3) From 1) and Lemma 4, part 1) we deduce for each \( \tau \)-invariant
\[ A_i(t \neq X) \]
\[ a_i = (h(Y))(2^i-1)E_i + (h^{-1}(Y))(2^i-1)(1 + Y^{d_i})^{-1}h(Y) + (h(Y))(2^i)E_i. \]

From Proposition 3 we deduce that \( \sigma(Y) \) is equal to
\[ I_1 T \tau(I_1) + (2^i+1)(h + h^2) \cdot \left( \sum_{j=0}^{2^i+1} E_j \right) E_n. \]

The sum is for \( i = 2k + 1, \ldots, N-1 \), and \( j = 0, \ldots, 2^i-1 \). Substituting \( h^{-1}(Y) \) to \( h(Y) \) and \( (T_{2^i+1})^{2^i} \) to \( T_{2^i+1} \) we obtain the desired \( \sigma^{-1}(Y) \).

**Construction of SCN Basis of \( GF(q^{2^i}) \) over \( GF(q) \) (t Odd)**

1) Compute \( h(Y) \) from the normal basis obtained in Section II.
2) With 3) of Lemma 3 compute \( h^{-1}(Y) \).
3) Compute \( I_1, h^{-1}(Y), T(I_1) \) and \( I_2 \).
4) Compute \( (h^{-1}(Y))(2^i-1) \cdot (h^{-1}(Y))(2^i) \cdot (h^{-1}(Y))(2^i-1)I_2 \) and finally
\[ h(2^i-1)(h^{-1} + h^{2^i}). \]
5) Compute
\[ \sum_{j=0}^{2^i-1} \sum_{j=0}^{2^i-1} Y^{(2^i+1)x_i} E_j. \]
6) Compute \( a^{-1}(Y) \).

**Example 5**: From 1) of Example 1, we find the following equalities:
\[ h(Y) = h^{-1}(Y) = 1 + Y + Y^2 + Y^4 + Y^8. \]
We also find
\[ I_1 = 0, I_2 = 1 + E_2 = Y^2 + Y^4. \]
We have
\[ Y^{d_1}(1 + Y^{d_1})^{-1} = Y^2(1 + Y^2)^{-1} = Y^2(1 + Y^4) = 1 + Y^2. \]
The polynomial \( a^{-1}(Y) \) is given by the equality
\[ a^{-1}(Y) = E_1 + (Y + Y^2 + Y^4)^{(1 + Y^2)E_1 + E_2} = Y^2 + Y^3 + Y^5. \]
The coefficients of the desired \( \alpha \) are \( 0, 0, 1, 0, 1 \) over the basis generated by \( J \). We find \( \alpha = X + X^2 + X^3 \), which generates an SCN basis.

**IV. CONCLUSION**

Starting from a simple deterministic construction of a normal basis of \( GF(q^{2^i}) \) over \( GF(q) \) (\( q = p^j, p \) prime), we propose two constructions of self-complementary normal bases in every possible case for which the characteristic is 2. For the case \( p = 2, t = 1, n \) odd, our first construction is as simple as that of Wang, who only considers that case. But this first construction also works for every possible \( \tau \). Our second construction works for \( n = 2t, t \) odd, \( p = 2 \). It does not work for all possible \( \nu \) because \( \sqrt{(h(Y)} \) does not always exist.

**ACKNOWLEDGMENT**

We wish to thank the referees who helped us improve this paper.

**REFERENCES**


---

**Linear Codes for the Sum Mod-2 Multiple-Access Channel with Restricted Access**

Gregory Poltyrev, Member, IEEE, and Jakov Snyders

**Abstract**—Transmission of information through a multiple-access modulo-2 adder channel is addressed for the situation that out of a fixed family of \( N \) potential users at most some \( m < N \) are active simultaneously. We assign codes to the \( 2^N \) users in such a way that the receiver is able to correct any \( t \) or less errors and separate the \( s < m \) messages without a priori knowledge of the subset of active users. A decoding procedure is presented. The efficiency of our method of code construction is demonstrated by some examples and by an upper bound, that asymptotically tends to zero, on the loss of rate.

**Index Terms**—Multiple-access channel, linear code, maximum distance separable code, modulo-2 separable codes.

**I. STATEMENT OF THE PROBLEM**

This correspondence addresses the problem of information transmission through a multiple-access channel (MAC), for the case...
that there are some $N$ potential users, but only $s$, $s \leq m < N$ of them are active simultaneously (i.e., at most some $m < N$ users are transmitting their messages). We assume that the active users are completely synchronized, in the sense that both the signals and blocks of the signals of all the users coincide in time. The identity of the set of active users is unknown to the users. Also, the receiver has no a priori knowledge about this identity. The mode of transmission through a MAC under these conditions will be named "synchronized restricted access." Such mode of transmission was considered earlier in [1]-[6]. For more recent constructions of codes for the MAC with synchronized restricted access, see [8]-[10].

