Random Coding in Noise-Free Multiple Access Networks over Finite Fields

Siddharth Ray[†], Muriel Médard[†] and Jinane Abounadi
Laboratory for Information and Decision Systems
Massachusetts Institute of Technology
Cambridge, MA 02139
e-mail: sray@mit.edu, medard@mit.edu, jinane@mit.edu.

Abstract— **A two transmitter single receiver multiple access noise-free network is considered where interference is additive and the transmit and receive alphabet size is the same. We consider two performance metrics - *Code Rate* and *Sum Rate*. Code Rate is defined as the ratio of the symbols recovered after Multiple Access Interference, to the symbols sent by the transmitters. The Sum Rate is the number of symbols successfully received per unit time. A packet by packet coding scheme is presented where we determine how these rates change with redundancy. We propose a coding mechanism that maximizes the Code and Sum Rates and show that it suffices to code at only one of the transmitters and that systematic codes are sufficient for this purpose. The development is independent of the alphabet size the symbols are defined over. We also show that we can achieve maximum rates by using a random code. This allows us to choose codes in a random fashion and the scheme achieves optimality with probability tending to 1 exponentially with the code length.**

I. Introduction

We consider a multiple access noise-free network where two transmitters are transmitting to a single receiver without coordination in fixed time slots. All transmissions begin at the beginning of the slot. The Multiple Access Interference (MAI) is additive but the alphabet size of the received vector is fixed and the same as that of the transmit vector. We will call this a *finite field adder channel*. Chang and Weldon in [1] have derived the capacity for a multiple access noise-free binary adder channel where the bits interfere additively over the real field. They proposed a coding technique which achieved capacity asymptotically with the number of users. Capacity achieving codes have also been proposed in [2,3,4]. Mathys in [6] determined the T-user capacity regions for the collision channel for asynchronous and slot synchronous users, and also gave constructive codes that approach all rates in these regions. Hughes in [5] considered the design of codes for M users that permit any sub-collection of up to T of the M to transmit at the same time. Caire *et.al* [7] presented a novel class of signal space codes for bandwidth efficient transmission on a random access collision channel.

All of the above works considered collisions where the cardinality of the received vector increased with the number of transmitters. In [10], transmission of information is considered for a modulo-2 multiple access channel where a proper subset of the transmitters transmit. However, it does not consider finite field channels in general. If the alphabet size of the received vector is allowed to grow with the number of transmitters, the receiver has more information about the transmissions than when the received vector is constrained to be in a field which has the same size as that of the transmitted vector. Thus, rates are lower for a finite field adder channel as the receiver can observe only over the field in which transmissions occur. However, the receiver design becomes independent of the number of users. We use two performance metrics : *Code Rate* and *Sum Rate*. *Code Rate* is defined as the ratio of the symbols recovered after MAI, to the symbols sent by the transmitters and *Sum Rate* is the information received per unit time. For fixed information received per slot, maximizing sum rate leads to minimizing the slot length. However, this does not tell us whether one or both transmitters should transmit over the slot duration. We can have situations where the sum rates are same but the energy required per slot is different because one transmitter does not transmit over the entire slot duration. In order to capture this energy efficiency of transmissions, we use the Code Rate metric. The Code Rate tells us what fraction of the energy spent in a slot is used for transmitting information. We show in Theorem 6 that Code Rate maximization gives us the maximum sum rate for this channel. We call the maximum Code Rate possible as the *Optimal Code Rate* and from it go on to derive the maximum sum rate. We present a coding mechanism that achieves
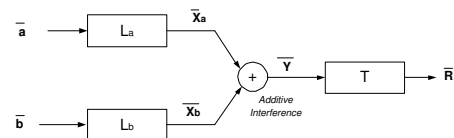

Fig. 1. Multiple Access Network Model.

the Optimal Code Rate for such a channel and also show that a random code becomes optimal with probability tending to 1 exponentially with the length of the code. We can therefore use a random code and achieve optimal rates for this channel with the codeword size well under practical limits. This is akin to the random coding theorem argument, such as the one established for noisy channels in [9]. This paper is divided into 7 sections. In Section II, we present the network model. In Section III, we develop the tools needed to construct codes and in Section IV, discuss code construction. Section V contains the derivation of the maximum code and sum rates that the codes can achieve and in Section VI, we show how random coding achieves maximum possible rates. We conclude in section VII.

