On the Computation of Capacity of Discrete Memoryless Channel

M. C. Cheng

Department of Mathematics, University of Malaya, Kuala Lumpur, Malaysia

An iterative method of computing the capacity of a discrete memoryless channel, whose channel matrix has \( m \) row vectors and is of rank \( t \), has been proposed independently by Arimoto (1972) and Blahut (1972). The amount of computation involved depends upon the size of the channel matrix used.

It is shown that it is sufficient to use a set of \( t \) linearly independent row vectors as channel matrix in the computation of the capacity of a discrete memoryless channel. For the case \( m > t \), a criterion for selecting a set of \( t \) linearly independent row vectors as channel matrix is presented.

1. Introduction

The well-known coding theorem of information theory as proposed by Shannon (1949) states that given a noisy channel with capacity \( C \), it is possible to transmit messages over this channel and still be able to decode them with an arbitrarily small probability of error, provided the rate of transmission is less than \( C \) and that messages may be encoded in blocks of symbols of length \( l \). However, if the rate of transmission exceeds \( C \), then the probability of error tends to one as \( l \) tends to infinity (see, for example, Wolfowitz (1961)).

A general method for determining the capacity of a discrete channel has been suggested by Muroga (1953), while Arimoto (1972) and Blahut (1972) independently presented an iterative method of computing the capacity of arbitrary discrete memoryless channel. In the iterative method, the convergence is monotonic; however, the amount of computation involved depends upon the size of the channel matrix used. Hence, it is desirable to keep down the size of the channel matrix in order to minimize the amount of computation.

In this note, we prove that the capacity of a discrete memoryless channel, whose channel matrix has rank \( t \), can be computed by using only \( t \) linearly independent row vectors as channel matrix.
independent row vectors as channel matrix. In the case \( m > t \), where \( m \) is the number of row vectors in the original channel matrix, a criterion for selecting a set of \( t \) linearly independent row vectors as channel matrix is presented. A geometrical interpretation of one of the conditions in the criterion is also given.

2. Definitions and Notations

Let \( X = \{1, 2, \ldots, m\} \) and \( Y = \{1, 2, \ldots, n\} \) represent the set of input alphabet with \( m \) letters and the set of output alphabet with \( n \) letters, respectively. Denote the probability distribution functions defined on \( X \) and \( Y \) by \( p(\cdot) \) and \( q(\cdot) \), respectively, with \( p = (p_1, p_2, \ldots, p_m) \), where \( p_i = p(i) \), and \( q = (q_1, q_2, \ldots, q_n) \), where \( q_i = q(i) \), as the corresponding probability vectors. Let the channel matrix of a discrete memoryless channel with input \( X \) and output \( Y \) be denoted by \( R = (r(i/j)) \), \( i = 1, 2, \ldots, n \), \( j = 1, 2, \ldots, m \), where \( r(\cdot/j) \) is a probability distribution function defined on the set \( [Y/j] \) for every \( j \in X \).

Let the set of all \( n \)-dimensional probability vectors be denoted as

\[
S_n = \left\{ x; x_i \geq 0, \sum_{i=1}^{n} x_i = 1 \right\}.
\]

It is easy to see that \( S_n \) is a \((n - 1)\)-dimensional convex polytope. We say that a vector \( x \in S_n \) is an affine combination of vectors \( x_1, x_2, \ldots, x_t \) in \( S_n \) if we can find real number \( \lambda_i \), \( i = 1, 2, \ldots, t \), with \( \sum_{i=1}^{t} \lambda_i = 1 \) such that

\[
x = \sum_{i=1}^{t} \lambda_i x_i.
\]

The combination is called a convex combination if all the number \( \lambda_i \) are positive.

A real-valued function \( f \) defined on \( S_n \) is said to be concave if

\[
f(\lambda x_1 + (1 - \lambda) x_2) \geq \lambda f(x_1) + (1 - \lambda) f(x_2),
\]

where \( 0 \leq \lambda \leq 1 \), \( x_1 \in S_n \), \( x_2 \in S_n \).
3. Capacity of a Discrete Memoryless Channel

The rate of transmission of a discrete memoryless channel, with input $X$ and output $Y$, can be written as

$$I(X; Y) = \sum_{i=1}^{m} \sum_{j=1}^{n} p(i) r(j|i) \log \frac{r(j|i)}{q(j)}$$

or, alternatively,

$$I(X; Y) = H(pR) - \sum_{i=1}^{m} p_i H(r_i),$$

where $r_i$ is the probability vector corresponding to the $i$th row of the channel matrix $R$,

$$q = pR = \sum_{i=1}^{m} p_i r_i,$$

for $p = (p_1, p_2, \ldots, p_m)$,

$$q(j) = \sum_{i=1}^{m} p(i) r(j|i), \quad j = 1, 2, \ldots, n,$$

and

$$H(q) = -\sum_{i=1}^{n} q_i \log q_i,$$

for $q = (q_1, q_2, \ldots, q_n)$.

