Coding for a Multiple-Access Channel

TADAO KASAMI, FELLOW, IEEE, AND SHU LIN, MEMBER, IEEE

Abstract—**In this paper, coding for a multiple-access discrete memoryless channel is investigated. Block codes which are uniquely decodable and capable of correcting errors are constructed.**

I. Introduction

CONSIDER a simple multiple-access communication system as depicted in Fig. 1. In this system, two geographically separated users attempt to communicate binary data to two data sinks over a common channel which is called a multi-access channel. User 1 sends codewords from a block code C_1; user 2 sends codewords from a block code C_2. The two users occupy the same frequency slot, transmit at the same time, and use the same type of modulation. We also assume, admittedly somewhat unrealistically, that the two users maintain bit and word synchronization. There is one decoder that serves both data sinks.

In this paper, we shall study coding for the two channel models depicted in Fig. 2. The first channel model is referred to as a *noiseless multiple-access binary erasure channel*. In this model, if the two transmitted bits from the two users are zeros, a zero is transmitted over the channel to the receiver; if the two transmitted bits from the two users are ones, a one is transmitted over the channel to the receiver; if the two transmitted bits from the two users are different, an erasure symbol ξ is transmitted to the receiver. This noiseless multiple-access channel was studied first by Liao [1] and then by Gaarder and Wolf [2]. The capacity region of this channel is the shaded area shown in Fig. 3. Liao has proved that if the users transmit data with a rate pair (R_1,R_2) as a point inside the capacity region, encoders and a decoder exist for which each user can communicate with the receiver with an arbitrarily small probability of error [1].

The second channel model shown in Fig. 2(b) is also a multiple-access binary erasure channel, but noise is introduced. For this channel, we say that a *single error* has occurred if any of the following transitions has taken place: 1) the transition from the input pair (00) to the output symbol ξ; 2) the transition from the input pair (11) to the output symbol ξ; 3) the transition from either the input pair (01) or the input pair (10) to either the output symbol 0 or the output symbol 1. We say that two errors have occurred

Fig. 1. Multiple-access communication system with two users.

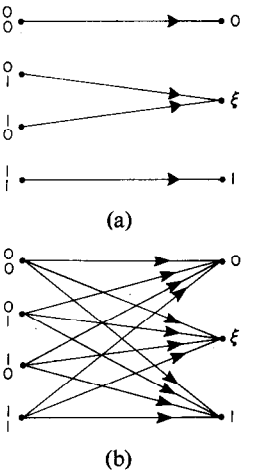

Fig. 2. (a) Noiseless multiple-access binary erasure channel. (b) Noisy multiple-access binary erasure channel.

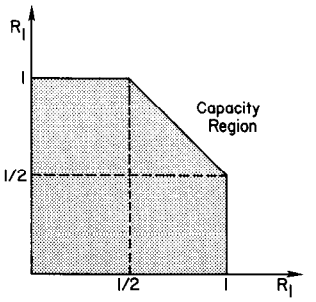

Fig. 3. Capacity region of multiple-access binary erasure channel.

if the transition is either from (00) to 1 or from (11) to 0. For both channel models described above, the two codewords transmitted from the two encoders are combined into a single vector $\boldsymbol{r}$ with symbols from the alphabet $\{0,1,\xi\}$. At the receiving end, the decoder will process the received vector $\boldsymbol{r}$ and decode it into two binary codewords, one in C_1 and the other in C_2, for the two data sinks.

In this paper, coding for the two multi-access channel models discussed above is investigated. Let $|C_1|$ and $|C_2|$ be the number of codewords in code C_1 and code C_2, respectively. Let n be the length of both codes. Then the rates for C_1 and C_2 are $R_1 = (\log_2 |C_1|)/n$ and $R_2 =$

Manuscript received January 3, 1975; revised May 30, 1975. This work was supported in part by the National Science Foundation under Grant GK-25128 and in part by the ALOHA System, a research project at the University of Hawaii, which is supported by the Advanced Research Projects Agency of the Department of Defense and monitored by NASA Ames Research Center under Contract NAS2-8590.

T. Kasami is with the Faculty of Engineering Science, Osaka University, Osaka, Japan.

S. Lin is with the Department of Electrical Engineering, University of Hawaii, Honolulu, HI 96822.

$(\log_2 |C_2|)/n$, respectively. The coding problem for the noiseless multi-access binary erasure channel is to construct the code pair C_1 and C_2 such that 1) the decoder is capable of decoding the received vector $\boldsymbol{r}$ without *ambiguity* into the two codewords that were transmitted from users 1 and 2, and 2) the rate pair (R_1,R_2) is a point inside the capacity region and is as close to the boundary as possible. A code pair (C_1,C_2) that has the first property is said to be *uniquely decodable*. The coding problem for the noisy multiple-access binary erasure channel is to construct a code pair (C_1,C_2) that is uniquely decodable and is capable of correcting t or fewer errors.

II. Definitions and Lemmas

Let V_n be the vector space of all the n-tuples over the field $GF(2)$. For $\boldsymbol{u} = (u_1,u_2,\cdots,u_n)$ and $\boldsymbol{v} = (v_1,v_2,\cdots,v_n)$ in V_n, let $E(\boldsymbol{u},\boldsymbol{v})$ denote the n-tuple

$$(E(u_1,v_1),E(u_2,v_2),\cdots,E(u_n,n_n))$$

where the ith component

$$E(u_i,v_i) = u_i = v_i, \qquad \text{for } u_i = v_i$$
$$E(u_i,v_i) = \xi, \qquad \text{for } u_i \neq v_i.$$

Thus $E(\boldsymbol{u},\boldsymbol{v})$ is a vector over $\{0,1,\xi\}$.

Definition 1: Let C_1 and C_2 be two subsets of V_n. Then (C_1,C_2) is said to be *uniquely decodable* if and only if, for any two distinct pairs $(\boldsymbol{u},\boldsymbol{v})$ and $(\boldsymbol{u}',\boldsymbol{v}')$ in $C_1 \times C_2$, $E(\boldsymbol{u},\boldsymbol{v}) \neq E(\boldsymbol{u}',\boldsymbol{v}')$.

It is clear from the above definition that if (C_1,C_2) is uniquely decodable, then C_1 and C_2 can have at most one vector in common.

Example 1: For $n = 2$, it is possible to construct a uniquely decodable pair with $C_1 = \{00,11\}$ and $C_2 = \{00,01,10\}$. The rate pair for C_1 and C_2 is (0.5,0.7925) which is a point inside the capacity region of Fig. 3. For $n = 2$ and $R_1 = 0.5$ it is impossible to construct a uniquely decodable code pair (C_1,C_2) with $R_2 > 0.7925$. Form a

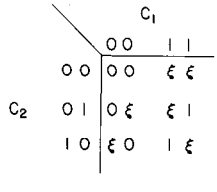

Fig. 4. Decoding table for uniquely decodable pair $C_1 = \{(00),(11)\}$ and $C_2 = \{(00),(01),(10)\}$.

two-dimensional array as shown in Fig. 4 where the column headings are the code vectors $\boldsymbol{u}$ of C_1, the row headings are the code vectors $\boldsymbol{v}$ of C_2, and the entry at the intersection of column $\boldsymbol{u}$ and row $\boldsymbol{v}$ is the n-tuple $E(\boldsymbol{u},\boldsymbol{v})$. This array may be used as a *decoding table* for the noiseless multiple-access channel. The received vector $\boldsymbol{r}$ at the input of the decoder must be an entry in the array. By table look up, the received vector $\boldsymbol{r}$ can be decoded without ambiguity into two codewords, one in C_1 and the other in C_2.

