Quadratic Permutation Polynomial Interleavers for LTE Turbo Coding

Ching-Lung Chi

***Abstract*—Interleaver is an important component of turbo code and has a strong impact on its error correcting performance. Quadratic permutation polynomial (QPP) interleaver is a contention-free interleaver which is suitable for parallel turbo decoder implementation. To improve the performance of LTE QPP interleaver, largest-spread and maximum-spread QPP interleavers are analyzed for Long Term Evolution (LTE) turbo codes in this paper. Compared with LTE QPP interleaver, those algorithms have low computing complexity and better performances from simulation results.**

***Index Terms*—Quadratic permutation polynomial (QPP) interleaver, Long Term Evolution (LTE), largest-spread QPP interleaver, maximum-spread QPP interleaver.**

I. Introduction

The selection of turbo coding was considered during the study phase of Long Term Evolution (LTE) standard to meet the stringent requirements. Following deliberations within the working group, the quadratic permutation polynomials (QPP) were selected as interleavers for turbo codes, emerging as the most promising solutions to the LTE requirements. The QPP interleavers for the LTE standard [1] involve 188 different lengths. In this paper we take two kinds of methods to improve the LTE QPP interleaver.

The polynomial interleavers offer the following benefits [2]: special performance, complete algebraic structure, and efficient implementation (high speed and low memory requirements). A QPP interleaver of length L is defined as:

$$\pi(x) = (q_0 + q_1 x + q_2 x^2) \bmod L\,, x = 0 \cdots L-1 \quad (1)$$

where q_1 and q_2 are chosen so that the quadratic polynomialin (1) is a permutation polynomial (i.e. the set $\{\pi(0), \pi(1), \cdots, \pi(L-1)\}$ is a permutation of the set $\{0,1,\cdots,L-1\}$ and q_0 determines a shift of the permutation elements.

In the following we only consider quadratic polynomials with free term $q_0 = 0$, as for the QPP interleavers in the LTEstandard. If $\mathbb{Z}_L = \{0,1,\cdots,L-1\}$, then the permutation function is$\pi: \mathbb{Z}_L \to \mathbb{Z}_L$.

The spread factor D is defined as

$$D = \min_{\substack{i \neq j \\ i,j \in \mathbb{Z}_L}} \{\delta_L(p_i, p_j)\} \quad (2)$$

$\delta_L(p_i, p_j)$ is the Lee metric between points $p_i = (i, \pi(i))$ and $\mathrm{p_j} = (\mathrm{j}, \pi(\mathrm{j}))$

$$\delta_L(p_i, p_j) = |i-j|_L + |\pi(i) - \pi(j)|_L \quad (3)$$

where

$$|i-j|_L = min\{(i-j) (\mathrm{mod}\, L), (j-i) (\mathrm{mod}\, L)\} \quad (4)$$

The quadratic polynomials which lead to the largest spreading factor $D$for some interleaver lengths are given in [2]. An algorithm for faster computation of D is also presented. It is based on the representatives of orbits in the representation of interleavercode.

Section II gives a brief review of QPP interleaver. Largest-Spread and Maximum-Spread QPP interleavers are the topics of Section III. Section IV presents the bit error rates (BER) resulted from simulations for LTE standard, LS and MS QPP inter leavers length 512. Section V concludes the paper.

II. QPP Interleavers

A. Permutation Polynomial(PP) over Integer N

Given an integer$N \geq 2$, a polynomial$F(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_m x^m$, where f_0, f_1, $f_2, \cdots, f_m$ and m are nonnegative integers, is said to be a permutation polynomial overZ_N when $F(x)$ permutes $\{0, 1, 2, \cdots, N-1\}$.

In this paper, all the summations and multiplications are modulo N unless explicitly stated. We further define the formal derivative of the polynomial $F(x)$ to be a polynomial $F'(x)$ such that $F'(x) = f_1 + 2f_2 x + 3f_3 x^2 + \cdots + mf_m x^{m-1}$. For any integer N, whether polynomial $F(x)$ is a permutation polynomial can be determined by the following theorem [3].

Theorem 1: Let $F(x) = f_1 + 2f_2 x + 3f_3 x^2 + \cdots + mf_m x^m$ be a polynomial with integer coefficients. $F(x)$ is a permutation polynomial over the integer ring $N = 2^n$ if and only if 1) f_1 is odd, 2) $f_2 + f_4 + f_6 + \cdots$ is even, and 3) $f_3 + f_5 + f_7 + \cdots$ is even.

