International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152
Volume No.-6, Issue No.-6, November, 2018

Selection of parameters of Quadratic Permutation Polynomial Interleavers of Turbo Codes

Simmi Garg
Department of Physics
I K Gujral Punjab Technical University
Kapurthala, India
E-mail: simmigarg89@gmail.com

Anuj Kumar Sharma
Department of Mathematics
L R DAV College
Jagraon, India
E-mail: anujsumati@gmail.com

Anand Kumar Tyagi
Department of Applied Sciences
S B S State Technical Campus
Ferozepur, India
E-mail: anandktyagi@gmail.com

Abstract: Turbo codes have potential to operate very close to Shannon limit. The performance of the turbo code mainly depends on the encoder, decoder and the choice of the interleaver used. In this paper, spread spectrum property of quadratic permutation polynomial (QPP) interleaver has been studied in terms of cycle correlation sum (CCS). QPP interleavers are classified into sub groups according to the CCS metric. Four interleaver lengths are considered to study the variation of CCS with the parameters of QPP interleavers. On the basis of results obtained, best suited parameters of QPP interleavers are estimated. Results are validated by studying the Bit error rate analysis of Turbo codes. Simulations are performed using MATLAB software.

Keywords: Turbo codes, QPP Interleaver, CCS, 3GPP, BER

I. INTRODUCTION

Turbo codes are a breakthrough in coding schemes [1]. Turbo codes leads to large improvement in the performance of wireless communication system. These codes works exceptionally well for low signal to noise ratio environment. In turbo codes, the data bit is encoded with first recursive systematic convolution encoder [2]. A scrambled version of the data is obtained with the help of an interleaver. Then, the scrambled version is encoded with the help of second recursive systematic convolution encoder [3-4]. Since, two encoded streams are independent of each other. Hence, turbo codes perform exceptionally well.

An interleaver is a major component of turbo codes [5]. There are many types of interleavers suggested by the researchers till date. Random, S-random, row-column, Algebric and Quadratic permutation polynomial (QPP) [6-7] are most popular one. Row-column interleaver is easy to implement but their performance degrades as length of the interleaver is increased. Random interleaver specially, S-random interleaver performs better than row-column interleaver but whole of the scrambled data has to be stored [8]. Algebric interleaver can be implemented on the fly using certain parameters. Moreover, they are easy to implement with the help of an algebraic formula [9-10].

Sun and Takeshita proposed the algebraic approach of using permutation polynomial based interleaver over integer rings [11-12]. QPP interleaver has excellent performance. Another, advantages of QPP interleaver are completely algebraic structure and low memory requirement. A QPP interleaver of length K is defined as

$\pi(x)= (a_0+ax+ bx^2)$ Mod(K) where x ε {0,1,2,3…….K-1} --- (1)

π (x) represents the permutated bit position of the bit with original position x. It is clear that a_0 merely provide a cyclic shift to the permutated data [13]. Since, it does not affect our results to a large extent. So we will consider the case for which $a_0 = 0$.

Hence, equation (1) becomes,

$\pi(x)=(ax+bx^2)$Mod(K)……..(2)

Here, K is the interleaver length, $\pi(x)$ is the permutated position to which bit position x is scrambled and Mod(K) denotes modulo K arithmetic. The parameters ‘a’ and ‘b’ are critical to choose. As these parameters greatly affect the performance of interleaver and hence that of the turbo codes [14]. The parameters ‘a’ and ‘b’ must satisfy the certain rules so that resulting equation is a QPP and mapping is from $Z_K \rightarrow Z_K$. These rules have been explained in section 2 of this paper. It is seen that with right parameters, the performance of QPP interleaver can be improved to a great extent. In this paper, we

will concentrate on QPP interleaver and will find the set of best suited parameters for different interleaver lengths. The paper is organized as follows. Section 2 presents the Quadratic permutation polynomial interleaver. Cycle correlation sum metric has been explained in section 3. Section 4 represents the proposed technique and results are discussed in section 5. Section 6 concludes the paper.

