On the Optimization of Number of Sub-interleavers for Turbo Codes

SIMMI GARG Department of Physics I K G Punjab Technical University Kapurthala-Jalandhar Highway, Kapurthala INDIA simmigarg89@gmail.com ANUJ KUMAR SHARMA Department of Mathematics L R DAV College Jagraon, Punjab INDIA anujsumati@gmail.com ANAND KUMAR TYAGI Department of Applied Physics S B S State Technical Campus Ferozepur, Punjab INDIA anandktyagi@gmail.com

Abstract: - Performance of the turbo codes mainly depends on the interleaver used. Recently, it is found that sub interleavers reduce the time complexity of the system to a large extent. This paper is an attempt to optimize the number of sub interleavers used for turbo codes. We have proposed a scheme that can optimize the number of sub interleavers. First of all, mathematical formulae have been derived for finding the possible number of sub interleavers for a given interleaver length. Secondly, a mathematical formula has been derived for choosing the best number of sub interleaver among all the possible sub interleavers. Results have been validated by considering sub interleaver composed of row-column and diagonal interleaver of length 1024.

Key-Words: - Turbo codes, Sub-interleaver, Time complexity, Row-Column interleaver, Diagonal Interleaver

1 Introduction

Several space missions have been set up to explore the universe and its origin. The information collected by theses space crafts is then transferred to earth. For a successful space mission, a number of information is send from earth to these space crafts. Also, the position of the space craft has to be traced at each and every second. So, there should be reliable communication with the space crafts. There are several factors that affect this communication and these factors must be taken into account. The biggest problem with such communications is the very large distance between the sender and receiver. This distance will lead to delay in communication. Errors are introduced during the transmission of the information from sender to receiver in the communication channel. A number of error controlling methods have been developed in the last few decades to combat these difficulties. Forward error correction (FEC) codes are found to be best among all [1]. In FEC, parity bits are sent along with the information bits. The parity bits help to detect the error in the received data and to possibly correct the corrupted data bits.

The most efficient code developed till date is Turbo codes [2]. Turbo codes are realized by using two recursive systematic convolution (RSC) codes with an interleaver. The interleaver is a critical component of turbo codes [3]. The error correction capacity of Turbo codes depends on the type of interleaver used. The function of an interleaver is to scramble the information bits. Two RSC works on same information bits but the ordering of the information bits is scrambled by the interleaver for one RSC. There are various interleavers designed so far. Algebric interleaver, Quadratic Permutation Polynomial interleaver based [4.5]. Block interleavers, Random interleaver [6] are mostly used for communication systems. The main function of using interleaver is to provide randomness to the input sequence and increase the weight of the code words [7]. Good interleaver leads to lower error floor. When turbo codes are used without an interleaver, the performance of the system degrades to a large extent. Hence, interleaver is vital part of the turbo codes [8]. But the disadvantage of using an interleaver is the time required for interleaving and de-interleaving. For a block interleaver with M rows and N column the time required for interleaving and de-interleaving is 2MN-2M+2 [9]. Due to this the overall timing and complexity of the system increases. It is advisable to reduce the timing and complexity of interleaving and de-interleaving. For

fast communication system, [10] proposed the concept of sub interleaver. In the proposed scheme, the whole length of the interleaver was divided into four parts. Each sub part is interleaved individually. The interleaved sub parts are scrambled as a whole among them. Hence, the overall interleaving is a two step phenomena. It was shown in that sub interleavers lead to large decrease in the timing and complexity, so the system response time decreases and communication becomes fast. There can be infinite number of sub interleavers possible and it is impossible to test each sub interleaver and compare them so as to find a suitable number of sub interleavers. Our paper is an attempt to focus on this crucial issue. In this paper, we have proposed a scheme to optimize the number of sub interleavers. From the propose scheme, the number of possible sub interleavers reduce to a large extent. And it can be very easily between the choices how many sub interleavers are possible for a particular interleaver length.

2. Matrix Interleaver

Matrix interleaver is the most commonly used interleaver in communication system. In this interleaver, the input data bits are written in rows of a matrix and bits are read column wise [11]. In matrix interleavers, data is represented by a matrix of dimensions $M \times N$. Matrix interleaver exists in four types.

