Kusume, K.; Bauch, G.: Quadratic permutation polynomial interleavers for 3GPP LTE turbo codes. *International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Lapland, Finland, September 8-11, 2008.

QUADRATIC PERMUTATION POLYNOMIAL INTERLEAVERS FOR 3GPP LTE TURBO CODES

Katsutoshi Kusume and Gerhard Bauch
DOCOMO Euro-Labs
Landsbergerstr. 312, 80687 Munich, Germany. Email: {kusume,bauch}@docomolab-euro.com

ABSTRACT

The contention-free property of interleavers is one of the key design requirements for the parallel decoding implementations of turbo codes in order to achieve high decoding throughput. *Quadratic permutation polynomial* (QPP) interleavers are *maximum contention-free* (MCF), i.e., every factor dividing the interleaver length becomes a possible degree of parallel decoding processing without any memory access contention. Despite the desirable MCF property, the performance of QPP interleavers has been demonstrated to be excellent. The simple algebraic construction is of particular interest for practical systems as well. However, an efficient method finding good QPP interleavers needs more studies. We propose a simple method, which finds QPP interleavers maximizing the randomness, while certain minimum spreading property is guaranteed. Although the design is code-independent, turbo codes using the interleavers found by our method result in a large free distance on top of the good randomness and spreading properties. Numerical simulations show that turbo codes using these interleavers perform very well.

I. INTRODUCTION

Turbo codes have been widely adopted in many application areas due to the excellent performance approaching the theoretical limit [3]. Since turbo codes comprise two constituent codes, which are concatenated by an interleaver as shown in Fig. 1, an interleaver design is an integrated part of the code design and has been intensively studied for improving the error correction capability of turbo codes.

It was soon recognized that parallel implementations of the decoding algorithm of turbo codes would be of particular importance in order to achieve very high data rates. This is due to the fact that, as shown in Fig. 1, the decoding results of one decoder are exchanged with the other in a successive and iterative manner. And each decoder applies forward and backward recursions of *a posteriori probability* (APP) decoding algorithm that introduces large delays.

Several proposals have been made to parallelize APP decoders (e.g. [8, 9, 15]). A code word is divided into M subblocks which are decoded by M processors operating in parallel. Although this technique can increase the throughput at each decoder, the interleaver between the two decoders can still be a bottleneck of the overall throughput improvement. This is because the decoding results of M subblocks have to be simultaneously exchanged according to the (de)interleaving rule without any memory access contention.

Fig. 2 illustrates an example of the memory contention problem. In this example, a code word is divided into $M = 4$ subblocks. Each subblock has a window size of $W = 4$ and needs to read/write data (in parallel to other subblocks) in 4 successive steps (or 4 clock cycles) in an ideal case, starting from the leftmost slot towards right. The second step is depicted in Fig. 2 and there is a collision between the second and the fourth subblocks simultaneously accessing the third subblock. Therefore, one memory access has to be scheduled after the other; causing a delay. Contention-free interleavers are desirable for the parallel decoding implementations of turbo codes.

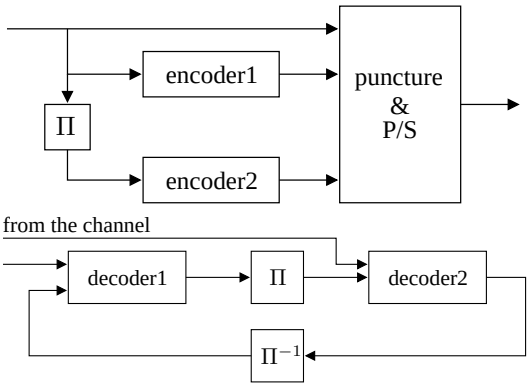

Figure 1: Turbo encoder and decoder.

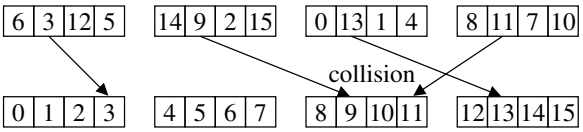

Figure 2: An example of memory access contention.