We consider the sum modulo-2 multiple-access channel (S2MAC). More specifically, we assume that all the users transmit by means of binary block codes of the same length $n$, the codewords of different users coincide in time, and the output is a binary sequence which is equal to the sum mod-2 of the codewords of the $s$ active users. We shall consider also the case where the output sequence of the S2MAC is a quantized version of the binary real adder MAC with noise; namely, the receiver of the real adder MAC decides first whether the received noisy signal is a result of transmission of an even or odd number of ones and thereafter it proceeds to decode the binary sequence thus obtained.

Let $C = \{x_1, x_2, \ldots, x_s\} : i = 1, 2, \ldots, N$ be binary codes of length $n$ assigned to the $N$ users. We assume here and subsequently that the number $M$ of codewords is the same for all users. Denote by $S(N, m, M)$ the set of all binary sequences which can appear at the output of the S2MAC (without errors) with restricted access, i.e.,

$$S(N, m, M) = \left\{ x : x = \sum_{i=1}^{t=2m} x_{i,t} ; \right\}$$

where $I_k \equiv \{1, 2, \ldots, K\}$ and the summation is over $GF(2)$.

Let $(d, \cdot)$ stand for the Hamming distance.

**Definition 1:** Let $m$ and $t$ be some integers, $m > 1, t \geq 0$. The collection of codes $\{C_i : i = 1, 2, \ldots, N\}$ is called $(m, t)$-decodable if $d(x, x') \geq 2t + 1$ for any pair of words $x, x' \in S(N, m, M), x \neq x'$, i.e., if the minimum distance of the code $S$ is not less than $d = 2t + 1$.

By assigning to the users codes from an $(m, t)$-decodable collection, the receiver is enabled to correct any $t$ or less errors and separate the $s \leq m$ messages without a priori knowledge of the subset of active users.

For any $t \geq 0$ the cardinality $T$ of the $S(N, m, M)$ code, corresponding to the output of the S2MAC when the users employ some collection of $(m, t)$-decodable codes, is equal to

$$T = \left| S(N, m, M) \right| = \sum_{s=1}^{m} M^{n} \begin{pmatrix} N \\ s \end{pmatrix}.$$

Therefore, the rate $R$ of the $S(N, m, M)$ code is given by

$$R = \frac{\log T}{n} = \frac{1}{n} \log \left( \sum_{s=1}^{m} M^{n} \begin{pmatrix} N \\ s \end{pmatrix} \right). \quad (1)$$

Hence

$$R > \frac{1}{n} \log \left( M^n \begin{pmatrix} N \\ m \end{pmatrix} \right) \equiv m R_0 + R_{ae} \quad (2)$$

for any $m \geq 2$, where $R_0 = n^{-1} \log M$ is the rate of information transmission of each user and $R_{ae}$ is a rate which corresponds to an information about the subset of active users.

Our aim is to allocate a collection of $(m, t)$-decodable codes, each of size $M$, to a large class of potential users. In our method of constructing the collection of $(m, t)$-decodable codes, the number $N$ of potential users is upperbounded essentially by $M$ for the practically interesting situation that the number $m$ of active users is a (not too large) fraction of $N$. The method of construction is described by the following Theorem 1 and its proof. The upper bound on $N$, expressed by Condition i) of Theorem 1, is attainable for some values of the parameters (see Example 3 of Section V).

**Theorem 1:** For some fixed integers $m \geq 2$, $k_i \geq 1$ and $t_i \geq 0$, let $N$, $n$ and $k_i \leq N$ be positive integers such that the following conditions are satisfied:

1) $N \leq \max\{2^{k_1} + t_1, m + 1\}$, where $t_1 = 1$ if $m \neq 3$, and $t_2 = 2$ if $m = 3$;
2) there exists a binary linear $(n, k, 2t + 1)$ code $C$ with $k \geq n k_1 + k_2$;
3) in case that $k_2 < N$, there exists a binary linear $(N, N - k_2, d)$ code $C_0$ with $d \geq 2m + 1$.

Then it is possible to construct a collection $\{C_i : i = 1, 2, \ldots, N\}$ of $(m, t)$-decodable codes, each code with size $M = 2^{n k}$. In the next section we introduce a class of codes that is suitable to use in case that the subset of active users is known to the receiver. In Section III collections of $(m, t)$-decodable codes are constructed and the rate of such collection is examined. A decoding procedure for a collection of $(m, t)$-decodable codes is described in Section IV. Examples that exhibit collections of $(m, t)$-decodable codes with low loss of rate are provided in Section V. Some concluding remarks are presented in Section VI.

