Forward Collision Resolution — A Technique for Random Multiple-Access to the Adder Channel[1]

I. Bar-David, E. Plotnik, R. Rom

Department of Electrical Engineering
Technion - Israel Institute of Technology
Haifa 32000, Israel

ABSTRACT

Consider M – HChoose $P - T$ communications: T users or less, out of M potential users, are chosen at random to simultaneously transmit binary data over a common channel. A method for constructing codes that achieve error-free M – HChoose $P - T$ communication over the noiseless Adder Channel (AC), at a nominal rate of $1/T$ bits per channel symbol per active user, is described and an efficient decoding procedure is presented. The use of such codes is referred to as Forward Collision Resolution (FCR), as it enables correct decoding of collided messages without retransmissions. For any $given\ T$ a code is available that yields a stable throughput arbitrarily close to 1 message/slot. Furthermore, if the occurrence of collisions is made known to the transmitters, such a throughput can be maintained for $arbitrary\ T$, $T \leq M$ as well. If such feedback is not available, and T is $random$, the probability of an unresolved collision is significantly smaller than the probability of a collision in an uncoded system, at comparable message-arrival and information rates.

Haifa, December 10, 1992

---

[1]Parts of this paper were presented at the IT workshop at Bellagio, Italy, June 1987, under the title The Capacity of the Random Multiple-Access Channel is at least 1, Achievable by Forward Collision Resolution and at INFOCOM 89,under the title An Efficient Multiple-Access Method for the Binary Adder Channel. It incorporates work from the doctoral program of E. Plotnik.The work of I. Bar-David was supported by the Technion Fund for the Promotion of Research.

I. INTRODUCTION

The problem of sharing a common channel by several users has been mostly treated within the framework of either of the two categories described by Gallager in his review paper [1 and references cited therein]:

(i) The multiuser channel: All users transmit simultaneously with their transmissions mutually interfering. The number of users is usually not large and certainly finite. Feedback is typically unavailable and redundant coding is used to enable correct reception of messages in the presence of interference [2].

(ii) The random access channel: A very large number, often modeled as infinite, of potential users is assumed, each having a very small, even vanishing rate of message generation.Then with high probability not more than a single transmission occurs in the channel in any specific transmission interval. In general, no provisions are made to correctly decode the messages when they interfere: interfering messages are assumed to be lost and their retransmission is scheduled by a collision resolution algorithm (CRA), which presumes some form of feedback [3]. Recently, new techniques for accessing channels that do not depend on feedback have been introduced [4, 5] and analyzed [5].

Pointing out this (unnatural) dichotomy of research efforts in his review paper, Gallager suggests that what is needed is a coding technology that is applicable for a large set of transmitters of which a small, but variable subset, simultaneously use the channel. One avenue in this direction is the formulation of the problem of $M\text{-}Choose\text{-}T\ communication$: A finite population of $M\ potential$ users is given and a number T or fewer users ($T \le M$) are $active$, that is only they are transmitting in any given time. The number and identity of the active users is not known to the receiver(s). Thus each receiver has to identify all active users and their respective messages. We distinguish among the following cases: T is given, arbitrary, or random. Tsybakov and Likhanov [6] and Bassalygo and Pinsker [7] have treated the $M - \text{HChoose}\, P - T$ problem

with given T over the collision channel that was defined in [5], and have shown that asymptotically (as M and $T \to \infty$), a throughput of e^{-1} is achievable.

In [8] Dyachkov and Rykov considered M-Choose-T Communication over the discrete-time and fully synchronized noiseless adder channel (AC). There, B_s-codes and (s,t)-plans were used to identify the active transmitters and the destinations of the messages that were sent. After the identification stage, the active users share the channel on a TDMA basis. Lower and upper-bounds for the length of the codewords needed to find the active users were derived, for a given $predetermined$ value of T.

Another related work by Lindstrom [9] addresses the problem of finding defective elements within a finite set by unramified experiments. In his work Lindstrom describes a method for constructing a matrix, such that distinct subsets of T columns in the matrix have distinct sums (the summation of the columns is carried over the real numbers). Matrices with this property will also be used by us, in the construction of codebooks for M-Choose-T Communication.

Recently, Mathys [10] also considered the M–Choose–T Communication over the AC. For a given value of T, he showed a construction of M codebooks, one for each potential user, such that if the decoder knows the set of active users, the sum of codewords of any T or fewer users is uniquely decodable. When the set of active users is not known to the receiver, it is shown that this set can be identified uniquely (in addition to unique decodability) provided that at most $T/2$ users are active simultaneously. When the inputs to the channel are binary, the information rate of each codebook approaches $1/T$ from above. Thus, the aggregate information rate of the codes is 1 bit per channel symbol when the set of active users is known to the decoder and it reduces to 0.5 bits per channel symbol when this set is not known.