II. QUADRATIC PERMUTATION POLYNOMIAL INTERLEAVER

Quadratic permutation polynomial has been proposed in 3rd Generation Partnership Project (3GPP) [15-17]. QPP interleavers have many advantages over existing interleavers. These interleavers are easy to construct. They have excellent error performance ability and require less memory. Further, they can easily be extended to higher orders of the permutation polynomial [18]. There are 188 interleavers for turbo codes in the 3GPP LTE as follows,

1. $40 \leq K \leq 512$, interleaver set contains all multiples of 8.
2. $512 < K \leq 1024$, interleaver set contains all multiples of 16.
3. $1024 < K \leq 2048$, interleaver set contains all multiples of 32.
4. $2048 < K \leq 6144$, interleaver set contains all multiples of 64.

The permutation rule of QPP interleaver of length 'K' is $\pi(x) = (ax + bx^2) \bmod K$. The allowed values of parameter 'a' and 'b' for a given interleaver length K can be found by the following rules [19]:

Lemma 1: For, K = 2, A polynomial $\pi(x) = (ax + bx^2) \bmod K$ is a permutation polynomial over Z_K, if and only if a + b is odd.

Lemma 2: For K≠2, A polynomial $\pi(x) = (ax + bx^2) \bmod K$ is a permutation polynomial over Z_K if and only if a≠ 0mod K and b = 0 mod K.

Lemma 3: Let K be a prime number and $n \geq 2$. A polynomial $\pi(x) = (ax + bx^2) \bmod (K^n)$ is permutation polynomial over if and only if $a \neq 0 \bmod K$ and $b = 0 \bmod K$.

Corollary: Let K = 2 and $n \geq 2$. A polynomial $\pi(x) = (ax + bx^2) \bmod (K^n)$ is a permutation polynomial if and only if 'a' is odd and 'b' is even.

In general, for any integer N that can be factored as $\prod_{K\in P} K^{n_{N,K}}$, where P is a set of prime numbers, the polynomial $\pi(x) = (ax + bx^2) \bmod N$ is a permutation polynomial if and only if following theorem is satisfied.

Theorem: For any $N = \prod_{K\in P} K^{n_{N,K}}$ where, P is set of prime numbers, $\pi(x)$ is a permutation polynomial modulo N if and only if $\pi(x)$ is also a permutation polynomial modulo $K^{n_{N,K}}$, ∀K such that $n_{N,K} \geq 1$.

Corollary: $\pi(x) = (ax + bx^2) \bmod N$ will be permutation polynomial if

a) If N is divisible by 2 and N is not divisible by 4, a + b is odd, gcd(a, N/2) =1 and $b = \prod_{K\in P} K^{n_{K,N}}$, $n_{f,K} \geq 1$, ∀K s.t. K≠2, $n_{N,K} \geq 1$

b) Either N is not divisible by 2 or N is divisible by 4 gcd(a,N) =1 and $b = \prod_{K\in P} K^{n_{N,K}}$, $n_{f,N} \geq 1$, ∀N , $n_{N,K} \geq 1$

It is clear that for a given interleaver length, there can be large number of allowed (a,b) pairs. The performance of the interleaver and of turbo code depends on these parameters. In this paper, we will find those parameter pair for which the performance of the turbo codes is the best.

III. CYCLE CORRELATION SUM (CCS)

Turbo codes gain popularity when iterative decoders came into existence. In iterative decoding, two decoder works in iterative manner [20]. They share their information with one another to complete iteration and finally decode the received bits. The performance of the iterative decoder will be better when the message from one component does not move back. For this to happen, the outbound message and next inbound message must have minimum correlation [21]. But, in turbo decoder after every iteration, some correlations always got introduced. Lets bits p and q are inserted in first component encoder and their interleaved position as $\pi(p)$ and $\pi(q)$ are inserted in second encoder. p and q are related to each other. By the decoder, bit q is related to $\pi(q)$. After the second component decoder, $\pi(q)$ gets linked with $\pi(p)$, which after de interleaving, get linked with p. So, the cycle of relation becomes $p \rightarrow q \rightarrow \pi(q) \rightarrow \pi(p) \rightarrow p$.

For a given interleaver, such correlations should be minimal.

