Journal of Zhejiang University SCIENCE A
ISSN 1009-3095 (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

A proof of maximum contention-free property of interleavers for Turbo codes using permutation polynomials over integer rings*

MA Xin-rui†1, XU You-yun[1,2], ZHANG Le[1]

([1]*Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*)

([2]*Institute of Communication Engineering, PLA University of Science and Technology, Nanjing 210007, China*)

†E-mail: maxinrui@sjtu.edu.cn

Received Feb. 26, 2006; revision accepted Apr. 13, 2006

Abstract: It is well known that interleavers play a critical role in Turbo coding/decoding schemes, and contention-free interleaver design has become a serious problem in the parallelization of Turbo decoding, which is indispensable to meet the demands for high throughput and low latency in next generation mobile communication systems. This paper unveils the fact that interleavers based on permutation polynomials modulo *N* are contention-free for every window size *W*, a factor of the interleaver length *N*, which, also called maximum contention-free interleavers.

Key words: Turbo codes, Integer ring, Permutation polynomial, Interleaver, Maximum contention-free (MCF)
doi:10.1631/jzus.2007.A0024 **Document code:** A **CLC number:** TN92

INTRODUCTION

In order to satisfy the high throughput and low latency requirements for next generation mobile communication systems, the parallelization of decoding of Turbo codes (Berrou *et al.*, 1993) has received remarkable attention. As the interleaving/deinterleaving operations may result in memory contentions, interleaver design (Dinoi and Benedetto, 2005; Dobkin *et al.*, 2005; Popovski *et al.*, 2004; Thul *et al.*, 2002) is the bottleneck of the parallel Turbo decoder. For certain interleaver length *N*, sub-window size *W* and processor number *M*, the contention-free interleaver must have the following condition (Nimbalker *et al.*, 2004) for both the interleaver and deinterleaver:

$$\lfloor \Pi(j+tW)/W \rfloor \neq \lfloor \Pi(j+vW)/W \rfloor, \qquad (1)$$

where $0\leq j<W$, $0\leq t$, $v<N/W=M$, $t\neq v$.

Recently, a new class of deterministic interleavers using permutation polynomials over integer rings was introduced (Sun and Takeshita, 2005; Ryu and Takeshita, 2005), where quadratic polynomials were paid much attention to, with these interleavers performing very well for 3G standard wireless transmission. Takeshita (2005) introduced the notion of maximum contention-free (MCF): an interleaver is maximum contention-free when it is contention-free for every window size *W* which is a factor of the interleaver length *N*. He showed that quadratic permutation polynomials generate MCF interleavers, and conjectured that interleavers based on permutation polynomials over integer rings are all MCF[1].

In this paper, we verify this conjecture and draw some important conclusions. In Section 2, we give a couple of lemmas and some known results about permutation polynomials modulo *N*. The main theorem, divided into 2 sub-theorems, is proved in Section 3. Finally, we conclude this paper in Section 4.

* Project (No. 60332030) supported by the National Natural Science Foundation of China

[1] After submitting the first draft of this paper, we noticed that Takeshita had already modified his paper and proved this conjecture. But in this paper, we use a different way to verify it in detail

OVERVIEW OF PERMUTATION POLYNOMIALS OVER Z_N

In this paper, all the summations and multiplications are modulo N and p is prime number unless explicitly stated.

First, let us give the definition of permutation polynomials over integer rings. Given an integer $N>2$, a polynomial $P(x)=a_1x+a_2x^2+\ldots+a_mx^m$ (mod N), where m, a_1, …, a_m are non-negative integers, is said to be a permutation polynomial over Z_N when $P(x)$ permutes $\{0, 1, \ldots, N-1\}$ (Hardy and Wright, 1979). Meanwhile, it is shown that the exclusion of the constant coefficient a_0 does not make the problem less general (Li, 2005; Sun and Takeshita, 2005). If $N=p^n$, there exists (Hardy and Wright, 1979):

Lemma 1 $P(x)$ is a permutation polynomial modulo p^n if and only if $P(x)$ is a permutation polynomial modulo p and $P'(x)\neq 0$ (mod p) for all integers $x\in\{0, 1, \ldots, p^n-1\}$.

In Lemma 1, n must be larger than 1. Since $P'(x)\neq 0$ (mod p) does not always hold for every integer $x\in\{0, 1, \ldots, p^n-1\}$, if $n=1$.

There is the general case (Sun and Takeshita, 2005; Li, 2005):

Lemma 2 For any $N=\prod_{i=1}^{k} p_i^{n_i}$, where p_i's are distinct prime numbers and $N_i=p_i^{n_i}$. $P(x)$ is a permutation polynomial modulo N if and only if $P(x)$ is a permutation polynomial modulo N_i, $\forall i$.

The Chinese Remainder Theorem, which was involved in the proof of Lemma 2, will also play a vital role in the proving of Theorem 1.1 presented in the next section.