- i) Columns are read left to right and rows are read top to bottom.
- ii) Columns are read left to right and rows are read bottom to top.
- iii) Columns are read right to left and rows are read top to bottom.
- iv) Columns are read right to left and rows are read bottom to top.

For example, if information bits are of the form [A B C D E F G H I J K L M N O P], they can be represented by 4×4 matrix [12,13]. As the data is filled row wise, the matrix will be of form

ΓA	В	С	D]
E	F	G	H
Ι	J	К	L
Μ	Ν	0	P

When columns are read left to right and rows are read from top to bottom, the interleaved bits will be given by a). Similarly, the outputs of (ii), (iii) and (iv) cases discussed above will be given by b), c) and d) below respectively.

- a) [AEIMBFJNCGKODHLP]
- b) [MIEANJFBOKGCPLHD]
- c) [DHLPCGKOBFJNAEIM]
- d) [PLHDOKGCNJFBMIEA]

De-interleaver performs the inverse operation of the interleaver. In the de-interleaver the information is written column wise in $M \times N$ matrix and are read row wise.

3. Sub- Interleaver

Sub-interleaver is a two stage interleaving scheme. In the first stage, the input bit stream is divided into number of sub parts. Bits in each sub parts are interleaved using standard interleaver. Interleaving of the bits in different sub parts can be done with same or different types of interleavers. Generally, half of sub parts are interleaved using one type of interleaver and another half by another type of interleaver. It is clear that by this type of interleaving the spread between the bits is limited to the length of the sub part only. So, to improve the spread between the information bits, the sub parts themselves are shuffled using a pre defined order. It is seen that sub interleavers lead to decreases in the time complexity and hence, are most suitable for the fast communication systems [14].

Suppose the information bits are arranged in M×N array. As bits cannot override, at the interleaving stage, total memory requirement is of 2MN bits. Same memory is required at the time of deinterleaving also. So, the total memory requirement for interleaving and de-interleaving is of 4MN. The time complexity for a block interleaver is found to be 2MN-2M+2. Suppose the information bit stream is divided into 4 parts. Each sub part will have MN/4 bits that can further be arranged into M/2 \times N/2 array. Time complexity for sub-interleaver will be 4(2 MN/4 - 2M/2+2). It is clear that time required for sub-interleaver is less than that of block interleaver. Hence, we can conclude that subinterleaver reduce the time complexity and make the communication fast.

4. Proposed Scheme

Interleaver plays very important role in Turbo codes. As discussed in [10], the time complexity of the system can be reduced with the help of sub interleavers. Now, the question arises, how many sub interleavers should be considered. [15] has tried to find the suitable number of sub-interleavers by simulating the system with different number of subinterleavers. As there can be large number of subinterleavers possible. But, this is not possible to test each and find the best among them. This will take much time and hence, not feasible practically. We have constructed rules that must be satisfied by the possible sub interleaver.

4.1 Possible sub-interleavers for a given interleaver length

In this section, we will develop a scheme for finding the sub-interleavers possible for a given interleaver length. Suppose total interleaver length is of MN bits, where M is the number of rows and N is the number of columns of the matrix representing the information bits.

Total number of bits to be interleaved = MN

Suppose there are x sub-interleavers.

Number of bits in each sub- interleaver $= \frac{MN}{x} = A_1$ A₂

A large number of combinations are possible for A₁ and A₂. In this paper, we will consider the case for which $A_1 = \frac{M}{\sqrt{x}}$ and $A_2 = \frac{N}{\sqrt{x}}$. As, A₁ and A₂ must be a positive integer, so *x* must be a perfect square. Also, M and N must be divisible by \sqrt{x} .

Total time taken by x sub interleavers for interleaving and de-interleaving = $x\left(\frac{2MN}{x} - 2A_1 + 2\right)$

As negative time has no significance, so the time taken by sub interleaver must be positive. Also, our prime motive is to reduce the time taken for interleaving and de interleaving. Hence, the time taken by sub interleaver should be less than that of block interleaver.