CCS metric accounts for such uncorrelated messages at each decoding iteration. Lesser the CCS value, lesser will be the uncorrelated message and hence better will be the performance of the turbo code. CCS accounts for standard correlations coefficients [22]. These correlation coefficients are used to measure the correlation between input and output extrinsic information of the decoder. It is shown in that these correlation coefficients are function of Hamming distance between two bits. The correlation between bits p and q is given as $e^{-a|p-q|}$ where 'a' is a parameter, roughly equal to length of the component encoder [23, 24]. Similarly, the correlation between $\pi(p)$ and $\pi(q)$ is given by $e^{-a|\pi(p)-\pi(q)|}$. The CCS metric is defined to be

CCS= $\sum_{p,q \in C} e^{-a(|p-q|+\pi(p)-\pi(q)|)}$

Where, C= (0, 1, 2, 3…….K-1), K is the interleaver length.

In this paper, we will study QPP interleavers in terms of CCS metric. Our aim is to find the parameters that will improve the performance of the system significantly.

IV. PROPOSED TECHNIQUE

As already mentioned, interleavers play important role in the performance of the turbo codes. The main function of the interleaver is to split the burst errors. As we know, interleavers scramble the communicated bits. Hence, in case, a complete frame is in error, the interleaver spread the corrupted bits into different frames. Hence, the error correction can perform well. So, the function of the interleaver is very crucial.

A good interleaver should have a large minimum spread. In general, an interleaver is said to have minimum spread 'x' if any two bits which are at a distance less than 'x' before interleaving, are at least 'x' distance apart after interleaving. A good interleaver should have large spread between the bits i.e. an interleaver that can separate the bits to a large distance will perform well. Recently, the spread between two bits 'p' and 'q', whose permuted positions are π(p) and π(q) respectively, is given by $S_{p,q}$ = | p-q | + | π(p) – π(q) |.

Till date, many researchers has worked to study the spread of QPP interleavers in terms of $S_{p,q}$ but to the best of our knowledge, study of spread property of QPP interleavers in terms of CCS is not found in the literature. This paper is an attempt to fill this gap and to study the QPP interleavers in terms of CCS metric. QPP interleavers of length of powers of 2 have been studied. Further, we will found the parameters that lead to better performance for QPP interleavers and turbo codes. Results are validated with the help of MATLAB simulations.

V. RESULT AND DISCUSSION

In this section, CCS evaluations of QPP interleavers and their results are presented. Figure 1-4 denotes the CCS variation with the parameter 'b' of the QPP interleaver. The simulations are performed for 'a'= 1, 3, 5…….33. QPP interleavers of length equals to128, 256, 512 and 1024 are considered. It is found from the results that QPP interleavers can be classified into four sub groups. Different sub groups are shown with different line colors and type in the figures. The conclusions drawn from the simulations are as follows:

a) For b= 4n+2, where n=0,1,2,……,

The CCS values are same irrespective of the value of parameter 'a'. Hence, there are some values of parameter 'b' at which the value of 'a' is of no significance. Performance of the system will remain same.

b) The second category consists of those interleavers for which the value of parameter 'a' equals 3,5,11,13,19,21,27,29. Their variation of CCS at all the values of 'b' (except at b= 16n) are same. This category can be subdivided into two parts.

i) One part consists of those having value of 'a' equals to 3,11,19,27. The general rule for a in this sub class is a= 8n+3, where n=0,1,2,3,….

ii) The second part consists of those interleavers having parameter 'a' equals to 5,13,21,29. The general rule of a in this sub class is a= 8n+5, where n= {0, 1, 2, 3,…..}.

So, our second category consists of those interleaver for which values of 'a' equals either 8n+3 or 8n+5. For all these 'a' the CCS variations remains same.

