Abstract—We investigate good coprime interleavers that perform well in turbo codes and allow for memory-efficient implementation. We first evaluate the spread and the randomness properties of these interleavers using the cycle correlation sum (CCS) and the variance of the second order spread spectrum (VSSS) criteria, respectively. A critical parameter $c_{\text{power}}$ is introduced for interleavers whose lengths are power of 2. It is found that a large $c_{\text{power}}$ typically associates with a small CCS value, indicating a good minimum spread of the coprime interleaver, but the degree of randomness decreases with growing $c_{\text{power}}$. We next develop rules on choosing good parameters that strike a good balance between minimum spread and degree of randomness. Simulation results confirm that the coprime interleavers designed from our rules perform as well as or better than $S$-random interleavers.

I. INTRODUCTION

Interleavers, which play a prominent role in turbo codes, have been the topic of serious research for a while. A good interleaver is ideally well-performing as well as easy to implement. Random interleavers, and especially $S$-random interleavers, generally perform better than row-column interleavers, but the need to store the entire scrambling pattern makes their application costly, especially in systems that have limited storage, require the use of an exceptionally long code, or have to support a few different code lengths. Algebraic interleavers, on the other hand, can be generated on-the-fly using only a few seeding parameters.

An algebraic interleaver permutes the elements of its input vector according to a well-defined algebraic formula. This paper considers an important class of algebraic interleavers, the coprime interleavers, whose interleaving pattern is defined recursively as [2]:

$$
\pi(0) = 0; \\
\pi(i) = \text{mod}(a\pi(i-1)+b, N), \quad i = 1, 2, \ldots, N-1,
$$

(1)

where $N$ is the interleaver length, $\pi(i)$ is the new position to which indice $i$ should be scrambled to, and $\text{mod}(x, N)$ denotes the modulo $N$ arithmetic. The seeding parameters $a$ and $b$ need to satisfy the following set of rules to ensure one-to-one mapping:

1) $0 < a < N$, $0 \leq b < N$, and $b$ be relatively prime to $N$;
2) $(a-1)$ be a multiple of $c$, for every prime $c$ dividing $N$;
3) $(a-1)$ be a multiple of 4, if $N$ is a multiple of 4.

Since the value of the starting point $\pi(0)$ has little impact on the interleaving performance, we have set it to 0 in (1) for convenience.

The recursion in (1) imposes a constraint for sequential implementation which may cause a long delay. An alternative form expresses $\pi(i)$ as a direct function of its indice $i$ and hence allows for parallel implementation:

1) $a \neq 1$:

$$
\pi(i) = \text{mod}(b \sum_{j=0}^{i-1} a^j, N) = \text{mod}\left(\frac{(1-a^i)b}{(1-a)}, N\right), \quad i = 0, 1, \ldots, N-1.
$$

(2)

2) $a = 1$:

$$
\pi(i) = \begin{cases} 
0, & i = 0, \\
\text{mod}(\pi(i-1)+b, N), & i = 1, \ldots, N-1 \\
\text{mod}(b i, N), & i = 0, 1, \ldots, N-1.
\end{cases}
$$

(3)

The reason for studying coprime interleavers is their simplicity. Notice that when $a = 1$ and $b$ is chosen to be the closest integer to the golden section of $N$, i.e. $b$ be closest to $\left(\sqrt{5}-1\right)xN + 0.5$ and relatively prime to $N$, (3) becomes the well-known Golden prime interleaver [7]. [7] showed that Golden prime interleavers in general perform as well as or better than $S$-random interleavers at short lengths. This suggests that with the right parameters, it is possible for a coprime interleaver to enjoy both high performance and memory-efficient implementation. Motivated by this observation, below we investigate how the parameters $a$ and $b$ affect the interleaving performance, and subsequently formulate rules to guide the selection of good parameters.