In the present paper, we also address the $M - \text{HChoose}\, P - T$ Communication problem over the fully synchronized noiseless AC. The time-discrete noiseless AC is defined [2] by the following relation between its output Z and its inputs $X_i \quad , i = 1, 2, \ldots, T$:

$$Z = \sum_{i=1}^{T} X_i , \qquad X_i \in \{ 0 , 1 \} ,$$

Each input X_i, $i = 1, 2, \ldots, T$ to the channel is either 0 or 1, and the channel output Z is the sum of the inputs where summation is over the *real* numbers.

We introduce (in section II) a class of codes that achieve an aggregate rate of 1 bit/channel use. A simple decoding procedure appropriate for the case of given T is presented in section III. We refer to the use of such codes as Forward Collision Resolution (FCR); they ensure correct reception of collided messages without the need for their retransmission. The aggregate transmission rate using these codes is 1 bit per channel symbol if T users are simultaneously active. If less than T users are active, the aggregate rate decreases proportionally.

Note however that an aggregate rate of 1 bit/channel use is far below the capacity of the AC. It is well known [11] that when all M users are simultaneously active, the capacity of the AC is approximately $\frac{1}{2}\log M$. For M-Choose-T Communications, applying the coding theorem of [12] to the AC case, reveals that the capacity is approximately $\frac{1}{2}\log T$. (This result is only an existence proof derived by random coding arguments).

In a realistic situation the value of T is neither constant nor can it be predetermined. In such a case, if feedback about collisions is available at the transmitters, we show in section IV that the FCR codes can be used in an efficient channel-accessing algorithm. The algorithm is adaptive in the sense that if L users are active simultaneously, the transmission rate for each user adjusts to $1 / L$, such that an aggregate rate of unity is maintained. Furthermore, it is shown that such performance is available with bounded transmission delay. This case is treated in section IV.

In other applications, such as the hidden terminal case [13], feedback about collisions is not available. In such cases an appropriate performance criterion is the probability of errorless reception. This can be evaluated if T is considered a random variable. It is shown in section V that if FCR codes are used, the probability of erroneous reception of messages is considerably

reduced.

II. CODING FOR M-CHOOSE-T COMMUNICATIONS OVER THE ADDER CHANNEL

We consider a symmetrical situation in which the information rate for each user is R, and each codeword has exactly N binary digits. In addition, perfect block and bit synchronization among the M potential users is assumed througout the paper.

Code construction:

Assign to each user i of the M users a codebook C_i, with $|C_i| = 2^{RN}$ binary codewords ($i = 1, ..., M$). A necessary condition for error free $M - \text{HChoose}\, P - T$ communication is $\{ C_i \} \cap \{ C_j \} = \varnothing$, $j \neq i$. Denoting by C the set $\bigcup_{i=1}^{M} C_i$, the requirement that $|C| = M 2^{RN}$ follows. Let the codebook C be the columns of a parity check matrix H of a T-error correcting primitive BCH code [14 ch. 7. 6]. Partition these columns equally among the M users to construct the codebooks $C_i \quad i = 1, 2, \cdots M$.

Claim: The construction ensures error free $M - \text{HChoose}\, P - T$ communication at a rate of 1/T per active user.

Proof: We first demonstrate the error-freedom property. This hinges on the property of a linear T-error correcting code that any $2T$ columns of its parity check matrix are linearly independent [14, pp. 33]. Thus, the sum of any T or fewer columns of H, differs from that of any other T or fewer columns, which is a sufficient condition to uniquely decode the transmitted codewords, when T or less users are active. Furthermore, since the columns are distinct it follows that $\{ C_i \} \cap \{ C_j \} = \varnothing$ ($i , j = 1 , 2 , ..., M ; i \neq j$). Hence correct decoding of the messages also uniquely identify the transmitters.