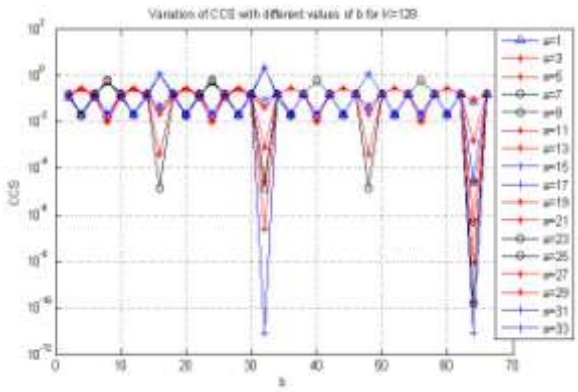

Figure 1. Variation of CCS with parameter 'b' for interleaver length of 128

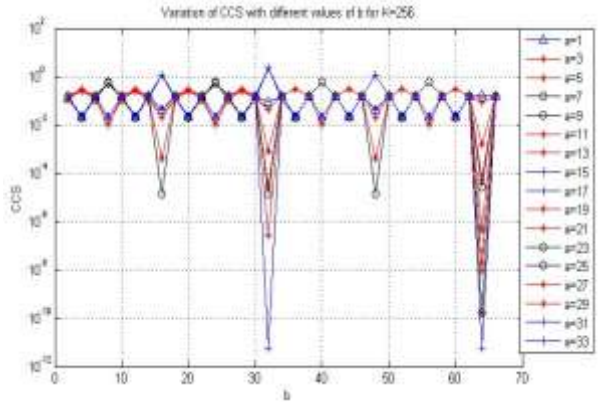

Figure 2. Variation of CCS with parameter 'b' for interleaver length of 256

c) The third category contains those interleavers having parameter 'a' equals to 7,9, 23and 25. Here, again the variation of CCS with values of parameter 'b' remains same (except for b equal to 16n). We can sub divide this category into two parts.

i) The first part consists of those interleavers with 'a' equals to 7, 23….. The rule that parameter 'a' follows in this sub class is a= 16n+7, where n=0, 1, 2, 3,…

ii) The second part consists of interleavers with 'a' equals to 9,25…. The rule that parameter 'a' follows in this sub class is a= 16n+9, where n=0,1, 2, 3…

d) The fourth and the last category consist of interleavers with values of 'a' equals to 15, 17, 31, 33… Here again the variation of CCS with that of 'b' remains same (except at b= 16n). here, again we can divide this category into two sub parts

i) First part consists of those interleavers with parameter 'a' equals to 15, 31.. the general rule for parameter 'a' in this category is 16n +15.

ii) Second part has those interleavers with parameter 'a' equals to 17, 33…. The value of 'a' in this category can be generalized to 16n+17.

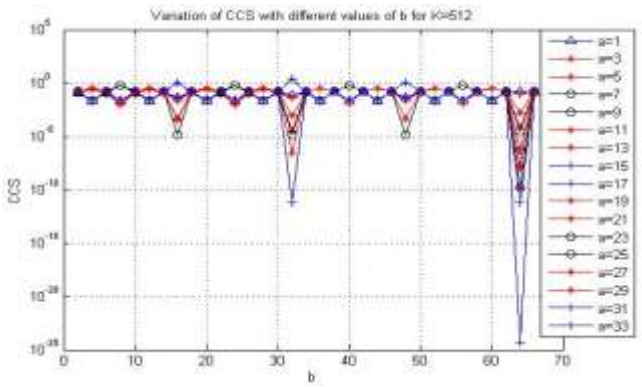

Figure 3. Variation of CCS with parameter 'b' for interleaver length of 512

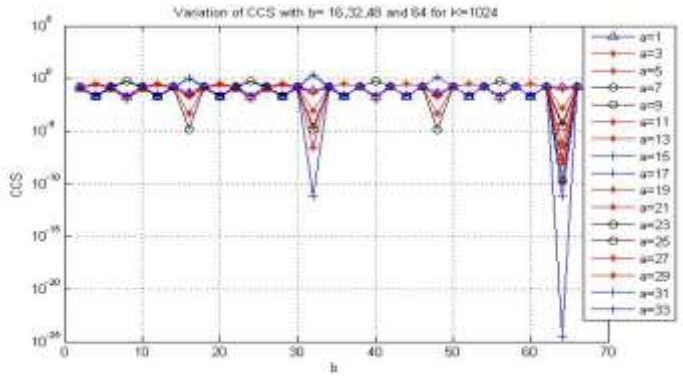

Figure 4. Variation of CCS with parameter 'b' for interleaver length of 1024

It must be mentioned here that, we have done the simulation for parameter 'a' equals to 1, 3, 5….33 only. But the categories formed are applicable for higher values of parameter 'a' as well. From the figures, it is clear that the variation of the interleavers falling in different categories is different at different values of 'b'. For example, in figure 3, at b= 20, the CCS values of category second is more than that of category third while at b=40, the behavior is exactly opposite.