**II. MODULO-2 SEPARABLE CODES**

Let us address now the case that the subset of active users is known to the receiver. We aim at equipping the users with codes in a way that the receiver is capable to separate the output of the S2MAC into the various messages.

**Definition 2:** For some integers $m \geq 2$ and $k \geq 1$, let $C$ be a binary linear $(n, m k)$ code. A collection $\{C_i : i = 1, 2, \ldots, N\}$ of $N$ binary linear $(n, k_1, k_2)$ codes is called $(m, n k)$- separable if $C_{i_1} \cap C_{i_2} \cap \cdots \cap C_{i_m} = \emptyset$ for any subset of $m$ indices $\{i_1, i_2, \ldots, i_m\} \subset \{1, 2, \ldots, N\}$. In case that $C$ is the $(m, m k)$-code we shall call this collection $C$ $(m, k)$- separable.

Let us assign to the users codes that belong to an $(m, C)$-separable collection. Since the subset of active users is assumed to be known to the receiver, separation of the messages of any $m$ or less active users is then indeed enabled. In addition, if the minimum distance of $C$ is $2t + 1$ then any $t$ or less errors can be corrected.

**Lemma 1:** Let $C$ be an $(n, m k)$ code. There is an $(m, n k)$- separable collection of $N$ codes if and only if there is an $(m, n k)$-separable collection of $N$ codes.

**Proof:** In any linear $(n, m k)$ code $C$ there are $m k$ positions which can be interpreted as information positions. Without loss of generality we assume that the first $m k$ positions are the information positions. Let $\{C_i : i = 1, 2, \ldots, N\}$ be some $(m, C)$- separable collection of $N$ codes. Let $C_i^t : i = 1, 2, \ldots, N$ be the $(n, m k)$ codes such that $C_i^t$ coincides with $C_i$ on the first $m k$ positions; $i = 1, 2, \ldots, N$. Clearly, the collection $\{C_i^t : i = 1, 2, \ldots, N\}$ is
two lemmas present a connection between MDS codes and then we obtain an \((m,k,m+1)\) MDS code over \(\text{GF}(2^k)\).

An \((n,k,d)\) code \(C\) over \(\text{GF}(q)\), where \(k = \log_q|C|\), is called maximum-distance-separable (MDS) if its minimum distance satisfies \(d = n - k + 1\) (since \(C\) is not assumed to be linear). The following two lemmas present a connection between MDS codes and \((m,k)\) separable collections of codes.

**Lemma 2:** If there exists an \((m,k)\)-separable collection of \(N\) codes then there exists an \((N,N-m+1)\) MDS code over \(\text{GF}(2^k)\).

**Proof:** Assume that there exists an \((m,k)\)-separable collection \(\{C_i\}\) of \(N\) codes, each code with parameters \((nk,k)\). Let \(G_i\) be a generator matrix of \(C_i\), \(i = 1,2,\ldots,N\). Consider the binary linear code \(C = (C_i)\) of length \(Nk\) specified by the following \(mk \times Nk\) check matrix

\[
H = (G_{i1}^T, G_{i2}^T, \ldots, G_{iN}^T)
\]

where the superscript \(T\) stands for transposition. By Definition 2, every set of columns of \(H\) belonging to \(k\) different submatrices \(G_{i}^T\) is linearly independent if and only if \(m \leq N\). Let us prepare a list of all codewords of \(C\), then partition each of these binary codewords into \(N\) segments of equal length \(k\). Now regard each such set as a member of \(\text{GF}(2^k)\) \((\text{by adopting some representation of the elements of } \text{GF}(2^k) \text{ as binary vectors of length } k)\). The \(q\)-ary, \(q = 2^k\), code \(C_i\) of length \(N\) thus obtained is not necessarily linear. However, the minimum Hamming distance of \(C_i\) is \(m+1\). This is induced by the parent linear code \(C\), in accordance with the previously mentioned property of its check matrix \(H\) [3]. Also, the number of codewords of \(C_i\) is equal to \(2^{mk-k}\). Consequently, \(C_i\) is an \((N,N-m+1)\) MDS code over \(\text{GF}(2^k)\).