For a and b in $\{0,1,\xi\}$, define $|a,b|^\xi$ as follows:

$$|a,b|^\xi = \begin{cases} 0, & \text{if } a = b \\ 1, & \text{if either } a \text{ or } b \text{ is } \xi \text{ but not both} \\ 2, & \text{if } a = 0 \text{ and } b = 1 \text{ or } a = 1 \text{ and } b = 0. \end{cases}$$

Let $V_n(\xi)$ denote the set of all n-tuples over the set $\{0,1,\xi\}$. For $\boldsymbol{a} = (a_1,a_2,\cdots,a_n)$ and $\boldsymbol{b} = (b_1,b_2,\cdots,b_n)$ in $V_n(\xi)$ define

$$|\boldsymbol{a},\boldsymbol{b}|^\xi = \sum_{i=1}^{n} |a_i,b_i|^\xi \tag{1}$$

which will be referred to as the *ξ-distance* between $\boldsymbol{a}$ and $\boldsymbol{b}$.

Definition 2: Let C_1 and C_2 be two subsets of V_n. Then the pair (C_1,C_2) is said to be *δ-decodable* ($\delta > 0$) if and only if, for any two distinct pairs $(\boldsymbol{u},\boldsymbol{v})$ and $(\boldsymbol{u}',\boldsymbol{v}')$ in $C_1 \times C_2$, $|E(\boldsymbol{u},\boldsymbol{v}),E(\boldsymbol{u}',\boldsymbol{v}')|^\xi \geq \delta$.

Clearly, if (C_1,C_2) is δ-decodable, it must be uniquely decodable. For a δ-decodable pair (C_1,C_2), define the following set

$$\Phi(C_1,C_2) = \{E(\boldsymbol{u},\boldsymbol{v}): \boldsymbol{u} \in C_1, \boldsymbol{v} \in C_2\}. \tag{2}$$

The parameter δ is referred to as the *minimum ξ-distance* of $\Phi(C_1,C_2)$. Suppose that a δ-decodable piar (C_1,C_2) is used for coding a noisy multi-access binary erasure channel. Let $\boldsymbol{u}$ and $\boldsymbol{v}$ be the transmitted codewords from C_1 and C_2, respectively. The vector transmitted over the channel is $E(\boldsymbol{u},\boldsymbol{v})$. If no errors occur during the transmission, the received vector at the output of the decoder is also $E(\boldsymbol{u},\boldsymbol{v})$. By using the decoding array formed from C_1 and C_2, the decoder will decode $E(\boldsymbol{u},\boldsymbol{v})$ without ambiguity into the two transmitted codewords $\boldsymbol{u}$ and $\boldsymbol{v}$ and deliver them to sinks 1 and 2. If errors occur during the transmission, the transmitted vector $E(\boldsymbol{u},\boldsymbol{v})$ is altered. Let $\boldsymbol{r}$ be the received vector. Suppose that there are $t = \lfloor(\delta - 1)/2\rfloor$ or fewer errors in $\boldsymbol{r}$ where $\lfloor q \rfloor$ denotes the largest integer less than or equal to q. It is easy to see that

$$|\boldsymbol{r},E(\boldsymbol{u},\boldsymbol{v})|^\xi < |\boldsymbol{r},E(\boldsymbol{u}',\boldsymbol{v}')|^\xi$$

for any $(\boldsymbol{u}',\boldsymbol{v}')$ in $C_1 \times C_2$ such that $(\boldsymbol{u}',\boldsymbol{v}') \neq (\boldsymbol{u},\boldsymbol{v})$. This says that if there are t or fewer errors in the received vector $\boldsymbol{r}$, then $\boldsymbol{r}$ is closer to the transmitted vector $E(\boldsymbol{u},\boldsymbol{v})$ than to any other vector $E(\boldsymbol{u}',\boldsymbol{v}')$. However, if more than t errors occur during the transmission, there exists at least one case where an error pattern results in a received vector $\boldsymbol{r}$ such that

$$|\boldsymbol{r},E(\boldsymbol{u},\boldsymbol{v})|^\xi \geq |\boldsymbol{r},E(\boldsymbol{u}',\boldsymbol{v}')|^\xi$$

for some pair $(\boldsymbol{u}',\boldsymbol{v}')$ in $C_1 \times C_2$. Therefore, if the decoder decodes the received vector $\boldsymbol{r}$ into a vector which is closest to $\boldsymbol{r}$, any error pattern of t or fewer errors will be corrected. From the above analysis, we see that a δ-decodable pair (C_1,C_2) is capable of correcting $\lfloor(\delta - 1)/2\rfloor$ or fewer errors in a noisy multi-access binary erasure channel.

In the rest of this section, we shall prove some properties of a δ-decodable code pair (C_1,C_2). Let $I(\boldsymbol{u},\boldsymbol{v};\boldsymbol{u}',\boldsymbol{v}')$ denote the number of places in vectors $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{u}'$, and $\boldsymbol{v}'$, where $u_i = v_i$, $u_i' = v_i'$, and $u_i \neq u_i'$. For $\boldsymbol{a} \in V_n$, let $w(\boldsymbol{a})$ denote the Hamming weight of $\boldsymbol{a}$. It follows directly from the definitions that we have the following lemma.

Lemma 1: Let (u,v) and (u',v') be two pairs in $C_1 \times C_2$. Then

$$|E(u,v),E(u',v')|^{\xi} = 2I(u,v;u',v') + w(u + v + u' + v'). \tag{3}$$

Corollary 1: If (C_1,C_2) is δ-decodable, then the minimum Hamming distances of both C_1 and C_2 are greater than or equal to δ.

Proof: Let $u = u'$ and $v \neq v'$. Then $I(u,v;u',v') = 0$. Since (C_1,C_2) is δ-decodable, it follows from (3) that $w(v + v') \geq \delta$. Thus the minimum distance of C_2 is greater than or equal to δ. If we let $u \neq u'$ and $v = v'$, we can show that $w(u + u') \geq \delta$. Thus the minimum distance of C_1 is at least equal to δ. Q.E.D.

Let $u = (u_1,u_2,\cdots,u_n)$ and $v = (v_1,v_2,\cdots,v_n)$ be two vectors in V_n. We say that the ith component of u *covers* the ith component of v if the following conditions are satisfied: 1) if $v_i = 0$, then $u_i = 0$ or 1; 2) if $v_i = 1$, then $u_i = 1$. Otherwise, we say that u_i *does not cover* v_i.

Definition 3: Let u and v be vectors in V_n. We say that u is an $(n - t)$-*cover* of v, denoted $u \xrightarrow{t} v$, if there are $n - t$ or more components of u that cover the corresponding components of v. Let $u \not\xrightarrow{t} v$ denote that u is not an $(n - t)$-cover of v; i.e., there are more than t components of u that do not cover the corresponding components of v.

Lemma 2: The code pair (C_1,C_2) is uniquely decodable if and only if, for any two distinct pairs (u,v) and (u',v') in $C_1 \times C_2$, one of the following conditions is satisfied:

1) $u + v \neq u' + v'$;

2) $u + v = u' + v'$ but $u + v \not\xrightarrow{0} v + v'$.

