Analysis and Design of Interleavers for CDMA Systems

A. Tarable, G. Montorsi, Member, IEEE, and S. Benedetto, Fellow, IEEE

Abstract—In the last years, the Turbo-principle has been applied to multiuser receivers in CDMA systems. However, the role of interleavers in these Turbo-receivers has not been studied yet. In this letter, we give a notion of optimality and of mutual optimality and a way to test it. Moreover, limiting to congruential interleavers and convolutional codes, we give sufficient conditions to construct a set of mutually optimal interleavers. Also, we provide some simulations to support our results.

Index Terms—Code division multiaccess, interleaver design, iterative multiuser receivers, permutations, turbo codes.

I. INTRODUCTION

T IS widely known that the multiaccess channel can be viewed basically as an encoder. From this consideration, many authors, induced by the powerful properties of Turbo-codes, thought of a Turbo-like iterative receiver for coded CDMA systems [1]–[3]. In this type of receiver, a user-separating soft-input soft-output block (called hereafter US-SISO) first attenuates the multiaccess interference (MAI) of the received signal and passes its output to a bank of single-user SISO channel decoders. These decoders, in their turn, provide some additional feedback information to the US-SISO, used, in the successive iteration, to improve the user separation, and so on. Simulations clearly show that the users should interleave their coded bit streams, before transmitting, in order to obtain good performance. However, the role of interleavers for these receivers, and so their design, is quite different from that of Turbo codes. In this letter, we propose a study on how these interleavers should be designed. In particular, we give a definition of optimality of an interleaver, and an easy way to test the distance from optimality. In order to give a practical rule of design, we consider the class of congruential interleavers, which are easy to study. For this subset, we identify certain sufficient conditions to obtain optimal interleavers and find the maximum number of users supported by such a system. Finally, some numerical simulations give a direct confirmation of the design approach.

II. SYSTEM DESCRIPTION

Let us consider $K$ users transmitting on the same AWGN channel. The $j$th user transmits a codeword, $\mathbf{x}^{(j)} \in \{0, 1\}^n$, belonging to the code $\mathcal{C}$, the same for all users, which can be a block or a terminated convolutional code. Each codeword is then interleaved according to the permutation $\Pi_j$, the sequence of codewords is BPSK modulated, spread and sent to the channel. We suppose all users are received word-synchronously. At the receiver, after a bank of matched filters, the US-SISO, which treats the bits as uncoded, performs some filtering and outputs $K$ streams, each entering a single-user SISO channel decoder. See [5] for more details. The observables in the $j$th stream have the following expression:

$$y_k^{(j)} = a_k^{(j)} b_k^{(j)} + \sum_{j \neq j} a_k^{(j')} b_{j'}^{(j')} + \mathbf{n}_k^{(j)} (1)$$

where $b_k^{(j)} \in \{-1, 1\}$ is the $j$th user’s $k$th modulated coded bit; $a_k^{(j)}$ is the corresponding amplitude after the filtering performed by the US-SISO; and $\mathbf{n}_k^{(j)}$ is a Gaussian random variable with zero mean and a given variance. The decoders perform a BCJR algorithm, which is nonoptimal in this case, since it assumes that the inputs are affected by uncorrelated noise, while the $b_k^{(j')}$s, being part of a codeword, have correlation. The purpose of the interleavers is to destroy this correlation, and to make the interferers’ coded bit streams “as memoryless as possible.” In the following sections, we will clarify this concept.

III. $\mathcal{C}$-OPTIMAL INTERLEavers

Let $\mathcal{C}$ be a binary linear block code with rate $R_c = k/n$ and denote with $\mathbf{G}$ and $\mathbf{H}$ its generator and parity-check matrix, respectively. Consider interleavers acting on codewords, constituted by permutations of the integers $\{0, \ldots, n-1\}$. Let $\Pi(\mathcal{C})$ be, with a slight abuse of notation, the equivalent code obtained by permuting with $\Pi$ all the codewords in $\mathcal{C}$ and define $\mathcal{C}' = \mathcal{C} \cap \Pi(\mathcal{C})$. It is easy to prove that $\mathcal{C}'$ is a subcode of $\mathcal{C}$. The following definition can now be stated.