II. Model Development

Let $\vec{a}$ and $\vec{b}$ be two vectors of size n_a and n_b, respectively. These represent the data packets that need to be sent to the receiver by the two transmitters. The data packets originate from discrete memoryless uncorrelated sources. For ease of presentation, we operate in the binary field but the results are not dependent on the field size. Since the packets are a sequence of bits, $\vec{a}$ and $\vec{b}$ are vectors in the binary field and henceforth, they will be known as transmit vectors. It is assumed that $n_a \geq n_b$. (Otherwise, the arguments still hold with $\vec{a}$ and $\vec{b}$ interchanged.). Let m_a and m_b be the increase in the size of $\vec{a}$ and $\vec{b}$ respectively due to coding. Therefore, l_a and l_b denote the lengths of the vectors obtained by coding on $\vec{a}$ and $\vec{b}$ respectively. In general $l_a \neq l_b$ and so both transmitters may not be transmitting for the entire slot duration. However, at least one transmitter will transmit for the whole duration. We have
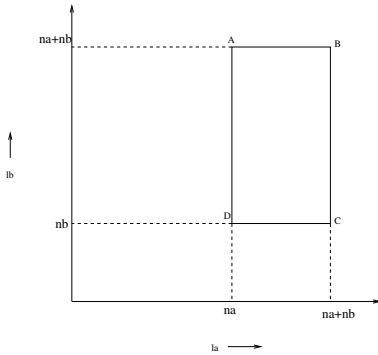
$$l_a = n_a + m_a \quad l_b = n_b + m_b. \tag{1}$$

Fig. 2. Region of Analysis.

If m_1 bits of $\vec{a}$ and m_2 bits of $\vec{b}$ are recoverable at the receiver for given m_a and m_b, we need to find functions that map (m_a, m_b) to m_1 and m_2 and the regions over which these functions are defined. Using these functions, we find the Optimal Code Rate and we show in Theorem 6 that we can derive the maximum sum rate from it. We call the codes that give the optimal code rate as *Optimal Codes*. Knowing these functions, we can find the subset of transmitted bits recoverable for given redundancy. Thus the code rate is $\frac{m_1+m_2}{l_a+l_b}$. The rates R_a of $\vec{a}$ and R_b of $\vec{b}$ are $\frac{m_1}{max(l_a,l_b)}$ and $\frac{m_2}{max(l_a,l_b)}$ respectively and the sum rate, R_{sum}, is $\frac{m_1+m_2}{max(l_a,l_b)}$.

By definition, $l_a \geq n_a$ and $l_b \geq n_b$. When $l_a = l_b = n_a + n_b$, all bits can be recovered after MAI at the receiver. Thereby, we can safely reduce the region for finding the solution to the region *ABCD* shown in Figure 2. All points not in *ABCD* will have a lower code rate as the received vector size remains same for increasing l_a and l_b. Hence, we confine our analysis of finding optimal codes to the region *ABCD*.

In this region $n_a \leq l_a \leq n_a + n_b$ and $n_b \leq l_b \leq n_a + n_b$. Thus $0 \leq m_a \leq n_b$ and $0 \leq m_b \leq n_a$. The received vector sizes are $0 \leq m_1 \leq n_a$ and $0 \leq m_2 \leq n_b$.

We construct a model that represents the multiple access network we are analyzing. Figure 1 shows this model. L_a is a $(n_a + n_b) \times n_a$ size matrix and L_b is a $(n_a + n_b) \times n_b$ size matrix. $\vec{X_a}, \vec{X_b}$ and $\vec{Y}$ are $n_a + n_b$ sized vectors. Receiver matrix

T has a dimension of $(m_1 + m_2) \times (n_a + n_b)$. R is a $m_1 + m_2$ sized vector containing m_1 bits of $\vec{a}$ and m_2 bits of $\vec{b}$ recovered at the receiver. The matrices L_a and L_b code on the input vectors $\vec{a}$ and $\vec{b}$ before transmission. The transmit vectors interfere additively over the binary field. The receiver matrix T decodes the received vector to generate a subset of $\vec{a}$ and $\vec{b}$.