It is generally recognized that a good interleaver usually possesses a big minimum “spread” [6][9]. In the strict sense, for an interleaver to have a spread of $S$ requires that any two bits within a distance of $S$ be mapped to two positions that are at least $S$ apart [6]. Recently, Crozier relaxed the definition of spread by noting the sum of the distances between two bit positions before and after interleaving [9], namely, the spread of a bit pair $i$ and $j$ given by $S_{i,j} = |i-j| + |\pi(i) - \pi(j)|$. The recent proposition of two important criteria, the iterative decoding suitability (IDS) [8] and the cycle correlation sum (CCS) [1], formally established a tight connection between the spread of the interleaver and its performance in a turbo code. Since CCS provides a quite accurate prediction (which is also better than IDS) on the interleaving performance (especially
for short lengths of a couple of hundred bits) [1], we take CCS as one of our evaluation metrics.

An equally important property for an interleaver, especially for median lengths of a few hundred to a few thousand bits, is randomness. For example, a row-column interleaver typically has a larger minimum spread and better IDS and CCS values than a random interleaver, and may exhibit a better performance at short lengths of no more than a few hundred bits. However, due to the lack of randomness, its performance may drop noticeably below that of the random interleaver as the length increases to a few thousand bits. To facilitate the measurement of randomness, we introduce the concept of first order and second order spread spectrum of an interleaver, and further develop a scalar metric which we refer to as the variance of the second order spread spectrum (VSSS) [10]. Although other ways are possible, in this paper we will access the spread and the randomness properties of a coprime interleaver by means of CCS and VSSS.

We mention that, in addition to Golden prime interleavers and their variations like Golden interleavers and dithered Golden interleavers, several other note-worthy algebraic interleavers were proposed in literatures. The Welch-Costas interleavers make essential use of the Costas array in spread-spectrum systems [4]. Takeshita-Costello interleavers [5] are defined through a very special recursive form which equip these interleavers with properties very similar to a random interleaver. Both Welch-Costa and Takeshita-Costello interleavers perform like random interleavers, which lags behind $S$-random interleavers at short and medium lengths. Our target here is to find good coprime interleavers that perform on par with, if not better than, $S$-random interleavers.

For practical purpose, in the sequel, we focus on interleavers whose lengths are powers of 2. Unless otherwise stated, the conclusions we draw only apply to them. We show that the parameter $a$, or, a new parameter defined by $c = (a - 1)/4$, can be used to classify coprime interleavers. The relationship between $c$ and the two important characters (minimal spread and degree of randomness) is first established, and rules for choosing good parameters $a$ and $b$ are subsequently developed. Effectiveness of our proposed design rule is verified by computer simulations.

II. ACCESS THE SPREAD OF COPRIME INTERLEAVERS

According to the definition, all the coprime interleavers having a length $N = 2^k$ for some integer $k$ can be generated by a pair of parameters $a$ and $b$, where $a = 4 \times c + 1, 0 \leq c < N/4$, and $b$ is an odd integer. Our first tool is the CCS metric, which regards the correlation between the extrinsic input and output sequences of a BCJR decoder as the indication of the quality of the interleaver [1].

From the coding theory, the performance of an iterative decoder will approximate that of the optimal decoder when the code graph is free of cycles or when the outbound message from any computing unit does not circulate back. That latter condition translates to minimal correlation between the outbound message and the subsequent inbound message. In the case of turbo decoders, completion of any round of message exchange between the two component decoders inevitably introduces such undesirable message correlation. To see this, consider bits $i$ and $j$ in the first component code which are interleaved to bits $\pi(i)$ and $\pi(j)$ in the second component code. Since $i$ and $j$ are part of a convolutional codeword, they are inherently correlated. Hence, the reliability information carried by $i$ is transferred to the output extrinsic information of $j$ (through the BCJR decoding), which in turn becomes the input extrinsic information for bit $\pi(j)$. After the BCJR decoding of the second decoder, this reliability information for $\pi(j)$, originated from bit $i$, gets relayed to bit $\pi(i)$ and, after deinterleaving, is passed back to bit $i$. Hence, an important measure for the goodness of an interleaver is its ability to minimize the average amount of such correlated message carried from one decoder iteration to the next, where average is performed over all the bits in the sequence.