$$0 < x \left(\frac{2MN}{x} - 2A_1 + 2\right) \le 2MN - 2M + 2$$

Using $A_1 = \frac{M}{\sqrt{x}}$,

$$0 < x \left(\frac{2MN}{x} - 2\frac{M}{\sqrt{x}} + 2\right) \le 2MN - 2M + 2$$
$$0 < 2MN - 2M\sqrt{x} + 2x \le 2MN - 2M + 2$$
$$-2MN < -2M\sqrt{x} + 2x \le -2M + 2$$

$$-MN < x - \sqrt{x} M \le 1 - M \dots (1)$$

Considering the first inequality,

$$-MN < x - \sqrt{x} M$$
$$x - \sqrt{x} M + MN > 0.....(2)$$

Considering the corresponding equation and solving for x in the equation, we will get

$$x - \sqrt{x} M + MN = 0$$
.....(3)
$$x = \left(\frac{M \pm \sqrt{M^2 - 4MN}}{2}\right)^2$$
....(4)

The solution for x depends on the values of M^2 and 4MN. M^2 can be greater, equal or less than 4MN. Now, we will consider all the three sub cases in detail.

Sub case-I $M^2 < 4MN$

For finding the solution for x in this case, we will proceed with equation 2. Equation 2 can be rewritten in the following form.

As square is always a positive quantity and second term is also positive. So, Equation (5) will always hold irrespective of the value of x. Hence, in this case, interleaver can be sub divided into any number of sub interleavers.

Now, we will discuss the second sub case when $M^2 = 4MN$. Here, again we will consider inequality (2). Substituting the value of MN in inequality (2), we will have

$$x - \sqrt{x} M + \frac{M^2}{4} > 0$$
$$\left(\sqrt{x} - \frac{M}{2}\right)^2 > 0$$

Again, this will hold for any value of x. Hence, any number of sub interleavers can be formed from the given interleaver.

Now consider the third sub case, when $M^2 > 4MN$. In this sub case, equation (5) will not always true for all the values of x. Hence, there are certain sub interleavers which are not allowed in this case. In order to find the allowed values of x, we will consider the solution of equation (3) that are given by equation (4) as follows.

$$x = \left(\frac{M \pm \sqrt{M^2 - 4MN}}{2}\right)^2$$

Let the two roots be denoted by α and β

Where, $\alpha = \left(\frac{M - \sqrt{M^2 - 4MN}}{2}\right)^2$ and $\beta = \left(\frac{M + \sqrt{M^2 - 4MN}}{2}\right)^2$

Hence, solution of inequality (2) is

$$x \in (-\infty \ to \ \alpha) \ \cup \ (\beta \ to \ \infty)$$

Now, we will find the solution for the second part (inequality) of equation (1).

$$-2M\sqrt{x} + 2x \le -2M + 2$$

$$-2M\sqrt{x} + 2x + 2M - 2 \le 0$$

$$x - M\sqrt{x} + M - 1 \le 0$$
(6)

In order to find the solution of inequality in equation (6), consider the corresponding quadratic equation as follows.

$$x - M\sqrt{x} + M - 1 = 0$$

For finding the roots of this equation, we will substitute $\sqrt{x} = y$. The equation will become

$$y^2 - My + M - 1 = 0$$

The roots this equation can be easily found by quadratic formula and the roots will be M-1 and 1.

Hence,
$$\sqrt{x} = M-1, 1$$

Or we can say, $x = (M-1)^2$, 1

Suppose the two roots are represented by γ and δ . where $\gamma = 1$ and $\delta = (M-1)^2$. From simple mathematics, we know that the solution of corresponding inequality (6) will be

 $x \in (\gamma to \delta)$

Complete solution of equation (1) is given by the intersection of the solutions of part 1 and 2. So, we can optimize the number of sub interleavers with the help of the above scheme. There can be large number of sub interleavers possible. With the help of above proposed scheme, the search for sub interleavers can be limited.

4.2 Value of *x* for minimum value of t

Certain communication systems demands very fast communication between sender and receiver. Sub interleavers are known for reducing the time of interleaving and de-interleaving. As explained in section [4.1], with the help of proposed scheme the possible sub interleavers become very limited for a given interleaver length. Now, our next aim is to choose the best among all the possible sub interleavers. In this section we will concentrate on this aim. As we know, the time for interleaving and de-interleaving of the bits is given by

$$t = 2MN - 2\sqrt{x}M + 2x$$

To find the point of maxima or minima, we will substitute $\frac{dt}{dx} = 0$, considering number of rows in the interleaver matrix (M) to be a constant. For a given interleaver length and given value of M,

$$-2 \times \frac{M}{2\sqrt{x}} + 2 = 0$$

Which on solving for x, gives $x = \frac{M^2}{4}$. Next, we will check whether, this is the point of maxima or minima by using second derivative test.