In this model, all operations, matrices and vectors are in the binary field. Even if we use symbols from a larger field, the vectors involved and the matrices L_a and L_b take on the same form. Further, we show in Lemma 1 that even if matrix T contains elements from a larger field, we do no better than when considering elements from a binary field. Therefore, we do not lose generality by confining our analysis to a field of size 2. Analyzing the model, we have the following equations:

$$\vec{X_a} = L_a\vec{a} \quad \vec{X_b} = L_b\vec{b} \quad \Rightarrow \vec{Y} = L_a\vec{a} + L_b\vec{b} \tag{2}$$

$$\vec{R} = T\vec{Y} = (TL_a)\vec{a} + (TL_b)\vec{b} \tag{3}$$

Define: $W_a = (TL_a)$ and $W_b = (TL_b)$.

We define a row vector having only one non-zero element as a 1row. In order to recover m_1 bits of $\vec{a}$ and m_2 bits of $\vec{b}$, W_a should be a $(m_1 + m_2) \times n_a$ size matrix with m_1 1rows, W_b a $(m_1 + m_2) \times n_b$ size matrix with m_2 1rows and the 1row positions for these matrices should not overlap. Let $W = \begin{bmatrix} W_a & | & W_b \end{bmatrix}$ and $L = \begin{bmatrix} L_a & | & L_b \end{bmatrix}$.

III. Coding Mechanism

In this section we develop the tools required in finding optimal codes. Consider matrices L and W. W is generated by receiver matrix T operating on L and because of the nature of W_a and W_b, it consists only of 1rows. The rows of W are thus linear combinations of the rows of L. We need to find, for given L, the maximum number of 1rows in W that can be generated by linear combinations of the rows of L. This maximizes $m_1 + m_2$ for given $l_a + l_b$ which in turn maximizes the Code Rate. The codes formed by this process are optimal codes. This also specifies the matrices L_a, L_b and T. Therefore, optimal codes are found by jointly optimizing the encoder and decoder matrices. We now prove the following theorems:

Theorem 1: Optimal codes are not contained in the region $0 < m_b \leq n_a - n_b$.

Theorem 2: Systematic coding gives rise to optimal codes.

Proof: In order to prove the theorems, we need to establish the following lemma:

Lemma 1: If s unique 1rows are inserted into a matrix J of the form $\begin{bmatrix} I_{n_b \times n_b} 0_{n_b \times (n_a - n_b)} I_{n_b \times n_b} \end{bmatrix}$ to obtain matrix C such that the number of independent row vectors in C is $s + n_b$ and k 1rows have 1 in the positions $[n_b + 1, n_a]$, then the maximum number of 1rows possible by any linear combination of the rows of C is $2s - k$.

Proof: Consider a linear combination $D = \sum_{i=1}^{s+n_b} \alpha_i C(i)$, where $C(i)$ denotes the ith row vector of C. This can be written as: $D = \sum_{j=1}^{n_b} \alpha_{i_j} C(i_j) + \sum_{p=1}^{s} \alpha_{l_p} C(l_p)$ where $i_1, i_2, ...i_{n_b}$ are positions in the matrix where the row vectors of J appear in C, and $l_1, l_2, ...l_s$ are positions in the matrix where the inserted 1rows appear in C. α_i can be in any field. Let $V_1 = \sum_{j=1}^{n_b} \alpha_{i_j} C(i_j)$ and $V_2 = \sum_{p=1}^{s} \alpha_{l_p} C(l_p)$. We will make use of the property of fields that 0 is an identity under addition and any element multiplied with 0 is 0.

Therefore, $V_1 = [\alpha_{i_1}\alpha_{i_2}....\alpha_{i_{n_b}} 0_{(n_a-n_b)\times 1}\alpha_{i_1}\alpha_{i_2}....\alpha_{i_{n_b}}]$. Since the number of independent row vectors in C is $s + n_b$, D can never be an all zero vector unless all α_is are 0. V_2 has k non-zero elements in positions $[n_b + 1, n_a]$ and $s - k$ non-zero elements in the first and last n_b positions. Since D is non-zero for all $\alpha_i \neq 0$, $V_2(i) \neq V_2(i + n_a)$ for $0 < i \leq n_b$. Therefore, in D we have k independent non-zero elements in positions $[n_b + 1, n_a]$ and $2(s - k)$ independent non-zero elements contained in the first and last n_b positions. When we generate 1rows, we force all but one of these independent elements to be 0. The dependent elements are always forced to 0 as they can never generate 1rows.