The capacity $C$ of the discrete memoryless channel is defined as the maximum value of the rate of transmission $I(X; Y)$, where the maximization is carried out over all $p \in S_m$.

Since $I(X; Y)$ is a concave function on $S_m$, then by applying the Kuhn-Tucker theorem, it is easily shown (see, for example, Gallager (1968)) that

**Lemma.** A set of necessary and sufficient conditions for an input probability vector $p^* = (p_1^*, p_2^*, \ldots, p_m^*)$ to achieve capacity $C$ on a discrete memoryless channel with input $X$, output $Y$, and channel matrix $R$ is

$$\sum_{j=1}^{n} r(j|i) \log[r(j|i)/q_i^*] = C \quad \text{for all } i \text{ with } p_i^* > 0,$$

$$\leq C \quad \text{for all } i \text{ with } p_i^* = 0,$$

where $q_i^* = \sum_{k=1}^{m} p_k^* r(j|k)$. 
From Eq. (2), it is clear that the corresponding $q^*$ in $S_n$ which achieves capacity $C$ must be a convex combination of $r_i$, $i = 1, 2, ..., m$, i.e., $q^*$ lies in the convex hull of $R$. To find this $q^*$, all we need to do is to move the hyperplane, which is determined uniquely by the probability vectors $r_i$, $i = 1, 2, ..., m$, parallel to itself until it just touches the function $H$ defined on $S_n$. Since $H$ is strictly concave, then there is only one point of $S_n$ at which the parallel hyperplane touches the function $H$, i.e., $q^*$ is unique.

**Theorem 1.** If the channel matrix $R$ of a discrete memoryless channel has rank $t$, then the channel capacity is also achieved by using a set of $t$ linearly independent vectors of $R$ as channel matrix.

**Proof.** Let $C$ be the capacity computed by using $R$ as channel matrix, and that $C$ is achieved at $q^*$. Then

$$q^* \in \text{convex hull of } R.$$ 

Since $R$ has rank $t$, by the Carathéodory Theorem (see, for example, Cheney (1966)),

$$q^* \in \text{convex hull of } T,$$

where $T$ consists of $t$ linearly independent vectors of $R$.

Hence $C$ is achieved by using $T$ as channel matrix.

**Corollary 1.** The channel capacity can be achieved by a probability vector in $S_m$ with at most $t$ of its elements positive.

**Corollary 2.** If $m > t$ and no two rows of the channel matrix are identical, then the input probability vector which achieves capacity is not unique.

**Corollary 3.** If $R = \{r_1, r_2, ..., r_m\}$ and $T = \{r_{i_1}, r_{i_2}, ..., r_{i_t}\}$, where \(\{j_1, ..., j_t\} \subseteq \{1, 2, ..., m\}\), then \(\exists \) positive numbers $p_i$, $i = 1, 2, ..., m$, and $p_{i_i}$, $i = 1, 2, ..., t$, with $\sum_{i=1}^{m} p_i = \sum_{i=1}^{t} p_{i_i} = 1$ satisfying

$$\sum_{i=1}^{m} p_i H(r_i) = \sum_{i=1}^{t} p_{i_i} H(r_{i_i}).$$

**4. Criterion for Selecting $T$**

From Theorem 1, when $m = t$, there is only one matrix $T$ of order $t \times n$, and hence it is the only channel matrix for computing the capacity of a
discrete memoryless channel. However, when \( m > t \), there are \( C_t^m \) matrices of order \( t \times n \), and the question arises in deciding which one should be chosen as \( T \) to replace \( R \) as channel matrix.

Before proceeding to answer the above question, a few observations might be helpful.

(1) Although one of the \( C_t^m \) matrices should be used as a channel matrix, it is not true that each of the \( C_t^m \) matrices can be used as a channel matrix.

(2) The purpose of choosing a \( t \times n \) matrix to replace the \( m \times n \) matrix as channel matrix is to reduce the amount of computation involved in evaluating the channel capacity.

