} \beta_i > 0 \text{ and}$$

$$\lambda_1\left(1 - \sum_{j=1}^{n} q_j\right) + \lambda_2 (\mu_o - \mu) + \sum_{i=1}^{m} \beta_i \left[\mu - r_i + \sum_{j=1}^{n} p_{ij} \log q_j\right] \leqq 0 \tag{14}$$

for all scalars μ and all vectors $q = (q_1, \ldots, q_n) > 0$.

One deduces from (14) that

$$\lambda_2 = \sum_{i=1}^{m} \beta_i > 0 ,$$

because otherwise $\lambda_2 = 0$ and $\beta = 0$, thus $\lambda_1 > 0$ and, by (14) $\Sigma_{j=1}^{n} q_j \geqq 1$ for all $q > 0$, which is obviously not the case. Letting $y = \lambda_2^{-1} \beta$ and using the relation between λ_2 and β, we obtain from (14) ; (with $\lambda_1' = \lambda_2^{-1} \lambda_1$)

$$y \geqq 0,\ \sum_{i=1}^{m} y_i = 1,$$

$$\mu_o \leqq \sum_{i=1}^{m} y_i r_i - \sum_{j=1}^{n} \left[\sum_{i=1}^{m} y_i p_{ij}\right] \log q_j + \lambda_1' \left[-1 + \sum_{j=1}^{n} q_j\right] \tag{15}$$

whenever $q = (q_1, \ldots, q_n) > 0$.

In (15) let $q = q^{(o)}$ be the minimizing vector obtained earlier in the proof; then using the fact that $q^{(o)}$ satisfies (12) with k = 0 we find that $\lambda_1' \left[-1 + \Sigma_{j=1}^{n} q_j^o\right] = 0$, and either $\lambda_1' = 0$ or $\Sigma_{j=1}^{n} q_j^0 = 1$. It cannot be that $\lambda_1' = 0$ because then, from (15), we would obtain $\mu_o = -\infty$, consequently

$$\sum_{j=1}^{n} q_j^o = 1 . \tag{16}$$

Next, let ϵ be a positive number and let

$$q_j = \epsilon + \sum_{i=1}^{m} y_i p_{ij}, \quad \text{all } j=1, \ldots, n.$$

If we substitute the above values of q_j in (15) and then let ϵ approach zero, we find that $\mu_o \leqq F(y)$; at the same time, since (12) holds for k = 0, we find that

$$\begin{aligned} F(y) \geqq \mu_o &\geqq \sum_{i=1}^{m} y_i r_i - \sum_{j=1}^{n} \left[\sum_{i=1}^{m} y_i p_{ij}\right] \log q_j^{(o)} \\ &\geqq \sum_{i=1}^{m} y_i r_i - \sum_{j=1}^{n} \left[\sum_{i=1}^{m} y_i p_{ij}\right] \log \left[\sum_{s=1}^{m} y_s p_{sj}\right] = F(y). \end{aligned} \tag{17}$$

The second part of the above inequality is obtained using Lemma 1; since equality must prevail in (17) Lemma 1 tells us, because $\Sigma_{j=1}^{n} \Sigma_{i=1}^{m} y_i p_{ij} = \Sigma_{j=1}^{n} q_j^{(o)} = 1$, that y and $q^{(o)}$ satisfy conditions (11), as required.

A straightforward check reveals that the y described in the statement of Lemma 2 [i.e., satisfying (11)] satisfied conditions (5). We thus have:

Corollary 1: There always exists a y satisfying (5).

The proof of Theorem 1 is now immediate: The fact that if y satisfies (5) then it solves (1) is a direct application of Lemma 1. Conversely, if $\bar{y}$ solves (1) then, comparing $\bar{y}$ with the y given by Corollary 1 (or Lemma 2) we see that $F(y) = F(\bar{y})$; if we multiply (5c) by $\bar{y}_i$ then sum over all i and apply Lemma 1 it follows then, as in the proof of Theorem 2, that

$$\sum_{i=1}^{m} y_i p_{ij} = \sum_{i=1}^{m} \bar{y}_i p_{ij}, \quad \text{all } j=1,\ldots,n$$

and thus $\bar{y}$ must satisfy (5).

As a final result we demonstrate the relation between (7) and (1). First, it is clear that (1) and the finding of the minimum of the set S in Lemma 2 are equivalent in the sense that the minimizing $q^{(o)}$ of S is precisely the unique output probability distribution described by Theorem 2. If, in addition, one observes that (7) is simply a restatement of the minimizing problem for S with $\omega_j = \log q_j$, the correspondence between (1) and (7) becomes obvious.

ACKNOWLEDGMENT

The author is pleased to acknowledge helpful discussions of this work with Prof. A. J. Thomasian of the University of California, Berkeley, California.

REFERENCES

1. E. Eisenberg, "Duality in homogeneous programming," Proc. Am. Math. Soc., Vol. 12, No. 5, pp. 783-787; 1961.

2. George B. Dantzig, Linear Programming and Extensions, Princeton University Press, 1963.

3. Ky Fan, I. Glicksberg and A. J. Hoffman, "Systems of inequalities involving convex functions," Proc. Am. Math. Soc., Vol. 8, pp. 617-622; 1957.

4. Robert M. Fano, Transmission of Information —A Statistical Theory of Communications, M.I.T. Press and John Wiley and Sons, New York, 1961.

5. Amiel Feinstein, Foundations of Information Theory, Mc Graw-Hill, New York, 1958.

6. Philip Wolfe, "Recent developments in nonlinear programming," The RAND Corporation, R-401-PR, May 1962.