Proof: Suppose that two distinct pairs (u,v) and (u',v') in $C_1 \times C_2$ satisfy the first condition. Then $E(u,v) \neq E(u',v')$. Suppose that the pairs (u,v) and (u',v') satisfy the second condition. It follows from Definition 3 that there exists at least one component in $u + v$, let us say $u_i + v_i$, that does not cover the corresponding component $v_i + v_i'$ of $v + v'$; i.e., $u_i + v_i = 0$ and $v_i + v_i' = 1$. Since $u_i + v_i = u_i' + v_i'$, thus $u_i = v_i$, $u_i' = v_i'$, and $v_i \neq v_i'$. Therefore, $E(u_i,v_i) \neq E(u_i',v_i')$. This implies that $E(u,v) \neq E(u',v')$. It follows from Definition 1 that (C_1,C_2) is uniquely decodable.

Now assume that (C_1,C_2) is uniquely decodable. Suppose that there exist two distinct pairs (u,v) and (u',v') in $C_1 \times C_2$ which do not satisfy either of the two conditions stated in the lemma. Then we must have $u + v = u' + v'$ and $u + v \xrightarrow{0} v + v'$. This implies that $E(u,v) = E(u',v')$ which is a contradiction to the assumption that (C_1,C_2) is uniquely decodable. Therefore, if (C_1,C_2) is uniquely decodable, any two distinct pairs (u,v) and (u',v') in $C_1 \times C_2$ *must* satisfy one of the two conditions of the lemma. Q.E.D.

Define $C_1 + C_2$ as the set of all distinct vectors $u + v$ with $u \in C_1$ and $v \in C_2$. If there exist distinct pairs (u,v) and (u',v') in $C_1 \times C_2$ such that $u + v = u' + v'$, we define

$$I(C_1,C_2) = \min_{\substack{(u,v) \neq (u',v') \text{ in } C_1 \times C_2 \\ u+v=u'+v'}} I(u,v;u',v'). \tag{4}$$

Lemma 3: Suppose that the minimum distance of $C_1 + C_2$ is greater than $\delta - 1$. The code pair (C_1,C_2) is δ-decodable if, for any two distinct pairs (u,v) and (u',v') in $C_1 \times C_2$, $u + v \neq u' + v'$.

Proof: Let (u,v) and (u',v') be two distinct pairs in $C_1 \times C_2$. Since $u + v \neq u' + v'$, $u + v$ and $u' + v'$ are two distinct vectors in $C_1 + C_2$. Since the minimum distance of $C_1 + C_2$ is greater than $\delta - 1$, $w(u + v + u' + v') > \delta - 1$. It follows from Lemma 1 that $|E(u,v), E(u',v')| \geq \delta$. Thus (C_1,C_2) is δ-decodable. Q.E.D.

Lemma 4: Suppose that the minimum distance of $C_1 + C_2$ is greater than $\delta - 1$, and suppose that there exist distinct pairs (u,v) and (u',v') in $C_1 \times C_2$ such that $u + v = u' + v'$. Then the code pair (C_1,C_2) is δ-decodable if and only if $2I(C_1,C_2) \geq \delta$.

Proof: Let (u,v) and (u',v') be two distinct pairs in $C_1 \times C_2$. It follows from Lemma 1 that

$$|E(u,v),E(u',v')|^{\xi} = 2I(u,v;u',v') + w(u + v + u' + v'). \tag{5}$$

Assume that $2I(C_1,C_2) \geq \delta$. There are two cases to be considered. Case 1: $u + v = u' + v'$. Clearly, $w(u + v + u' + v') = 0$. Since $2I(C_1,C_2) \geq \delta$, it follows from the definition of $I(C_1,C_2)$ that $2I(u,v;u',v') \geq \delta$. From (5), we obtain

$$|E(u,v),E(u',v')|^{\xi} \geq \delta. \tag{6}$$

Case 2: $u + v \neq u' + v'$. Clearly, $u + v$ and $u' + v'$ are two distinct vectors in $C_1 + C_2$. Since the minimum weight of $C_1 + C_2$ is greater than $\delta - 1$, $w(u + v + u' + v') \geq \delta$. From (5), we obtain

$$|E(u,v),E(u',v')|^{\xi} \geq \delta. \tag{7}$$

From (6) and (7), we conclude that (C_1,C_2) is δ-decodable. Assume now that (C_1,C_2) is δ-decodable. It follows from this assumption and (5) that

$$2I(u,v;u',v') + w(u + v + u' + v') \geq \delta. \tag{8}$$

For any two distinct pairs (u,v) and (u',v') such that $u + v = u' + v'$, $w(u + v + u' + v') = 0$. It follows from (8) that $2I(u,v;u',v') \geq \delta$. This implies that $2I(C_1,C_2) \geq \delta$. Q.E.D.

Lemma 5: For any two distinct pairs (u,v) and (u',v') in $C_1 \times C_2$ such that $u + v = u' + v'$, $u + v \not\xrightarrow{t} v + v'$, if and only if $I(C_1,C_2) > t$.

Proof: Assume that $I(C_1,C_2) > t$. It follows from the definition of $I(C_1,C_2)$ that, for any two distinct pairs (u,v) and (u',v') in $C_1 \times C_2$ such that $u + v = u' + v'$, we have $I(u,v;u',v') > t$. This implies that there are more than t places in u, v, u', and v', where $u_i = v_i$, $u_i' = v_i'$, and $v_i \neq v_i'$. Therefore, there are more than t places in

u and v and $v + v'$, where $u_i + v_i = 0$ and $v_i + v_i' = 1$. Thus there are more than t places where $u + v$ does not cover $v + v'$. This implies that $u + v \not\xrightarrow{t} v + v'$.

Assume that, for any two distinct pairs (u,v) and (u',v') such that $u + v = u' + v'$, $u + v \not\xrightarrow{t} v + v'$. It follows from this assumption and the definition of the relation $\xrightarrow{t}$ that there are more than t places in u, v, u', and v', where $u_i = v_i$, $u_i' = v_i'$, and $v_i \neq v_i'$. This implies that, for $u + v = u' + v'$, $I(u,v;u',v') > t$. It follows from the definition of $I(C_1,C_2)$ that $I(C_1,C_2) > t$. Q.E.D.

III. Bounds

In Section II we defined some basic concepts on coding a multi-access binary erasure channel. We also proved some general properties of the δ-decodable code pairs. In this and the following sections, we shall present some results on the construction of uniquely decodable and δ-decodable code pairs. Our approach to the construction is that *one code, let us say C_1, is chosen as an (n,k) linear code, and the vectors in C_2 are chosen from the cosets of C_1.* Using this approach we must determine *how many* and *what* vectors from each coset of C_1 can be used as codewords in C_2.

Theorem 1: Let C_1 be a linear code which contains the all-one vector $(111\cdots1)$. Let S be a coset of C_1 whose minimum weight $w_{\min}$ is greater than t. Then there exist at least two vectors v and v' in S such that, for any vector u in S, $u \not\xrightarrow{t} v + v'$.

Proof: Since the minimum weight of S is $w_{\min}$, the maximum weight of S is $n - w_{\min}$. Since $w_{\min} > t$, $n - w_{\min} < n - t$. This implies that every vector u in S has more than t zeros. Let v be any vector in S. Let $v' = (111\cdots1) + v$. Then $v + v' = (111\cdots1)$. Clearly, for any vector u in S, there are more than t components in u which do not cover the corresponding components of $v + v' = (111\cdots1)$. Thus we have $u \not\xrightarrow{t} v + v'$. Q.E.D.