A mathematical description of the contention-free condition from [10] is given below. An interleaver $\Pi(n)$, $0 \leq n < N$, is contention-free for window size W ($M = N/W$ processors operating on M subblocks in parallel), if the following condition holds for both $\Pi(n)$ and its deinterleaver $\Pi^{-1}(n)$:

$$\lfloor g(w + uW)/W \rfloor \neq \lfloor g(w + vW)/W \rfloor, \qquad (1)$$

where $0 \leq w < W$, $0 \leq u < v < N/W$, and $g(\cdot)$ is either $\Pi(n)$ or $\Pi^{-1}(n)$. If an interleaver is contention-free for all window sizes W dividing the interleaver length N, it is called a *maximum contention-free* (MCF) interleaver.

In general, interleavers are not contention-free. For instance, the interleavers designed for turbo codes according to the *Third Generation Partnership Project* (3GPP) [1] are not contention-free. This can be evidenced by Fig. 3, which illustrates an example of clock cycles necessary for parallel memory ac-

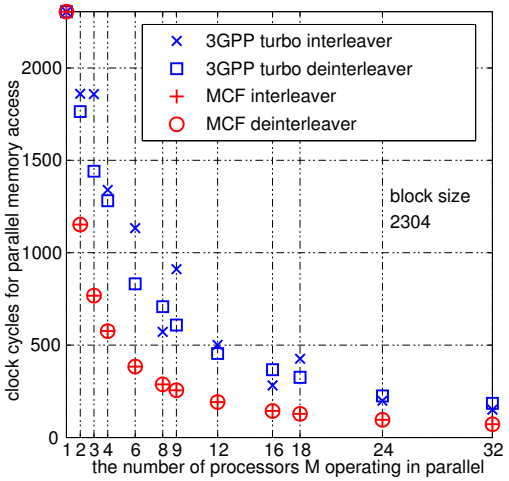

Figure 3: An example of clock cycles necessary for parallel memory access versus the number of processors operating in parallel for block size of 2304.

cesses versus the number of processors when interleaver size is $N = 2304$. Here, the number of clock cycles is simply counted by summing up the largest number of simultaneous accesses to a subblock at each access step. For example, in Fig. 2, there are $W = 4$ memory access steps and the number of clock cycles necessary is computed as $7 = 1 + 2 + 2 + 2$ (only the first step is contention free, starting from the leftmost slot of each subblock). In Fig. 3, we see that the number of clock cycles for MCF interleavers ($W = N/M$) is decreasing, inversely proportional to the number of processors M, for both interleaver and deinterleaver. The 3GPP turbo (de)interleaver needs significantly higher number of memory accesses.

In literature, several contention-free interleavers can be found (e.g. [4, 6, 10]). These interleavers are designed contention-free for certain window sizes and are generally not MCF interleavers.

Quadratic permutation polynomial (QPP) interleavers have been proposed for the use with turbo codes [11]. It has been shown in [13] that any QPP interleaver is maximum contention-free. Besides this remarkable MCF property, its simple algebraic construction is desirable for practical systems. Only two nonnegative integers are needed to represent each interleaver. Moreover, despite its simple construction rule and the MCF property, the performance of turbo codes using QPP interleavers are surprisingly good, even better than using the 3GPP non contention-free interleavers for some block lengths as demonstrated in [13].

However, QPP interleaver parameters are provided only for a small number of block lengths, and an efficient method for finding good QPP interleavers needs more studies. The original criterion for the exhaustive search in [13] is the maximization of free distance of codes. As mentioned in [13], it is impractical for large block lengths. In [12], a new metric was proposed to find good QPP interleavers. However, the new metric in [12] may not be optimum since, as we will show later by simulation results, QPP interleavers found by our proposed criterion perform better at least for certain block length.

Recently, there have been several discussions about contention-free interleavers in the 3GPP *long term evolution* (LTE) meetings, and there has been an agreement on using QPP interleavers and the parameters [2]. We will show the performance of turbo codes using QPP interleavers obtained from our scheme in comparison to those defined in [2].

It is worth noting that there is an alternative method to the contention-free interleaver design. In [14], it was shown that mapping interleaving laws could be found for any interleaver to be contention-free. However, large memory is required for storing mapping rules that is of disadvantage for practical systems.