Thus, the maximum number of 1rows possible is $2s - k$. ∎

This lemma shows that the maximum number of 1rows possible by linear combination is independent of the size of the field. Thus, we can safely assume T to contain elements from the binary field. Using this lemma, we establish the type of coding that needs to be done. Throughout our paper, $I_{k\times k}$ represents a $k\times k$ identity matrix and $0_{p_1 \times p_2}$ represents a $p_1 \times p_2$ null matrix.

Let $P = \left[\begin{array}{c|c} I_{n_a\times n_a} & \begin{array}{c} I_{n_b\times n_b} \\ 0_{(n_a-n_b)\times n_b} \end{array} \end{array}\right]$. We form matrix G by inserting 1rows to P in any position (non-systematic coding). Let matrix W, consisting of $m_1 + m_2$ unique 1rows, be formed such thats its rows are linear combinations of the rows of G. For given m_a and m_b, we need to maximize $m_1 + m_2$. Adding redundancy of m_a generates m_a 1rows (by Lemma 1) in G and reduces the number of 1rows the redundancy m_b can generate by $m_a + n_a - n_b$. Thus, if $m_b \leq m_a + n_a - n_b$, setting $m_b = 0$ is the only way that the redundancy will not be forced on $\vec{b}$. Thus m_b can never be in $(0, n_a - n_b]$.

If $m_b > m_a + n_a - n_b$, 1row vectors can be introduced after the first $n_a + m_a$ positions in G and the number of 1row vectors inserted into G to form L is $k = m_b - [m_a + n_a - n_b]$. Thus L_b is of the form $\left[\begin{array}{c} I_{n_b\times n_b} \\ 0_{n_a\times n_b} \end{array}\right]$ for $m_b = 0$ and $\left[\begin{array}{c} I_{n_b\times n_b} \\ 0_{(n_a-n_b)\times n_b} \\ I_{k\times k}0_{k\times(n_b-k)} \\ 0_{(n_b-k)\times n_b} \end{array}\right]$ for $m_b > m_a + n_a - n_b$.

Since, the number of 1rows added to G by m_a does not depend on where they are inserted, L_a can be systematic, i.e. $L_a = \left[\begin{array}{c} I_{n_a\times n_a} \\ I_{m_a\times m_a}0_{m_a\times(n_a-m_a)} \\ 0_{(n_b-m_a)\times n_a} \end{array}\right]$. Thus systematic coding gives rise to optimal codes and the rows of P form the first n_a rows of L.

IV. CONSTRUCTION OF OPTIMAL CODES

Using the results of the previous section, we now construct optimal codes. Two cases arise:

Case 1: $m_b = 0$

In this case, coding is done on $\vec{a}$ only. Let the redundancy added to $\vec{a}$ be m_a. This corresponds to appending m_a 1row vectors to P such that the 1 in each of these vectors lie in the first n_a positions and the resulting matrix consists of independent rows. Using Lemma 1:

$$m_1 = [n_a - n_b] + m_a \quad m_2 = m_a \tag{4}$$

$$L_a = \left[\begin{array}{c} I_{n_a\times n_a} \\ M_{m_a\times n_a} \\ 0_{(n_b-m_a)\times n_a} \end{array}\right] \tag{5}$$

$$L_b = \left[\begin{array}{c} I_{n_b\times n_b} \\ 0_{n_a\times n_b} \end{array}\right] \tag{6}$$

where $m_b = 0$, $0 \leq m_a \leq n_a$ and M is a matrix containing 1rows.

Case 2 : $n_a - n_b < m_b$. Let $m_b = n_a - n_b + k$ where $0 < k \leq n_b$. In this case coding is done on $\vec{a}$ and $\vec{b}$. Redundancies of m_a and m_b are added to $\vec{a}$ and $\vec{b}$ respectively.