We next estimate the rate of error-free transmission. The matrix H has $2^m - 1$ columns of $m \cdot T$ bits each, where m is an arbitrarily large, free design parameter. The code rate R of each

user is given by setting $N = mT$ and $M \cdot 2^{RN} = 2^m - 1$. Then

$$R = \frac{1}{T \cdot m} \cdot \log \frac{2^m - 1}{M} \underset{m>>1}{\approx} \frac{1}{T} \left(1 - \frac{\log M}{m}\right) \underset{m\to\infty}{\to} \frac{1}{T}$$

■

It follows from the above relation that, in order to achieve a rate of $\frac{(1-\varepsilon)}{T}$ per user, the codeword length $N = mT \approx T \log(\frac{M}{\varepsilon})$ increases only logarithmically with M. For example if $M = 200$, $T = 10$ and the designed aggregate sum rate is 0.95, then we have $m = 153$ and $N = mT = 1530$. Although the codebook size for each user is $(2^m - 1)/M = 5.71 \cdot 10^{43}$, the encoding complexity is proportional to the complexity of raising the primitive element α of $GF(2^m)$ to the appropriate powers, as can be seen from the structure of H in Fig. 1a. There the construction of the H matrix is illustrated in terms of the binary m-tuple α which is the generator of the multiplicative group of $GF(2^m)$ [14, p. 204]. The symbol $\underline{1}$ represents the m-tuple (1 0 0 $\cdots$ 0). An example for $T=2$ and $m=4$ is presented in Fig. 1b: every 4 columns are linearly independent over $GF(2)$.

III. DECODING PROCEDURE FOR GIVEN T

Let $\underline{Z}$ be the output vector from the AC. From $\underline{Z}$, a second vector $\underline{Y}$ is derived,via a symbol by symbol modulo 2 operation, i.e. $\underline{Y} = \underline{Z} \mod 2$. It follows from the code construction that $\underline{Y}$ is a modulo 2 sum of up to T columns of H. Denote the transmitted columns by $\underline{X}_{i_1}, \underline{X}_{i_2}, \ldots, \underline{X}_{i_r}$ ($r \le T$), where $i_1, i_2, \ldots, i_r \in \{0, 1, 2, \ldots, 2^m - 2\}$ are the ordinal numbers of the corresponding columns, selected from H for transmission, increasing from left to right. Owing to the structure of H (Fig. 1a), it is sufficient to recover from $\underline{Y}$ the first m bits of each transmitted codeword $\underline{X}_j$, that is α^j, $j = i_1, \ldots, i_r$; the remaining $(T-1) \cdot m$ bits of each codeword are found by raising α^j to its odd powers from 1 up to $2T-1$, to yield α^{3j}, α^{5j}, $\alpha^{(2T-1)j}$. Here, multiplications are in $GF(2^m)$.

In error-correcting code terminology the term *syndrome vector* is used to denote the sum of those columns of H whose indices correspond to the locations of "1" elements in the error vector [14, p. 17]. The vector $\underline{Y}$, being the mod 2 sum of T or fewer columns of H, can therefore play the role of a syndrome in a T-error correcting BCH code; the indices $i_1,\ldots,i_r$ playing the role of the "1" elements in the error vector. Thus,the proposed decoding procedure uses steps from the decoding of BCH codes. The computation of the syndrome, which is the initial step in BCH decoding is not needed in our case since $\underline{Y}$ is the syndrome itself. The first step then, is to find the error-locating polynomial. If the Berlekamp-Massey algorithm is used, this step requires $O((2T+1)^2 \cdot \log^2(2^m-1)) \approx O(N^2)$ operations over $GF(2)$, since $N = mT$.

The next step is to find the roots of the error-locating polynomial in $GF(2^m)$. This yields $\alpha^{i_1}, \alpha^{i_2}, \cdots \alpha^{i_r}$, which are the first m bits of each transmitted codeword. This requires $O((2T+1)^3 \cdot \log^3(2^m-1)) \approx O(N^3)$ operations over $GF(2)$ [15]. The consecutive $(T-1) \cdot m$ bits of each codeword are found by rasing to the appropriate odd powers, as pointed out above.

The complexity of the decoding procedure is thus polynomial in the length N (of the order of N^3 operations), and the decoding can be implemented on sequential machines as discussed in [15]. For the previous example, taking $M = 200$, $T = 10$ and $m = 153$, we find that $N \approx 3.6 \cdot 10^9$ operations over $GF(2)$. However, when m is not too large, implementation of the decoding steps can be done with shift registers circuits, with m cells in each register.