PROOF OF THE MAIN THEOREM

Theorem 1 Permutation polynomials over integer rings generate maximum contention-free interleavers.

In group theory parlance, permutation polynomials modulo a given N form a finite group G under function composition in the form of $f(f(x))$, thus a permutation polynomial $f(x)$ has a finite order k, then obviously, its inverse function $f^{-1}(x)=f^{k-1}(x)$ is also a permutation polynomial and can be always found by this way. So we study $f(x)$ in the general sense, showing $f(x)$ modulo N always satisfies Eq.(1).

We divide the main theorem into two sub-theorems and prove them one by one.

Theorem 1.1 For any $N=\prod_{i=1}^{k} p_i^{n_i}$, where p_i's are distinct prime numbers and $N_i=p_i^{n_i}$, if permutation polynomial $f(x)=a_1x+a_2x^2+\ldots+a_mx^m$ modulo N_i generates MCF interleavers $\forall i$, then $f(x)$ modulo N generates MCF interleavers.

Proof Assume $f(x)$ modulo N does not generate MCF interleavers, then there exist some certain W, j, t, v such that

$$\lfloor [f(j+tW)(\operatorname{mod} N)]/W \rfloor = \lfloor [f(j+vW)(\operatorname{mod} N)]/W \rfloor,$$

where $0\leq j<W$, $t-v\neq 0$ (mod M). Let

$$W=\prod_{i=1}^{k} p_i^{d_i}=\prod_{i=1}^{k} W_i,$$
$$M=\prod_{i=1}^{k} p_i^{n_i-d_i}=\prod_{i=1}^{k} M_i.$$

Since $gcd(M_i, M_j)=1$, $\forall 1\leq i, j\leq k$, $i\neq j$, then there exists M_x such that $t-v\neq 0$ (mod M_x). Let $j_x=(j \bmod W_x)$, $t_x=(t \bmod M_x)$, $v_x=(v \bmod M_x)$, by the Chinese Remainder Theorem, we can easily conclude

$$\lfloor [f(j_x+t_xW_x)(\operatorname{mod} N_x)]/W_x \rfloor$$
$$=\lfloor [f(j_x+v_xW_x)(\operatorname{mod} N_x)]/W_x \rfloor,$$

which contradicts the assumption. Thus, $f(x)$ generates MCF interleavers over Z_N.

Now, we turn to discuss the $N_i=p_i^n$ case, where p_i is an any prime number.

Theorem 1.2 Permutation polynomial $f(x)=a_1x+a_2x^2+\ldots+a_mx^m$ modulo p^n generates maximum contention-free interleavers.

Proof Following the way in (Takeshita, 2005), let

$$Q_t=\lfloor f(j+tW)/W \rfloor \text{ and } Q_v=\lfloor f(j+vW)/W \rfloor,$$

then

$$f(j+tW)=Q_tW+[f(j+tW)(\text{mod W})],$$
$$f(j+vW)=Q_vW+[f(j+vW)(\text{mod } W)].$$

Let $W=p^{n_1}$, $M=p^{n_2}$, where $n_1>0$, $n_2>0$ and $n_1+n_2=n$. We should notice that there is no sense for $W=1$ or N.

Then we must prove that $Q_t\neq Q_v$ for any $0\leq j<W$ and $0\leq t$, $v<N/W=M$, $t\neq v$.

Assume $Q_t \neq Q_v$, then

$$Q_t - Q_v = \frac{1}{W}\{f(j+tW) - [f(j+tW)(\bmod\ W)] \qquad (2)$$
$$- f(j+vW) + [f(j+vW)(\bmod\ W)]\} = 0.$$

Observing that

$$f(j+tW)=f(j+vW)=a_1j+a_2j^2+\ldots+a_mj^m \ (\bmod\ W).$$

So Eq.(2) can be simplified as

$$\{[f(j+tW)-f(j+vW)]\ (\bmod\ N)\}/W$$
$$=\left\{\sum_{i=1}^{m} a_i[(j+tW)^i-(j+vW)^i](\bmod N)\right\}\Big/W,$$

that is

$$(t-v)\sum_{i=1}^{m}\sum_{k=1}^{i}\sum_{s=0}^{k-1} a_i\tbinom{i}{k} j^{i-k}W^{k-1}t^s v^{k-1-s} = 0 \ \ (\bmod M). \ (3)$$

By the assumption that $t \neq v$ (mod M), we can simplify Eq.(3) as

$$\sum_{i=1}^{m}\sum_{k=1}^{i}\sum_{s=0}^{k-1} a_i\tbinom{i}{k} j^{i-k}p^{n_1(k-1)}t^s v^{k-1-s} = 0 \ \ (\bmod p^{n_2}). \ (4)$$

Because the product of two non-zero numbers in a ring may be zero, so we must check when

$$\sum_{i=1}^{m}\sum_{k=1}^{i}\sum_{s=0}^{k-1} a_i\tbinom{i}{k} j^{i-k}W^{k-1}t^s v^{k-1-s} = 0 \ \ (\bmod \gamma), \quad (5)$$

where γ is factor of M and $\gamma>1$. If this is satisfied, then we must check if $t-v=M/\gamma$ (mod M). If yes, then Eq.(4) is satisfied.