**Lemma 3:** The maximum number \(N(m)\) of \((m,k)\)-separable codes satisfies the following conditions

\[
N(m) = 2^k + m - 1, \quad m = 2,3 \quad (4)
\]

\[
2^k + m - 1 \geq N(m) \geq \max\left\{2^k + m - 1, m + 1\right\}, \quad m > 3. \quad (5)
\]

**Proof:** Let us proof first the upperbound \(N(m) \leq 2^k + m - 1\). \(m \geq 2\). We shall show that the existence of an \((m,k)\)-separable collection of \(N\) codes implies the existence of an \((m-1,k)\)-separable collection of \(N-1\) codes, \(m > 2\). Let \(\{C_i\}\) be an \((m,k)\)-separable collection of \(N\) codes. Consider a generator matrix \(G_i = (G_{i1}, G_{i2}, \ldots, G_{im})\) of \(C_i\); \(i = 1,2,\ldots,N\). Each \(G_{ij}\) is an \(Nk\times k\) matrix. We assume, without loss of generality, that \(G_{im}\) is the identity matrix and \(G_{ij}\), \(j = 1,2,\ldots,m - 1\), are zero matrices. Let \(C_i^*\) be the code generated by \(G_i^* = (G_{i1}, G_{i2}, \ldots, G_{i(m-1)})\); \(i = 2,3,\ldots,N\). Then \(\{C_i^*\}\) is clearly an \((m-1,k)\)-separable collection of \(N-1\) codes. Consequently,

\[
N(m) \leq N(m - 1) + 1, \quad m > 2. \quad (6)
\]

It follows by Definition 2 that codes \(C_i^*; i = 1,2,\ldots,N\) belonging to any \((m,k)\)-separable collection are intersected only on the zero codeword. Hence \(N(m) \leq 2^k - 1\), \(m = 2\). In particular, \(N(2) \leq 2^k + 1\). This inequality and (6) yield the result.

We proceed now to prove the right inequality in (5) and to show that the previously proved upper bound on \(N(m)\) is attained for \(m = 2,3\). Let \(H_{RS}\) be an \(N \times N\) check matrix of a Reed–Solomon code \(C_{RS}\) over \(\text{GF}(2^k)\). Consider a binary representation of \(H_{RS}\), which is obtained by regarding the elements of \(\text{GF}(2^k)\) as binary \(k \times k\) matrices (see the Appendix) and replacing each entry of \(H_{RS}\) accordingly. Then any column of \(H_{RS}\) becomes an \(mk \times k\) binary matrix. Denote such matrix, which corresponds to the \(i\)th column of \(H_{RS}\), by \(G_i^{TS}; i = 1,2,\ldots,N\) (where the superscript \(T\) indicates transposition). Let \(C_i\) be the linear span of the rows of \(G_i\); i.e., \(C_i\) is a binary linear \((mk,k)\) code. Since any \(m\) columns of \(H_{RS}\) are linearly independent, the collection of codes \(\{C_i; i = 1,2,\ldots,N\}\) thus obtained is \((m,k)\)-separable. The right inequality in (5) and \(N(m) \geq 2^k + m - 1\) for \(m = 2,3\) are now implied by the existence of the following codes: doubly-extended Reed–Solomon codes with any number \(m, 2 \leq m \leq 2^k + 1\), check symbols, triply extended Reed–Solomon codes with \(m = 3\) check symbols, and repetition codes of any length over \(\text{GF}(2^k)\).

**Remark:** Lemma 2 asserts that an \((N,N-m+1)\) MDS code over \(\text{GF}(2^k)\), which is not necessarily linear, can be constructed with the aid of every \((m,k)\)-separable collection of \(N\) codes. Furthermore, it follows by Lemma 3 that the upper bound on the maximum length of such codes coincides with the known upper bound [7] on the maximum length of linear MDS codes over \(\text{GF}(2^k)\).

### III. \((m,t)\)-Decodable Codes

The essence of our method to construct an \((m,t)\)-decodable collection of codes is the following. The \((n,k,2t+1)\) code \(C\) (see Theorem 1) is partitioned into two codes: an \((n,mk)\) code \(C_1\) and an \((n,m-k)\) code \(C_2\). According to Lemma 3, we can construct an \((m,C')\)-separable collection of \(N, X \leq 2^k + 1\) codes \(\{C_i; i = 1,2,\ldots,N\}\). There are \(2^m - k_0 = k - mk\) cosets of \(C_1\) in \(C\), and different codewords of \(C_2\) belong to different cosets \(C_1^i\). We assign to the \(i\)th user the code \(C_i^* = a_i - C_i\), where \(a_i\) is some codeword of \(C_2\). Then the sum modulo-2 of any \(s, s \leq m\), of the codes \(\{C_i^*\}\) belongs to some coset \(C_i^*\). It can be shown that due to Condition 3 of Theorem 1 it is possible to choose \(\{a_i\}\) such that different cosets correspond to different users. Thereby the decoder is able to detect the set of active users. Now we proceed to prove Theorem 1.