When $m_a < k$, m_a 1rows are appended to P such that each 1row contains a 1 in the first n_a positions. Then, $k - m_a$ 1rows are appended to the matrix resulting from the previous step so that 1 is contained in one of the last n_b positions. 1rows are appended such that the resulting matrix consists of independent rows. Using Lemma 1:

$$m_1 = m_b \quad m_2 = m_b - [n_a - n_b] \tag{7}$$

$$L_a = \left[\begin{array}{c} I_{n_a\times n_a} \\ G_{m_a\times n_a} \\ 0_{(n_b-m_a)\times a} \end{array}\right] \tag{8}$$

$$L_b = \left[\begin{array}{c} I_{n_b\times n_b} \\ 0_{(n_a-n_b+m_a)\times n_b} \\ H_{(m_b-m_a-[n_a-n_b])\times n_b} \\ 0_{(n_a-m_b)\times n_b} \end{array}\right] \tag{9}$$

where, $[n_a - n_b] < m_b \leq n_a$ and $0 \leq m_a < m_b - [n_a - n_b]$. G and H are matrices containing unique 1rows.

When $m_a > k$, coding involves appending k 1rows to P such that each row contains the 1 in the last n_b positions. Then, $m_a - k$ 1rows are appended to the matrix resulting from the previous step so that a 1 is contained in the first n_a positions for each vector. 1rows are appended such that the resulting matrix consists of independent rows. Using Lemma 1:

$$m_1 = m_a + [n_a - n_b] \quad m_2 = m_a \tag{10}$$

$$L_a = \left[\begin{array}{c} I_{n_a\times n_a} \\ 0_{(m_b-[n_a-n_b])\times n_a} \\ S_{(m_a-m_b+[n_a-n_b])\times n_a} \\ 0_{(n_b-m_a)\times n_a} \end{array}\right] \tag{11}$$

$$L_b = \left[\begin{array}{c} I_{n_b\times n_b} \\ 0_{(n_a-n_b)\times n_b} \\ K_{(m_b-[n_a-n_b])\times n_b} \\ 0_{(n_b-m_b+n_a-n_b)\times n_b} \end{array}\right] \tag{12}$$

where, $[n_a - n_b] < m_b \leq n_a$ and $0 \leq m_a < m_b - [n_a - n_b]$. S and K are matrices containing 1rows.

We now prove the following theorem which removes a region from our further analysis:

Theorem 3: Optimal codes are not contained on the line $m_a = m_b - [n_a - n_b]$.

Proof: Let P be defined as before. Coding in this region results in the insertion of at least one row vector to P which is not a 1row. The inserted rows that are not 1rows contain a 1 in the first n_a positions and a 1 in the last n_b positions. The other elements are 0. The number of 1 rows decide the size of the subset recoverable at the receiver. But in this case, the rows that are not 1rows increase redundancy but do not give us a larger subset. Thus, we should not insert any row that is not a 1row. This is not possible on the line $m_a = m_b - [n_a - n_b]$. Hence, this line does not contain optimal codes. ∎

A. Regions

Based on the analysis done, the regions over which optimal codes exist are shown in Figure 3.
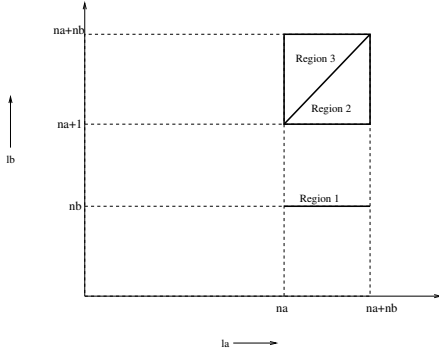

Fig. 3. Gross (un-optimized) regions over which optimal codes exist.

Region 1: $n_b \leq l_a \leq n_a + n_b$ and $l_b = n_b$

$$m_1 = m_a + [n_a - n_b] \quad m_2 = m_a \tag{13}$$

$$CodeRate_{R_1} = \frac{2m_a + [n_a - n_b]}{n_a + n_b + m_a} \tag{14}$$

Region 2: $l_b < l_a \leq n_a + n_b$ and $n_a < l_b \leq n_a + n_b$

$$m_1 = m_a + [n_a - n_b] \quad m_2 = m_a \tag{15}$$

$$CodeRate_{R_2} = \frac{2m_a + [n_a - n_b]}{n_a + n_b + m_a + m_b} \tag{16}$$

Region 3: $n_a \leq l_a < l_b$ and $n_a < l_b \leq n_a + n_b$

$$m_1 = m_b \quad m_2 = m_b - [n_a - n_b] \tag{17}$$

$$CodeRate_{R_3} = \frac{2m_b - [n_a - n_b]}{n_a + n_b + m_a + m_b} \tag{18}$$

B. Optimized Regions

Theorem 4: To achieve the optimal code rate, it suffices to code on only one vector.