Theorem 1 implies a method of constructing a class of uniquely decodable code pairs. A code pair (C_1,C_2) in this class is constructed as follows. Let C_1 be a linear (n,k) code which contains the all-one vector $(111\cdots1)$. Let S be a coset of C_1 such that $S \neq C_1$. Let v be the coset leader of S. Let v' be the one's complement of v. We include v and v' in C_2. There are $2^{n-k} - 1$ cosets of C_1 which are not equal to C_1. From these $2^{n-k} - 1$ cosets, we can choose $2^{n-k+1} - 2$ vectors and put them in C_2. We also choose the all-zero vector $(000\cdots0)$ from C_1 and include it in C_2. Therefore, C_2 has $2^{n-k+1} - 1$ vectors. The code pair (C_1,C_2) is uniquely decodable. This can be seen as follows. Consider two distinct pairs (u,v) and (u',v') in $C_1 \times C_2$. If v and v' are chosen from two different cosets of C_1, then $u + v \neq u' + v'$. Suppose that v and v' are chosen from the same coset S. Then $v + v' = (111\cdots1)$. Without loss of generality, we assume that v is the coset leader of S. Then $u + v$ is a vector in S. Since the all-one vector is in C_1, there is at least one component in $u + v$ which is zero. Therefore, if $u + v = u' + v'$, then $u + v \not\xrightarrow{0} v + v'$. It follows from Lemma 2 that (C_1,C_2) is uniquely decodable. The sum rate $R_1 + R_2$ of this pair is about $1/n$ bits higher than the rate achieved by using the time-sharing technique of Shannon [3].

For a uniquely decodable pair (C_1,C_2) with C_1 as a linear code, Theorem 1 provides a lower bound on the number of vectors that can be chosen from each coset of C_1 and used as vectors in C_2.

Corollary 2: Let C_1 be an (n,k) linear code that contains the all-one vector. Then at least two vectors can be chosen from each coset of C_1 as code vectors in C_2 so that (C_1,C_2) is a uniquely decodable pair.

When the code length n is large, there may be many cosets of C_1 such that each may contribute more than two vectors in C_2. The following lemma and theorem will give an upper bound on the number of vectors that each coset of C_1 may contribute to C_2.

Lemma 6: Let (C_1,C_2) be uniquely decodable. Suppose that C_1 contains a linear code S_0. Let S be a coset of S_0. For any $v \in S$, define the following set of vectors

$$S_0(v) = \{u: u \in S_0 \text{ and } w(u + v) = w(u) + w(v)\}.$$

Let x and y be two distinct vectors in S_0. If $v + x$ and $v + y$ are in $S \cap C_2$, then $x + y \notin S_0(v)$.

Proof: If $v + x$ and $v + y$ are in $S \cap C_2$, $(y, v + x)$ and $(x, v + y)$ are two distinct pairs in $C_1 \times C_2$. Suppose that $x + y$ is in $S_0(v)$. Then $E(y, v + x) = E(x, v + y)$. This is a contradiction to the fact that (C_1,C_2) is uniquely decodable. Thus $x + y \notin S_0(v)$. Q.E.D.

Theorem 2: Let (C_1,C_2) be a uniquely decodable pair where C_1 is an (n,k) linear code. Let S be a coset of C_1 whose maximum and minimum weights are $w_{\max}$ and $w_{\min}$, respectively. Then

$$|C_2 \cap S| \leq \min(2^{n-w_{\max}}, 2^{w_{\min}}). \tag{9}$$

Proof: Let v be a vector in S such that $w(v) = w_{\max}$. Consider the set

$$\Gamma = \{E(u, u + v): u \in C_1\}.$$

The ith component of $E(u, u + v)$ is ξ, if and only if the ith component of v, $v_i = 1$. Hence the number of distinct vectors in Γ, denoted $|\Gamma|$, is less than or equal to $2^{n-w_{\max}}$. This implies that $|C_2 \cap S| \leq 2^{n-w_{\max}}$. However, it follows from Lemma 6 that $|C_2 \cap S| \leq 2^{w_{\min}}$. Therefore, the theorem is proved. Q.E.D.

Theorem 2 yields the following bound.

Corollary 3: Let C_1 be an (n,k) linear code. Then *at most* $\min(2^{n-w_{\max}}, 2^{w_{\min}})$ vectors can be chosen from each coset of C_1 as codewords in C_2 so that (C_1,C_2) is a uniquely decodable pair, where $w_{\max}$ and $w_{\min}$ are the maximum and minimum weights of the coset, respectively.

Example 2: Let C_1 be the $(2^m - 1, 2^m - m - 1)$ Hamming code with distance 3. This code contains the all-one vector. There are $2^m - 1$ cosets with respect to C_1. The minimum weight $w_{\min}$ of each of these cosets is one,

and the maximum weight $w_{\max}$ of each of these cosets is $2^m - 2$. It follows from Corollary 3 that no more than two vectors can be chosen from each coset of C_1 as codewords in C_2 such that (C_1,C_2) is uniquely decodable. However, it follows from Corollary 2 that at least two vectors can be chosen from each coset of C_1 as codewords in C_2. Therefore, exactly two vectors can be chosen from each coset of C_1 as codewords in C_2 so that (C_1,C_2) is uniquely decodable. Hence we can construct C_2 with $2(2^m - 1) + 1$ codewords (two from each coset of C_1 plus the all-zero vector). This example shows that if C_1 is the $(2^m - 1, 2^m - m - 1)$ Hamming code, then for (C_1,C_2) to be uniquely decodable, the maximum number of codewords that C_2 may contain is $2^{m+1} - 1$. Let $m = 3$. Then C_1 is the (7,4) Hamming code. We can construct C_2 with 15 codewords. For this code pair, the rate pair is (0.571,0.558).

IV. Construction of Some δ-Decodable Codes

Let V_m be the vector space of all the 2^m m-tuples over $GF(2)$. For any integer i between zero and $2^m - 1$, there exists one and only one m-tuple, $(a_{i1},a_{i2},\cdots,a_{im})$, in V_m such that $a_{i1},a_{i2},\cdots,a_{im}$ are the coefficients in the radix-2 expansion of i; i.e., $i = a_{i1} + a_{i2}2 + a_{i3}2^2 + \cdots + a_{im}2^{m-1}$. We shall refer to $(a_{i1},a_{i2},\cdots,a_{im})$ as the *coordinate vector* of i. Let $X_1,X_2,\cdots,X_m$ be m variables over $GF(2)$. We define P_m to be the set of polynomials $f(X_1,X_2,\cdots,X_m)$ of degree m or less in $X_1,X_2,\cdots,X_m$ with coefficients in $GF(2)$. Clearly, $f(X_1,X_2,\cdots,X_m)$ is a binary function over V_m. Now, consider the vector space V_{2^m} over $GF(2)$. It is known that each vector in V_{2^m} is uniquely specified by a polynomial in P_m [4]. The vector in V_{2^m} that is specified by $f(X_1,X_2,\cdots,X_m)$ is given below:

$$v(f) = (v_0,v_1,v_2,\cdots,v_{2^m-1}) \tag{10}$$

with ith component

$$v_i = f(a_{i1},a_{i2},\cdots,a_{im}) \tag{11}$$

where $(a_{i1},a_{i2},\cdots,a_{im})$ is the coordinate vector of i. We shall also refer to $(a_{i1},a_{i2},\cdots,a_{im})$ as the coordinate vector of the ith bit position of a vector in V_{2^m}. Let $f(X_1,X_2,\cdots,X_m)$ and $g(X_1,X_2,\cdots,X_m)$ be two polynomials in P_m. If $v(f) \xrightarrow{t} v(g)$, we write $f \xrightarrow{t} g$. If $f(X_1,X_2,\cdots,X_m)$ can be transformed into $g(X_1,X_2,\cdots,X_m)$ by an invertible affine transformation, $f(X_1,X_2,\cdots,X_m)$ is said to be affine equivalent to $g(X_1,X_2,\cdots,X_m)$. Let r be a nonnegative integer less than or equal to m. Let P_r be the set of polynomials of degree r or less in P_m. It is known that there exists a one-to-one correspondence between a code vector in the rth-order Reed–Muller (RM) code of length 2^m and a polynomial $f(X_1,X_2,\cdots,X_m)$ in P_r; i.e., each code vector in the rth-order RM code is uniquely specified by one polynomial in P_r according to (10) and (11), and each polynomial in P_r specifies a code vector in the rth-order RM code of length 2^m [4], [5]. Let $|f|_m$ denote the weight of $v(f)$.