**Proof of Theorem 1:** With the aid of the \((n,k,2t+1)\) code \(C\) we form two codes: an \((n,m-k)\) code \(C'\) and an \((n,k)\) code \(C''\) such that \(C = C' + C''\). According to Lemma 1 and Lemma 3 we are able to construct an \((m,C')\)-separable collection of \(N, X \leq 2^k + t + m + 1\) codes \(\{C_i; i = 1,2,\ldots,N\}\), where \(t = 1\) if \(m \neq 3\) and \(t = 2\) if \(m = 3\). Consider first the case \(k_0 \leq X\). Then the \((N,N-k_0,2m+1)\) code \(C_0\) exists. Let \(H_{RS} = (H_{1}, H_{2}, \ldots, H_{N})\) be a \(k_0 \times N\) check matrix of \(C_0\), and let \(G''\) be an \(N \times k_0\) generator matrix of \(C''\). Denote

\[
a_i = H_i^T G''. \quad i = 1,2,\ldots,N. \quad (7)
\]

Then \(a_i \in C''\) and \(a_i^* = a_i - C_i^*\) constitute an \((m,t)\)-decodable collection.

For a fixed set of \(s \leq m\) different indices \(J_s = \{j_1,j_2,\ldots,j_s\}\), let

\[S(J_s) = C_{j_1} + C_{j_2} + \cdots + C_{j_s}\]

\[\equiv b(J_s) \oplus S(J_s)
\]
where
\[
b(J_s) = a_{i_1} \oplus a_{i_2} \oplus \cdots \oplus a_{i_s}.
\]

Clearly, the code \( S(\mathcal{N}, m, M) \), which corresponds to the collection \( \{C_i\} \), is the union of the codes \( S(J_s) \) over all possible sets of indices \( J_s \), \( 1 \leq s \leq m \). Because \( \{C_i; i = 1, 2, \ldots, N\} \) is an \((m, C')\)-separable collection and \( S'(J_s) \subseteq C' \subseteq C \) for any \( J_s \), the minimum Hamming distance of \( S'(J_s) \), hence also of \( S(J_s) \), is at least \( 2r + 1 \). Evidently, \( S(J_s) \) belongs to some coset \( C'/C' \). Since the minimum Hamming distance of \( C' \) is not less than \( 2r + 1 \), we may prove that \( \{C_i; i = 1, 2, \ldots, N\} \) is an \((m, t)\)-decodable collection by showing that for any \( J_s \neq J'_s \) the codes \( S(J_s) \) and \( S(J'_s) \) belong to different cosets.

Thus we have \( b(J_s) = b(J'_s) \), i.e.
\[
a_{i_1} + a_{i_2} + \cdots + a_{i_s} = a_{j_1} + \cdots + a_{j_t} = 0.
\]

Because \( s + s' \leq 2m \), it follows by (7) and (9) that there exists a set of less than \( 2m + 1 \) linearly independent columns of the check matrix \( H_0 \), contradicting the condition that the minimum distance of \( C_0 \) is \( 2m + 1 \).

For the case \( k_0 = N \) we use the \( X \times Y \) identity matrix instead the check matrix \( H_0 \). The rest of the proof is the same.

For some \((n, k, 2r + 1)\) code \( C \) satisfying the conditions of Theorem 1, the difference
\[
\Delta(N, m) = \frac{k}{n} - \left( \frac{1}{2} \log \left( \sum_{x=1}^{2^m} \left( \frac{X}{m} \right) \right) \right)
\]

between the rate of \( C \) and the rate of the code \( S(\mathcal{N}, m, M) \) (see (1)) represents a loss of rate which is due to the multiple-access nature of the \((m, t)\)-decodable collection of codes. It follows by (2) and Theorem 1 that
\[
\Delta(N, m) < \frac{k}{n} - \left( \frac{1}{2} \log \left( \frac{2^{m+1}}{X} \right) \right).
\]

\[\text{Corollary: Given any integers } N, 2 \leq m < N \text{ and } t \geq 0, \text{ there is an } (m, t)\text{-decodable collection of } X \text{ codes with length } n \text{ such that}
\]
\[
\Delta(N, m) < \left\{ \begin{array}{ll}
\frac{n^{-1}}{(N - m) \log N + m \log m}, & \text{if } m \leq m \log 2N. \\
\frac{n^{-1}}{(m + m \log m)}, & \text{if } m > m \log 2N.
\end{array} \right.
\]

\[\text{Proof: It follows by (10) with } k_0 = N = \text{that}
\]
\[
\Delta(N, m) < \frac{1}{n} \log \left( \frac{2^N}{N^m} \right)
\]
\[
< \frac{1}{n} (N - m \log N + m \log m)
\]

where we have used \( \binom{N}{m} \leq \frac{N^m}{m!} \). If \( N > m \log (2N) \), we can choose as the \((N, N - k_0, 2m + 1)\) code \( C_0 \) a (possibly shortened) BCH code of length \( N \) with \( k_0 \) check bits, \( k_0 \leq m \log (2N) \).