**Definition 1:** The interleaver $\Pi$ is called $\mathcal{C}$-optimal if and only if

$$\dim(\mathcal{C}') = k_0 \triangleq k - \min\{k, n-k\}. \quad (2)$$

The rationale of this definition lies in the operation performed by the decoders. In fact, they accept the input as if coming from a single-user memoryless channel, while the other users’ coded signals give rise to an interference with memory.

Suppose $k \geq n-k$. If $\Pi$ is $\mathcal{C}$-optimal, the fraction of codewords in $\mathcal{C}$ that are also in $\Pi(\mathcal{C})$ is $2^{k-n}$, by Definition 1. But this is also the probability of belonging to $\mathcal{C}$, for an $n$-dimensional word output by a binary memoryless source. If $k \leq n-k$, then $\mathcal{C}'$ contains only the all-zero codeword, always present in a linear code and obviously resistant to all permutations.
Note that, if $\Pi(\mathbf{G})$ is the matrix obtained from $\mathbf{G}$ by permuting its columns according to $\Pi$, the product $\Pi(\mathbf{G})\Pi^T$ will have a rank equal to $k - \dim(C')$. Keeping in mind that the maximum value of this rank is $\min\{k, n-k\}$, if $\Pi$ is $C$-optimal, the intersection between $C$ and $\Pi(C)$ is also the minimum possible.

From Definition 1, it follows that codes with $k \leq n-k$ that possess the all-one codeword do not have $C$-optimal permutations, because the all-one codeword belongs to $C'$ for every choice of $\Pi$.

By defining the distance of $C$ from $C'$-optimality as $d_0(\Pi, C) = \dim(C') - k$, the maximal distance is reached by the identity permutation $\Pi_I$, i.e., $\Pi_I(i) = i$, since $d_0(\Pi_I, C) = k - k_0$.

Proposition 1: If $\Pi$ is $C$-optimal, then $\Pi^{-1}$ is also $C$-optimal.

Proof: Applying successively first $\Pi$ and then $\Pi^{-1}$ is just equivalent to apply the identity permutation, which obviously maintains all the codewords. If $\Pi$ maintains $2^{k_0}$ codewords, which we denote $c_1, \ldots, c_{2^{k_0}}$, then the other $2^k - 2^{k_0}$ codewords in $\Pi(C)$ do not belong to $C$. $\Pi^{-1}$ sends all these words into $C$. So, $\Pi^{-1}$ maintains $c_1, \ldots, c_{2^{k_0}}$, and, since it is an injective correspondence, it cannot maintain other codewords in $C$.

Returning to the CDMA system with $K$ users, the $i$th user will see the code of the $j$th user through the permutation $\Pi^{-1} \Pi_j$. From this simple consideration, the Definition 2 arises.

Definition 2: The $K$ interleavers $\Pi_1, \ldots, \Pi_K$ are said to be mutually $C$-optimal if, for every choice of $i$ and $j$, $i \neq j$, $\Pi^{-1} \Pi_j$ is $C$-optimal.

Definition 2 gives a criterion to design the set of $K$ interleavers. Thanks to Proposition 1, it is sufficient to check the $C$-optimality of $K(K-1)/2$ pairs of interleavers. An important point is the following: what is the maximum number of mutually $C$-optimal interleavers? Unfortunately, it does not seem easy to answer this question. In the following section, we restrict the search for a set of mutually $C$-optimal interleavers to a subclass of permutations and we give a partial answer which concerns convolutional codes.

IV. A SET OF MUTUALLY C-OPTIMAL INTERLEAVERS

In this section, we consider an $(n_0, k_0 = 1, N)$ convolutional code, terminated after a block of $L$ trellis steps, corresponding to a linear block code $C$ with parameters $n = n_0L$ and $k = k_0L - \nu$, where $\nu = N - 1$ is the memory. Denote by $N^T$ the constraint length of the dual code. Also, we limit the analysis to symbol interleavers, which are permutations of the integers $0, \ldots, L - 1$.

It is useful to consider the particular subset of congruential interleavers $[4]$, defined as

$$\Pi_g(i) = ig \mod L \equiv (ig)_L,$$

where $g$ is an integer and is relatively prime with $L$, for which the following theorem holds:

Theorem 2: Consider a block length $L$ such that

$$1 + Z + \ldots + Z^{L-1} = \frac{1 + Z^L}{1 + Z}$$

is an irreducible polynomial over $GF(2)$. If $L > N N^T / k_0(n_0 - k_0)$, then $\Pi_g$ is $C$-optimal for $1 < g < L - 1$.