Lemma 7: Suppose that the $f(X_1,X_2,\cdots,X_m)$ and $g(X_1,X_2,\cdots,X_m)$ are in P_r and $g(X_1,X_2,\cdots,X_m)$ is a linear polynomial. Let t be a nonnegative integer such that $t < 2^{m-r-1}$. If $f \xrightarrow{t} g$, then $f = 1 + \bar{g}h$, where $\bar{g} = 1 + g$, $h \in P_{r-1}$, and h is independent of g.

Proof: Without loss of generality, we assume that $g = X_1$. The polynomial $f(X_1,X_2,\cdots,X_m)$ can be expressed as follows:

$$f(X_1,X_2,\cdots,X_m) = f_0(X_2,X_3,\cdots,X_m) + X_1f_1(X_2,X_3,\cdots,X_m) \tag{12}$$

where the degree of f_0 is less than or equal to r and the degree of f_1 is less than r. Setting $X_1 = 1$, we obtain

$$f(1,X_2,\cdots,X_m) = f_0(X_2,X_3,\cdots,X_m) + f_1(X_2,X_3,\cdots,X_m). \tag{13}$$

It follows from (12) and (13) that

$$\begin{aligned} f(X_1,X_2,\cdots,X_m) &= f(1,X_2,\cdots,X_m) + (1 + X_1)f_1(X_2,X_3,\cdots,X_m) \\ &= f(1,X_2,\cdots,X_m) + \bar{X}_1f_1(X_2,X_3,\cdots,X_m) \\ &= f(1,X_2,\cdots,X_m) + \bar{g}f_1(X_2,X_3,\cdots,X_m) \end{aligned} \tag{14}$$

where $f(1,X_2,\cdots,X_m)$ is a polynomial of degree r or less in $m - 1$ variables $X_2,X_3,\cdots,X_m$. Let $v[f(1,X_2,\cdots,X_m)]$ be the vector of length 2^{m-1} specified by $f(1,X_2,\cdots,X_m)$ with $(X_2,X_3,\cdots,X_m)$ running over V_{m-1}. Let $|f(1,X_2,\cdots,X_m)|_{m-1}$ denote the weight of $v[f(1,X_2,\cdots,X_m)]$. Since $g = X_1$ is a linear polynomial, $|g|_m = 2^{m-1}$. If $f \xrightarrow{t} g$, then

$$|f(1,X_2,\cdots,X_m)|_{m-1} \geq 2^{m-1} - t.$$

Since $t < 2^{m-r-1}$, thus

$$|f(1,X_2,\cdots,X_m)|_{m-1} > 2^{m-1} - 2^{m-r-1}. \tag{15}$$

Since the largest possible value of $f(1,X_2,\cdots,X_m)$ is 2^{m-1} and the next largest possible value of $f(1,X_2,\cdots,X_m)$ is $2^{m-1} - 2^{m-r-1}$ [4], it follows from (15) that $|f(1,X_2,\cdots,X_m)|_{m-1} = 2^{m-1}$. This implies that $f(1,X_2,\cdots,X_m) = 1$. From (14) we obtain $f = 1 + \bar{g}f_1(X_2,X_3,\cdots,X_m)$. Q.E.D.

The proof of Lemma 7 implies the following lemma.

Lemma 8: Suppose that $f \in P_r$. Let t be a nonnegative integer such that $t < 2^{m-r-1}$. If $f(1,X_2,\cdots,X_m) \neq 1$, then $f \not\xrightarrow{t} X_1$.

Let C_1 be a linear code of length 2^m. Let S be a coset of C_1 such that $S \neq C_1$. Let $f(X_1,X_2,\cdots,X_m)$ be a polynomial in P_m such that the vector $v(f)$ is in S. Let $l(f)$ denote the number of independent linear factors of f. Define

$$l(S) = \max_{v(f) \in S} l(f). \tag{16}$$

Theorem 3: Suppose that C_1 is the first-order RM code of length 2^m. Let S be a coset of C_1 such that $S \neq C_1$. Suppose that the polynomials which specify the vectors in S are in P_r. Let f be a polynomial which satisfies the following conditions: 1) $v(f) \in S$; 2) $l(f) = l(S)$. Let $Y_1,Y_2,\cdots,Y_{l(S)}$ be the independent linear factors of f. Choose linear polynomials $Y_{l(S)+1},\cdots,Y_m$ in such a way that $Y_1,Y_2,\cdots,Y_m$

are linearly independent. Form the following set

$$S_0 = \left\{ v(g) : g = f + c_0 + \sum_{i>l(S)} c_i Y_i \text{ with } c_0, c_i \in GF(2) \right\}. \tag{17}$$

If $t < 2^{m-r-1}$, then, for any two distinct pairs (u,v) and (u',v') in $C_1 \times S_0$ such that $u + v = u' + v'$, we have $u + v \not\xrightarrow{t} u + u'$.

Proof: Without loss of generality, we use $Y_1, Y_2, \cdots, Y_m$ as independent variables. Let

$$f = Y_1, Y_2, \cdots, Y_{l(S)} h(Y_{l(S)+1}, \cdots, Y_m)$$

where $h \in P_{r-l(S)}$ and h has no linear factor. Let (u,v) and (u',v') be two distinct pairs in $C_1 \times S_0$ such that $u + v = u' + v'$. Note that

$$u + u' = v + v' = v(Z) \tag{18}$$

where Z is a polynomial of the form $c_0 + \sum_{i>l(S)} c_i Y_i$. Also

$$u + v = v(f + q) \tag{19}$$

where $q(X_1, X_2, \cdots, X_m) \in P_1$. Clearly, $f + q \in P_r$. By the assumption, $f \notin P_1$. Suppose that Z is not a constant. The variables $Y_1, Y_2, \cdots, Y_{l(S)}, Z$ are linearly independent. Express f in the following form

$$f = Y_1, Y_2, \cdots, Y_{l(S)}(h_0 + \bar{Z}h_1)$$

where $h_0 \in P_{r-l(S)}$, $h_1 \in P_{r-l(S)-1}$, and h_0 and h_1 are independent of $Y_1, Y_2, \cdots, Y_{l(S)}, Z$. If $h_1 = 0$, then $f_{Z=1} = f \notin P_1$. If $h_1 \neq 0$ and $f_{Z=1} = Y_1, Y_2, \cdots, Y_{l(S)} h_0$ is in P_1, then $f + f_{Z=1}$ specifies a vector in S. The polynomial $f + f_{Z=1}$ has at least $l(S) + 1$ linear factors. This is a contradiction to the definition of $l(S)$. Therefore, we conclude that $f_{Z=1} \notin P_1$. Hence, by Lemma 8, we have

$$f + q \not\xrightarrow{t} Z. \tag{20}$$

It follows from (18), (19), and (20) that we have $u + v \not\xrightarrow{t} u + u'$. If $Z = 1$, then the above relation holds. Q.E.D.