Theorem 2: $F(x)$ is a permutation polynomial over the integer ring$N = 2^n$if and only if$F(x)$is a permutation polynomial over $\mathrm{Z}(p)$ and $F'(x) \neq 0$ modulo p for all integers$x p^n$.

Theorem 3: For any $N = \prod_{i=1}^{n_{pi}} p^{n_{pi}}$, where $p_i's$ are distinctprime numbers,$F(x)$is a permutation polynomial modulo N if and only if $F(x)$ is also a permutation

Manuscript received October 25, 2012; revised November 25, 2012.

Ching-Lung Chi is with the Dept. of Computer and Communication SHU-TE University Kaohsiung City 824, Taiwan (e-mail: pipn@stu.edu.tw)

polynomial modulo$p_i^{n_{pi}}$, $\forall\, i$.

TABLE I: EXAMPLES OF MAXIMUM-SPREAD QPP INTERLEAVER

k	N	$f(x)$	$f^{-1}(x)$	$D = ub_D(N)$	ζ	ζ'	$\in$
4	128	$15x + 32x^2$	$-17x + 32x^2$	16	2	2	64
5	512	$31x + 64x^2$	$-33x + 64x^2$	35	4	3	128
6	2048	$63x + 128x^2$	$-65x + 128x^2$	64	8	4	256
7	8192	$127x + 256x^2$	$-129x + 256x^2$	128	12	7	512
8	32768	$255x + 512x^2$	$-257x + 512x^2$	256	32	12	1024
9	131072	$511x + 1024x^2$	$-513x + 1024x^2$	512	64	23	2048

Because the function of interleaver is to permute $\{0,1,\cdots,L-1\}$, we can apply the construction of permutation polynomial over integer N to Turbo interleavers by properly choosing N and polynomial coefficients f. The first-degree polynomial $F(x) = f_0 + f_1 x$ (linear interleaver) is the simplest one among all permutation polynomials. However, the linear interleaver has very bad input weight 4 error event characteristics, causing a higher error floor for medium or long frame size cases. And quadratic permutation polynomial can overcome these defects, this leaves it the next in the chain. When $m = 2$, $F(x)$ becomes $F(x) = f_0 + f_1 x + f_2 x^2$. Notice that the coefficient f_0 just corresponds to a cyclic rotation in the interleaved sequence. It does not appear in the conditions for $F(x)$ to be a permutation polynomial and it does not affect the performance. We ignore f_0 for simplification, so $F(x)$ becomes quadratic polynomial $F(x) = f_1 x + f_2 x^2$..

B. QPP Interleavers

QPP Interleaver completes interleaving by making QP (Quadratic Polynomial) satisfy some conditions. In order to make$F(x)$be a QPP, coefficients f_1 and $f_2$have to meet some special conditions. Then the following 2 corollaries deduced from theorem 1 and 2 are given.

Corollary 1 [3]: A quadratic polynomial of the form $F(x) = f_1 x + f_2 x^2$ is a permutation polynomial overZ_{p^n} if and only if$f_1 \neq 0$and$f_2 = 0 \mod p$.

Corollary 2 [4]: Let$N = \prod_{p\in P} p^{n_{N,p}}$, denote y divides z by $y|z$ and denote y can not divides z by $y \perp z$. The necessary and sufficient condition for a quadratic polynomial$F(x) = f_1 x + f_2 x^2 (mod\ N)$to be a permutation polynomial can be divided into two cases.

1) $2|N$and$4 \perp N$ (i.e., $n_{N,2} = 1$)

$f_1 + f_2$is odd, $\gcd(f_1, N/2) = 1$, and$f_2 = \prod_{p\in P} p^{n_{F,p}}$,

$n_{F,p} \geq 1$, $\forall$ psuch that$p \neq 2$and$n_{N,p} \geq 1$.

2) Either $2 \perp N$ or $4|N$ (i.e., $n_{N,2} \neq 1$) $\gcd(f_1, N) = 1$and$f_2 = \prod_{p\in P} p^{n_{F,p}}$, $n_{F,p} \geq 1$, $\forall$ psuch that$n_{N,p} \geq 1$.

Apply above corollaries, we can find some available coefficients f_1 and f_2 in QPP interleavers by computer searching. However, the interleavers with different coefficients have different performances, so we have to choose better based on these coefficients. Then we discuss search metric on choosing better coefficients, before this we present some definitions firstly:

1) δ_N Distance

$$\delta_N(p_{x1}, p_{x2}) = |x_1 - x_2|_N + |f(x_1) - f(x_2)|_N \quad (5)$$

where$|i-j|_N = \min\{(i-j)(\mathrm{mod}\ N), (i-j)(\mathrm{mod}\ N)\}$.

