On the Equivalence of Cubic Permutation Polynomial and ARP Interleavers for Turbo Codes

Kwame Ackah Bohulu

June 20, 2018

Abstract - Recently, it was shown that the dithered relative prime interleavers and quadratic permutation polynomial (QPP) interleavers can be expressed in terms of almost regular permutation (ARP) interleavers. In this paper, the conditions for a QPP interleaver to be equivalent to an ARP interleaver are extended for cubic permutation polynomial (CPP) interleavers. It is shown that the CPP interleavers are always equivalent to an ARP interleaver with disorder degree greater than one and smaller than the interleaver length, when the prime factorization of the interleaver length contains at least one prime number to a power higher than one and it fulfills the conditions for which there are true CPPs for the considered length. When the prime factorization of the interleaver length contains only prime numbers to the power of one, with at least two prime numbers pi , fulfilling the conditions $p_i > 3$ and $3 \not| (p_i - 1)$, values of disorder degree smaller than the interleaver length are possible under some conditions on the coefficients of the second and third degree terms of the CPP.

1 Introduction

- There are 3 commonly used high performing interleavers for turbo codes, Dithered Relative Prime (DRP) interleaver[1], Almost Regular Permutation (ARP) Interleavers[2] and Permutation Polynomial(PP) interleaver[3][4].
- in [5] it was shown that DRP and Quadratic Permutation Polynomials (QPP) interleavers can be expressed in terms of ARP interleavers.
- in [19][20] Cubic Permutation Polynomial (QPP) interleavers of small length have been shown to have better performance a little better than QPP interleavers.
- The conditions for expressing CPP interleavers interms of ARP interleavers are presented and some specific examples are shown for different lengths.
- The following notations are used in this paper:
  - $\mathbb{N}$ is the set of natural numbers, $\mathbb{N}^+$ is the set of natural numbers greater than zero, $\mathbb{N}_o$ is the set of odd natural numbers.
  - $\mathbb{Z}$is the set of integers, $\mathbb{Z}_K = \{0, 1, \cdots, K-1\}$ is the integer ring, where K is a positive integer.
  - $a \mod b$ denotes a modulo b, $a|b$ denotes a divides b, and $a \not| b$ denotes a does not divide b, where $a, b \in N$.

2 Mathematical Model for ARP and CPP Interleavers

2.1 ARP interleavers

This interleaver was proposed in [2] by Berrou et al and is based on a regular permutation of period P and a vector of shifts S

$$\Pi_{ARP(x)} = \Big(P.x + S_{(x \mod Q)}\Big) \mod K \tag{1}$$

where $x = 0, \cdots, K-1$ denotes the address of the data symbol after before interleaving and $\Pi_{ARP(x)}$ represents its corresponding address after interleaving. P is a positive integer relatively prime to the interleaver length K. The disorder cycle or disorder degree in the permutation is denoted by Q and it corresponds to the number of shifts in S. K must be a multiple of Q.

2.2 CPP interleavers

PP interleavers are based on permutation polynomials over integer rings $\mathbb{Z}_{\mathbb{K}}$ and were proposed by Sun et al.[3][4]. The interleaver function for a CPP is shown in (2)

$$\Pi_{CPP(x)} = \Big(f_1 \cdot x + f_2 \cdot x^2 + f_3 \cdot x^3\Big) \mod K \tag{2}$$

where $x = 0, \cdots, K-1$ denotes the address of the data symbol after before interleaving and $\Pi_{CPP(x)}$ represents its corresponding address after interleaving.

The necessary and sufficient conditions for generating CPP interleavers depends on the prime factorization of K, where the prime factorization of K is considered below.

$$K = 2^{a_{K,1}} \cdot 3^{a_{K,2}} \cdot \prod_{i=3}^{w(K)} p_i^{a_{K,i}} \tag{3}$$

Where $w(K)$ is a positive integer greater than or equal to 2. if $w(K) = 2, \prod_{i=3}^{w(K)} p_i^{a_{K,i}} = 1$ (by definition)

The conditions on the coefficients are given in Table I.

Note - these conditions have to be fulfilled only for the prime factors of K.

3 Conditions for a CPP Interleaver to be Expressed as an ARP Interleaver

Resulting from the definition of the ARP interleaver, a suitable first condition is that the value of Q should be a submultiple of K. In this section, an expression for for the value of Q for the equivalent ARP is derived which depends of three(3)

variables, which are the value of K, the coefficient f_3 of the CPP and on a positive integer denoted by l.