Proof: In Region 1 and Region 2, it is seen that m_1 and m_2 do not depend upon m_b. Thus, for higher code rate, m_b should be kept as low as possible. We thus set $m_b = 0$ for Region 1 and $m_b = n_a - n_b + 1$ for Region 2. As $n_a \geq n_b$

$$CodeRate_{R_1} \geq CodeRate_{R_2}. \tag{19}$$

Thus optimal codes cannot be in Region 2 as this region does not contain codes with higher code rate than Region 1. Hence, we do not consider this region in our further search for optimal codes. In Region 3, m_1 and m_2 do not depend on m_a. Therefore, it is best to keep m_a at its lowest, i.e. $m_a = 0$. We thus consider codes over Region 1 and Region 3 where we set $m_b = 0$ and $m_a = 0$ respectively. Thus, in order to achieve the optimal code rate, it suffices to code on only one vector. ∎
The optimized regions are shown in Figure 4.

Region A : $n_a \leq l_a \leq n_a + n_b$ and $l_b = n_b$

$$m_1 = m_a + [n_a - n_b] \quad m_2 = m_a \tag{20}$$

$$CodeRate_{R_A} = \frac{2m_a + [n_a - n_b]}{n_a + n_b + m_a} \tag{21}$$

Region B: $l_a = n_a$ and $n_a + 1 \leq l_b \leq n_a + n_b$

$$m_1 = m_b \quad m_2 = m_b - [n_a - n_b] \tag{22}$$

$$CodeRate_{R_B} = \frac{2m_b - [n_a - n_b]}{n_a + n_b + m_b} \tag{23}$$
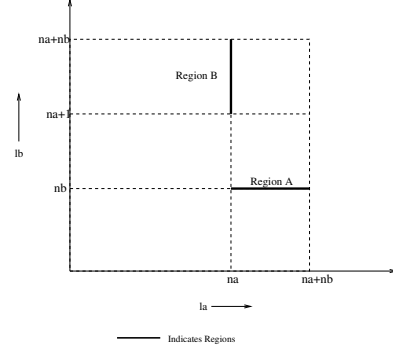
These are the *Optimal Code Rate Equations*.

Fig. 4. Optimized regions.

V. OPTIMAL CODE RATE AND SUM RATE

Theorem 5: Optimal Code Rate and Sum Rate are achieved by coding on the larger vector with codes that allow complete retrieval of the transmitted data vectors.

Proof: From Theorem 4 we see that it suffices to code on only one vector. Let the redundancy be m. In *Region A*, $0 \leq m \leq n_b$ and $CodeRate_{R_A} = \frac{2m + [n_a - n_b]}{n_a + n_b + m}$. In *Region B*, $(n_a - n_b + 1) \leq m \leq n_b$ and $CodeRate_{R_B} = \frac{2m - [n_a - n_b]}{n_a + n_b + m}$.
Case 1 : $n_a > n_b$. When $0 \leq m \leq n_a - n_b$ Region B is excluded and Region A provides the only solution. For all other m, $CodeRate_{R_A} > CodeRate_{R_B}$. Thus, Region A always provides a higher code rate than Region B. From the code rate equations derived earlier, we see that the optimal code rate is obtained when m is largest, i.e. $m = n_b$. Therefore, $(m_a, m_b) = (n_b, 0)$ is the optimal point. This corresponds to $(l_a, l_b) = (n_a + n_b, n_b)$. Thus, for obtaining the highest code rate, we code on the *larger vector* and the redundancy size is the size of the smaller vector. The optimal code rate is

$$CodeRate = \frac{n_a + n_b}{n_a + 2n_b}. \tag{24}$$

Case 2: $n_a = n_b = n$ Here, for given m, both regions give the same code rate and we can code on any of the two vectors. A symmetry exists about the line $l_a = l_b$ and there are two optimal points. The optimal code exists when m is maximum, i.e. $m = n$. These points are $(m_a, m_b) \in [(0, n), (n, 0)]$ corresponding to $(l_a, l_b) \in [(2n, n), (n, 2n)]$. In this case, optimal coding results in the size of redundancy being equal to the transmit vector size and the optimal code rate is $\frac{2}{3}$.
We see from (20-23) that Optimal Code Rate and Sum Rate arise with codes that recover all data sent by the transmitters. ∎