Second derivative of 't' will be given by

$$S = \frac{d^2t}{dx^2} = \frac{M}{2x^{\frac{3}{2}}} + 2$$

At $x = \frac{M^2}{4}$, $S = \frac{4}{M^2} + 2 > 0$. By second derivative test, it is clear that $x = \frac{M^2}{4}$ is the point of minima. Hence, the interleaver should be divided into $\frac{M^2}{4}$ sub interleavers. So as to have minimum value of time required for interleaving and de-interleaving. Now, we will find the minimum value of time required for interleaving and de-interleaving.

t=
$$2MN - 2\sqrt{x} M + 2x$$

at $x = \frac{M^2}{4}$, t= t_{min}
t_{min} = $2MN - 2\sqrt{\frac{M^2}{4}} M + 2\frac{M^2}{4} = 2MN - 2MN$

It should be mentioned here that as $\frac{M}{\sqrt{x}}$ and $\frac{N}{\sqrt{x}}$ should be a positive integer. At $x = \frac{M^2}{4}, \frac{N}{\sqrt{x}}$ will be

 $\frac{M^2}{2}$

equal to $\frac{2N}{M}$. For $\frac{N}{\sqrt{x}}$ to be an integer, 2N should be divisible by M. So, it is should be keep in mind

that above formula is valid only when 2N is divisible by M.

5. Results and Discussions

In this section, the proposed schemes are validated. The interleaver of length 1024 has been considered for discussion. All possible combinations of number of rows and columns for interleaver length of 1024 are discussed. Suppose x be the number of sub-interleavers. We will consider all the three cases discussed in section [4.1].

Firstly, consider the case when $M^2 < 4MN$. M = 32 and N = 32 belong to this class. As discussed in section 4.1, solution of the first part of inequality is $x \in \mathbb{R}$ and according to the solution of the second part, x will vary from 1 to $(M-1)^2$. For our present case, x will vary from 1 to $(31)^2$. So, as shown in (e) part of figure 1 the common solution of x for both parts of the inequality will vary from 1 to 961. As x should be a perfect square, so allowed values of x are 1^2 , 2^2, $(31)^2$. Also, M and N should be divisible by \sqrt{x} . So, the finally allowed values of

x are 1,4,16,64 and 256. This shows the usefulness of the proposed scheme. The possible sub interleavers have reduced to five only. This will make our task of selecting sub interleaver very straightforward. It is clear that when x = 1, sub interleaver is same as block interleaver. From the table 2 it is apparent that more the number of sub interleavers, lesser will be the time required for interleaving and de interleaving. So, for the fast communication, the interleaver should be sub divided into large number of sub interleavers. Also, as explained in section 4.2 for a particular M (number of rows of the interleaver), the best value of $x = \frac{M^2}{4}$. In our case, $x = \frac{32 \times 32}{4} = 256$. This result is in agreement with that expected from theoretical calculations.

Consider the second case, when $M^2 > 4MN$. M = 512, N = 2 will belong to this category. As explained in section 4.1, the roots of equation of first part are given by

$$\alpha = \left(\frac{M - \sqrt{M^2 - 4MN}}{2}\right)^2$$
 and $\beta = \left(\frac{M + \sqrt{M^2 - 4MN}}{2}\right)^2$

On solving for the considered values of M and N, we will get $\alpha = 4.031$ and $\beta = 260089.8001$. The solution of the first inequality of the equation (1) by be given $(-\infty to 4.031)$ U will $(260089.8001 to \infty)$. Also, according to the solution of second part x will vary from 1 to $(M-1)^2$. For our case, x will vary from 1 to $(511)^2$. The common solution of both the parts can be found using number line. As shown in part (i) of figure 1, the allowed values of x varies from (1 to 4.031) U (260089.8001 to 261121). As x should be a perfect square and M and N should be divisible by \sqrt{x} . From these conditions, the allowed values of x can be 1 and 4. For x = 1, the sub-interleaver behaves same as block interleaver. Hence, there performance in terms of timing complexity remains same. For the present case, the only possible value of x is 4. Hence, the interleaver can be sub-divided into 4 sub-interleavers only. It is obvious that the best timing performance will be for x = 4 only. This shows the utility of the proposed scheme. Because of the proposed scheme, we do not have to simulate all the sub-interleavers. This will save much of our time and calculations complexity will reduce to a great extent.



