Minimum Free Distance of CCSDS Turbo Encoders Under (Truncated) Mobius Interleavers

Kwame Ackah Bohulu

May 20, 2020

1 Introduction

1. A lot of research has been done concerning different turbo code interleavers in relation to error performance [14], [18], [20]

2. Main purpose of interleaver is to increase the minimum hamming distance of the turbo code. The performance of the turbo code depends on the minimum distance and the multiplicity of the minimum distance codewords in the high SNR region

3. Lower and upper bounds for Turbo codes provided in [3], [6], [13]. In [2] an interleaver acheiving the upper bound is constructed.

4. Deterministic interleavers are used due to to simple implementation and analysis, some examples are given in [5], [17],[18]

5. One of the interleavers introduced in [17] is the Mobius Interleaver, which is based on the Mobius permutation function in finite fields.

6. In this paper, the analysis of the minimum distance and error performance of turbo codes implementing Mobius Interleavers is presented.

7. The Binary Fixed Point (BFP) algorithm as well as Monte Carlo Simulations are used for the analysis of minimum distance and error performance respectively.

8. The BFP algorithm uses patterns that pass through the interleaver unchanged for estimation of minimum free distance. The unchanged pattens are found by determining the cycle structure of the interleaver and all its shifted versions.

9. In this Paper, the Consultative Committee for Space Data System (CCSDS) turbo code standard is used[23]. A new class of deterministic interleaver (Truncated Mobius Interleaver) based on the Mobius Interleaver is introduced.

10. Since it is easy to find the cycle structure of the interleaver and all shifted versions easily, the parameters Total Number of Cycles(TNC) and an upper-bound of the Total Number of Binary fixed points (TNB) are easily found.

11. A subclass of the truncated Mobius interleaver with small TNB (which means faster BFP algorithm processing) is also provided.

12. Error performance comparison of the new interleaver with random and S-Random interleavers is done via simulation.

2 Turbo Codes and Interleavers

Brief Recap of Turbo Codes

1. Turbo encoder is made up 2 recursive convolutional encoders (usually of the same type) that are parallelly concatenated via interleaver. An example of the CCSDS turbo encoder standard is shown in Fig.1 of main paper.
2. It is known that there are certain inputs that produce low-weight parity outputs when fed into the first encoder. The interleaver's job is to rearrange such inputs so that they do not occur in the second encoder and generate a low-weight turbo codeword.
3. An interleaver is a device that permutes(re-arranges) the order of a bit sequence fed into it. It is represented by $\Pi(\mathbf{x})$, where $\mathbf{x} = (x_0, x_1, ..., x_{k-1})$ and k is the length of the interleaver.
4. Denoting the codeword length by n, the rate $r = \frac{k}{n}$
5. Asuming BPSK modulation and transmission over the AWGN channel the following union bound estimates are used to measure the Frame Error Rate(FER) and the Bit Error Rate(BER).

$$FER \approx \frac{N_{\text{free}}}{2}\text{erfc}\Big(\sqrt{rd_{\text{free}}SNR}\Big) \tag{1}$$

$$BER \approx \frac{W_{\text{free}}}{2k}\text{erfc}\Big(\sqrt{rd_{\text{free}}SNR}\Big) \tag{2}$$

   Where $d_{\text{free}}, N_{\text{free}}$ and W_{free} are the minimum free distance of the turbo code, The number of codewords with weight equal to d_{free} and the sum of the weights of all information sequences that generate codewords with weight equal to d_{free} SNR $\triangleq E_b/N_o$
6. From the equations, we deduce that is a turbo code has large d_{free} and small N_{free} and W_{free},it has a low FER and BER and high SNR.

Mobius Interleaver vs Truncated Mobius Interleaver

1. The Mobius Interleaver is based on the Mobius permutation function over $\mathbb{F}_q$ and it was investigated in terms of cycle structure in [17]
2. The Mobius permutation function is represented by

$$T(x) = \begin{cases} \frac{ax+b}{cx+d} & x \neq \frac{-d}{c} \\ \frac{a}{c} & x = \frac{-d}{c} \end{cases} \tag{3}$$

   where $a, b, c, d \in \mathbb{F}_q, c \neq 0$ and $ad - bc = 0$

3. The Mobius interleaver is then constructed using the equation

$$\Pi_T(i) = \ln(T(\alpha^i)) \tag{4}$$

where ln(.), α are the discrete logarithm with $\ln(0) = 0$ and the primitive element of $\mathbb{F}_q$ respectively