To quantify the above measure, [1] proposes to evaluate the correlation between the input and output extrinsic information of the BCJR decoding using the standard correlation coefficients. It is shown that correlation coefficients are a function of the Hamming distance between two bits and can be approximated by an exponential function. Specifically, [1] formulates the correlation between bits $i$ and $j$ as $e^{-c|i-j|}$, where $c$ is a parameter. Likewise, the correlation between bits $\pi(i)$ and $\pi(j)$ follows $e^{-c|\pi(i) - \pi(j)|}$, and the correlations induced by cycle $i \rightarrow j \rightarrow \pi(j) \rightarrow \pi(i) \rightarrow i$ becomes $e^{-c(|j-i|+|\pi(j) - \pi(i)|)}$. Averaging over all such cycles gives rise to the metric of cycle correlation sum [1]:

$$CCS = \sum_{i,j \in A} e^{-c(|j-i|+|\pi(j) - \pi(i)|)}$$

where $A \equiv \{0, 1, 2, ..., N - 1\}$, and $N$ is the interleaver length. The parameter $c$ is a constant that is dependent on the component convolutional code, or loosely, the memory size of the component convolutional codes [1]. A lower value of CCS implies less undesirable message correlation introduced in each decoding iteration, a higher efficiency in the iterative turbo decoder, and therefore a better performance achieved by the code. For a more detailed discussion including the computation of CCS, please refer to [1].

We now evaluate coprime interleavers using CCS. Figure 1 plots the CCS values of a set of coprime interleavers with length $N = 128$ bits. The y-axis represents the CCS value and the x-axis represents the value of parameter $b$. From the figure, we find that the CCS curve of a subclass in general fluctuates with $b$. Hence, we group subclasses of coprime interleavers into categories with respect to their CCS variations. Different categories are marked by different line types and colors as shown in figure 1.

Let us start with the category (represented by blue lines without any other marks) whose $a$ equals 5, 13, 21, ..., 125. Their CCS values are not sensitive to $b$ and form a (nearly) straight horizontal line. This category, referred to as regular coprime interleavers in [3], has its $a$’s following the rule of $(a = 4c_{od} + 1$ where $c_{od}$ is an odd integer.
When \( a = 9, 25, 41, \ldots, 121 \), the CCS curves (marked with red crosses) exhibit a small wave, indicating a small variation among their CCS values. The parameter \( a \) in this category follows the rule of \( a = 8c_{	ext{odd}} + 1 \) where \( c_{	ext{odd}} \) is an odd integer. Similarly, \( a = 16c_{	ext{odd}} + 1 \) form the third category and so on.

To summarize, we grouped coprime interleavers like this: Let \( a = 4c + 1 \) and \( c = 2^{	ext{power}} \times c_{	ext{odd}}, \) where \( c_{	ext{odd}} \) is an odd integer. The subclasses have the same \( c_{	ext{power}} \), the same number of 2 factors in \( c \) contained in \( c \), the larger the CCS curve, exhibiting the same level of CCS variations.

When \( c_{	ext{power}} = 0 \), we have the category of regular coprime interleavers, whose CCS values remain near constant regardless of \( b \). The variation of CCS curves increases with \( c_{	ext{power}} \); that is, the more the factors of 2 contained in \( c \), the larger the CCS wave. The limiting case is when \( c = 0 \) (which may be interpreted as \( c \) containing uncountable factors of 2 that the effect of the odd divider in \( c \) disappears), which leads to a category having the biggest CCS variation. Further, the bigger the CCS curve waves, the lower the lowest CCS values in this curve. Hence, the bigger \( c_{	ext{power}} \) indicates a smaller possible CCS values which is one of the attributes to guarantee a good performance.

In the next section, we will prove that regular coprime interleavers \( (c_{	ext{power}}=0) \) have the largest randomness degree among all the coprime interleavers and that the degree of randomness decreases with the increase of \( c_{	ext{power}} \). Hence, it appears that randomness and spread can not be optimized at the same time, which calls for a balance in the design process.

III. ACCESSING THE RANDOMNESS OF COPRIME INTERLEAVERS

In this section we introduce the concept of variance of the second-order spread spectrum to characterize the degree of randomness for an interleaver [10]. We next show that regular coprime interleavers have the maximal degree of randomness.