Using the idea from [5] we see that a sufficient condition for an ARP equivalent form of the CPP interleaver is that

$$(P \cdot x) \mod K = (f_1 \cdot x) \mod K, \forall\, x = 0, \cdots, K-1 \tag{4}$$

and

$$S_{(x \mod Q)} \mod K = \left(f_2 \cdot x^2 + f_3 \cdot x^3\right) \mod K, \forall\, x = 0, \cdots, K-1 \tag{5}$$

(4) and (5) are satisfied if $P = f_1$ and

$$\begin{aligned}
&\left(f_2 \cdot x^2 + f_3 \cdot x^3\right) \mod K = \left(f_2 \cdot (x+Q)^2 + f_3 \cdot (x+Q)^3\right) \mod K, \forall\, x = 0, \cdots, K-1 \\
&\left(f_2 \cdot x^2 + f_3 \cdot x^3\right) \mod K = \Big(f_2 \cdot x^2 + f_3 \cdot x^3 + (f_2 \cdot Q^2 + f_3 \cdot Q^3) \\
&+ (2 \cdot f_2 \cdot Q + 3 \cdot f_3 \cdot Q^2) \cdot x + (3 \cdot f_3 \cdot Q) \cdot x^2\Big) \mod K, \forall\, x = 0, \cdots, K-1
\end{aligned} \tag{6}$$

(6) is true if

$$\begin{aligned}
&(f_2 \cdot Q^2 + f_3 \cdot Q^3) \\
&\quad + (2 \cdot f_2 \cdot Q + 3 \cdot f_3 \cdot Q^2) \cdot x + (3 \cdot f_3 \cdot Q) \cdot x^2 = 0 \mod K, \forall\, x = 0, \cdots, K-1
\end{aligned} \tag{7}$$

(7) is true if the coefficient of the x term is a quadratic or linear null polynomial and from [12] we know that a quadratic null polynomial $\mod K$ only exists when $2 \mid K$ and it is

$$Z_{QNP}(x) = (\frac{K}{2} \cdot x \frac{K}{2} \cdot x^2) \mod K \tag{8}$$

also from [23] we know that there are no linear null polynomials. From the above equations (**??**) is true if and only if

$$\begin{cases}
(f_2 \cdot Q^2 + f_3 \cdot Q^3) = 0 \mod K \\
(2 \cdot f_2 \cdot Q + 3 \cdot f_3 \cdot Q^2) = 0 \mod K \\
(3 \cdot f_3 \cdot Q) = 0 \mod K
\end{cases} \tag{9}$$

or when $2 \mid K$

$$\begin{cases}
(f_2 \cdot Q^2 + f_3 \cdot Q^3) = 0 \mod K \\
(2 \cdot f_2 \cdot Q + 3 \cdot f_3 \cdot Q^2) = \frac{K}{2} \mod K \\
(3 \cdot f_3 \cdot Q) = \frac{K}{2} \mod K
\end{cases} \tag{10}$$

using the third equation in (9) we see that

$$Q = \frac{l \cdot K}{3 \cdot f_3}, \, l \in \mathbb{N}^+$$

and we may rewrite (9) as

$$\begin{cases} Q = \frac{l \cdot K}{3 \cdot f_3}, \, l \in \mathbb{N}^+ \\ \frac{l^2 \cdot K^2 \cdot (3 \cdot f_2 + l \cdot K)}{3^3 \cdot f_3^2} \in \mathbb{N}^+ \\ \frac{l \cdot K \cdot (2 \cdot f_2 + l \cdot K)}{3 \cdot f_3} \in \mathbb{N}^+ \end{cases} \tag{11}$$

also from the third equation in (10) we get

$$Q = \frac{l_o \cdot K}{2 \cdot 3 \cdot f_3} \in \mathbb{N}_o$$

and we may rewrite (10) as

$$\begin{cases} Q = \frac{l_o \cdot K}{2 \cdot 3 \cdot f_3} \in \mathbb{N}_o \\ \frac{l_o^2 \cdot K^2 \cdot (2 \cdot 3 \cdot f_2 + l_o \cdot K)}{2^3 \cdot 3^3 \cdot f_3^2} \in \mathbb{N}^+ \\ \frac{l_o \cdot K \cdot (2 \cdot f_2 + l_o \cdot K)}{2^2 \cdot 3 \cdot f_3} - \frac{1}{2} \in \mathbb{N}^+ \end{cases} \tag{12}$$

4 CPP Interleavers Seen as Particular Cases of ARP Interleavers

In this section, the conditions on powers of prime numbers from the factorization l for the CPP to be espressed as ARP are presented in Theorem 1. It is shown that the powers depend on the powers from the prime factorization of K and the CPP coefficients f_2 and f_3.