II. Quadratic Permutation Polynomials

QPP interleavers of block size N are defined for $0 \leq n < N$ over integer rings as

$$\Pi_{f_1,f_2}(n) \triangleq f_1 n + f_2 n^2 (\mathrm{mod}\ N), \tag{2}$$

where nonnegative integers f_1 and f_2 have to be chosen to satisfy certain conditions. The necessary and sufficient conditions for a quadratic polynomial to be a permutation polynomial, i.e., $\Pi_{f_1,f_2}(n)$ taking each element of $\{0, \ldots, N-1\}$ once and only once, are given in [13]. In general, the number of possible permutation polynomials is not a smooth function of N. However, in a special case of N being a power of two, then there are approximately $N^2/4$ possible pairs of f_1 and f_2 [13]. Therefore, it is impractical to find the best pair by computing free distance of turbo codes using all possible pairs for a large N.

A. *Tradeoff between Spreading and Dispersion Properties*

The computation of free distance of turbo codes is computationally intensive and also code-dependent. Instead, we consider the spread property of interleavers as one of search criteria. The spread property is known as one of key indicators for a good interleaver and is defined as

$$S \triangleq \min_{n_1,n_2} |\Delta_x(n_1,n_2)| + |\Delta_y(n_1,n_2)|, \tag{3}$$

where $0 \leq n_1 < n_2 < N$ and

$$\Delta_x(n_1,n_2) \triangleq n_2 - n_1, \quad \Delta_y(n_1,n_2) \triangleq \Pi(n_2) - \Pi(n_1). \tag{4}$$

In [5], the upper bound of the spread is shown to be $\sqrt{2N}$. Keeping a high spread property ensures that error patterns for one decoder are well-spread for the other decoder, and correlations among neighboring bits are also avoided. With a high spread, low-weight code words for the first decoder are not interleaved to low-weight patterns for the second decoder. That improves the code weight spectrum and lowers the error floor for high SNR values; there is a certain connection to the free distance of codes although the spread property is code-independent.

The maximization of the spread property alone, however, does not guarantee good performance in general. Another well-known key indicator for a good interleaver is the randomness.

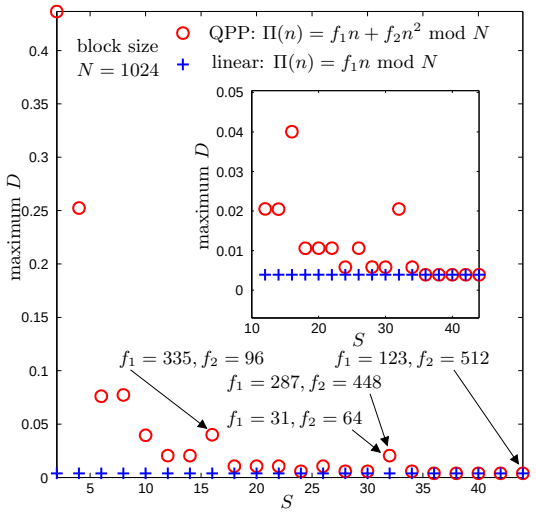

Figure 4: Tradeoff between spread and dispersion properties for $N = 1024$.

It is widely known that the performance of turbo codes using regularly structured interleavers is poor, especially for medium to large block sizes. Then, the randomness plays an important role for a good convergence behavior. The randomness can be measured by the so-called *dispersion* [6]:

$$D' \triangleq |\{\Delta_x(n_1, n_2), \Delta_y(n_1, n_2)\}|, \tag{5}$$

for all $0 \le n_1 < n_2 < N$ where $|\cdot|$ denotes a cardinality of set. Since D' is upper bounded by $N(N-1)/2$, it is usually normalized to get

$$D \triangleq \frac{D'}{N(N-1)/2} \quad \text{where} \quad \frac{2}{N} \le D \le 1. \tag{6}$$

In the following, the terms "dispersion" and "randomness" are used interchangeably.

From (3) and (5), it is clear that the spread property and randomness cannot be maximized at the same time: for a certain value of $\Delta_x(n_1, n_2)$, the smaller number of different but large values of $\Delta_y(n_1, n_2)$ is preferred to get a large S, i.e., "regular" structure is appropriate, while the opposite is true for obtaining a large D. Therefore, there is a tradeoff between these two properties.