**Definition 1:** Let \( i \) and \( j \) be the input bit-pair of an interleaver with length \( N \), \( \pi(i) \) and \( \pi(j) \) be the corresponding interleaved bit-pair. Let \( u \) and \( v \) be the distances where \( 1 \leq u = |i - j| \leq N - 1 \) and \( 1 \leq v = |\pi(i) - \pi(j)| \leq N - 1 \). Let \( S_{u,v} \) be the number of the weight-2 patterns \((i,j)\) pairs with the same \( u \) and \( v \). Then the set of \( S_{u,v} \) forms an \((N-1)\)-by-\((N-1)\) matrix (termed the second-order spread spectrum matrix [10]), with \( u \) indexing the rows and \( v \) indexing the columns. \( VSSS \) is defined as \( \sum_{u,v} (\text{var}(S_{u,v}))/\left((N-1)\right) \), where \( \text{var}(S_{u,v}) \) stands for the variance of \( u \)th row in the spread matrix. [10] shows that a smaller \( VSSS \) indicates a larger degree of randomness of the interleaver.

**Definition 2:** Consider a function \( z = F(x,y) \), \( 0 < x < m \), \( 0 \leq y < m - 1 \). Let \( m_{z,x} \) denote the number of \( y \) which generates the same \( z \), for a given \( x \). We define the matrix
Given a pair $(x, y)$, the variance of $F(x, y)$ is defined as $\sum x (\text{var}(m_x)) / (m - 1)$.

**Lemma 1:** For a given $u \in \{1, 2, \ldots, N - 1\}$, the elements contained in the set $\{A(i)\}$, where $A(i) = \mod(b \times \frac{a^u - 1}{a - 1} \times a^i, N)$, $i = 0, 1, \ldots, N - 1$, (5) will not exist in the set $\{B(i)\}$, where $B(i) = N - \mod(b \times \frac{a^u - 1}{a - 1} \times a^i, N)$, $i = 0, 1, \ldots, N - 1$.

**\n Proof:** Please refer to the Appendix. $\triangle$

**Theorem 1:** If $F(x, y)$ is in the form of $F(x, y) = \mod(b \times \frac{a^x - 1}{a - 1} \times a^y, N)$, then the VSSS of the length-$N$ coprime interleaver generated with parameters $a$ and $b$ is less than the variance of $F(u, i)$, where $i$ and $j$ are any input pair of the interleaver, and $u = |i - j|$.

**\n Proof:** Given a pair $(u, v)$, we can find a set $C_i$ of $i$ satisfying $v = F(u, i)$, then $m_{u, v}$ equals the size of $C_i$.

On the other hand, according to the definition of coprime interleavers, we have

$$v = \begin{cases} \mod(b \times \frac{a^u - 1}{a - 1} \times a^i, N), & \pi(j) > \pi(i), \\ N - \mod(b \times \frac{a^u - 1}{a - 1} \times a^i, N), & \pi(j) \leq \pi(i). \end{cases}$$

(7)

We divide $C_i$ into two subsets: $C_i^{(1)}$ for $\pi(j) > \pi(i)$ and $C_i^{(2)}$ for $\pi(j) < \pi(i)$, such that $C_i^{(1)} \cup C_i^{(2)} = C_i$ and $C_i^{(1)} \cap C_i^{(2)} = \phi$. Hence the size of $C_i^{(1)}$ is not larger than the size of $C_i$, which equals to $m_{u, v}$.

For a coprime interleaver $\pi$, using (7), under $u$ and $C_i^{(1)}$, we get the unique output $V_1$. Now from Lemma 1, given $u$, $C_i^{(1)}$ contains all the $i$s that will generate $V_1$. Hence, $S_{u, v_1}$ equals the size of $C_i^{(1)}$, and it is smaller than $m_{u, v}$.

Following the same line of derivation, when we assume that the set $C_i^{(2)}$ will generate $V_2$ under $u$, we will get that $m_{u, v} \leq S_{u, v_2}$.

Hence, the value of each element in $M_F$ is divided into two parts which correspond to two elements in VSSS. Therefore, VSSS is less than the variance of $M_F$ of $F(u, i)$. $\triangle$

Additionally, because $F(u, i)$ is periodic for a given $x$, we can convert the problem of maximizing the VSSS of a coprime interleaver to one of increasing the period of $F(u, i)$.

