(1,1,0), (0,1,1), and (0,1,1). In the first case $s^*$ remains equal to 2, in the next three cases $s^*$ is equal to 1, and in the last three cases $s^*$ becomes 0.

If the triple $(x, y, z)$ is $(1,1,1)$, similar derivations can be made. As a result, we can construct the two matrices

$$
M_0 = \begin{bmatrix}
1 & 0 & 0 \\
1 & 1 & 0 \\
3 & 3 & 1
\end{bmatrix}, \quad M_1 = \begin{bmatrix}
1 & 0 & 1 \\
3 & 1 & 0 \\
3 & 3 & 3
\end{bmatrix}.
$$

$M_0$ (resp. $M_1$) refers to the situation where $(0,0,0)$ (resp. $(1,1,1)$) is transmitted by $F$. The rows of $M_0$ are indexed by the values 0, 1, or 2 of $s$ (resp. $s^*$). In position $(s, s^*)$ the entry of $M_1$ is the number of triples that can be generated when the triple $(x, y, z)$ is transmitted to the mailbox in state $s$ and modified in such a way that the new state of the mailbox is $s^*$. The characteristic polynomial of $M_1 M_0$ is $\lambda^3 - 6 \lambda^2 + 11 \lambda - 6$ and the largest eigenvalue of $M_1 M_0$ is $\lambda_{\text{max}} = 27.9629$. Using the same ideas as in the case $b=1$, we see that, for any $\omega \in [0,1]$, the pair of rates $R_F = \omega^3/3, R_G = (\omega \log \lambda_{\text{max}})/6$, is achievable. In the present case these pairs improve only slightly on the time-sharing strategy in the region of intermediate rates. Generalizing this strategy for larger values of $b$ does not lead to any further improvement.

**References**


tion shows that \( E^+ \) is characterized by
\[
E^+ = \{ p \mid D(p\|q^*) + D(q^*\|q) \leq D(p\|q) \}.
\]
Then we have the following Proposition.

**Proposition 1:** If \( q^* = \pi(q|V) \), \( V \subset E^+ \).

**Proof:** See Csizár [3, theorem 2.2].

In the \( n \)-dimensional Euclidean space, let \( \text{con}(Q', \ldots, Q^m) \) denote the convex hull of \( Q', \ldots, Q^m \), i.e., the minimum convex set including \( Q', \ldots, Q^m \), and let \( Q', \ldots, Q^m \) denote the minimum subspace including \( Q', \ldots, Q^m \).

We now consider the problem of maximizing the mutual information under a linear input constraint:
\[
c(p) = \sum_{i=1}^{m} c_i p_i \leq \Gamma
\]
where \( c_1, \ldots, c_m \) are nonnegative real numbers. We denote the maximum by \( \Gamma \), call it a capacity-constraint function, i.e.,
\[
C(\Gamma) = \max_{p : c(p) \leq \Gamma} I(p, Q).
\]

\( C(\Gamma) \) exists only for \( \Gamma \geq \Gamma_0 \), \( \min_{c_1, \ldots, c_m} = 0 \), otherwise the set of \( p \) 's satisfying the constraint is empty. If \( \Gamma \) is greater than some \( \Gamma_0 \), \( C(\Gamma) \) equals the capacity \( C \) of the channel. It is well-known [2, p. 137] that \( C(\Gamma) \) has the following properties.

**Proposition 2:** \( C(\Gamma) \) is a nondecreasing concave function. \( C(\Gamma) \) is strictly increasing for \( \Gamma_0 \leq \Gamma \leq \Gamma^* \) and differentiable at \( \Gamma > \Gamma_0 \) except for \( \Gamma = \Gamma^* \).

Fig. 1 shows a typical graph of capacity-constraint function.

![Typical graph of capacity-constraint function](image)

**II. PRELIMINARIES TO THE THEOREMS**

We first consider a supportive maximization problem:
\[
F(\gamma) = \max_{p \in \Delta^n} (I(p, Q) - \gamma c(p)).
\]
It is known [2, pp. 137–142] that the following properties hold.

**Proposition 3:** We obtain
\[
C(\Gamma) = \min_{\gamma \geq 0} \{ F(\gamma) + \gamma \Gamma \}, \quad \Gamma \geq \Gamma_0.
\]

If, for some \( \gamma \geq 0 \), a \( p \) maximizes \( I(p, Q) - \gamma c(p) \) and \( c(p) = \Gamma \), then \( I(p, Q) = C(\Gamma) \).