2) Spread Factor $D(f)$

$$D(f) = \min\{\delta_N(p_i, p_j) | p_i, p_j \in F\} \quad (6)$$

where$i, j \in N$ and $i \neq j$.

3) Nonlinearity Metric of QPP Interleavers$\zeta\ (F)$

$$\zeta\ (F) = N/\gcd(2f_2, N) \quad (7)$$

Obviously, QPP interleaver can be viewed as a linear interleaver $f_1 x$ that is "disturbed" by quadratic interleaver$f_2 x^2$, the periodicity of the disturbance is at mostζ.This disturbance can overcome a higher error floor of linear interleaver at a certain extent.

Since the minimum distance of a turbo code is now known to grow at most logarithmically, therefore, the spread factor that controls the effective free distance should be "rewarded" at most logarithmically. The nonlinearity$\zeta$is expected to have a proportional reduction in the multiplicities of low-weight code words so it is reasonable to leave it. So we can get a simple metric of searching coefficients of QPP interleaver [4].

$$\max\{\Omega(f) = \ln(D(f))\,\zeta(f)\} \quad (8)$$

Further choosing coefficients f_1 and f_2 by maximization$\Omega(f)$, we can get some coefficients with good performances. Sinceζwill grow fast as N grows, it is not good for improving decoding performance, so it must be modified. We define a new modified nonlinearity metric ζ' which can avoid above defect. So we have a corresponding refined metric

$$\max\{\Omega'(f) = \ln(D(f))\,\zeta'(f)\} \quad (9)$$

where $\zeta' = \{f_2 x^2 (\mathrm{mod}\ N) | x = 0,1,\cdots,\zeta - 1\}$

Through this refined metric, we search coefficients more than one couple, since the up-bound of interleavers spread factor $D(f)$ is $\sqrt{2N}$, in order to avoid $D(f)$ not becoming so small when frame size$N$is small that we limit the search process under the condition of $D(f) \geq \beta\sqrt{2N}$,

where $\beta = 0.45$. While $N > 2000$, must decrease to 0.30 properly.

III. Largest-Spread and Maximum-Spread QPP Interleavers

A. Largest-Spread QPP Interleaver

In this section we present a theorem which states sufficient conditions to be satisfied by the coefficients of two quadratic polynomials [4], so that the resulting interleavers are identical. For the LTE standard, the interleaver's length is always an even number.

Theorem 4: Consider two QPP interleavers described by the following polynomials (the free term is considered zero):

$$\pi_1(x) = (p_1 x + p_2 x^2) \bmod L,\ \mathrm{x} = 0,1,\cdots,\mathrm{L}-1 \quad (10)$$

$$\pi_2(x) = (q_1 x + q_2 x^2) \bmod L,\ \mathrm{x} = 0,1,\cdots,\mathrm{L}-1 \quad (11)$$

If L is even, then $p_1 > q_1$, and the following relation is fulfilled:

$$p_1 - q_1 = \pm(p_2 - q_2) = L/2 \quad (12)$$

The two quadratic polynomials lead to identical permutations.

Proof:

For the two QPP to lead to identical permutations, it is required that

$$\pi_1(x) = \pi_2(x),\ \forall x = 0,1,\cdots,L-1 \quad (13)$$

We denote

$$p_1 x + p_2 x^2 = k_1 \cdot L + \pi_1(x) \quad (14)$$

$$q_1 x + p_2 x^2 = k_2 \cdot L + \pi_2(x) \quad (15)$$

where $k_1,\ k_2 \in \mathbb{N}$. Under the conditions above we have to

Show that there are $k_1,\ k_2 \in \mathbb{N},\ \forall x = 0,1,\cdots,L-1$, which verify relationship (13). Subtracting (14) from (15) and considering (13), we have:

$$(p_2 - q_2)x^2 + (p_1 - q_1) = (k_1 - k_2) \cdot L \quad (16)$$

The solution of this quadratic equation is:

$$x = \frac{-(p_1 - q_1) + \sqrt{(p_1 - q_1)^2 + 4(p_2 - q_2)(k_1 - k_2)L}}{2(p_2 - q_2)} \quad (17)$$