IV. M-CHOOSE-T COMMUNICATION WITH ARBITRARY T

In a realistic situation the value of T is neither constant nor can it be predetermined. Then if the actual number of active users is less than T, channel resources are wasted, and if larger than T, disrupting collisions occur. However, we show below that for applications where feedback about collisions is available to all transmitters an efficient adaptive channel-accessing algorithm, based on the FCR codes that overcomes this difficulty, does exist. The algorithm ensures

errorless transmission at a throughput of unity for any number of active users up to M. More precisely, the proposed algorithm yields a nominal rate of $1/L$ per active user, for any number L of active users $1 \leq L \leq M$. The algorithm is suited for a slotted system, in which the duration of each slot is equal to the time needed for transmission of m bits by an active user. It also assumes that there exists an independent, errorless feedback channel through which all users are notified at the end of every slot about one of two outcomes success or collision.

A. The Algorithm

The algorithm is based on the observation that if exactly k users transmit, then a $M-$HChoose$P-k$ code is sufficient. It also requires the availability of a mechanism to determine whether more than k users had been active when a $M-$HChoose$P-k$ code was used. One such mechanism for the BAC is described below.

Denote by H_k the H matrix of a $M-$HChoose$P-k$ code. In this notation Fig. 1a is an H_T matrix and Fig. 1b an H_2 matrix.

The algorithm proceeds as follows: Each active user transmits an m-tuple which is the column in H_1 that corresponds to its message. If there was a single user the operation is successfully completed and success is fed back. If however, there were more users, collision is fed back, whereupon each active user transmits the second m-tuple of the column in H_2 that corresponds to its message. Two users will succeed at this stage.

In general if there are v users the algorithm will end when the columns of the H_v will have been used, that is after exactly v slots. Thus, the algorithm does achieve an aggregate throughput of unity for arbitrary number of users, up to M. One mechanism to determine the required feedback is to require every active user to prefix the signal "1" to its transmitted m-tuple. At the receiver of the AC these signals sum up so that at the end of the first slot the receiver knows exactly the number of transmitters. Note, however, that the transmitters need not know the number of active users, and therefore a success/collision feedback suffices.

B. Delay-Throughput characteristics of the algorithm

In this section we use a network model that was presented in [16, 17] and discuss the average delay that a message incurs from the time it is generated until it is successfully transmitted with the use of our channel access algorithm.

Consider M identical users each having a single-message buffer. Every user having an empty buffer generates a message in any slot with probability $p(= 1 - q)$; Once the user schedules its message for tranmission (i.e, after having received success feedback in the previous slot) the buffer is considered empty and the generation process restarts. Transmission rules follow our access method.

A detailed analysis of the delay-throughput characteristics of the algorithm can be found in [18]. Fig. 2 depicts the average normalized delay versus throughput for message length m=200 and M=5,10,15. If $\overline{D}$ is the average delay of a message then the normalized delay D is defined by $D = \frac{\overline{D}}{M}$. It can be seen that if the traffic is light the average delay is close to two slots. At high load the average delay approaches 2M slots. We have compared these results with a slotted ALOHA system having the same number of potential users and the same statistical assumptions about arrivals. The average delay for ALOHA systems in moderate or heavy traffic is larger, about 3M to 10M. Another advantage of our algorithm is that its maximal throughput is $(1 - \frac{\log M}{m})$, while for the finite ALOHA system the maximal throughput is about 0.4. However, we mention again the necessity of full (block and bit) synchronization in our algorithm, which is not required in the Slotted Aloha system.

A similar (but much more complex), analysis can be done in the case that each potential user has a K-message buffer $(K > 1)$. With our channel access algorithm, the system remains stable as long as the aggregate message generation rate does not exceed $\frac{M}{2}$ messages per slot, since in heavy load M messages are successfully transmitted after a delay of $2M$ slots.

V. COMMUNICATION WITHOUT FEEDBACK WITH RANDOM T

When feedback about collisions is not available, an appropriate performance measure is the probability P_e of erroneous reception of messages. For its evaluation we assume Poisson arrivals with an (aggregate) average of λ messages per slot. Our purpose is to compare the merit of using FCR codes. If we keep the transmission bandwidth fixed, namely we use the same symbol durations for encoded and uncoded messages, the encoded messages (which we name packets) are $1/R$ times longer after encoding. Therefore P_e is given by:

$$P_e = \sum_{T=T_0+1}^{\infty} \frac{(\lambda/R)^T \cdot e^{-\lambda/R}}{T!}$$

where T_0 is the number of resolvable colliding messages and is a design parameter of the system. In the proposed FCR codes the rate is $R \approx 1/T_0$. Table I presents P_e for $\lambda = 0.5$ and various values of T_0 which the advantage of the technique is apparent. Note that $T_0 = 1$ corresponds to uncoded transmissions.