**Proposition 4:** For any \( \gamma \geq 0 \),
\[
F(\gamma) = \min_{q \in \Delta^n} \max_{1 \leq i \leq m} D(Q_i\|q^i). \quad \sum_{i=1}^{m} c_i R_{ji} = \delta_{ji}
\]
where \( \delta_{ji} \) is Kronecker's delta and \( \sum_{i=1}^{m} R_{ji} = 1 \), \( j = 1, \ldots, n \).

Furthermore, a PD \( q^i \) exists that satisfies \( D(Q_i\|q^i) = \cdots = D(Q^m\|q^m) \).

**III. THEOREMS**

Now, since input PD \( p \) is in the set \( \{ p | c(p) \leq \Gamma \} \), the corresponding output PD \( q \) is in \( V(\Gamma) \) and \( \{ q | q = pQ \}, \quad c(p) \leq \Gamma \}. \) This condition of \( V(\Gamma) \) can be rewritten in terms of \( q \). From \( q_i = \sum_{j=1}^{m} p_j Q_{ji} \), we have \( p_i = \sum_{j=1}^{m} q_j R_{ji} \), (or \( p = qR \)), then
\[
F(\gamma) = \min_{q \in \Delta^n} \max_{1 \leq i \leq m} D(Q_i\|q^i) - \gamma c_i.
\]

Letting \( s_j = \sum_{i=1}^{m} c_i R_{ji} \) and \( s(q) = s_j \), we have \( V(\Gamma) = \{ s(q) \in \Delta^n | q \leq \Gamma \} \cap \text{con}(Q', \ldots, Q^m) \). In addition, we have \( c_i = \sum_{j=1}^{m} Q_{ji} \). Furthermore, we define a linear set \( E(\Gamma) \) by \( E(\Gamma) = \{ s(q) = \Gamma \} \). Here we have the following theorem.

**Theorem 1:** Let \( q^* \) be a probability distribution equidistant from \( Q', \ldots, Q^m \), i.e., \( q^* \) satisfies \( D(Q_i\|q^i) = \cdots = D(Q^m\|q^m) \). If we denote \( \tilde{q} = \pi(q^*|V(\Gamma)) \), then \( \tilde{q} \) achieves the capacity-constraint function \( C(\Gamma) \).

Before this is fully proved, we show that it holds in a simple concrete example. If \( m = n = 1 \) and \( Q = I_n \), ( \( n \times n \) unit matrix), then \( p = q \). In this case, since \( q^* = (1/n, \ldots, 1/n) \) and \( D(q\|q^*) = \)
\[ \log n - H(q) \]

Therefore, we see that \( 4 \) attains \( C(r) \).

Next, if \( c(\hat{p}) = \Gamma \), without loss of generality, we can assume that

\[ \hat{p}_1, \ldots, \hat{p}_k > 0 \]

\[ \hat{p}_{k+1} = \cdots = \hat{p}_m = 0. \quad (k \geq 1) \]

If \( k = 1 \), this problem is trivial because \( V(\Gamma) \) consists of only one point and therefore \( C(\Gamma) = 0 \). Let \( k \geq 2 \).

We calculate the coordinate of \( \hat{q} \). Since \( \hat{q} = \pi(q^0|V(\Gamma)) \) is also the projection of \( q^0 \) onto the linear set

\[ E(\Gamma) \cap \text{con}(Q^0, \ldots, Q^0) \]

\[ = \left\{ q^0 s(q) = \Gamma, p_i = \sum_{j=1}^{n} q_i R_{ij} = 0 \ (i = k+1, \ldots, m) \right\}, \]

from (1) we have

\[ \hat{q}_j = a q^0_j \exp \left( -\gamma_j - \sum_{i=k+1}^{m} \xi_{ij} R_{ij} \right), \quad j = 1, \ldots, n \]

where \( a = \exp(-1 + \gamma) \) and \( \gamma, \xi_{ij}, \xi \) are determined by

\[ s(\hat{q}) = \Gamma, \sum_{j=1}^{n} \hat{q}_j R_{ij} = 0, \quad i = k+1, \ldots, m, \sum_{j=1}^{n} \hat{q}_j = 1. \]

Now, denote

\[ s_j' = s_j + (1/\gamma) \sum_{j=1}^{n} \xi_{ij} R_{ij}, \quad j = 1, \ldots, n \]

\[ c_j' = \sum_{j=1}^{n} s_j' Q_{ij}, \quad i = 1, \ldots, m \]

and define a hyperplane \( E'(\Gamma) \) by

\[ E'(\Gamma) = \left\{ q^0 s'(q) = \sum_{j=1}^{n} s_j' q^0_j = \Gamma \right\}. \]