Using (12) from the theorem statement, we have

$$x = \frac{-\frac{L}{2} + \sqrt{\left(\frac{L}{2}\right)^2 \pm 4\left(\frac{L}{2}\right)(k_1 - k_2)L}}{\pm L} = \frac{-1 + \sqrt{1 \pm 8(k_1 - k_2)}}{\pm 2} \quad (18)$$

where

$$k_1 - k_2 = \frac{1 - (-2x + 1)^2}{8} = \frac{x(x-1)}{2} \quad (19)$$

or

$$k_1 - k_2 = \frac{(-2x + 1)^2 - 1}{8} = \frac{x(x-1)}{2} \quad (20)$$

Relationships (19) and (20) could also be obtained as follows. From (12) we have

$$p_1 = q_1 + L/2 \quad (21)$$

$$p_2 = q_2 + L/2 \quad (22)$$

Then, from (14) we get

$$k_1 \cdot L = p_1 x + p_2 x^2 - \pi_1(x) \quad (23)$$

Or, taking into account (21), (22) and (13),

$$k_1 \cdot L = q_1 x + q_2 x^2 - \pi_2(x) + (L/2) \cdot (x \pm x^2) \quad (24)$$

Or, from (15),

$$k_1 \cdot L = (L/2) \cdot (x \pm x^2) + k_2 \cdot L \quad (25)$$

From here, (19) and (20) result immediately.

Because $\forall\ x = 0,1,\cdots,L-1$, $x(x-1)$ and $x(x+1)$ are divisible by 2, i.e. $k_1 - k_2 \in \mathbb{Z}$ then, there are $k_1,\ k_2 \in \mathbb{N}$ which verify relation (13).

The theorem shows that two QPPs generate identical permutation functions, if the coefficients are at the same distance $(L/2)$. Therefore, we can only consider coefficients $q_1 = 0, 1, \cdots, (L/2) - 1$ in polynomial searching, because the interleaver $\pi_1(x) = (px + p_2 x^2) \bmod L$ is the same as the interleaver $\pi(x) = \big((q_1 + L/2)x + (q_2 + L/2)x^2\big) \bmod L$, if $q_2 < L/2$, or as the interleaver described by the permutation $\pi(x) = \big((q_1 + L/2)x + (q_2 - L/2)x^2\big) \bmod L$, if $q_2 \geq L/2$. As the number of searched QPPs is halved, so is the search time, therefore speeding up the search process.

B. Maximum-Spread QPP Interleaver

Theorem 5: The following is an infinite sequence of QPPs that generate maximum-spread interleavers:

$$f(x) = (2^k - 1)\mathrm{x} + 2^{k+1}x^2 (\mathrm{mod} 2^{2k-1}) \quad \mathrm{k} = 1,2,3,\cdots \quad (26)$$

Strictly, we have QPP interleavers only when $k > 3$. The first observation is that for $k = 1$ and $k = 2$, the corresponding

QPPs $f(x)$ are immediately reduced to first-degree polynomials because the second-degree coefficient $f_2 \equiv 0\ (\mathrm{mod} N)$. We now show after some preliminaries that for $k = 3$, the QPP $f(x)$ is also reducible to a first-degree polynomial although $f_2 = 2^{k+1} = 16 \not\equiv (\mathrm{mod} N = 32)$.

Definition: A polynomial $z(x) (\mathrm{mod} N)$ that evaluates to zero for all x, i.e., $z(x) \equiv 0\ (\mathrm{mod} N)\ \forall x$ is called a *zero-polynomial*.

Proposition : Let N be an integer factorable as $N = pq$. The following is a zero-polynomial of degree p:

$$z(x) = mq \prod_{i=0}^{p-1} (x + k + i) (\mathrm{mod}\ N)\ \ \forall k, m \in \mathbb{Z}_N. \quad (27)$$

Proof: Exactly one of the numbers in the sequence $x + k + i$, $0 \leq i \leq p$ is congruent to 0 modulo p. Therefore, $z(x)$ mod N. Then $s(x) \equiv p(x) + z(x)$ (mod N), i.e., $s(x)$ and $p(x) + z(x)$ are equivalent functions modulo N.

Proof: This follows directly from the definition of a zero polynomial.

From Proposition 1, the following is a zero polynomial of second degree for $N = 32$:

$$z(x) = 16x(x+1) = 16x^2 + 16x \pmod{32} \quad (28)$$

Therefore, for $k = 3$, by adding $f(x)$ to $z(x)$ we obtain the equivalent first-degree polynomial

$$s(x) \equiv f(x) + z(x) = (16x^2 + 7x) + (16x^2 + 16x)$$
$$\equiv 23x \pmod{32} \quad (29)$$

For $k > 3$, the polynomials are not reducible to first-degree polynomials because they have a degree of nonlinearityζ, larger than 1 as explained in Section III (In fact, for k=1,2,3, we have $\zeta = 1$). The first six terms of maximum-spread QPPs that are not reducible to first-degree polynomials are shown in Table I. The last three columns of the Table I are the degrees of nonlinearity ζ, the refined degree of nonlinearity ζ', and the degree of shift-invariance $\in$.