Fig. 4 illustrates an example showing the tradeoff between the spread property and the randomness for the block size of $N = 1024$. Both S and D are computed for all possible QPP interleavers, which are grouped according to the value of S. In each group having a certain value of S, the maximum randomness D is computed and plotted in Fig. 4. It can be observed that the maximum randomness D tends to become smaller as the spreading property gets larger, illustrating the tradeoff. However, it should be noted that larger spread property does not always lead to smaller randomness, as we can see, for instance, at $S = 16, 32$.

For the comparison, we have performed the same analysis for linear interleavers which can be considered as a special case of QPP interleavers in (2) where $f_2 = 0$. It can be clearly observed that having the second order term makes indeed a big difference in terms of the maximum achievable randomness. The randomness of QPP interleavers, however, becomes as low as linear interleavers for a very high spreading property.

B. *A Proposed Criterion for Finding Good QPP Interleavers*

Having observed the tradeoff between the spread property and the randomness in the previous section, we propose the simple criterion for finding good QPP interleavers:

$$\max D \qquad \text{subject to: } S \ge S_{\text{const}}, \tag{7}$$

where S_{const} is the minimum spread that has to be satisfied. Among interleavers having the spread factor equal to or above S_{const}, we choose the one providing the largest randomness.

The constraint on the spread property efficiently reduces the search space. That is due to the fact that the spread property in (3) is determined by the minimum distance $|\Delta_x(n_1, n_2)| + |\Delta_y(n_1, n_2)|$ computed from all possible pairs of n_1 and n_2, while only those pairs within a window size of S_{const}, i.e., $|\Delta_x(n_1, n_2)| \le S_{\text{const}}$, have to be considered, since otherwise the distance already exceeds S_{const} irrespective of $|\Delta_y(n_1, n_2)|$. Furthermore, the computation can immediately stop and skip the rest of pairs when any pair of n_1 and n_2 yields the distance above S_{const}. This scheme is far simpler than comparing free distance and the search time is reasonable even for a large block size.

What remains is the proper choice of S_{const}. From a number of numerical simulations, we found that the following empirical choice leads to good performance for a wide range of block size N:

$$S_{\text{const,empirical}} \triangleq \sqrt{\frac{N}{\max\left(\lfloor N/1000 \rfloor, 1\right)}}. \tag{8}$$

This choice emphasizes the importance of the randomness for medium-to-large block size by compromising the spread property as compared to the frequently used value of $\sqrt{N}$ for the criterion to find S-random interleavers (see e.g. [6]).

III. Simulation Results

We have performed the search procedure finding good QPP interleavers based on the proposed criterion. In the following, various aspects and properties of the obtained interleavers are discussed and compared with the QPP interleavers from the latest 3GPP LTE proposal [2] as well as with the non contention-free 3GPP interleaver [1]. FER performance of turbo codes [1] using different interleavers is provided for the four rates: $1/3$, $1/2$, $3/4$, and $8/9$. The results for three different block sizes are presented: small ($N = 40$), medium ($N = 1024$), and large ($N = 6144$). We start with our discussion on the results for the medium size: $N = 1024$.

A. *An Example of Medium Block Size:* $N = 1024$

In this example, we have performed the search process based on three different criteria: maximizing D with a constraint $S \ge \sqrt{N}$ (as proposed in Eqn. 8) or $S \ge \sqrt{N/4}$ (just for

Table 1: QPP Interleavers and 3GPP non contention-free turbo interleaver for $N = 1024$.

N	f_1	f_2	S	D	d_{free}				Note
					$R = 1/3$	$R = 1/2$	$R = 3/4$	$R = 8/9$	
1024	31	64	32	0.020501	27	14	6	4	$\max d_{\text{free}}$ [13], [12], 3GPP LTE [2]
	287	448	32	0.020511	27	15	6	5	$\max D$ s.t.: $S \geq \sqrt{N}$ (as in Eqn. 8)
	335	96	16	0.040046	16	11	5	4	$\max D$ s.t.: $S \geq \sqrt{N/4}$ (for comparison)
	123	512	44	0.003887	27	16	5	4	$\max S$
	–	–	9	0.746537	25	14	4	3	3GPP non contention-free interleaver [1]

comparison), and maximizing S. The results are summarized in Table 1. We also computed the free distance d_{free} of the resulting code using the algorithm in [7].