Since \( \hat{q}_j = a q^0_j \exp(-\gamma_j) \), \( j = 1, \ldots, n \), from (3), we obtain \( \hat{q} = \pi(q^0|E'(\Gamma)) \). Let 1, 2, be two elements chosen arbitrarily from the set \{1, \ldots, m\} (and renumbered for the sake of reducing the number of symbols). Since

\[ D(Q^0||\hat{q}_i) - D(Q^0||\hat{q}_j) \]

we have

\[ D(Q^0||\hat{q}_i) - \gamma c'_i = F, \quad i = 1, \ldots, m \]

where \( F \) is a constant. Notice that, by Propositions 3–5, \( \hat{q} \) achieves the minimum of the mutual information under the constraint \( \sum_{j=1}^{m} c'_j p_j \leq \Gamma \). The corresponding set of constraints in \( \Delta \) is \( V(\Gamma) = \{ q^0 s'(q) \leq \Gamma \} \cap \text{con}(Q^0, \ldots, Q^0) \). Now since \( \hat{q} \) attains the minimum of \( D(q^0||q^0) \) in \( q \in V(\Gamma) \) and also in \( q \in E'(\Gamma) \) at the same time, \( V(\Gamma) \) must lie on the opposite side of \( q^0 \) with respect to \( E'(\Gamma) \) by Proposition 1. Therefore, we have \( V(\Gamma) \subset V(\Gamma) \). Since \( \hat{q} \in V(\Gamma), \hat{q} \in V(\Gamma) \), we conclude that \( \hat{q} \) achieves the maximum of the mutual information in \( V(\Gamma) \).

In the above proof, we assumed that we knew beforehand which \( \hat{p}_i \) are 0. As shown below, we introduce a concrete algorithm for determining which \( i \) is equal to 0.

**Theorem 2:** For \( \Gamma_0 \leq \Gamma \leq \Gamma^* \), we can obtain \( \hat{q} \) which achieves \( C(\Gamma) \) by at most \( m-2 \) projections onto linear sets.

At this point, it is necessary to explain Theorem 2 more concretely. For \( \Gamma_0 \leq \Gamma \leq \Gamma^* \), \( \hat{q} \) satisfies \( s(\hat{q}) = \Gamma \). Then, let \( E^0 = E(\Gamma) \), \( q^0 = \pi(q^0|E^0) \) and put \( p^0 = q^0 R \) as an input PD corresponding to \( q^0 \). If \( p^0 \geq 0 \) for all \( i = 1, \ldots, m \), \( q^0 \) equals the \( \hat{q} \) which achieves \( C(\Gamma) \). However, if \( p^0 \leq 0 \) for some \( i \), \( q^0 \) does not achieve \( C(\Gamma) \). We must therefore look for another PD. Now, without loss of generality, assume that

\[ p^0_1, \ldots, p^0_k > 0 \]

\[ p^0_{k+1}, \ldots, p^0_m \leq 0. \]

Then denote \( E^0 = \{ q^0 s(q) = \Gamma \} \cap \{ Q^0_1, \cdots, Q^0_m \} \) and project \( q^0 \) onto \( E^0 \) to obtain \( q^* \) corresponding to positive coefficients \( p^* \). Next, let \( p^* = q^0 R \) and check whether or not \( p^* \leq 0 \). If \( p^* \leq 0 \), exclude the corresponding \( Q^0 \) and obtain \( q^0 \) by projection. We repeat this procedure until all coefficients become positive. Since the worst case is that one \( Q^0 \) is excluded at each step, we obtain a maximum of \( m-2 \) projections onto linear sets.

**Proof:** The fundamental part of the proof is similar to that of Theorem 1. The reader may also refer to [1, theorem 2].

**IV. EXAMPLES**

**Example 1**

\[ Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \]

\[ c_1 = 0, \ c_2 = 1, \ c_3 = 2. \]

We look for the maximum value of \( I(p, Q) = H(p) \), the entropy of \( p \). In this case, since the \( \hat{p} \) which achieves the maximum always lies in the interior of \( \text{con}(Q^0, Q^0, Q^0) \), we can obtain the following representation by Lagrange's method of indeterminate coefficients (Fig. 2):

\[ C(\Gamma) = H(\hat{p}) = \log \alpha^{-1} + \gamma \Gamma, \quad 0 \leq \Gamma \leq 1, \]

where

\[ \gamma = \log \frac{1 - \Gamma + \sqrt{1 + 6 \Gamma - 3 \Gamma^2}}{2 \Gamma} = \frac{7 - 3 \Gamma + \sqrt{1 + 6 \Gamma - 3 \Gamma^2}}{2(2 - \Gamma)^2}. \]

**Example 2**

\[ Q = \begin{pmatrix} 2/3 & 1/6 & 1/6 \\ 1/6 & 2/3 & 1/6 \\ 1/6 & 1/6 & 2/3 \end{pmatrix}, \]

\[ c_1 = 0, \ c_2 = 1, \ c_3 = 2. \]