Before proving the theorem, we state the following lemma, whose proof is omitted.

Lemma 3: If a permutation $\Pi$ applied to an $(n_0, k_0 = 1, N)$ convolutional code, is such that $\Pi(C) = C$, i.e., it is useless, then every $N$-length subset of indices $\{i_0, \ldots, i_0 + N - 1\}$, $0 \leq i_0 \leq L - N$, is sent into an $N$-length subset of indices $\{j_0, \ldots, j_0 + N - 1\}$, for some $j_0$.

Proof (of Theorem 2): First note that the values of $L$ that satisfy (4) are surely prime. Then, every $1 \leq g < L$, defines an interleaver.

Let the generator matrix of a $(n_0, k_0 = 1, N)$ convolutional code be

$$\mathbf{G} = \begin{pmatrix} m_0 & m_1 & \cdots & m_N & \cdots & \cdots \\ 0 & m_0 & m_1 & \cdots & m_N & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & m_0 & m_1 & \cdots & m_N \end{pmatrix}$$

where the elements $m_i$ are drawn from $GF(2^{n_0})$. It has $k_0 L - \nu$ rows and columns. Its parity-check matrix $\mathbf{H}$ has $(n_0 - k_0)L + \nu$ rows and $L$ columns.

Define, for a given $i$, $q_i(D) = m_i \cdot (\sum_{j=0}^{N-1} p_j D^{j+i-j})$, where the polynomial between parentheses is a column of $\mathbf{H}$. The $p_j$s are drawn from $GF(2^{n_0})$ and the operation between any $m$ and $p$ is defined as

$$m \cdot p = mp^T$$

being $m$ the representation of $m$ as a binary row vector. The $j$th row of the product $\mathbf{P} = \Pi_g(\mathbf{G}) \cdot \mathbf{H}^T$, $0 \leq j < k_0 L - \nu$, will be in polynomial form:

$$r_j(D) = \sum_{i=0}^{(N/k_0)-1} Z^{(j+i)g}q_i(D)$$

where $Z = D^{n_0 - k_0}$. $\Pi_g$ is $C$-optimal iff the rank of $\mathbf{P}$, denoted $\rho(\mathbf{P})$, is full.

Consider now the matrix $\mathbf{P}_L$, whose rows are defined as

$$r_j'(D) = \left(\sum_{i=0}^{(N/k_0)-1} Z^{(j+i)g}q_i(D)\right)^{1+Z^L}$$

which has exactly $(n_0 - k_0)L$ columns. It is easy to see that $\mathbf{P}_L$ is the matrix obtained by summing the columns of $\mathbf{P}$ whose indices are congruent mod $(n_0 - k_0)L$. Hence,

$$\rho(\mathbf{P}) \geq \rho(\mathbf{P}_L).$$

Suppose $\mathbf{P}_L$ does not have full rank. Since $\mathbf{P}_L$ has more columns than $\mathbf{P}$, it means that its rows are linearly dependent. Since every row of $\mathbf{P}_L$ is the cyclic shift of its first row, $r_j'(D)$, there will exist a polynomial $g(Z)$ such that

$$(g(Z)r_j'(D))_{1+Z^L} = 0$$

or, for some $\alpha(D)$,

$$g(Z)r_j'(D) = \alpha(D)(1 + Z^L).$$

Now, if $p(Z) \equiv \sum_{i=0}^{L-1} Z_i$, which is a factor of $1 + Z^L$, is irreducible, then it must divide either $g(Z)$ or $r_j'(D)$. The maximum degree of $g(Z)$ is $L - 1$, so, if $p(Z)$ divides $g(Z)$, then it must be $g(Z) = p(Z)$. But, since there are only $L - \nu$ rows, there are no more than $L - \nu$ terms in $g(Z)$, and then $g(Z) \neq p(Z)$. 