T_0	P_e
1	.090
2	.080
4	.053
6	.034
8	.021
10	.014
12	.009
14	.006

Table 1: Error Probability For $\lambda = 0.5$ against T_0

An illustrative sample of messages arrivals and their encoded transmission with rate $1/2$ coding is given in Fig. 3. Because of the encoding of transmitted packets the slots used for transmission are twice as large as that needed without encoding. This lengthening does cause some collisions that wouldn't have occurred in the uncoded case; these events are however much rarer than those resolved by the coding.

REFERENCES

[1] R. G. Gallager, A Perspective on Multiaccess Channels, IEEE Trans. on Information Theory, Vol. IT-31, pp. 124–142, March 1985.

[2] E.C. Van der Meulen, A Survey of Multi-Way Channels in Information Theory: 1961 - 1976, IEEE Trans. Information Theory, Vol. IT-23, pp. 1-37, January 1977.

[3] J. L. Massey, Collision Resolution Algorithms and Random Access Communications, in *Multi-User Communication Systems*,edited by G. Longo,New-York,1982.

[4] J. L. Massey, The Capacity of the Collision Channel without Feedback, Abstracts of Papers, IEEE Int. Symp. Information Theory, Les Arcs, France, p. 101, June 1982.

[5] J. L Massey and P. Mathys, The Collision Channel without Feedback, IEEE Trans. on Information Theory, Vol. IT-31, pp. 192–204, March 1985.

[6] B. S. Tsybakov and N. B. Likhanov, Packet Switching in a Channel without Feedback, , Probl. Perdachi Inform., Vol. 19, pp. 69–84, April–June 1983 (in Russian).

[7] L. A. Bassalygo and M. S. Pinsker, Restricted Asynchronous Multiple Access, Probl. Perdachi Inform., Vol. 19, pp. 92–96, October–December 1983 (in Russian).

[8] A. G. Dyachkov and V. V. Rykov, A Coding Model for a Multiple-Access Adder Channel, Probl. Perdachi Inform. vol. 17, pp. 26–32, Aprilne 1981 (in Russian).

[9] B. Lindstrom, Determining subsets by unramified experiments, Survey of Stat. Design and Linear Models, North-Holland, Amsterdam (1975).

[10] P. Mathys, A Class of Codes for a T Active Users out of N Multiple-Access Communication System, Light and Short Codewords, IEEE Trans. on Information Theory, Vol. IT-36, pp.1206-1219, November 1990.

[11] J. K. Wolf, Multi-User Communication Networks, In Communication Systems and Random Process Theory, J.K. Skwirgynski, Ed., Alphen aan den Rijn. The Netherlands, 1978, pp. 37-53.

[12] E. Plotnik, The Capacity Region of the Random Multiple-Access Channel, Proc. 1990 Int. Symp. on Information Theory, San-Diego.

[13] F.A. Tobagi and L. Kleinrock, Packet Switching in Radio Channels: Part II - The Hidden Terminal Problem in CSMA and Busy-Tone Solution, IEEE Trans. on Communications COM-23, pp. 1417-1433, December 1975.

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. North-Holland, Amsterdam, 1977.

[15] R. M. Roth and G. Seroussi, Encoding and Decoding of BCH Codes using Light and Short Codewords, IEEE Trans. on Information Theory, Vol. IT-34, pp.593-596, May 1988.

[16] L. Kleinrock and S. S. Lam, Packet Switching in a Multiaccess Broadcast Channel:Performance Evaluation, IEEE Trans. on Communications, Vol. 23(4) pp. 410-423 april 1975.

[17] R. Rom and M. Sidi, *Multiple Access Protocols:Performance and Analysis*, Springer-Verlag.

[18] I. Bar-David, E. Plotnik and R. Rom, An Efficient Multiple-Access Method to the Binary Adder Channel. EE Technical Publication No. 731 1989, Technion, Israel Institute of Technology Dept. of Electrical Engineering.

$$H = \begin{bmatrix} \underline{1} & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \\ \underline{1} & \alpha^3 & \alpha^6 & & \alpha^{3(2^m-2)} \\ \underline{1} & \alpha^5 & \alpha^{10} & & \alpha^{5(2^m-2)} \\ . & & & & \\ . & & & & \\ . & & & & \\ \underline{1} & \alpha^{2T-1} & \alpha^{2(2T-1)} & & \alpha^{(2T-1)(2^m-2)} \end{bmatrix}$$

a. General Construction

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ - & - & - & - & - & - & - & - & - & - & - & - & - & - & - \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$2^4 - 1 = 15$$

b. Example for $T = 2$, $m = 4$. 15 codewords of length 8

Fig. 1. Codebook H