The inverse functions $f^{-1}(x)$ are also provided in Table I. The closed-form expression for$f^{-1}(x)$ is

$$f^{-1}(x) = (-2^k - 1)x + 2^{k+1}x^2 (\mathrm{mod} 2^{2k-1}). \quad (29)$$

One easily verifies that

$$f\left(f^{-1}(x)\right) \equiv f^{-1}\left(f(x)\right) \equiv x \pmod{N}. \quad (30)$$

For general QPPs, we are not aware of a closed-form expression for the inverse functions. Further, not all QPPs have an inverse polynomial that is a QPP. However, if it exists, it is efficiently computed algebraically using the extended Euclidean algorithm [4]. It is easily verified that the necessary and sufficient condition for the existence of a QPP inverse [4] for the polynomials in Theorem 2 is satisfied.

IV. Simulation Parameters

The simulations were performed for a turbo code having the global coding rate of 1/3, without puncturing, over an AWGN (Additive White Gaussian Noise) channel, with a BPSK (Binary Phase Shift Keying) modulation.

The decoding algorithm is Max Log- MAP with iteration stopping criterion named LLR (Logarithm Likelihood Ratio) module. The maximum number of iteration is 12 .

The interleavers we have used are QPP interleaver, MS QPP interleaver and LS QPP interleaver for comparison. The data length is10^6, 2048 for a block data cutting.

Fig. 1 presents BER curves for the without coding and LTE QPP interleavers length 2048.

Fig. 2 presents BER curves for the LTE, MS and LS QPP interleavers for length 512. From Fig. 2 we note that BER for the MS interleaver is lower than for LS and LTE QPP interleavers.

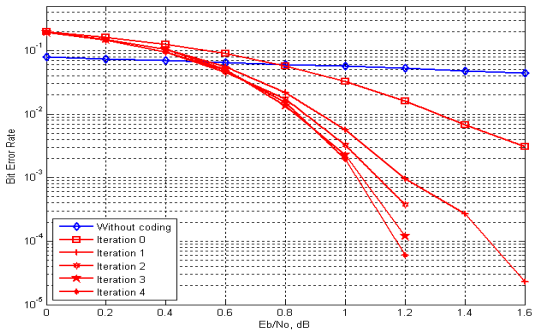

Fig. 1. BER curves for the interleaver length 2048

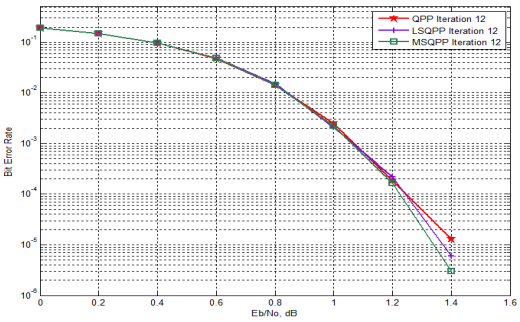

Fig. 2. BER curves for the interleaver length 512

V. Conclusion

To improve the performance and reduce the complexity, largest-spread and maximum-spread QPP interleavers are analyzed and the Max-Log MAP algorithm is used for Long Term Evolution (LTE) turbo codes in this paper. The simulated BER curves outlined in Figure 3 show that the performance of the MS-QPP interleaver is better compared to the LTE and LS QPP interleavers. Because of the simplicity in structure, MS-QPP interleaver is suitable for LTE standard.

References

[1] 3GPP TS 36.212 V10.3.0, 3rd Generation Partnership Project, Multiplexing and channel coding, 2011.

[2] O. Y. Takeshita, "Permutation Polynomial Interleavers: An Algebraic-Geometric Perspective," in *Proc. of Information Theory, IEEE Transactions on*, vol.53, no.6, pp.2116-2132, June 2007.

[3] J. Sun and O.Y. Takeshita, "Interleavers for turbo codes using permutation polynomials over integer rings,"in *Proc. of Information Theory, IEEE Transactions on* , vol.51, no.1, pp.101-119, Jan. 2005.

[4] J. Ryu and O. Y. Takeshita, "On quadratic inverses for quadratic permutation polynomials over integer rings,"in *Proc. of Information Theory, IEEE Transactions on*, vol. 52, no. 3, pp. 1254-1260, March 2006.