Substitution of \( m \log (2N) \) for \( k_0 \) into (10) yields
\[
\Delta(N, m) < \left( \frac{2^N}{N^m} \right) < \frac{1}{n} (m + m \log m).
\]

We conclude from this Corollary that the overall rate of information transmission by an \((m, t)\)-decodable collection of \( X \) codes approaches, asymptotically as the length of code \( n \) tends to infinity, the rate of the basic \((n, k)\) code \( C \). This implies that any asymptotic bound on the rate of binary linear codes, e.g., the Gilbert-Varshamov bound, holds also for an \((m, t)\)-decodable collection of \( X \) codes, for any fixed values of \( N, m \) and \( t/n \).

IV. Decoding \((m, t)\)-Decodable Codes

We address now the decoding of an \((m, t)\)-decodable collection of codes constructed in the previous section.

**Lemma 4**: Let \( C \) be a binary linear \((n, k)\) code and let \( C' \subseteq C \) where \( C_1 \) and \( C_2 \) are binary linear \((n, k_1)\) and \((n, k_2)\) codes, respectively, \( k_1 + k_2 \). Pick \( \mathbf{b} \) in \( C_1 \), \( \mathbf{b} = [1, 2, \ldots, k_1] \) such that \( \mathbf{b} H^T = \mathbf{e} \), where \( \mathbf{e} \) is the unit vector with the one at the \( i \)th position. Such set of vectors always exists because different codewords of \( C_1 \) belong to different cosets of \( C' \), and the number of the cosets is equal to the number of codewords of \( C_1 \). Denote by \( B \) the matrix whose \( i \)th row is \( \mathbf{b} \), \( i = 1, 2, \ldots, k_1 \).

Since \( \{b_i; i = 1, 2, \ldots, k_1\} \) is a basis for \( C_1 \), any \( x_i \in C_1 \) can be represented as \( x_i = \gamma_1 b_1 + \cdots + \gamma_i b_i + \cdots \), where \( \gamma_i \in \{0, 1\} \) for all \( i = 1, 2, \ldots, k_1 \). Thus we have
\[
x H^T B = x_1 H^T B = (\gamma_1, \gamma_2, \ldots, \gamma_{k_1}) B = b_i.
\]

For completing the proof, set \( A = H^T B \).
Decoding Algorithm:

Step 1 (Correction of channel errors): Decode the output sequence y of the channel into a codeword \( \mathbf{z} \in \mathcal{C} \).

Step 2 (Determination of the set of active users): Compute \( \mathbf{z}' = \mathbf{z} + \mathbf{y} \). Regard the first \( k \) symbols of \( \mathbf{z}' \) as the syndrome with respect to the \((N, N-k-2m+1)\) code \( \mathcal{C}_0 \) (without loss of generality we can assume that \( \mathcal{C}' \) is systematic) and decode this syndrome into a binary \( N \)-sequence of weight \( s \leq m \). The support of the \( N \)-sequence obtained is the index set \( J_s = \{ j_1, j_2, \ldots, j_s \} \) of the active users.

Step 3 (Determination of the transmitted codewords): Select \( J_m \) such that \( J_s \subset J_m \) and

\[
\mathbf{z}_i' = (z + b(J_i))(A(J_m-1,i)) \in \mathcal{C}'_{J_s}.
\]

V. EXAMPLES

The efficiency of our method of constructing \((m,t)\)-decodable codes is demonstrated by the following examples.

Example 1: An \((m = 3, t = 1)\)-decodable collection of \( N = 23 \) codes with \( M = 32 \) can be constructed with the aid of the \((31,26,3)\) Hamming code \( \mathcal{C} \) and the \((23, 12, 7)\) Golay code \( \mathcal{C}_0 \). According to the proof of Theorem 1, we express \( \mathcal{C}' \) as the sum \((31,15)\) code \( \mathcal{C}' = \mathcal{C}'' \) and \((31,11)\) code \( \mathcal{C}''' \) (i.e., \( k_0 = 14 \) and \( k_1 = 15/3 = 5 \)). By Lemma 1 and Lemma 3, it is possible to construct a \((3, C')\)-separable collection of \( 23 \) codes. Thereafter, an \((m = 3, t = 1)\)-decodable collection of \( 23 \) codes is obtained with the aid of \( \mathcal{C}_0 \). The rate of the code \( S(23,3,32) \) at the output of the S2MAC, corresponding to this construction, is equal to

\[
R = 31^{-1} \log \left( \sum_{s=1}^{32} 23^s \right) = 0.8322
\]

and the loss of rate \( \Delta \) is given by

\[
\Delta = 26/31 - R = 0.0065.
\]

Note that

\[
\sum_{s=1}^{32} 23^s = 2^{23} - 1.
\]

Therefore, every coset of \( \mathcal{C}' \) in \( \mathcal{C} \) contains some subcode \( S(J_s) \). The only reason for the loss of rate of \( S(23,3,32) \) is that sometimes the number of active users is less than \( m = 3 \).