Several interesting observations can be made from the table. The tradeoff between S and D can be observed for the three different criteria. This tradeoff can be visually observed when referring back to Fig. 4. $\Pi_{287,448}$ is the most balanced choice which applies our proposed empirical constraint in (8). $\Pi_{335,96}$ has a superior randomness with the compromised spread property, which leads to smaller free distance. $\Pi_{123,512}$ has the best spreading property and also good free distance for most of the rates, but the randomness is extremely low (also cf. Fig. 4). Actually, $\Pi_{123,512}$ is equivalent to a linear interleaver due to the choice of $f_2 = N/2$. With $f_2 = N/2$ (when N is an even number), any QPP interleaver can be represented by an equivalent linear interleaver because it holds

$$\Pi_{f_1,\frac{N}{2}}(n+1) - \Pi_{f_1,\frac{N}{2}}(n) = f_1 + \frac{N}{2} \pmod N, \quad (9)$$

which is independent of n, and thus we get

$$\Pi_{f_1,\frac{N}{2}}(n) = (f_1 + N/2) \cdot n \pmod N. \quad (10)$$

$\Pi_{31,64}$ was obtained by maximizing free distance in [13] or by the new metric in [12]. And it is also chosen by 3GPP LTE [2]. It has the very similar properties as $\Pi_{287,448}$ that we found. Surprisingly, the free distance properties of $\Pi_{287,448}$ are even better than $\Pi_{31,64}$ for the rates $1/2$ and $8/9$, although the criterion of our proposal is code-independent and we do not attempt to maximize the free distance.

The properties of the 3GPP interleaver [1] are rather poor except the very high randomness (last row in Table 1) regardless of its non contention-free property.

The FER performance versus E_b/N_0 after 8 iterations is plotted in Fig. 5. Code bits are QPSK modulated and transmitted over an AWGN channel. The performance of $\Pi_{123,512}$ is poor due to its regular structure. The best performance of the proposed $\Pi_{287,448}$ can be observed for all the rates.

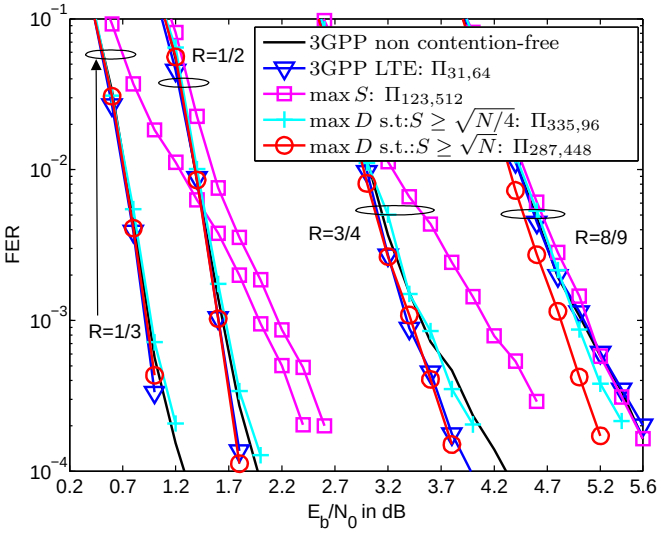

Figure 5: FER versus E_b/N_0 for $N = 1024$ after 8 iterations.