From the figures 1-4, it can be concluded that CCS value remain below the 10^{-2} for all values of parameter 'b' (except b= 16n) regardless of the value of parameter 'a'. For b= 16n, the behavior of CCS is quite different. CCS values drop sharply for b= 16n for all the interleaver length considered. To find the pair of parameters 'a' and 'b' for which CCS is minimum, we will consider these values of 'b' separately. Figure 5 represents the behavior of CCS at b= 16, 32, 48 and 64 for K=128. It is clear from the graph that behavior of CCS for a=15 and 17 is same. Moreover, for a=15 or 17 and b= 32 or 64, CCS achieve its minimum values. Hence, for K=128, the best (a, b) parameters are (15, 32), (15, 64), (17, 32) and (17, 64). The second best choice is either (25, 64) or (11, 64).

For K= 256, there is slight variation in the results. Here, the best choice of parameters are (15, 32), (15,64), (17,32), (17,64) along with (31,64) and (33,64). The CCS values are minimum for all theses pairs.

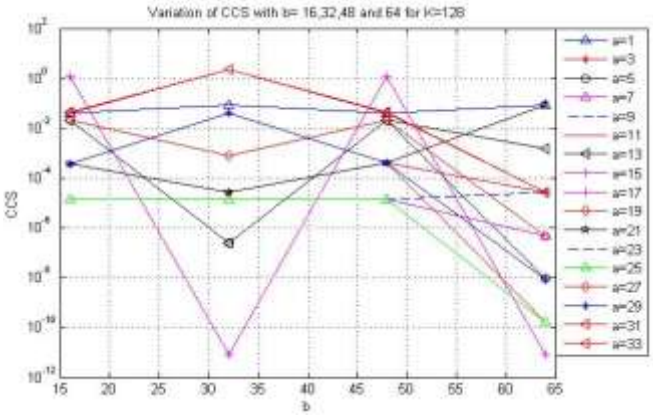

Figure 5. Variation of CCS with b= 16, 32, 48 and 64 for interleaver length of 128

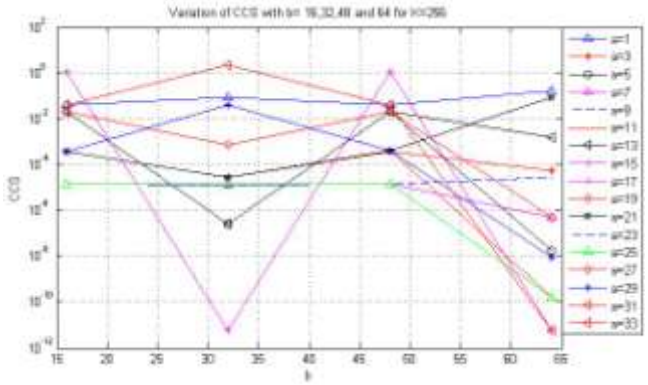

Figure 6. Variation of CCS with b= 16, 32, 48 and 64 for interleaver length of 256

For K=512, the results differs to a large extent. The CCS values are exceptionally small for b= 64 and a= 31 or 33. So, the best choice of the parameters is (31, 64) or (33, 64). For b=32, the metric attain minimum value for a= 15 or 17. So the second best choice for K=512 case, is (15, 32), (15, 64), (17, 32) or (17, 64). Similar results have been found for K=1024 case.

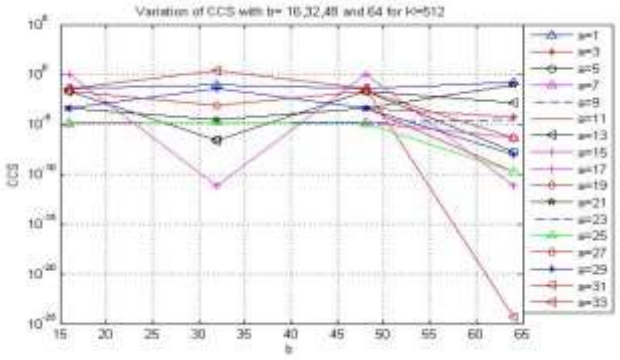

Figure 7. Variation of CCS with b= 16, 32, 48 and 64 for interleaver length of 512