If the first-order RM code of length 2^m is used as C_1, Theorem 3 tells us what vectors from each coset of C_1 can be used as vectors in C_2 so that the pair (C_1,C_2) is δ-decodable. The vectors that can be chosen from a coset of C_1 are the vectors in S_0 of (17). The number of vectors in S_0 is $2^{m-l(S)+1}$. However, to be able to use Theorem 3, the coset leaders of the cosets of C_1 must be known. Several δ-decodable code pairs (C_1,C_2) with C_1 as the first-order RM code are given in the following examples.

Example 3: Let C_1 be the first-order RM code of length 16. The coset leaders of this code are listed in Table I which was obtained by Dick and Sloane [6]. Types of coset leaders in terms of Boolean polynomials are given in column 1. Each coset leader is an affine equivalent to one of the polynomials listed in column 1. The second column gives the number of coset leaders that are equivalent to the polynomials of the same row. The third column gives the value of $l(C)$ of each coset. Let $r = 4$ and $t = 0$. By Theorem 3, we can choose $1 + 35 \cdot 2^3 + 28 \cdot 2^5 + 120 \cdot 2^2 + 840 \cdot 2^4 + 16 \cdot 2 + 560 \cdot 2^3 + 448 \cdot 2^5 = 33945$ vectors from the cosets of C_1 as vectors in C_2 so that (C_1,C_2) is uniquely decodable. C_1 and C_2 give a rate pair (0.312, 0.941) which is very close to the boundary of the capacity region of the multiple-access binary erasure channel.

Example 4: Let C_1 be the first-order RM code of length 16. Let $C_1 + C_2$ be the second-order RM code. Let $t = 1$. It follows from Lemmas 4 and 5 and Theorem 3 that we can choose $1 + 35 \cdot 2^3 + 28 \cdot 2^5 = 1177$ vectors from cosets of type X_1X_2 and type $X_1X_2 + X_3X_4$ as vectors in C_2, so that (C_1,C_2) is 4-decodable and is capable of correcting any single error. The rate of C_1 is $R_1 = 5/16$, and the rate of C_2 is $R_2 = (1/16) \log_2 1177 = (10.19/16)$. The sum rate of (C_1,C_2) is $R_1 + R_2 = 15.19/16$. For $n = 16$, if we choose C_1 with $R_1 = 5/16$, it follows from Corollary 1 that the maximum possible rate of C_2 is less than or equal to 11/16.

TABLE I
COSET LEADERS OF FIRST-ORDER RM CODE OF LENGTH 16

Coset Types (Boolean Polynomials)	No. of Such Cosets	$\ell(S)$
0	1	-
X_1X_2	35	2
$X_1X_2 + X_3X_4$	28	0
$X_1X_2X_3$	120	3
$X_1(X_2X_3 + X_4)$	840	1
$X_1X_2X_3X_4$	16	4
$X_1X_2(X_3X_4 + 1)$	560	2
$X_1X_2X_3X_4 + X_1X_2 + X_3X_4$	448	0

TABLE II
COSET LEADERS WITH POLYNOMIAL REPRESENTATION OF DEGREE 3 OR LESS FOR FIRST-ORDER RM CODE OF LENGTH 32

Cosets with Boolean Polynomials of degree 3 or less	No. of Such Cosets	$\ell(S)$
0	1	-
X_1X_2	155	2
$X_1X_2 + X_3X_4$	868	0
$X_1X_2X_3$	155 × 8	3
$X_1X_2X_3 + X_4X_5$	155 × 512	0
$X_1X_2X_3 + X_1X_4$	155 × 168	1
$X_1X_2X_3 + X_1X_4 + X_2X_5$	155 × 336	0
$X_1X_2X_3 + X_1X_4X_5$	868 × 32	1
$X_1X_2X_3 + X_1X_4X_5 + X_2X_3$	868 × 320	0
$X_1X_2X_3 + X_1X_4X_5 + X_2X_4$	868 × 480	0
$X_1X_2X_3 + X_1X_4X_5 + X_2X_3 + X_2X_4 + X_3X_5$	868 × 192	0

Example 5: Let C_1 be the first-order RM code of length $2^5 = 32$. Let $C_1 + C_2$ be the third-order RM code of the same length. The coset leaders of C_1 whose polynomial representations have degree 3 or less are given in Table II (obtained from Berlekamp and Welch [7]). Let $t = 1$ and $r = 3$. It follows from Lemmas 4 and 5 and Theorem 3 that we can choose 65 309 809 vectors from those coset types given in Table II as vectors in C_2 so that (C_1,C_2) is a 4-decodable code and is capable of correcting any single error in noisy multiple-access binary erasure channel. This code pair has a rate pair (6/32,25.96/32). It follows from Corollary 1 that if we choose C_1 with $R_1 = 6/32$, then $R_2 \leq 26/32$ for (C_1,C_2) to be 4-decodable.

Example 6: Again, let C_1 be the first-order RM code of length 32. Let $C_1 + C_2$ be the second-order RM code. Let $t = 3$ and $r = 2$. Then we can choose $1 + 115 \cdot 2^4 + 868 \cdot 2^6 = 58\,033$ vectors from the cosets of type 0, X_1X_2, and $X_1X_2 + X_3X_4$ as vectors of C_2 so that (C_1,C_2) is 8-decodable. This code pair is capable of correcting three or fewer errors in a noisy multi-access binary erasure channel. The rate pair for C_1 and C_2 is (6/32,15.824/32).

V. On a Class of 4-Decodable Code Pairs (C_1,C_2) with $R_1 = \frac{1}{2}$

In this section, a class of 4-decodable (or single-error-correcting) code pairs are presented. For each code pair (C_1,C_2), one code, let us say C_1, is a linear (n,k) code; and the vectors of the second code are chosen from the cosets of C_1.

Let $n = 2^m$. Let each bit position i of an n-tuple in V_n be represented by an m-tuple in V_m which is the coordinate vector of position i. Let $\beta = (b_2,b_3,\cdots,b_m)$ be a $m-1$ tuple in V_{m-1}. Define the following set of polynomials in $X_1,X_2,\cdots,X_m$ over $GF(2)$,

$$F_1 = \Big\{ f(X_1,X_2,\cdots,X_m) = \sum_{\beta \in V_{m-1}} c_\beta (X_2 + \bar{b}_2)(X_3 + \bar{b}_3)\cdots(X_m + \bar{b}_m) : c_\beta \in GF(2) \text{ and } \sum_{\beta \in V_{m-1}} c_\beta = 0 \Big\} \quad (21)$$

where $\bar{b}_i = 1 + b_i$, for $i = 2,3,\cdots,m$. Based on (10) and (11), F_1 specifies a subset of vectors in V_{2^m},

$$C_1 = \{v(f): f(X_1,X_2,\cdots,X_m) \in F_1\}. \quad (22)$$

It follows from the definition of F_1 that C_1 is a linear $(2^m, 2^{m-1} - 1)$ code which contains the all-one vector $(111\cdots1)$. For any vector $v(f)$ in C_1, the component at the bit position with coordinate vector $(a_1 = 0,a_2,a_3,\cdots,a_m)$ is identical to the component at the bit position with coordinate vector $(a_1 = 1,a_2,a_3,\cdots,a_m)$. In fact, C_1 is equivalent to the product of the (2,1) code $\{(00),(11)\}$ and the $(2^{m-1}, 2^{m-1} - 1)$ even parity code. Also, since we note $\sum_{\beta \in V_{m-1}} c_\beta = 0$, that $F_1 \subseteq P_{m-2}$. Therefore, C_1 is a linear subcode of the $(m-2)$th-order RM code of length 2^m.