Let \( T = \{ r_1, r_2, \ldots, r_t \} \) be a set of \( t \) linearly independent row vectors of \( R \). Then \( r = \sum_{i=1}^{t} \lambda_i r_i, \lambda_i \) real with \( \sum_{i=1}^{t} \lambda_i = 1, \forall r \in R - T \). Test whether

\[
H(r) \geq \sum_{i=1}^{t} \lambda_i H(r_i), \quad \forall r \in R - T.
\] (5)

If Eq. (5) is false, repeat with a new set \( T \). However, if Eq. (5) is true, treat \( T \) as a channel matrix and solve for \( p^* = (p_{1*}^*, p_{2*}^*, \ldots, p_{t*}^*) \).

Either

(i) \( p_{j_i}^* > 0, \) for \( i = 1, 2, \ldots, t \), or

(ii) \( p_{j_i}^* = 0, \) for some \( j_i \in M \subseteq \{ j_1, j_2, \ldots, j_t \} \). In this case, examine whether

(a) \( \lambda_i \geq 0, \forall j_i \in M; \)

(b) \( \lambda_i < 0 \) for some \( j_i \in M. \)

If (b) is true, repeat the tests with a new set \( T \) until Eq. (5) and either criterion (i) or criterion (ii)(a) are satisfied.

**Theorem 2.** If the channel matrix \( R \) of a discrete memoryless channel has rank \( t \), then a sufficient condition for a \( t \times n \) matrix \( T \) to replace \( R \) as channel matrix is that \( T \) must satisfy Eq. (5) and either criterion (i) or criterion (ii)(a).

**Proof.** Since the rank of the channel matrix \( R \) is \( t \), then \( n \geq t \), and \( m \geq t \).

Without loss of generality, we may let the first \( t \) rows \( r_i, i = 1, 2, \ldots, t \), be linearly independent which constitute \( T \), and let \( p = (p_1^*, p_2^*, \ldots, p_t^*) \).
be the input probability vector that achieves capacity $C$ by using $T$ as channel matrix, i.e., we have

$$\sum_{j=1}^{n} r(j|i) \log \left[ \frac{r(j|i)}{q_j*} \right] = C, \quad \text{for } p_i^* > 0,$$

$$\leq C, \quad \text{for } p_i^* = 0.$$  

We need to show that the input probability vector

$$p^* = (p_1^*, p_2^*, \ldots, p_t^*, 0 \ldots 0)$$

in $S_m$, $m \geq t$, also achieves capacity $C$ with the channel matrix $R$. To do this, we need only show that if $m > t$,

$$\sum_{j=1}^{n} r(j|i) \log \left[ \frac{r(j|i)}{q_j*} \right] \leq C \quad \text{for } i = t + 1, \ldots, m.$$  

For $i = t + 1, \ldots, m$,

$$r_i = \sum_{i=t}^{t} \lambda_i r_i, \quad \lambda_i \text{ real with } \sum_{i=1}^{t} \lambda_i = 1.$$  

\[ \therefore \quad \sum_{j=1}^{n} r(j|i) \log \left[ \frac{r(j|i)}{q_j*} \right] = \sum_{j=1}^{n} r(j|i) \log r(j|i) - \sum_{j=1}^{n} r(j|i) \log q_j*, \]

\[ \leq \sum_{i=1}^{t} \lambda_i \left[ \sum_{j=1}^{n} r(j|i) \log r(j|i) - \sum_{j=1}^{n} r(j|i) \log q_j* \right], \]

\[ = \sum_{\lambda_i \geq 0} \lambda_i \left[ \sum_{j=1}^{n} r(j|i) \log \left( r(j|i)/q_j* \right) \right] \]

\[ + \sum_{\lambda_i < 0} \lambda_i \left[ \sum_{j=1}^{n} r(j|i) \log \left( r(j|i)/q_j* \right) \right], \]

\[ \leq \sum_{\lambda_i \geq 0} \lambda_i [C] + \sum_{\lambda_i < 0} \lambda_i [C], \]

\[ = \sum_{i=1}^{t} \lambda_i C, \]

\[ = C, \]
where the first inequality is obtained by using Eq. (5) and the second inequality is obtained by using criterion (i) or criterion (ii)(a).

**Remark.** Equation (5) is capable of a geometrical interpretation, namely, every value $H(r)$ must lie on or above the hyperplane passing through the $t$ points $H(r_i), i = 1, 2, ..., t$. In particular, when $\lambda_i \geq 0, i = 1, 2, ..., t$, then the geometrical interpretation is necessarily true since $H$ is a concave function and that every row vector of $R$ lies in the convex hull of $T$. The result for the later case was reported earlier in Cheng (1973).

**RECEIVED:** June 5, 1973

**REFERENCES**