4. In [4],[17], the authors found the cycle structure of Mobius interleavers using the characteristic polynomial when the permutation function T is known. The characteristic polynomial t(x) is given by

$$t(x) = x^2 + (a+d)x + (ad - bc) \tag{5}$$

5. By setting $b = 0$ in (3), we make 0 a fixed point and removing 0 from both the input and output, we still have an interleaver. This new interleaver is known as the *truncated Mobius interleaver*

6. Its permutation function is denoted by T' and its characteristic polynomial $t'(x)$ is given by

$$t'(x) = x^2 + (a+d)x + ad = (x-a)(x-d) \tag{6}$$

7. Results about cycle structure of the truncated Mobius interleaver are given below.

Proposition 1.
Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements for some prime p and positive integer m and ord (z) denotes the order of $z \in \mathbb{F}_q$. For the truncated Mobius permutation T', we have

(a) If $a \neq d$ and $k = \text{ord}\left(\frac{a}{d}\right) = \frac{q-1}{s}$, then T' has $s-1$ cycles of length k, one cycle of length $k-1$ and one cycle of length 1

(b) Suppose $t'(x) = (x-a)^2$, for $a \in \mathbb{F}_q^*$. Then T' has $p^{m-1} - 1$ cycles of length p and one cycle of length $p-1$

8. The most useful property of the truncated Mobius interleaver is that the cycle structure is known for the primary interleaver as well as all of its shifted version. The cycle shift is defined as follows.

Definition 1.
The s-th cycle shift to left (right) of a permutation Π of length k is defined as a transformation that applies to all of the outputs of the primary permutation from left (right, respectively) for all $0 < s < k$. More precisely, the s-th cycle shift to left (right) of Π denoted by $\Pi_s^{(\ell)}$ $\left(\Pi_s^{(r)}\right)$ is another permutation, which acts as

$$x \mapsto \Pi(x) + s \,(\text{mod} k),\ (x \mapsto \Pi(x) - s \,(\text{mod} k))$$

9. Given any interleaver, cycle shifts to the left or right of that interleaver are reffered to as its shifted versions. It is worth noting that all shifted versions of the truncated Mobius interleaver are also truncated Mobius interleavers.

10. More precisely, given a truncated Mobius interleaver with coefficients $(a, 0, c, d)$, the s-th shift interleaver has coeffiecients $(a', b', c', d') = (a\alpha^s, 0, c, d)$ when shifted to the left and $(a', b', c,' d') = (a/\alpha^s, 0, c, d)$ when shifted to the right

11. An example to review to review the all the properties of the truncated Mobius interleaver are given in the main paper.

3 Binary Fixed Point (BFP) Algorithm

1. Finding the exact value of d_{free} for a turbo code by checking all input is not the best way to go. Instead some efficient algorithms in [9], [15] are used instead.

2. The downside to these algorithms is that as the interleaver length increases, the computation complexity and runtime also increases and for that reason, this paper focuses on algorithms with lower runtime that [9]

3. There are input patterns that pass throught the interleaver unchanged. If such inputs pass through the first component encoder and produce low-weight parity outputs, the turbo codeword will also have a low weight.

4. Combining this with the fact that the convolutional encoder is time invariant, these patterns will produce low weight codewords through out the encoder.

5. The BFP algorithm[7] uses these Binary Fixed Points to estimate the value of d_{free}. What is different about this interleaver is that, the interleaver (not the inputs) is shifted to the left and to the right.

6. The following steps are involved in using the BFP algorithm

   (a) Find the cycle structure of the primary interleaver and all of its shifted versions and collect them in a set. Suppose that we have the following interleaver

   $$\Pi_T = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 0 & 4 & 2 \end{pmatrix}$$

   We find the cycle structure of the respective permutation and collect these cycles in a set $\mathcal{T} = \{(0,1,3),(2,5),(4)\}$

(b) Find all of the subsets of the aforementioned set in previous step. For the example given in previous step, we have:

$$P(\mathcal{T}) = \{\phi, \{(0,1,3)\}, \{(2,5)\}, \{(4)\}, \{(2,5),(4)\}, \{(0,1,3),(2,5)\}, \{(0,1,3),(4)\} \{(0,1,3),(2,5),(4)\}\}$$

(c) Generate a binary sequence (pattern) for each of these subsets with placing 1 in places, where the elements belong to the subset and 0 in other places in the pattern. The above power set $P(\mathcal{T})$ corresponds to the following set of binary vectors:

$$\mathcal{B}_T = \{000000, 110100, 001001, 000010 \; 111101, 110110, 001011, 111111\}$$

(d) Feed the turbo encoder with these patterns and nominate the Hamming weight of the output codeword with less Hamming weight as minimum free distance.