Any polynomial $f(X_1,X_2,\cdots,X_m)$ in P_m can be expressed as

$$f(X_1,X_2,\cdots,X_m) = \sum_{\beta \in V_{m-1}} (a_\beta X_1 + c_\beta)(X_2 + \bar{b}_2)\cdots(X_m + \bar{b}_m) \quad (23)$$

where $\beta = (b_2,b_3,\cdots,b_m)$. Consider the coefficients of the following terms: $X_1X_2\cdots X_m$, $X_1X_3X_4\cdots X_m$, $X_1X_2X_4\cdots X_m$, $X_1X_2\cdots X_{m-1}$, $X_2X_3\cdots X_m$. The polynomial $f(X_1,X_2,\cdots,X_m)$ of (23) is in P_{m-2}, if and only if the following equalities hold

$$\sum_{\beta \in V_{m-1}} a_\beta = 0 \quad (24a)$$

$$\sum_{\substack{\beta \in V_{m-1} \\ \bar{b}_i = 1}} a_\beta = 0, \qquad \text{for } 2 \leq i \leq m \quad (24b)$$

$$\sum_{\beta \in V_{m-1}} c_\beta = 0. \quad (24c)$$

Now consider the cosets of C_1. Let

$$f_1(X_1,X_2,\cdots,X_m) = \sum_{\beta \in V_{m-1}} (a_\beta X_1 + c_\beta)(X_2 + \bar{b}_2)\cdots(X_m + \bar{b}_m)$$

$$f_2(X_1,X_2,\cdots,X_m) = \sum_{\beta \in V_{m-1}} (a_\beta' X_1 + c_\beta')(X_2 + \bar{b}_2)\cdots(X_m + \bar{b}_m)$$

be two polynomials in P_{m-2}. Then $v(f_1)$ and $v(f_2)$ belong to the same coset of C_1, if and only if $a_\beta = a_\beta'$, for any $\beta \in V_{m-1}$. It follows from the definition of RM codes [8] that the coefficient vector

$$\alpha = (a_{(0,0,\cdots,0)},a_{(0,0,\cdots,1)},\cdots,a_{(1,1,\cdots,1)}) \quad (25)$$

satisfies the equalities (24a) and (24b) if and only if α is a code vector in the $(m-3)$th-order RM code of length 2^{m-1}. For each code vector, $\alpha = (a_{(0,0,\cdots 0)},a_{(0,0,\cdots 1)},\cdots,a_{(1,1,\cdots,1)})$ in the $(m-3)$th-order RM code of length 2^{m-1}, define the following set of polynomials in $X_1,X_2,\cdots,X_m$ over $GF(2)$:

$$F_2(\alpha) = \Big\{ \sum_{a_\beta = 1} (X_1 + c_\beta)(X_2 + \bar{b}_2)\cdots(X_m + \bar{b}_m) : \sum_{a_\beta = 1} c_\beta = 0 \text{ and } c_\beta \in GF(2) \Big\} \quad (26)$$

where $\beta \in V_{m-1}$, a_β is a component of α, and the sum is over the β with $a_\beta = 1$. Let $w(\alpha)$ be the weight of α. Then the number of polynomials on $F_2(\alpha)$, denoted $|F_2(\alpha)|$, is

$$|F_2(\alpha)| = 2^{w(\alpha)-1}. \quad (27)$$

If α is the all-zero vector, then $F_2(\alpha) = \{0\}$.

Lemma 9: Assume that α is a code vector in the $(m-3)$th-order RM code of length 2^{m-1} and is not the all-zero vector. Let $f(X_1,X_2,\cdots,X_m)$ and $f'(X_1,X_2,\cdots,X_m)$ be two distinct polynomials in $F_2(\alpha)$. If there exist two polynomials $g(X_1,X_2,\cdots,X_m)$ and $g'(X_1,X_2,\cdots,X_m)$ in F_1 such that $f + g = f' + g'$, then

$$g + f \xrightarrow{1} f + f'. \quad (28)$$

Proof: Let

$$\alpha = (a_{(0,0,\cdots,0)}, a_{(0,0,\cdots,1)}, \cdots, a_{(1,1,\cdots,1)}).$$

Let

$$f(X_1,X_2,\cdots,X_m) = \sum_{a_\beta = 1} (X_1 + c_\beta)(X_2 + \bar{b}_2)\cdots(X_m + \bar{b}_m)$$

$$f'(X_1,X_2,\cdots,X_m) = \sum_{a_\beta = 1} (X_1 + c_\beta')(X_2 + \bar{b}_2)\cdots(X_m + \bar{b}_m)$$

and

$$g(X_1,X_2,\cdots,X_m) = \sum_{\beta \in V_{m-1}} c_\beta''(X_2 + \bar{b}_2)(X_3 + \bar{b}_3)\cdots(X_m + \bar{b}_m).$$

Since $f \neq f'$ and

$$\sum_{a_\beta = 1} (c_\beta + c_\beta') = 0$$

there exist different $\beta = (b_2,b_3,\cdots,b_m)$ and $\beta' = (b_2',b_3',\cdots,b_m')$ such that

$$c_{(b_2,b_3,\cdots,b_m)} + c'_{(b_2,b_3,\cdots,b_m)} = 1$$

$$c_{(b_2',b_3',\cdots,b_m')} + c'_{(b_2',b_3',\cdots,b_m')} = 1$$

$$a_{(b_2,b_3,\cdots,b_m)} = a_{(b_2',b_3',\cdots,b_m')} = 1.$$

Hence for any $c''_{(b_2,b_3,\cdots,b_m)}$ and $c''_{(b_2',b_3',\cdots,b_m')}$, we have

$$v(f+g)_{X_2=b_2,\cdots,X_m=b_m} \overset{0}{\not\to} v(f+f')_{X_2=b_2,\cdots,X_m=b_m} \tag{29a}$$

$$v(f+g)_{X_2=b_2',\cdots,X_m=b_m'} \overset{0}{\not\to} v(f+f')_{X_2=b_2',\cdots,X_m=b_m'} \tag{29b}$$

where $v(f+g)_{X_2=b_2,\cdots,X_m=b_m}$ denotes the following two components

$$[f(0,b_2,\cdots,b_m) + g(0,b_2,\cdots,b_m), f(1,b_2,\cdots,b_m) + g(1,b_2,\cdots,b_m)]$$

in the vector $v(f+g)$, and $v(f+f')_{X_2=b_2,\cdots,X_m=b_m}$ denotes the two components

$$[f(0,b_2,\cdots,b_m) + f'(0,b_2,\cdots,b_m), f(1,b_2,\cdots,b_m) + f'(1,b_2,\cdots,b_m)]$$

in the vector $v(f+f')$. It follows from (29) that we obtain (28). Q.E.D.

Now we define the following set of polynomials:

$$F_2 = \bigcup_\alpha F_2(\alpha) \tag{30}$$

where the union is over all the code vectors α in the $(m-3)$th-order RM code of length 2^{m-1}. Let C_2 be the following set of vectors of length 2^m

$$C_2 = \{v(f): f(X_1,X_2,\cdots,X_m) \in F_2\}. \tag{31}$$

Consider the bit position with coordinate vector $(b_1 = 0, b_2,\cdots,b_m)$ and the bit position with coordinate vector $(b_1 = 1, b_2,\cdots,b_m)$. This pair of bit positions is called a *slot*, and the $(m-1)$-tuple $(b_2,b_3,\cdots,b_m)$ is referred to as the coordinate vector of this slot. It follows from the definition of $F_2(\alpha)$ that the two components at any slot in a vector of C_2 must be in one of the following three configurations (00), (01), and (10). Also, the number of configuration (10) in each vector is even.