Theorem 6: The maximum sum rate for a multiple access finite field adder channel is 1 and this is obtained from the optimal code rate.

Proof: From Theorem 5 we see that $max(l_a, l_b) = n_a + n_b$, $m_1 = n_a$ and $m_2 = n_b$. All quantities are normalized with

respect to the field size under consideration.

$$R_a = \frac{n_a}{n_a + n_b} \quad R_b = \frac{n_b}{n_a + n_b} \quad \Rightarrow R_{sum} = 1. \quad (25)$$

For this channel we know that $I(Y; X_a, X_b) = H(Y) = 1$. Thus $R_{sum} \leq 1$. We have thus reached the upper limit in (25) and get the maximum sum rate from the optimal code rate for this channel. ∎

VI. RANDOM CODING

In the previous section, we derived the optimal code and sum rates (24, 25) for a two-transmitter multiple access binary adder channel where the transmit vectors $\vec{a}$ and $\vec{b}$ ($n_a \geq n_b$) interfere additively over the binary field. We had also shown that it is sufficient if we code on only one of the transmit vectors and that we achieve the optimal code rate by coding on $\vec{a}$ with a redundancy of n_b. We now show that we can achieve optimal rates by randomly coding over the transmit vectors. We assume that the receiver has knowledge of the code being used at the transmitter.

Theorem 7: For a two transmitter multiple access binary adder channel where the transmit vectors interfere additively over the binary field, random coding gives the optimal code rate as code lengths tend to infinity.

Proof: We had established in Theorem 5 that coding on the larger transmit vector is sufficient to achieve optimal rates. When the two transmit vectors have the same length, it does not matter where we put the code and for our subsequent analysis we choose $\vec{a}$ to have the code. Thus, we now code randomly over the larger transmit vector $\vec{a}$ to generate redundancy $\vec{g}$ having a length of n_b.

We can break $\vec{a}$ into two vectors $\vec{a_1}$ and $\vec{a_2}$ where $\vec{a_1}$ is a vector representing the first n_b bits of $\vec{a}$ and $\vec{a_2}$ is a vector representing the last $n_a - n_b$ bits of $\vec{a}$. Thus $\vec{a} = \begin{bmatrix} \vec{a_1} & \vec{a_2} \end{bmatrix}$. The vectors coming out of the encoders are $\vec{X_a} = \begin{bmatrix} \vec{a_1} & \vec{a_2} & \vec{g} \end{bmatrix}$ and $\vec{X_b} = \begin{bmatrix} \vec{b} \end{bmatrix}$. Now, consider any vector of length n as an element belonging to a finite field of size 2^n represented by F_{2^n}. Thus for any x_1, x_3 and $y_1 \in F_{2^{n_b}}$ and $x_2 \in F_{2^{n_a - n_b}}$ we can consider $x_1 \equiv \vec{a_1}, x_2 \equiv \vec{a_2}, x_3 \equiv \vec{g}$ and $y_1 \equiv \vec{b}$. $\vec{g}$ is generated from $\vec{a_1}$ using a random code. This corresponds to generating x_3 from x_1 such that $x_3 = \alpha x_1$ where α is randomly (uniformly) picked from $F_{2^{n_b}}$. *This multiplication by a random field element represents the random coding.*. After Multiple Access Interference (MAI) we get $\vec{Y}$ of length $n_a + n_b$ such that $\vec{Y} = \vec{X_a} + \vec{X_b}$. $\vec{Y} \equiv \begin{bmatrix} x_1 + y_1 & x_2 & x_3 \end{bmatrix}$ where addition is over $F_{2^{n_b}}$. $x_1 + y_1$ corresponds to the first n_b, x_2 to the next $n_a - n_b$ and x_3 to the last n_b bits of $\vec{Y}$. From Theorem 5, we see that we can achieve the optimal code and sum rates only with complete recovery at the receiver. Thus, we need to get x_1, x_2 and y_1 after decoding. We get x_2 as it does not suffer MAI. For $m \in F_{2^{n_b}}$ denote: $m = x_1 + y_1$ with addition corresponding to finite field addition and m represents the first n_b bits of $\vec{Y}$. Now, for any $\alpha \in F_{2^{n_b}}, \alpha \neq 0, \exists \alpha^* \in F_{2^{n_b}}$ such that