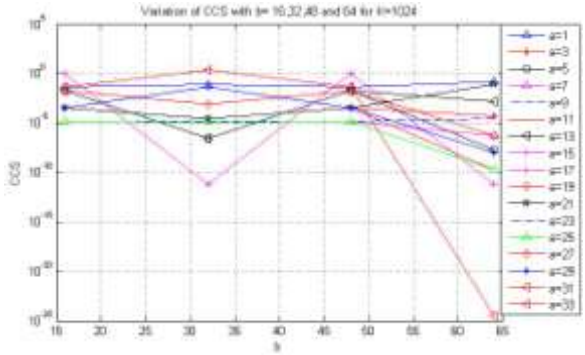

Figure 8. Variation of CCS with b= 16, 32, 48 and 64 for interleaver length of 1024

To validate the results obtained from CCS metric, the BER performance of Turbo codes with QPP interleavers is studied. QPP interleavers of length 128, 256, 512 and 1024 has been considered for simulations. One pair of parameters from each sub group formed above has been selected to compare the results. Figure 9 represents the performance of the Turbo code with QPP interleaver of length 128. At Eb/No = 1.6 dB, the BER for (a, b) equals to (15, 32), (15, 52), (19, 44) and (23, 56) is 0.0003, 0.0005, 0.0015 and 0.0025 respectively. Hence, the best choice of parameter (a, b) for interleaver length of 128 is (15, 32). Same parameters were predicted on the basis of CCS metric. Similar results are obtained for interleaver length of 256 in figure 10.

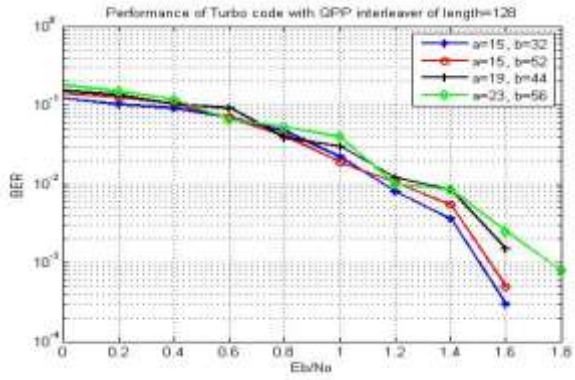

Figure 9. Performance of Turbo code with QPP interleaver of length 128

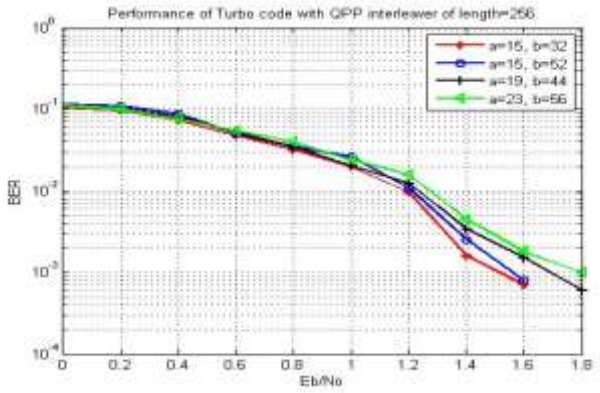

Figure 10. Performance of Turbo code with QPP interleaver of length 256

Figure 11 represents the performance of Turbo codes with QPP interleaver of length 512. The pair of parameters chosen for comparison is (31, 64), (15, 32), (19, 44) and (23, 56). These pairs are chosen because they belong to different sub groups. At Eb/No= 1.6 dB, the BER values for (31, 64), (15, 32), (19, 44) and (23, 56) is 0.0006, 0.0014, 0.0018 and 0.0037 respectively. Hence, the best choice of the parameters (a, b) is (31, 64). Here, again same results are obtained as predicted by CCS metric. Figure 12 denotes the performance of turbo codes with interleaver length of 1024. Here, the best parameter is found to be (31, 64), in well accordance with CCS metric prediction.