Example 2: An \((m = 2, t = 2)\)-decodable collection of \( N = 15 \) codes with \( M = 64 \) can be constructed by means of the \((30, 20, 5)\) shortened BCH code \( \mathcal{C} \) and the \((15, 7, 5)\) BCH code \( \mathcal{C}_0 \). The rate of the corresponding code \( S(15,2,64) \) is given by

\[
R = 30^{-1} \log \left( 64 \cdot 15 + 64^2 \cdot 105 \right) = 0.6239.
\]

and

\[
\Delta = 2/3 - R = 0.0428.
\]

Example 3: An \((m = 4, t = 2)\)-decodable collection of \( N = 63 \) codes with \( M = 64 \) can be constructed by employing the \((60, 18, 5)\) shortened BCH code \( \mathcal{C} \) and the \((63, 30, 9)\) BCH code \( \mathcal{C}_0 \). The rate of \( S(63,4,64) \) in this case is

\[
R = 60^{-1} \log \left( \sum_{s=1}^{64} 63^s \right) = 0.7198
\]

and

\[
\Delta = 4/5 - R = 0.0802.
\]

We may also provide an \((m = 4, t = 2)\)-decodable collection of codes of size \( N = 64 \) to \( N = 65 \) users, thereby attaining the bound of Theorem 1. Indeed, we may use for the construction a \((62, 50, 5)\) BCH code \( \mathcal{C} \) and a \((65, 39, 10)\) code \( \mathcal{C}_0 \).

VI. CONCLUDING REMARKS

Let the \((binary)\) check matrix \( \mathbf{H} = (h_1, h_2, \cdots, h_N,m) \) of a BCH code with length \( N \) and minimum distance \( 2m+1 \) be partitioned as follows: \( H = (H_1, H_2, \cdots, H_M) \), where each \( H_i \) has \( M \) columns. Provide user \( i \) with the code \( C'_i \), consisting of the columns of \( H_i \): \( i = 1, 2, \cdots, N \), i.e., let \( C'_i = \{ h_i^{(1)}, h_i^{(2)}, \cdots, h_i^{(M)} \} \).

Then [8] the collection

\[
\{ C'_1, C'_2, \cdots, C'_N \}
\]

is evidently \((m, 0)\)-decodable. Consequently, if \( G \) is a generator matrix of a code with minimum distance \( 2t+1 \) and dimension that is equal to the codimension of the BCH code, then the collection of codes \( \{ C'_1, C'_2, \cdots, C'_N \} \) where

\[
C'_i = \{ c: c = eG, \ e \in C_i \} \quad i = 1, 2, \cdots, N
\]

is \((m, t)\)-decodable.

In contrast to this construction, our method amounts to the following. We utilize a \( k_0 \times N \) check (or the \( N \times N \) identity) matrix \( H_0 = (h'_1, h'_2, \cdots, h'_N) \) of an \((N, N - k_0, 2m + 1)\) code, together with an \((m, k_1)\)-separable collection

\[
\{ C'_1, C'_2, \cdots, C'_N \}
\]

doing, each of size \( M = 2^k \). Let \( G \) be the generator matrix of an \((m, k_0 + m k_1, 2t + 1)\) code. Then the collection of codes \( \{ C'_1, C'_2, \cdots, C'_N \} \) given by

\[
C'_i = \{ c: c = (h'_i, C'_i)G \} \quad i = 1, 2, \cdots, N
\]

is \((m, t)\)-decodable. According to this expression of \( C'_i \), identification of user \( i \) is enabled by a prefix \( h'_i \) which is appended, prior to the encoding that provides error correction capability, to any codeword of \( C'_i \).

Both methods yield the same asymptotic behavior, as expressed by the bound (11) on \( \Delta(N, m) \). However, our construction yields a smaller loss of rate for many of the interesting situations where the users are confined to employ codes with moderate lengths. Also, we are able to get close to, and for some values of the parameters attain (see Example 3) the upper bound

\[
U = \max \{ 2^t + i, m + 1 \}
\]

where \( t = 1 \) if \( m \neq 3 \)

and \( t = 2 \) if \( m = 3 \)

of Condition 1) of Theorem 1. In view of the proof of Lemma 3, the upper bound on \( \Delta \) according to our method would exceed \( U \) (yet remain less than or equal to the bound \( 2^t + m + 1 \) of (5)), if a method to construct linear MDS codes with size larger than presently known had become available.