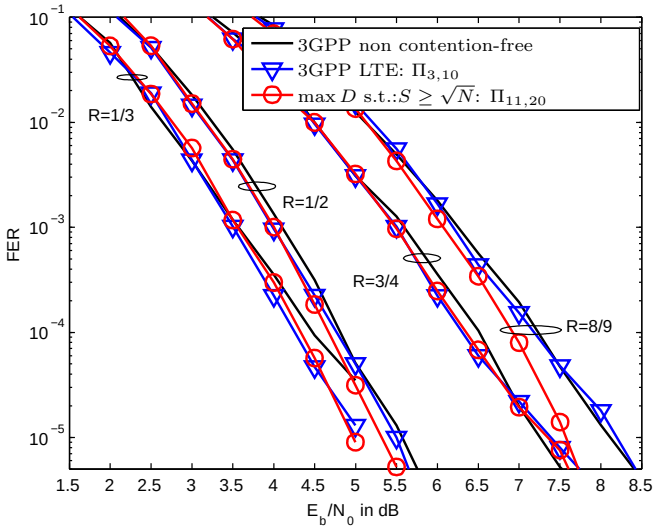

Figure 6: FER versus E_b/N_0 for $N = 40$ after 8 iterations.

B. *An Example of Short Block Size:* $N = 40$

This example is a very short block size of $N = 40$. For such a short block, there are not many choices for QPP interleavers. Nevertheless, study of such an extreme case is helpful to understand some important implications for the proper design. The upper part of Table 2 summarizes the results for $N = 40$.

Our solution $\Pi_{11,20}$ is equivalent to a linear interleaver due to the choice of $f_2 = N/2$ as discussed in the previous subsection (cf. Eqns. 9 and 10). Thus, the regular structure leads to the low randomness, but the highest spread property and the largest free distance among three interleavers are achieved. The FER performance results in Fig. 6 evidence the best performance of our choice $\Pi_{11,20}$.

C. *An Example of Large Block Size:* $N = 6144$

The last example is a large block size of $N = 6144$. In contrast to the short block size, the randomness plays a more important role. The results found by applying the proposed criterion in (7)

Table 2: QPP Interleavers and 3GPP non contention-free turbo interleaver for $N = 40$ and 6144.

N	f_1	f_2	S	D	d_{free}				Note
					$R = 1/3$	$R = 1/2$	$R = 3/4$	$R = 8/9$	
40	3	10	4	0.137179	11	8	3	2	3GPP LTE [2]
	11	20	8	0.096154	15	10	4	3	max D s.t.: $S \geq \sqrt{N}$ (as in Eqn. 8)
	–	–	5	0.611538	9	7	4	2	3GPP non contention-free interleaver [1]
6144	263	480	24	0.013663	26	16	8	4	3GPP LTE [2]
	1295	480	48	0.013628	31	17	7	4	max D s.t.: $S \geq \sqrt{N/6}$ (as in Eqn. 8)
	5615	2016	48	0.013628	31	20	8	4	max D s.t.: $S \geq \sqrt{N/6}$ (as in Eqn. 8)
	–	–	12	0.788381	28	16	5	4	3GPP non contention-free interleaver [1]

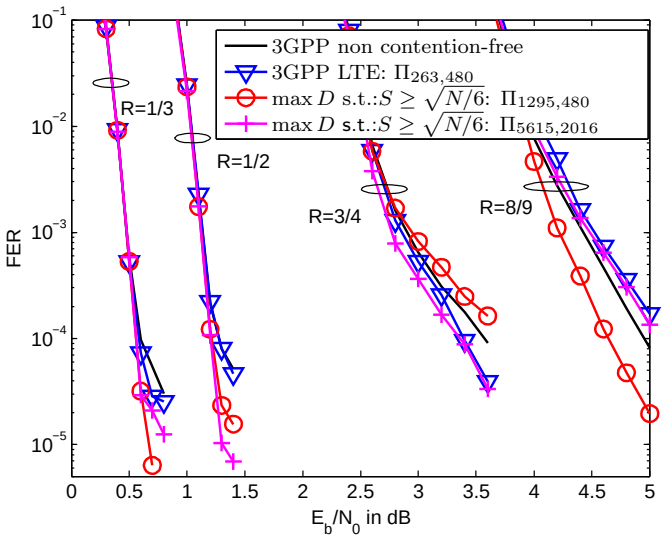

Figure 7: FER versus E_{b}/N_0 for $N = 6144$ after 8 iterations.

using the empirical spreading property constraint in (8) are summarized in the lower part of Table 2. Two QPP interleavers $\Pi_{1295,480}$ and $\Pi_{5615,2016}$ are presented. These two interleavers are obtained from the same criterion, i.e., they are equivalent in terms of the spread property and randomness, but are different in terms of free distance properties. These interleavers exhibit the different FER performance as illustrated in Fig. 7, but both are performing quite well, except for $\Pi_{1295,480}$ at rate $3/4$.