First the general form of the factorization of K is shown below

$$K = 2^{a_{K,1}} \cdot 3^{a_{K,2}} \cdot \prod_{i=3}^{w(K)} p_i^{a_{K,i}} \prod_{w(K)-n_{4_a}+1}^{w(K)} p_i \tag{13}$$

where n_{4_a} is the number of prime factors that satisfy the conditions $(p_i - 1)$ is not divisible by 3 when $p_i > 3$ and $a_{K,i} = 1$. It should be noted that the prime factors that satisfy this condition are written out last in the prime factorization of K.

Example 1a. : For $K = 22540$, we have a prime factorization of the form $2^2 \cdot 3^0 \cdot 7^2 \cdot 5^1 \cdot 23^1$. We therefore have

- $w(K) = 5, n_{4_a} = 2$
- $p_3 = 7, p_4 = 5, p_5 = 23$

- $a_{K,1} = 2, a_{K,2} = 0, a_{K,3} = 2, a_{K,4} = 1, a_{K,5} = 1$

The general form of the factorization of the coefficients $f_j, j = 2, 3$ is shown below

$$\begin{aligned} f_j =& 2^{a_{f_j,1}} \cdot 3^{a_{f_j,2}} \cdot \prod_{i=3}^{w(K)-n_{4_a}} p_i^{a_{f_j,i}} \\ & \cdot \prod_{i=w(K)-n_{4_a}+1}^{w(K)} p_{i,f_j}^{a_{f_j,i}} \cdot \prod_{w(K)+1}^{w(f_j)} p_{i,f_j}^{a_{f_j,i}} \end{aligned} \tag{14}$$

where $w(f_j)$ is an integer greater than or equal to $w(K)$

We have to mention that for a true CPP it is possible to have the coefficient $f_2 = 0$. In this case, the factorization of f_2 as in (18) is not valid and the terms which contain the variables f_2 in systems (11) and (12) must be removed.

Example 1b. : Let the coefficients of the CPP be $f_1 = 11, f_2 = 4186 = 2^1 \cdot 3^0 \cdot 7^1 \cdot 5^0 \cdot 23^1 \cdot 13^1$ and $f_3 = 322 = 2^1 \cdot 3^0 \cdot 7^1 \cdot 5^0 \cdot 23^1$. According to (**??**), we have

- $w(f2) = 6, w(f3) = w(K) = 5$
- $a_{f_2,1} = 1, a_{f_2,2} = 0, a_{f_2,3} = 1, a_{f_2,4} = 0, a_{f_2,5} = 1, a_{f_2,6} = 1$
- $a_{f_3,1} = 1, a_{f_3,2} = 0, a_{f_3,3} = 1, a_{f_3,4} = 0a, a_{f_3,5} = 1$

The decomposition of l from (11) is

$$K = 2^{a_{l,1}} \cdot 3^{a_{l,2}} \cdot \prod_{i=3}^{w(K)} p_i^{a_{l,i}} \prod_{w(K)+1}^{w(f_3)} p_{i,f_3}^{a_{l,i}} \tag{15}$$

The decomposition of l_o from (12) is

$$K = 3^{a_{l_o,2}} \cdot \prod_{i=3}^{w(K)} p_i^{a_{l_o,i}} \prod_{w(K)+1}^{w(f_3)} p_{i,f_3}^{a_{l_o,i}} \tag{16}$$

Rewriting the conditions from systems (11) and (12) and taking into account (13) - (16), we obtain the conditions for CPP interleavers to be expressed as ARP interleavers. These conditions are given in Theorem 1 below. (refer to paper)

Example 2 : Let K, f_1, f_2 and f_3 be as in Example 1. Then, a valid value of l is $l = 42 = 2^1 \cdot 3^1 \cdot 7^1 \cdot 5^0 \cdot 23^0$, for which $Q = 980$ results. Thus, according to (15), we have $a_{l,1} = 1, a_{l,2} = 1, a_{l,3} = 1, a_{l,4} = 0, and a_{l,5} = 0$