Then, we show that Eq.(4) never holds. Eq.(4) can be expanded as

$$a_1+a_2[2j+p^{n_1}(t+v)]+a_3[3j^2+\ldots]+\ldots+a_m[mj^{m-1}+\ldots]$$
$$=0 \quad (\bmod\ p^{n_2}).$$

Pick out the first item of every a_i[], and put all the others together into a single term pX (there always exists factor p in each of them), then we get

$$a_1+2a_2j+3a_3j^2+\ldots+ma_mj^{m-1}+pX=0 \ (\bmod\ p^{n_2}), \ (6)$$

which is just

$$f'(j)+pX=0 \ (\bmod\ p^{n_2}).$$

Since $f(x)$ is permutation polynomial modulo N, by Lemma 1

$$f'(j)\neq 0 \ (\bmod p), \qquad (7)$$

then obviously

$$f'(j)\neq 0 \ (\bmod\ p^{n_2}) \text{ and } f'(j)+pX\neq 0 \ (\bmod\ p^{n_2}).$$

So we can conclude that Eq.(6) never holds.

Let us come back to Eq.(5), and consider the case of γ. Since we have shown that Eq.(7) never holds, then $f'(j)+pX=0$ (mod p) never holds, and $p|\gamma$, so Eq.(5) never holds, which completes the proof of Theorem 1.2.

With the verification of Theorems 1.1 and 1.2, the proof of Theorem 1 is completed.

CONCLUSION

In this paper, we focused on the maximum contention-free property of interleavers using permutation polynomials over integer rings. For any $N=\prod_{i=1}^{k}p_i^{n_i}$, where p_i's are distinct prime numbers and $N_i=p_i^{n_i}$, we first showed that if $\forall i$ permutation polynomial $f(x)$ modulo N_i generates MCF interleavers, then $f(x)$ modulo N generates MCF interleavers, and next, we verified that for any prime number p, permutation polynomial $f(x)$ modulo p^n generates MCF interleavers. In this way, we finally reached the conclusion that interleavers based on permutation polynomials over integer rings are all maximum contention-free.

References

Berrou, C., Glavieux, A., Thitimajshima, P., 1993. Near Shannon Limit Error-correcting Coding and Decoding: Turbo-codes. Proc. ICC'93. Geneva, p.1064-1070.

Dinoi, L., Benedetto, S., 2005. Variable-size interleaver design for parallel Turbo decoder architectures. *IEEE Trans. Commun.*, **53**(11):1833-1840. [doi:10.1109/TCOMM.2005.858685]

Dobkin, R., Peleg, M., Ginosar, R., 2005. Parallel interleaver design and VLSI architecture for low-latency MAP Turbo decoders. *IEEE Trans. VLSI Syst.*, **13**(4):427-438. [doi:10.1109/TVLSI.2004.842916]

Hardy, G.H., Wright, E.M., 1979. An Introduction to the Theory of Numbers. Oxford University Press.

Li, S.J., 2005. Permutation Polynomials Modulo *m*. Http://www.hooklee.com

Nimbalker, A., Blankenship, T.K., Classon, B., Fuja, T.E., Costello, D.J.Jr, 2004. Contention-free Interleavers. Proc. ISIT'04. Chicago, IL, p.54.

Popovski, P., Kocarev, L., Risteski, A., 2004. Design of flexible-length S-random interleaver for Turbo codes. *IEEE Commun. Lett.*, **8**(7):461-463. [doi:10.1109/LCOMM.2004.832737]

Ryu, J., Takeshita, O.Y., 2005. On Quadratic Inverses for Quadratic Permutation Polynomials Over Integer Rings. Http://arxiv.org/PS_cache/cs/pdf/0511/0511060.pdf

Sun, J., Takeshita, O.Y., 2005. Interleavers for Turbo codes using permutation polynomials over integer rings. *IEEE Trans. Inform. Theory*, **51**(1):101-119. [doi:10.1109/TIT.2004.839478]

Takeshita, O.Y., 2005. On Maximum Contention-free Interleavers and Permutation Polynomials Over Integer Rings. Http://arxiv.org/PS_cache/cs/pdf/0506/0506093.pdf

Thul, M.J., Gilbert, F., Wehn, N., 2002. Optimized Concurrent Interleaving Architecture for High-throughput Turbo-decoding. Proc. ICECS'02, **3**:1099-1102.