IV. Conclusions

We studied QPP interleavers, which have several desirable properties such as the simple algebraic construction rule and the MCF property. In particular, the MCF property of interleavers is one of the key design requirements for the parallel decoding implementations of turbo codes, aiming at very high decoding throughput. We proposed the simple criterion to efficiently find good QPP interleavers for various block lengths. Our method finds QPP interleavers which maximize the randomness while certain minimum spreading property is guaranteed. We also proposed the empirical value for the minimum spreading property constraint which is a function of the block length. The resulting interleavers exhibit various favorable properties and the excellent FER performance has been demonstrated by numerical simulations for different block lengths.

Acknowledgment

The authors would like to thank Tetsushi Abe for fruitful discussions and also for providing us with the calibrated simulation environment of turbo codes.

References

[1] 3GPP TS 25.212. 3rd generation partnership project; technical specification group radio access network; multiplexing and channel coding (FDD) (release 1999), March 2000.

[2] 3GPP TSG RAN WG1 #48, R1-071195. QPP interleaver parameters, February 2007.

[3] C. Berrou and A. Glavieux. Near optimum error correcting coding and decoding: Turbo-codes. *IEEE Transactions on Communications*, 44(10):1261–1271, October 1996.

[4] C. Berrou, Y. Saouter, C. Douillard, S. Kerouédan, and M. Jézéquel. Designing good permutations for turbo codes: Towards a single model. In *Proc. IEEE International Conference on Communications (ICC2004)*, volume 1, pages 341–345, June 2004.

[5] E. Boutillon and D. Gnaedig. Maximum spreading of d-dimensional multiple turbo codes. *IEEE Transactions on Communications*, 53(8):1237–1242, August 2005.

[6] L. Dinoi and S. Benedetto. Variable-size interleaver design for parallel turbo decoder architectures. *IEEE Transactions on Communications*, 53(11):1833–1840, November 2005.

[7] R. Garello, P. Pierleoni, and S. Benedetto. Computing the free distance of turbo codes and serially concatenated codes with interleavers: Algorithms and applications. *IEEE Journal on Selected Areas in Communications*, 19(5):800–812, May 2001.

[8] J. Hsu and C. Wang. A parallel decoding scheme for turbo codes. In *Proc. of IEEE Int. Symp. on Circuits and Systems (ISCAS'98)*, volume 4, pages 445–448, May/June 1998.

[9] K. Kusume and G. Bauch. A parallel APP decoding algorithm for accelerating decoding throughput of turbo codes. In *Proc. IEEE Int. Symp. on Wireless Communication Systems (ISWCS 2008)*, 2008. submitted.

[10] A. Nimbalker, T. E. Fuja, D. J. Costello Jr., T. K. Blankenship, and B. Classon. Contention-free interleavers. In *Proc. IEEE Int. Symposium on Information Theory (ISIT 2004)*, page 54, June–July 2004.

[11] J. Sun and O. Y. Takeshita. Interleavers for turbo codes using permutation polynomials over integer rings. *IEEE Transactions on Information Theory*, 51(1):101–119, January 2005.

[12] O. Y. Takeshita. A new metric for permutation polynomial interleavers. In *Proc. IEEE International Symposium on Information Theory (ISIT 2006)*, pages 1983–1987, July 2006.

[13] O. Y. Takeshita. On maximum contention-free interleavers and permutation polynomials over integer rings. *IEEE Transactions on Information Theory*, 52(3):1249–1253, March 2006.

[14] A. Tarable, S. Benedetto, and G. Montorsi. Mapping interleaving laws to parallel turbo and LDPC decoder architectures. *IEEE Transactions on Information Theory*, 50(9):2002–2009, September 2004.

[15] S. Yoon and Y. Bar-Ness. A parallel map algorithm for low latency turbo decoding. *IEEE Communications Letters*, 6(7):288–290, July 2002.