Let A_i denote the number of code vectors of weight i in the $(m-3)$th-order RM code of length 2^{m-1}. It follows from (27) and (30) that the number of vectors in C_2, denoted by $|C_2|$, is given below:

$$|C_2| = 1 + \frac{1}{2}\sum_{i=1}^{2^{m-1}} A_i 2^i. \tag{32}$$

Since the $(m-3)$th-order RM code of length 2^{m-1} is a Hamming code of distance 4, the weight generating function of this code is

$$\sum_{i=0}^{2^{m-1}} A_i X^i = 2^{-m}\{(1+X)^{2^{m-1}} + (1-X)^{2^{m-1}} + 2(2^{m-1}-1)(1-X^2)^{2^{m-2}}\}. \tag{33}$$

(See Peterson [8].) Combining (32) and (33), we obtain

$$|C_2| = \tfrac{1}{2} + 2^{-(m+1)}\{3^{2^{m-1}} + 2(2^{m-1}-1)3^{2^{m-2}} + 1\}. \tag{34}$$

For large m, $R_2 \approx \frac{1}{2}\log_2 3$.

Now consider the code pair C_1 and C_2. It follows from the definitions of F_1 and F_2 that $C_1 + C_2$ is the $(m-2)$th-order RM code of length 2^m. Based on Lemmas 4, 5, and 9, we obtain the following result.

Theorem 4: Let C_1 be the code specified by

$$F_1 = \Big\{ f(X_1,X_2,\cdots,X_m) = \sum_{\beta \in V_{m-1}} c_\beta (X_2 + \bar{b}_2)(X_3 + \bar{b}_3)\cdots(X_m + \bar{b}_m): c_\beta \in GF(2) \text{ and } \sum_{\beta \in V_{m-1}} c_\beta = 0 \Big\}.$$

Let C_2 be the code specified by

$$F_2 = \bigcup_\alpha \Big\{ \sum_{a_\beta = 1} (X_1 + c_\beta)(X_2 + \bar{b}_2)\cdots(X_m + \bar{b}_m): \sum_{a_\beta = 1} c_\beta = 0 \text{ and } c_\beta \in GF(2) \Big\}$$

where the union is over all the code vectors α in the $(m-3)$th-order RM code of length 2^{m-1}, and a_β is the component of α at the bit position with coordinate vector $\beta = (b_2,b_3,\cdots,b_{m-1}) \in V_{m-1}$. Then C_1 and C_2 form a 4-decodable (or single error-correcting) code pair for a noisy multiple-access binary erasure channel. As m (or n) becomes large, the rates R_1 and R_2 of the single error-correcting codes C_1 and C_2 of Theorem 4 approaches $\frac{1}{2}$ and $\frac{1}{2}\log_2 3$, respectively, which are the rates for the noiseless case of Example 1.

Decoding

The decoding of the above class of 4-decodable code pairs is simple. Let $\boldsymbol{r}$ be the received vector. Define a mapping τ from $\{0,1,\xi\}$ to $GF(2)$ as follows:

$$\tau(0) = 0 \qquad \tau(1) = 0 \qquad \tau(\xi) = 1.$$

Applying the mapping τ to the components of $\boldsymbol{r}$, we obtain a binary vector $\tau(\boldsymbol{r})$. If there is no error in $\boldsymbol{r}$, then $\tau(\boldsymbol{r})$ is a code vector in $C_1 + C_2$ which is the $(m-2)$th-order RM code of length 2^m (or the extended Hamming code of length 2^m). If there is a single error in $\boldsymbol{r}$ at the certain location, then there is a single error in $\tau(\boldsymbol{r})$ at the same location. The decoding of $\boldsymbol{r}$ consists of three steps.

Step 1: The binary vector $\tau(\boldsymbol{r})$ is decoded according to the decoding procedure for the $(m-2)$th-order RM code. The error location is determined. Suppose that $(b_1,b_2,\cdots,b_m)$ is the coordinate vector of the error position.

Step 2: Each slot of $\boldsymbol{r}$, except the one with coordinate vector $(b_2,b_3,\cdots,b_m)$,[1] is decoded into two binary slots according to the decoding array of Fig. 4. Suppose that $\boldsymbol{u}$ and $\boldsymbol{v}$ were the transmitted vectors from C_1 and C_2, respectively. Then this step reproduces $2^{m-1}-1$ slots of $\boldsymbol{u}$ and $2^{m-1}-1$ slots of $\boldsymbol{v}$.

Step 3: The slot of $\boldsymbol{r}$ with coordinate vector $(b_2,b_3,\cdots,b_m)$ is examined. If the symbol at the error location $(b_1,b_2,\cdots,b_m)$ is either zero or one, then change this symbol to ξ and decode the corrected slot according to the decoding array in Fig. 4. If the symbol at the error location $(b_1,b_2,\cdots,b_m)$ is ξ and the symbol at location $(\bar{b}_1,b_2,\cdots,b_m)$ is zero, then we change the symbol ξ at location $(b_1,b_2,\cdots,b_m)$ to zero and decode the slot according to the array in Fig. 4. (Due to the structure of C_1 and C_2, the combination with the symbol ξ at error location $(b_1,b_2,\cdots,b_m)$ and the symbol 1 at location $(\bar{b}_1,b_2,\cdots,b_m)$ does not exist.) If the symbol at the error location $(b_1,b_2,\cdots,b_m)$ is ξ and the symbol at location $(\bar{b}_1,b_2,\cdots,b_m)$ is also ξ, then the slot of $\boldsymbol{u}$ and the slot of $\boldsymbol{v}$ at location $(b_2,b_3,\cdots,b_m)$ are either (0,0) and (0,1) or (1,1) and (1,0). Decode these slots in such a way that the number of slots in $\boldsymbol{v}$ with configuration (1,0) is even.

[1] This slot consists of two bits, one with coordinate vector $(b_1, b_2,\cdots,b_m)$ and the other with coordinate vector $(\bar{b}_1,b_2,\cdots,b_m)$.

References

[1] H. H. J. Liao, "Multiple access channels," Ph.D. dissertation, Dep. Elec. Eng., Univ. Hawaii, Honolulu, 1972.

[2] N. T. Gaarder and J. K. Wolf, "The capacity region of a multiple-access discrete memoryless channel can increase with feedback," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-21, pp. 100–102, Jan. 1975.

[3] C. E. Shannon, "Two-way communication channels," in *Proc. 4th Berkeley Symp. Math. Stat. and Prob.* Berkeley, Calif.: Univ. Calif. Press, 1961.

[4] D. E. Muller, "Application of Boolean algebra to switching circuit design and to error detection," *IRE Trans. Electron. Comput.*, vol. EC-3, pp. 6–12, Sept. 1954.

[5] T. Kasami, S. Lin, and W. W. Peterson, "Generalized Reed–Muller codes," *J. Inst. Elec. Commun. Eng. Japan*, vol. 51-C, Mar. 1968.

[6] R. J. Dick and N. J. Sloane, "Enumeration of cosets of first-order Reed–Muller codes," in *Proc. IEEE Int. Conf. on Communications*, vol. 7, June 1971.

[7] E. R. Berlekamp and L. R. Welch, "Weight distributions of the cosets of the (32,6) Reed–Muller codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 203–207, Jan. 1972.

[8] W. W. Peterson, *Error-Correcting Codes.* Cambridge, Mass.: M.I.T. Press, 1961, p. 69.