Thus we have \( q^0 = (1/3, 1/3, 1/3) \). Letting \( \hat{q} = \pi(q^0|V(\Gamma)) \) and \( \hat{p} = \hat{q} R \), we find by a simple calculation that \( \hat{p}_1 > \hat{p}_2 > \hat{p}_3 \).
always holds. Therefore, depending on whether \( \hat{p}_1 \) is positive or not, \( \hat{q} \) lies in \( \text{con}(Q^t, Q^t, Q^t) \) or in \( \text{con}(Q^t, Q^t) \). Then we have the following representation (Fig. 3):

\[
C(\Gamma) = \begin{cases} 
(2/3)\log(2/3) + (1/6)\log(1/6) \\
-((1/2)\Gamma + (2/3))\log((-1/2)\Gamma + (2/3)) \\
-((1/2)\Gamma + (1/6))\log((1/2)\Gamma + (1/6)) \\
-\left(\frac{1}{2}\log\left(1 - \Gamma + \sqrt{13 + 6\Gamma - 3\Gamma^2}\right)\right) \\
H(2/3, 1/6, 1/6) + \log \alpha^{-1} + \gamma \Gamma, \\
\Gamma_i < \Gamma \leq \Gamma_1 
\end{cases}
\]

where

\[
\gamma = \frac{1 - \Gamma + \sqrt{13 + 6\Gamma - 3\Gamma^2}}{2(1 + \Gamma)}, \\
\alpha^{-1} = \exp \gamma + \exp(-\gamma) + \exp(-3\gamma)
\]

and \( \Gamma_i \) is the solution in the interval \((0, 1)\) of

\[
\frac{-1 + \Gamma + \sqrt{13 + 6\Gamma - 3\Gamma^2}}{2(3 - \Gamma)} = \frac{1 + \sqrt{21}}{10}, \quad \Gamma_i \neq 0.264.
\]

\( H(2/3, 1/6, 1/6) \) is the entropy of the PD \((2/3, 1/6, 1/6)\).

**V. Conclusion**

In this correspondence a geometric method for computing a capacity-constraint function \( C(\Gamma) \) is considered. The K-L divergence, having properties like a metric between two PD's is used to look for the output PD that attains \( C(\Gamma) \). It has been shown that \( C(\Gamma) \) is attained by the projection of \( q^t \) equidistant from each row vector of \( Q \) onto the set of PD's satisfying a given constraint condition. Moreover, the PD attaining \( C(\Gamma) \) is obtained by using Lagrange's method of indeterminate coefficients at most \( m - 2 \) times. We would like to be able to attack the case where the rank assumption is not valid. More study is needed to determine whether this geometric method can be applied to compute the rate-distortion function \( R(D) \) directly.

**Acknowledgment**

The authors would like to thank the reviewers for their helpful suggestions and comments.

**References**


More on the Decoder Error Probability for Reed–Solomon Codes

KAR-MING CHEUNG

Abstract—McEliece and Swanson offered an upper bound on \( P_E(u) \), the decoder error probability for Reed–Solomon codes (more generally, linear maximum distance separable codes), given that \( u \) symbol errors occur. Their upper bound is slightly greater than \( 2^{-n} \). We use a combinatorial technique similar to the principle of inclusion and exclusion to obtain an exact formula for \( P_E(u) \). The \( P_E(u) \)'s for the \((255,223)\) Reed–Solomon code used by NASA, and the \((31,15)\) Reed–Solomon code (JTIDS code) are calculated using the exact formula and are observed to approach the \( Q(u) \)'s of the codes rapidly as \( u \) gets large. An upper bound for the expression \( (P_E(u)/Q(u)) \) is derived and subsequently shown to decrease nearly exponentially as \( u \) increases.

I. Introduction

We begin with the following definitions. Let \( C \) be a linear code of length \( n \), dimension \( k \), and minimum distance \( d \). Let \( q \) be a positive power of a prime. An \((n, k, d)\) linear code \( C \) over GF(\( q \)) is maximum distance separable (MDS) if the Singleton bound is achieved; that is, \( d = n - k + 1 \). A code is \( e \)-error correcting if for some integer \( t \), \( 2t \leq d - 1 \).

Manuscript received August 7, 1987; revised September 15, 1988. This paper was partially presented at the 1986 International Symposium on Information Theory, Ann Arbor, MI, October 8, and at the 1988 IEEE Military Communications Conference, San Diego, CA, October 23.

The author is with the Jet Propulsion Laboratory, 238-420, 4800 Oak Grove Drive, Pasadena, CA 91109, USA.

IEEE Log Number 8929772.