Fig. 1 Number line depicting the possible values of x for interleaver length of 1024 with number of rows (M) and number of columns (N) as (a) 2 and 512 (b) 4 and 256 (c) 8 and 128 (d) 16 and 64 (e) 32 and 32 (f) 64 and 16 (g) 128 and 8 (h) 256 and 4 (i) 512 and 2

Sub Case –III $M^2 = 4MN$

M= 64 and N= 16 belongs to this group. As discussed in section 4.1, for this case the solution of first part of equation (1) is the set of all real integers and the solution of the second part of equation (1) varies from 1 to $(M-1)^2$ i.e. from 1 to $(63)^2$. As explained in the (f) part of the figure 1, the common solution for both the parts varies from 1 to 3969. But as per the conditions that M and N must be divisible by \sqrt{x} and x be a perfect square, the only allowed values for x are 1, 4, 16, 64 and 256. Hence, there can be five sub interleavers possible for the present case. As we know x = 1, case lead to same results as that of a block interleaver. So, we have liberty to choose among the rest four sub interleavers. Now, to choose the best among the

allowed four, we will consider the mathematical formula derived in section 4.2. The best value of xis given by $\frac{M^2}{4}$ i.e. $x = \frac{64 \times 64}{4} = 256$. This can be observed in the table 2 that for the present case, the time of interleaving and de-interleaving is minimum for x = 256. Hence, the proposed scheme leads to expected results. We have study all the possible combination of number of rows and columns for an interleaver length of 1024. The solutions of the equations can be found using number line. Figure 1 depicts the number line for all the possible solutions of equation (1) for all the cases possible. We have find all the possible sub interleavers for all the combinations of M and N for an interleaver length of 1024 and tabulated them in table 1. As x = 1, behaves simply as a block interleaver, hence not written in the table 1.

Table 1 Possible sub interleavers for an interleaverlength of 1024

Number of Rows (M)	Number of Columns (N)	Possible Sub- interleavers (x)
2	512	-
4	256	4
8	128	4,16
16	64	4,16,64
32	32	4,16,64,256
64	16	4,16,64,256
128	8	4,16,64
256	4	4,16
512	2	4

Further, we have also calculated the time required for interleaving and de-interleaving for all these possible sub-interleavers and tabulated in table 2. From the tabular data, it is clear that as the number of sub interleavers increases, the time required for interleaving and de-interleaving reduces to great extent.

М	Ν	Bloc k Interl eaver	Sub Interl eaver (x = 4)	Sub Interl eaver (x = 16)	Sub Interl eaver (x = 64)	Sub Interl eaver (x = 256)
2	512	2046	-	-	-	-
4	256	2042	2040	-	-	-
8	128	2034	2024	2016	-	-
16	64	2018	1992	1952	1920	_
32	32	1986	1924	1824	1664	1536
64	16	1922	1800	1568	1152	512
128	8	1794	1544	1056	128	_
256	4	1538	1026	32	-	-
512	2	1026	8	-	-	-

Table 2 Calculated time for block and possible sub-interleaver of length 1024

Now, to find the best among all the possible subinterleavers, we will consider the proposed mathematical formula $x = \frac{M^2}{4}$. The results are summed in the table 3. In the table, we have also summed the best sub interleaver depending upon the theoretical calculations as per table 2. It must be kept in mind that the proposed formula for selecting best sub interleaver is valid only when 2N is divisible by M. Keeping this in mind the combinations of (M,N) = (64, 16), (128,8), (256, 4)and (512, 2) are not considered when finding the best sub interleaver from the proposed formula. It is clear from the table 3 that results obtained from the proposed formula are in complete agreement with that predicted from the theoretical calculations. Hence, this shows that the proposed scheme is highly useful in predicating the best sub interleaver.