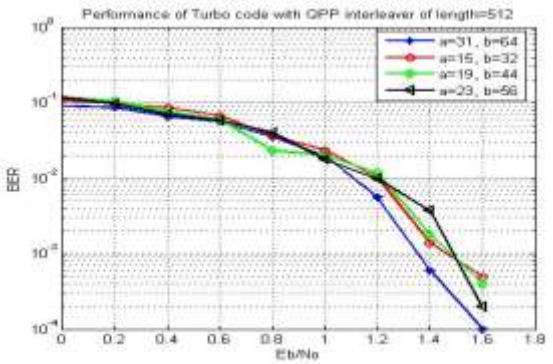

Figure 11. Performance of Turbo code with QPP interleaver of length 512

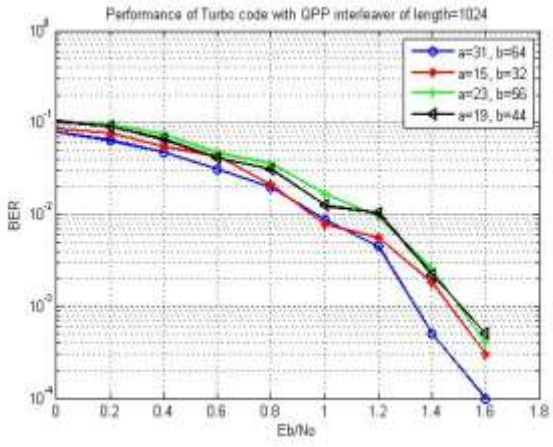

Figure 12. Performance of Turbo code with QPP interleaver of length 1024

Table 1. Relation between CCS and BER

K	A	b	CCS	BER
1024	31	64	3.1924e-25	0.0045
	15	32	6.4115e-12	0.0056
	23	56	0.2932	0.0096
	19	44	0.5863	0.0104

From the Table 1, it can be concluded that the metric CCS has a close relation with BER performance of Turbo codes. The lower value of CCS represents less uncorrelated messages from one component decoder to other. Lesser the uncorrelated messages better the performance of the interleaver as well as of the turbo codes. Hence, CCS can be considered to account for the performance of the turbo codes and to find the suitable parameters.

VI. CONCLUSION

In this paper, the minimum spread of the QPP interleavers are studied. Cycle Correlation Sum (CCS) is used as the measuring metric. The interleavers whose length are powers of 2 are considered. On the basis of CCS metric, the interleavers are divided into four sub groups. It is found that the performance of the interleavers falling in the same sub group is alike. The best suited parameters are found for interleaver lengths of 128, 256, 512 and 1024. Further, to verify the parameters selected, MATLAB simulations are performed. Turbo codes with QPP interleaver of length 128, 256, 512 and 1024 and different parameter pairs are simulated. Simulations have shown that the interleavers with proposed parameters performs better than the rest others.

ACKNOWLEDGEMENT

Authors are thankful to anonymous reviewers for their careful reading and useful comments for the improvement of the present reserch work. Also, authors gratefully acknowledge the support provided by the I K Gujral Punjab Technical University, Kapurthala, Punjab, India.