Our construction draws substantially on the binary representation of MDS codes, particularly Reed-Solomon codes, over GF(2^4). An interesting different application of such codes is presented in [10] for the convolutionally encoded version of the S2MAC, under the assumption that the set of active users is known to the receiver. For this application, the entries of an \( m \times N \) check matrix \( H_{R} \) of a
Reed–Solomon code $C_{RS}$ over $GF(2^k)$ are expanded, unlike in the proof of Lemma 3, as binary polynomials of degree less than $k$. Denote by $H_{RS}(x)$ the version of $H_{RS}$ thus obtained. Let $G_j(x)$ be the transpose of column $j$ of $H_{RS}(x); i = 1, 2, \ldots, N$. Since the minimum distance of $C_{RS}$ is $m + 1$, any set of $m$ columns of $H_{RS}$ is linearly independent over $GF(2^k)$. As observed in [10], this implies linear independence over the ring of polynomials $GF(2)[x]$ of any set of $m$ columns of $H_{RS}(x)$. Consequently, if $G_j(x)$ is assigned to user $i; i = 1, 2, \ldots, N$ as the generator matrix of a rate $1/m$ binary convolutional code, then separation of information transmitted by a known set of at most $m$ active users (out of $N$ users) is enabled. We remark that if $H_{RS}$ has dimensions $2m \times N$ then the same procedure yields a convolutional-coding version of an $(m, 0)$-decodable collection of codes of rate $1/(2m)$, which then may be utilized to obtain an $(m, 1)$-decodable collection of codes of smaller rate through encoding via an appropriate convolutional code.

In [10] there is still another application of Reed–Solomon codes for a multiple-access channel which, however, addresses encoding over the extension field.

**APPENDIX**

Let $\alpha$ be a root of some binary primitive polynomial $p(x)$ of degree $k$. Then $\{\alpha^i; i = 0, 1, 2, \ldots, 2^k - 2\}$ are the nonzero elements of $GF(2^k)$. Let us adopt

$$B = \{\alpha^i; i = 0, 1, 2, \ldots, k - 1\}$$

as the basis of $GF(2^k)$ over $GF(2)$, and identify $\alpha^i \in B$ with the unit row vector $w_i$ of length $k$ with the 1 entry at the $(i + 1)$th position. Thus

$$B = \{w_i; i = 0, 1, 2, \ldots, k - 1\} \quad (15)$$

The binary representation of any $\alpha^i \in GF(2^k)$, expressed according to this basis, will be denoted $w_i$, i.e.,

$$GF(2^k) = \{0\} \cup \{w_i; \: i = 0, 1, 2, \ldots, 2^k - 2\}.$$

Now let $H$ be an $m \times n$ check matrix of an $(n, n - m)$ code $C$ over $GF(2^k)$. The syndrome $s$ associated with any $y \in GF(2^k)^n$ is a vector of length $m$, given by $s = yH^T$ (a row vector). By transforming this equation into its binary version we obtain $s_0 = y_0H_0^T$, where $s_0$ and $y_0$ are of length $km$ and $kn$, respectively. Hence $H_0$ is a $km \times kn$ matrix. Evidently, $s = yH^T$ and $s_0 = y_0H_0^T$ are concordant for every $y \in GF(2^k)^n$ if and only if any scalar relation

$$s = yh$$

—where $h$ is an entry of $H$ and $y \in GF(2^k)$—is concordant with its binary version

$$s_0 = y_0h_0.$$

(17)

As $s_0$ and $y_0$ are vectors of length $k$, $h_0$ is a $k \times k$ matrix. Obviously $h_0 = 0$ if $h = 0$. Considering the case $h \neq 0$, set $y = \alpha^i$ and $h = \alpha^j$ into (16). The resulting expression

$$\alpha^{i+j} = \alpha^i \cdot \alpha^j$$

has then to be equivalent to

$$w_{i+j} = w_i h_0,$$

where $h_0$ represents $\alpha^j$.

(19)

with the subscripts evaluated modulo $2^k - 1$. If the matrix $h_0$ is determined such that (19) is satisfied for $i = 0, 1, 2, \ldots, k - 1$, i.e., for all the vectors belonging to the basis $B$ (15), then (19) is satisfied for all $w_i \in GF(2^k)$. Consequently, the binary version of any entry $\alpha^i$ of $H$ is the following $k \times k$ matrix:

$$\begin{pmatrix}
    w_j \\
    w_{j+1} \\
    w_{j+2} \\
    \vdots \\
    w_{j+k-1}
\end{pmatrix}$$

with the subscripts evaluated modulo $2^k - 1$.

The set of $2^k$ binary $k \times k$ matrices thus obtained (also) forms the field $GF(2^k)$ under the matrix addition and multiplication operations.

**REFERENCES**