**Theorem 2:** If we break $\frac{a^u - 1}{a - 1}$ down to the product of $2^q$ (even component) and $l$ (odd component), where $l$ is odd and $q$ is a nonnegative integer, then $F(u, i)$ and sequence $\mod(a^i, N/2^q)$ have the same period.

**\n Proof:** Assume the period of $F(u, i)$ is $P_f$, then

$$F(u, i + P_f) = F(u, i) \equiv 0.$$  

(8)

From the definition of $F(u, v)$'s definition, we get

$$\mod(b \times \frac{a^u - 1}{a - 1} \times (a^{i+P_f} - a^i), N) \equiv 0.$$  

(9)

Under the assumption in Theorem 2, (9) becomes

$$\mod((b \times 2^q \times l \times (a^{P_f} - a^i)), N) \equiv 0.$$  

(10)

Since both $b$ and $l$ are odd, we have

$$\mod((a^{P_f} - a^i), N/2^q) \equiv 0.$$  

(11)

This essentially states that $P_f$ is also the period of sequence $\mod(a^i, N/2^q)$. $\triangle$

**Theorem 3:** For a coprime interleaver with length $N = 2^m \geq 4$ and parameters $a$ and $b$, if $c = (a - 1)/4$ is odd, then the period of sequence $\mod(a^i, N/2^q)$ is maximized.

**\n Proof:** Since $N$ is a multiple of 4 and $a = 4c + 1$ (see the definition of coprime interleavers), (11) can be simplified to

$$\mod((4 \times c + 1)^{P_f} - 1), N/2^q) \equiv 0.$$  

(12)

Expanding (12), we get

$$\mod(\sum_k P_f (4c + 1)^{k}) (4c + 1)^{2} \ldots + (4c)^{P_f}), N/2^q) \equiv 0.$$  

(13)

which can be re-written as

$$\mod(\sum_k P_f (4c + 1)^{k}) (4c + 1)^{2} \ldots + (4c)^{P_f}), N/2^q) \equiv 0.$$  

(14)

Similarly, we can factorize $P_f$ into a product of an odd component $O_p$ and an even component $E_p$. Observing that all the terms in $\sum_k P_f (4c + 1)^{k}$ contain at $4c \times E_p$, we can extract it and move it before the summation. The remainder can be denoted by an odd number $A$. Finally, (14) becomes

$$\mod((4 \times A \times E_p), c \times N/2^q) \equiv 0.$$  

(15)

Consequently, only when $c$ is odd, can $E_p$ be maximized as $N/2^{q+2}$. On the other hand, since $P_f$ is the period, it is the smallest number satisfying (11). Thus the smallest possible value $P_f$ is $E_p$ (when $O_p = 1$). Finally, $P_f = N/2^{q+2}$ is the largest period possible, obtained when $c$ is odd. $\triangle$

**Corollary 1:** Among all the coprime interleavers, the regular coprime interleavers ($c_{\text{power}} = 0$) provide the minimal VSSS.

**Corollary 2:** Let $c = 2^{c_{\text{power}}} \times c_{\text{odd}}$. The degree of randomness decreases with the increase of $c_{\text{power}}$. The degrees of randomness of all the coprime interleavers remain at the same level for the same $c_{\text{power}}$.

**IV. INTERLEAVER DESIGN AND SIMULATIONS**

From Sections II and III, we have learnt that the largest degree of randomness and the largest spread can not be achieved at the same time for a coprime interleaver. As $c_{\text{power}}$ increases, the best spread (the lowest CCS) in the category of coprime interleavers increases, but the degree of randomness reduces. Additionally, they both stay at the same level for the same $c_{\text{power}}$, irrelevant to $c_{\text{odd}}$. Hence for convenience we can take $c_{\text{odd}} = 1$.

When we design a coprime interleaver,

- At first, we will choose $c_{\text{power}}$ which determines both the randomness character and the range of spread character.

As the code length $N = 2^k$, $c_{\text{power}}$ could be any integer from $0$ to $k - 3$, since $a \leq N$. To balance the spread
and randomness, we might take some middle value of $c_{power}$. On the other hand, for convenience, we also let $c_{odd} = 1$. Then we can obtain the parameter $a$ and $a = 4 + 2^{c_{power}} + 1$.