IV. A SET OF MUTUALLY C-OPTIMAL INTERLEAVERS

In this section, we consider an $(n_0, k_0 = 1, N)$ convolutional code, terminated after a block of $L$ trellis steps, corresponding to a linear block code $C$ with parameters $n = n_0L$ and $k = k_0L - \nu$, where $\nu = N - 1$ is the memory. Denote by $N^T$ the constraint length of the dual code. Also, we limit the analysis to symbol interleavers, which are permutations of the integers $0, \ldots, L - 1$.

It is useful to consider the particular subset of congruential interleavers $[4]$, defined as

$$\Pi_g(i) = ig \mod L \equiv (ig)_L,$$

where $g$ is an integer and is relatively prime with $L$, for which the following theorem holds:

Theorem 2: Consider a block length $L$ such that

$$1 + Z + \cdots + Z^{L-1} = \frac{1 + Z^L}{1 + Z}$$

is an irreducible polynomial over $GF(2)$. If $L > N N^T / k_0(n_0 - k_0)$, then $\Pi_g$ is $C$-optimal for $1 < g < L - 1$.
Consider \( r_0(D) \). It is composed by a sum of \( N/k_0 \) terms, each of length \( N/k_0 \), and starting from an offset which is a multiple of \( n_0 - k_0 \). Then dividing the columns in blocks of \( n_0 - k_0 \), there are at most \( (N/k_0)(N'/k_0) \) such blocks covered by \( r_0(D) \) [the maximum is reached if the \( q_k(D) \) do not overlap]. There are \( L \) blocks in all, so if \( L > (N/k_0)(N'/k_0) \), at least one is entirely composed by zeros.

If \( r_0(D) \) is divisible by \( p(Z) \), then we have
\[
r_0(D) = \beta(D)p(Z)
\]
where \( \deg(\beta(D)) < n_0 - k_0 \). Then, \( r_0(D) \) can be viewed as the periodic repetition of \( \beta(D) \) every \( n_0 - k_0 \) columns. Since at least one of these repetitions is zero, then \( \beta(D) = 0 \).

Then, \( \Pi_{2L}(C) = C \). The only congruential permutations that can be useless, by Lemma 3, are for \( g = 1 \), which is the identity permutation, always useless, and for \( g = L - 1 \), useless only for a time-reversal code.

The other congruential permutations, for \( 1 < g < L - 1 \), are then \( C \)-optimal.

Now, since \( \Pi_{2L}(\Pi_{2L})^{-1} = \Pi_{g_0}g_{0}^{-1} \), the set of mutually \( C \)-optimal interleavers is easily found. Imagine to assign to the \( j \)th user the interleaver \( \Pi_{Lg} \). When the code is not time-reversal, it must be \( g_i \neq g_j \); so we can allocate a maximum of \( L - 1 \) mutually \( C \)-optimal interleavers. Instead, if the code is time-reversal, then there is the additional requirement \( g_i \neq L - g_j \), so there can be at most \( (L - 1)/2 \) mutually \( C \)-optimal interleavers.

V. RESULTS OF SIMULATIONS

In Fig. 1 we show the effect of interleaving in terms of bit-error-rate in a frame synchronous CDMA scenario with four equal-power users and the iterative receiver introduced in [5]. The code has generators 238, 35a. The correlation between every pair of users is 0.7. The US-SISO is MMSE until the third iteration, then it is a conventional one. The solid lines correspond to optimal interleaving while the dashed lines refer to absence of interleaving. Fig. 1 shows how effective a good interleaving can be in such a system.

Fig. 2 shows the different performance obtained by choosing two different congruential interleavers. Here we have two equal-power users, with correlation 0.9 and ten iterations of the receiver in [5] with a conventional US-SISO. The parameters are \( L = 107, g = 63 \) for the solid lines, [optimum interleaving since \( L = 107 \) satisfies (4)] and \( L = 128, g = 63 \) and \( g = 31 \) for the dashed and the dots and dashes lines, which are not optimal.

VI. CONCLUSIONS

In this letter, we give a criterion of optimality for a set of interleavers in a coded CDMA system. Although not proved, it is sensible that this choice gives substantial improvement in performance, in terms of bit error rate. Also, we restrict to the simple class of congruential interleavers and we give sufficient conditions to find optimal interleavers inside this class, if the code employed by the users is a convolutional code. We also find the maximal number of users that can be supported by such a system.

REFERENCES