7. By considering all shifted versions we are able to test all extended binary fixed point patterns

8. In order to obtain a true cycle shift, we place s zeros at the beginning of the primary pattern.

9. Also, in s-th shift to left, we ignore cycles with any number less that s and in the similar manner in the s-th shift to right we should ignore cycles with any number greater that $k - s$ with interleaver length k.

4 Truncated Mobius Interleaver and the Binary Fixed Point (BFP) Algorithm

1. The speed and computational complexity of the BFP algorithm depends on the number of binary fixed points present in the interleaver.

2. There are two important parameters in relation to the BFP algorithm, these are the Total Number of Cycles(TNC) and the Total Number of Binary fixed points (TNB)

3. TNC is an integer value which shows the total number of cycles present in the primary interleaver as well as its shifted versions.

4. TNB is also an integer value that expresses the number of binary inputs that should be fed into the turbo encoder to figure out d_{free}.It goes without saying that there is a relationship between TNC and TNB.

5. Unlike the Mobius Interleaver, it is possible to find the exact value of TNC for the truncated Mobius interleaver. We can also obtain an upperbound on the value of TNB

6. It is only possible to obtain an upper bound on the value of TNB since some cycles are gotten rid of during the left and right shifts of the interleaver. The exact number of cycles gotten rid off is not known and we assume that one cycle is lost for every shift.

7. The following Theorem summarizes how to calculate for TNC and TNB

Theorem 1.
Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements for some prime p and primitive element α. Let us also assume $\frac{a}{d} = \alpha^z$ and ord $(\alpha^z) = f$ for some positive integers f and z In a truncated Möbius permutation constructed based on T' over $\mathbb{F}_q$ as in (3), we distinguish between two cases: If $a \neq d$, then we have:

$$TNC = \left[\sum_{t_i|q-1, t_i\neq 1} 2\phi(t_i)\left(\frac{q-1}{t_i}+1\right)\right] - \left(\frac{q-1}{f}+1\right) + 2p^{m-1}$$

and (7)

$$TNB \leq \left[\sum_{t_i|q-1, t_i\neq 1} 2\phi(t_i)\, 2^{\frac{q-1}{t_i}}\right] + 2^{p^{m-1}} - 2(q-2)$$

If $a = d$:

$$TNC = \left[\sum_{t_i|q-1, t_i\neq 1} 2\phi(t_i)\left(\frac{q-1}{t_i}+1\right)\right] + p^{m-1}$$

and (8)

$$TNB \leq \left[\sum_{t_i|q-1, t_i\neq 1} 2\phi(t_i)\, 2^{\frac{q-1}{t_i}}\right] + 2^{p^{m-1}} - 2(q-2)$$

8. The Corollary below shows how the TNC can be made to grow linearly instead of exponentially.

Corollary 1.
Let $\mathbb{F}_q$ be a finite field with $q = p = 2p' + 1$ elements for some primes p, p' and in a truncated Möbius permutation constructed based on T' over $\mathbb{F}_q$ we put $a = d$ then we have

$$\begin{aligned} TNC =& 1 + 2\left(2 + \frac{q-3}{2}\right) + 3\left[2\left(\frac{q-1}{2}-1\right)\right] \\ &+ 2\left[2\left(\frac{q-1}{2}-1\right)\right] = 6q - 13 \end{aligned}$$

The upper bound on TNB can also be presented as follows:

$$TNB \leq 2 + 2\left(2^{1+\frac{q-3}{2}}\right) + 2^2\left[2\left(\frac{q-1}{2} - 1\right)\right]$$
$$+2^1\left[2\left(\frac{q-1}{2} - 1\right)\right] - 2(q-2) = 2^{2+\frac{q-3}{2}} + 4q - 12$$