- After choosing the parameter $a$, we have fixed the randomness and possible maximal spread. Then we will search the parameter $b$ to obtain the maximal spread by minimizing the CCS.

As an example, consider $N = 2048$. We have 10 categories of coprime interleavers, exemplified by $a = \{1, 5, 9, 17, 33, 65, 129, 257, 513, 1025\}$, each associated with a different $c_{power}$: $c_{power} = \infty, 0, 1, \ldots, 7, 8$. To get the balance between the spread and randomness, we choose $c_{power} = 5$, that is $a = 129$. Then we will search the parameter $b$ to obtain the lowest CCS associated with $a = 129$. Finally we get $a = 129$ and $b = 161$.

We compares the BER performance of the coprime interleaver ($a = 129, b = 161$) and two $S$-random interleavers (spread $s = 10, 20$) based on a turbo code with code length as 2048 in AWGN channel. We use [5,7] as the component of turbo code, and the code rate is 1/3. For each frame, we did 8 rounds iteration. From Figure 2, we see the optimized coprime interleaver outperforms the $S$-random interleaver with $s = 10$ by 0.2db. It provides a performance better than the $S$-random interleaver with $s = 20$ at low to medium SNRs and a comparable performance at high SNR.

![Fig. 2. BER of the optimized coprime interleaver ($a = 129, b = 161$) and $S$-random interleavers ($s=10,20$) for $N = 2048$.](image1)

V. Conclusion

Algebraic interleavers are preferable due to their simplicity in hardware implementation and economy in storage. Algebraic interleavers with good randomness and spread properties promise great performances at low cost.

This paper investigates the coprime interleavers, a rich subset of algebraic interleavers. For interleavers whose lengths are powers of 2, we formulated a critical parameter $c_{power}$, which captures some important behavioral properties of coprime interleavers. We used the cycle correlation sum criterion (CCS), to measure the minimum spread, and the variance of the second order spread spectrum, to measure the degree of randomness, for coprime interleavers. With the increasing $c_{power}$, the CCS property becomes better, while the randomness property becomes worse. Since the optimal degree of randomness and the optimal spread cannot be simultaneously achieved for coprime interleavers, we formulated a rule to find interleaver parameters that strike the a good balance between them. Simulations confirm the effectiveness of our rule by demonstrating that optimized coprime interleavers perform as well as or better than $S$-random interleavers.

VI. Appendix: Proof of Lemma 1

$\nabla$ Proof: (Proof by contradiction) If an element $A(i_1)$ in sequence 5 equals to an element $B(i_2)$ in sequence 6, it means:

$$\text{mod}(b \times a^u - 1 \times a^{i_1}, N) + \text{mod}(b \times a^u - 1 \times a^{i_2}, N) = N. \quad (16)$$

Without loss of generality, we assume $i_1 \leq i_2$ and let $t = i_2 - i_1$, we can rewrite the previous equation as

$$\text{mod}(b \times a^u - 1 \times a^{i_1} \times (1 + a^t), N) = 0. \quad (17)$$

Consider that $\frac{a^n - 1}{a - 1} = q_2^n \times q_2$ (where $q_2$ is odd), we have

$$\text{mod}(b \times q_2 \times a^{i_1} \times (1 + a^t), N/2^{q_1}) = 0 \quad (18)$$

$$\text{mod}(1 + a^t), N/2^{q_1}) = 0 \quad (19)$$

Following the definition of coprime interleavers and substituting $a = 4c + 1$, we expand this equation as:

$$\text{mod}((\sum_{k=1}^{t} (\frac{t}{k}) \times (4 \times c)^k) + 2, N/2^{q_1}) = 0. \quad (20)$$

It is easy to see that $\sum_{k=1}^{t} (\frac{t}{k}) \times (4 \times c)^k + 2$ is a multiple of 2, and the remainder is odd. This makes $\text{mod}(B \times 2), N/2^{q_1}) = 0$, (21) where $B$ is odd. Since $N > 2^{n+1}$, (21) can not hold. Contradiction. $\triangle$

REFERENCES