Table 3 Validation of proposed formula for number

 of sub-interleaver with minimum time requirement

 with theoretical results

М	Ν	$x = \frac{M^2}{4}$	Theoretical
2	512	1	1
4	256	4	4
8	128	16	16
16	64	64	64
32	32	256	256

6. Conclusions

This paper is an attempt to optimize the number of sub interleavers used for reducing the time complexity of the turbo codes. There can be a large number of sub interleavers possible for a given interleaver length. But it is not possible to test each sub interleaver by simulation method to find the best among them. In this paper, a scheme has been proposed to find the sub interleavers possible for a given interleaver length. Further, a mathematical formula has been derived to get the best among all the possible interleavers. To validate the proposed scheme, a sub interleaver is formed from matrix interleaver and diagonal interleaver of interleaver length 1024. Results obtained from proposed scheme are found to be in agreement with that expected from theoretical calculations. Possible sub interleavers for all the combinations of number of rows and columns, have been found and the best among them is predicted using mathematical formula derived. It is found that results are in agreement with that predicted using derived formula.

References:

[1] Hamming, R.W., Error detecting and error correcting code, *The bell System technical journal*, Vol. 29, No.2, 1950, pp. 147-160.

[2] Berrou, C., Glavieux, A., Near optimum error correcting coding and decoding: Turbo codes, *IEEE Trans. Commun.*, Vol. 44, 1996, pp. 1261-1271.

[3] Sadjadpour, H.R., Sloane, N.J.A., Salehi, M., Nebe, G., Interleaver design for turbo codes, *IEEE*

Proceedings of International conference on Information security and intelligent control, Yunlin, Taiwan, 2012.

[6] Dinoi, L., Benedetto, S., Design of fast-prunable S-random interleavers, *IEEE Trans. Wireless Commun.*, Vol. 4, No. 5, 2005, pp. 2540-2548.

[7] Hokfelt, J., Edfors, O., Maseng, T., A turbo code interleaver design criterion based on the performance of iterative decoding, *IEEE Commun. Lett.*, Vol. 5, No. 2, 2001, pp. 52-54.

[8] Benedetto, S., Divsalar, D., Monstorsi, G., Pollara, F., Serial concatenation of interleaved codes: Performance analysis, design and iterative decoding, *IEEE Trans. Inf. Theory*, 44(3), 1998, pp. 909-926.

[9] Das, B., Sarma, M.P., Sarma, K.K., Mastorakis, N., Implementation of block interleaver structure for use in wireless channels, In: Proceedings of 16th international conference on Automatic Control, Modelling and simulation, Romania, 2014.

[10] Devi, M.R., Ramanjaneyulu, K., Krishna, B.T., Design of Cascaded Hybrid Interleaver for Fast Turbo Coding and Decoding, In: Computer Communication, Networking and Internet Security, Lecture Notes in Networks and Systems 5, Springer, 2017

[11] Kousa, M.A., Performance of Turbo codes with Matrix Interleavers, *The Arabian Journal for Science and Engineering*, Vol. 28 (2B), 2003, pp.211-220.

[12] Rachinger, C., Huber, J.B., Muller, R.R., Comparison of Convolutional and block codes for low structural delay, *IEEE Trans. Commun.*, Vol. 63, No.12,2015, pp.1. J. Sel. Areas Commun., Vol. 19, No. 5, 2001, pp. 831-837.

[4] Sun, J., Takeshita. O.Y., Interleavers for Turbo Codes Using Permutation Polynomials Over Integer Rings, *IEEE Trans. Inf. Theory*, Vol. 51, No.1, 2005, pp. 101-119.

[5] Chi C.L., Kuo, C.H., Quadratic permutation polynomial interleaver for LTE turbo coding, In:

[13] Gazi, O., Yilmaz, A.O., Collision free row column S-random interleaver, *IEEE Commun. Lett.*, Vol. 13, No. 4, 2009, pp.257-259.

[14] Tallapragada, V.V.S., Sunkara, J.K., Prasad K.L., Nagaraju, D., Fast Turbo codes using subblock based interleaver, In: Proceedings of International conference on Circuits, Controls and Communications, Banglore, India, 2017.

[15] Devi, M.R., Ramanjaneyulu, K., Krishna, B. T., Performance analysis of sub-interleaver based turbo codes, Cluster Computing, 2018