REFERENCES

1. Heegard C and Wicker S B, “Turbo Coding”, Kluwer Academic Publishers Norwell, MA, USA, 1999.
2. Berrou C, Glavieux A and Thitimajshima P, “Near Shannon limit error correcting coding and decoding: Turbo codes”, In: Proc. Of IEEE International Conference on Communications, Geneva, Switzerland, May, 2003.
3. Hokfelt J, “On the design of turbo codes”, Ph.D. dissertation, Lund University, Lund, Sweden, 2000.
4. Vafi S and Wysocki T, “Weight distribution of turbo codes with Convolutional interleavers”, IET Communications, Vol.1, No.1, pp. 71-78, 2007.
5. Sadjadpour H R, Sloane N J A, Salehi M, Nebe G, “Interleaver design for turbo codes”, IEEE J. Sel. Areas Commun, Vol. 19, No.5, pp. 831-837, 2001
6. Chi C L, “Quadratic Permutation Polynomial Interleavers for LTE Turbo Coding”, Int. J Future Comp. Comm., Vol. 2, No.4, 2013
7. Kim B, Yoo I, Park I, “Low complexity parallel QPP interleaver based on Permutation patterns”, IEEE Trans. Circuits Syst. II, Express Briefs, Vol. 60, No. 3, pp. 162-166, 2013
8. Omeira M S, Hamad G M, Elbayoumy A D, “A code-matched collision free S-random interleaver for turbo codes”, In: Proc. of IEEE seventh international conference on intelligent computing and information systems, Cairo, Egypt, December 2015
9. Zhao H, Fan P and Tarokh V, “On the equivalence of interleavers for turbo codes using quadratic permutation polynomials over integer rings”, IEEE Commun. Lett. ,Vol. 14, No.3, pp.236-238, 2010
10. Bohorquez R G, Nour C A and Douillard C, “On the equivalence of interleavers for turbo codes”, IEEE Wireless Commun. Lett., Vol. 4, No. 1, pp. 58-61, 2015
11. Sun J and Takeshita O Y, “Interleavers for Turbo Codes Using Permutation Polynomials over Integer Rings”, IEEE Trans. Inf. Theory, Vol. 51, No.1, pp. 101-119, 2005
12. Takeshita O Y, “Permutation polynomial interleavers: An algebraic- geometric perspective”, IEEE Trans. Inf. Theory, Vol. 53, No. 6, pp. 2116-2132, 2007.
13. Takeshita O Y, “On Maximum Contention-Free Interleavers and Permutation Polynomials over Integer Rings”, IEEE Trans. Inf. Theory, Vol. 52, No. 3, pp. 1249-1253, 2006
14. Cojocariu E, Trifina L, Lazar A G, “Selection of component codes for asymmetric turbo codes matched to QPP interleaver”, In: Proc. Of 8th International conference on Communications, Bucharest, Romania: 203-206, 2010
15. Xie K, Tan P, Li J, and Wang W, “Interleaver design for short-length turbo codes”, In: Proc. of 39th Conference on Information Sciences and Systems, Baltimore, Maryland, March,2005
16. 3rd generation partnership project; technical specification group radio access networks; evolved universal terrestrial radio access (E-UTRA); multiplexing and channel coding (Release 8) 3GPP TS 36.212 V8.5.0, Dec 2008.
17. Sun Y, Cavallaro J R, “Efficient hardware implementation of a highly-parallel 3GPP LTE/LTE-advance turbo decoder”, Integrat. VLSI J., Vol. 44, No. 4, pp. 305-315, 2011
18. Zarrinkoub H, “Understanding LTE with MATLAB from mathematical modeling to simulation and prototyping”, John Wiley & Sons Ltd, United Kingdom, 2014

19. Jong Hoon Ryu, "Permutation polynomial based interleavers for turbo codes over integer rings: theory and applications", Ph.D Thesis, Ohio State University, Columbus, 2007
20. Langton C, "Turbo coding and MAP decoding", Intuitive guide to principles of communications http://www.complextoreal.com/chapters/turbo1.pdf
21. Xie K, Wang W and Li J, "On the analysis and design of good algebraic interleavers", In: Proc. of 4th International Symposium on Turbo Codes and Related Topics, Munich, Germany April, 2006
22. Xie K, "Advanced digital and analog error correction codes", Ph.D Thesis, Lehigh University, Bethlehem, Pennsylvania, 2011
23. Takeshita O Y and Costello D J, "New deterministic interleaver designs for turbo codes", IEEE Trans. Inf. Theory, Vol. 46, No. 6, 1988-2006, 2000
24. Rosnes E, "On the minimum distance of Turbo codes with quadratic permutation polynomial interleavers", IEEE Trans. Inf. Theory, Vol. 58, No. 7, pp. 4781-4795, 2012

Author's Biographies

Simmi Garg is a research scholar in I K Gujral Punjab Technical University, Kapurthala, Punjab, India. Her area of interest is Wireless Communications and Digital Signal Processing.

Anuj Kumar Sharma is Associate Professor in L R DAV college, Jagraon, Punjab, India. He has published several research papers in various International and National Journals. His area of research is mathematical modeling in ecology. His current area of research is signal processing and Wireless Communications.

Anand Kumar Tyagi is Professor in S B S State Technical Campus, Ferozepur, Punjab, India. He has published around 138 research papers in international, national journals and conference proceedings. He has also published 3 books.