THE CAPACITIES OF CERTAIN CHANNEL CLASSES UNDER RANDOM CODING[1]

By David Blackwell, Leo Breiman, and A. J. Thomasian

University of California, Berkeley

1. Introduction and Summary. For any two finite sets U, V, a Markov matrix s with row set U and column set V will be called a *U, V channel*. Thus a U, V channel is any nonnegative function s, defined for all pairs (u, v), $u \varepsilon U$, $v \varepsilon V$, for which

$$\sum_v s(u, v) = 1 \qquad \text{for all } u.$$

The sets U, V will be called the *input* and *output* sets, respectively, of the channel. We shall denote by $M(U, V)$ the set of all U, V channels. A channel s may be thought of as a random device which, on being given an input element $u \varepsilon U$, produces an output element $v \varepsilon V$, with the probability of a particular output v given by $s(u, v)$.

A U, V channel s may be used as a means of communication from one person, the sender, to another person, the receiver. There is given in advance a finite set D of messages, exactly one of which will be presented to the sender for transmission. The sender encodes the message by an *encoding channel* $s_1 \varepsilon M(D, U)$, with $s_1(d, u)$ being the probability that input u is given to channel s when message d is presented to the sender for transmission. When the receiver observes the output v of the transmission channel s, he decodes it by a *decoding channel* $s_2 \varepsilon M(V, D)$, with $s_2(v, d)$ being the probability that, on receiving the transmission channel output v, the receiver will decide that message d is intended. The pair (s_1, s_2) will be called a (D, U, V) code. For a U, V channel s and a (D, U, V) code $c = (s_1, s_2)$, the matrix $\epsilon(s, c) = s_1 s s_2$, which is an element of $M(D, D)$ will be called the *error matrix* of code c in channel s. Its (d, d') element is the probability that, when message d is presented to the sender, the receiver will decide that message d' is intended, when code c is used on channel s. We shall be especially interested in the *average error probability* over all messages in the set D. This is the number

$$\pi(s, c) = 1 - |D|^{-1} \text{ trace } \epsilon(s, c),$$

where $|D|$ denotes the number of elements in the set D.

A code $c = (s_1, s_2)$ will be called *pure* if only 0's and 1's occur as elements of s_1, s_2. The (finite) set of all pure (D, U, V) codes will be denoted by $C(D, U, V)$, and a probability distribution k over $C(D, U, V)$ will be called a *random*

Received October 21, 1959.

[1] This paper was prepared with the partial support of the Office of Naval Research (Nonr-222-53). This paper in whole or in part may be reproduced for any purpose of the United States Government.