$$\alpha^* \alpha = 1. \quad (26)$$

x_3 corresponds to the last n_b bits of $\vec{Y}$ and we get y_1 from: $y_1 = m + \alpha^* x_3$. Using y_1, we get x_1 in the next step : $x_1 = m + y_1$ where all operations are confined to $F_{2^{n_b}}$. Thus,

we recover x_1, x_2 and y_1 and achieve optimal rates.

We achieve the optimal code rate as long as (26) holds, i.e. multiplicative inverse of α exists. Equation (26) holds iff $\alpha \neq 0$. Thus, the probability that a random code is an optimal code, P_R is given by

$$P_R = 1 - P(\alpha = 0). \quad (27)$$

Since α is chosen randomly (uniformly) from $F_{2^{n_b}}$,

$$P(\alpha = 0) = \frac{1}{2^{n_b}} \Rightarrow P_R = 1 - \frac{1}{2^{n_b}}. \quad (28)$$

Since, $n_a \geq n_b$, by letting $n_a, n_b \rightarrow \infty$ we get

$$lim_{n_a, n_b \rightarrow \infty} P_R = 1. \quad (29)$$

∎

Since the probability of a random code being optimal tends to 1 exponentially with n_b, we may achieve the optimal code rate with moderate code lengths. Also, the number of attempts to get an optimal code falls exponentially with code length. This is a Strong Coding Theorem for this channel and the result is akin to the Schwartz-Zippel Theorem in [8].

VII. CONCLUSION

We have looked at a multiple access noise-free network where the transmit and receive alphabet size is the same. We derived the *Optimal Code Rate* and *Sum Rate* for such a channel and developed a coding mechanism that achieves these rates. We obtained the relation between the size of the subset that can be recovered following MAI and redundancy added at the transmitters which led to the derivation of optimal code and sum rates. We derived a Strong Coding Theorem for this channel where we showed that a random code gives the optimal code rate with probability tending to 1 exponentially with code length.

VIII. REFERENCES

[1] S. Chang and E.J.Weldon,"Coding for T-user Multiple-Access Channels", *IEEE Transactions on Information Theory, Vol.IT-25, No.6, Nov 1979.*

[2] B.L. Hughes and A.B. Cooper, "Nearly Optimal Multiuser Codes for the Binary Adder Channel", *IEEE Transactions on Information Theory, Vol.-42, No.2, March 1996.*

[3] G.H. Khachatrian and S.S. Martirossian,"Code Construction for the T-user Noiseless Adder Channel", *IEEE Transaction on Information Theory, Vol.44, No.5, Sep 1998.*

[4] J. Cheng and Y. Watanabe,"T-User Code with arbitrary code length for Multiple-Access Adder Channel", *IEICE Transactions Fundamentals, Vol.E82-A, No.10, October 1999.*

[5] B. Hughes,"Capacity and Coding for T active users out of M on the collision channel.", *ISIT 1993.*

[6] P. Mathys, "A class of codes for T active users out of N multiple-access communication system", *IEEE Transactions on Information Theory, Vol. 36, No. 6, November 1990.*

[7] G.Caire, E.Leonardi, E. Viterbo,"Improving performance on wireless networks using collision resistant modulations.", *Globecom '98.*

[8] R. Motwani and P. Raghavan, "Randomized Algorithms", *Cambridge University Press, 2000.*

[9] R.G. Gallager, "Information Theory and Reliable Communication", *Wiley, 1968.*

[10] G. Poltyrev and J. Snyders, "Linear Codes for the Sum Mod-2 Multiple-Access Channel with Restricted Access.", *IEEE Transactions on Information Theory, Vol. 41, No.3, May 1995.*