Applied Mathematics & Information Sciences
An International Journal

On Dispersion and Nonlinearity Degree of QPP Interleavers

Lucian Trifina, Daniela Tarniceriu and Valeriu Munteanu

Gheorghe Asachi Technical University of Iasi, Faculty of Electronics, Telecommunications and Information Technology, Iasi, Romania

Received: Feb. 24, 2012; Revised Apr. 28, 2012; Accepted 28 Apr. 2012
Published online: 1 Sep. 2012

Abstract: This paper shows a link between the dispersion and the nonlinearity degree of QPP (quadratic permutation polynomial) interleavers. An upper bound for the dispersion of QPP interleavers is derived. This upper bound is computed very simple, only depending on the coefficient of x^2 of the polynomial and of the length of interleaver. The comparison with the real dispersion of QPP interleavers given by Takeshita in [1] leads to insignificant difference. Searching of QPP interleavers based on a metric including upper bound of dispersion and D parameter is equivalent with that based on Ω metric.

Keywords: Dispersion, nonlinearity degree, randomness, QPP interleaver.

1. Introduction

QPP interleavers are characterized by [1]: completely algebraic structure, efficient implementation (high speed and low memory requirements) and very good performances. A QPP interleaver of length L is defined in [1], [2], [3], [4] as:

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

where q_1 and q_2 are chosen so that the quadratic polynomial in 1 is a permutation polynomial and q_0 only determines a shift of the permutation elements.

The randomness analysis of these interleavers considering the nonlinearity degree was performed in [1] and associates each interleaver defined by permutation $\pi(\cdot)$, with a geometrical representation called interleaver-code by the transformation $\Phi : \pi(i) \rightarrow F(i)$, where $F(i) = \{(i, \pi(i)) | i \in I\}$, and $I = \{0, 1, \ldots, L-1\}$ is the set of indices corresponding to the bits to be interleaved. The pair $(i, \pi(i))$ is called point and a set of points in the interleaver/code, which are equivalent under the action of a isometry group, is called orbit. The isometries of interest for turbo code distances are translations of a point in the interleaver-code, i.e. the transformation that circularly shifts a point with k_0 units to the right along dimension i and with k_1 units up along dimension:

$$A(k_0, k_1) : (i, \pi(i)) \rightarrow (i + k_0, \pi(i) + k_1), k_0, k_1 \in I \quad (2)$$

In order for the translation to lead to a point in the interleaver-code, we have

$$\pi(i + k_0) = \pi(i) + k_1 \quad (3)$$

Takeshita defines *the degree of nonlinearity* ζ as the number of distinct orbits. Thereby, the degree of nonlinearity is the number of distinct solutions of Equation (3). It is shown in [1] that the degree of nonlinearity ζ of a QPP interleaver is given by

$$\zeta = L / gcd(2q_2, L) \quad (4)$$

where gcd means the greatest common divisor.

Usually, the dispersion is used as a measure of the interleaver randomness. It is defined as the number of distinct displacement vectors (Δ_x, Δ_y) [5]:

$$\Gamma = \Big| \{ (\Delta_x, \Delta_y) \in Z^2 | \Delta_x = j - i, \Delta_y = \pi(j) - \pi(i), 0 \leq i < j \leq L-1 \} \Big| \quad (5)$$

The normalized dispersion is the value of Γ normalized to its maximum value, i.e.:

$$\gamma = \frac{2\Gamma}{L(L-1)} \quad (6)$$

[*] Corresponding author: e-mail: luciant@etti.tuiasi.ro

The dispersion of an interleaver influences the multiplicities of the low weight code words, therefore a high dispersion is desirable [5]. However, QPP interleavers have small dispersion and still lead to good performances, if they are properly chosen.

In this paper we show that a very close upper bound of a QPP interleaver exists. As the nonlinearity degree, it only depends on the coefficient q_2 and on the interleaver length (formulas (13)-(14)). The paper aims to perform a theoretical analysis of QPP interleaver randomization, establishing a relationship between the two quantities known and used for this: dispersion (more exactly, a very tight upper bound of it) and the degree of nonlinearity.

In Section II an upper bound for the dispersion of QPP interleavers is established and it is compared with the real dispersion for QPP interleavers from [1]. Section III concludes the paper.

2. An Upper Bound for a QPP Interleaver Dispersion

In order to establish an upper bound for the dispersion of a QPP interleaver we have to compute the number of distinct values $\Delta_y = \pi(x + \Delta_x) - \pi(x)$ for each value $\Delta_x = 1, \dots, L-1$, and $x = 0, \dots, L-1-\Delta_x$. For a QPP interleaver, it follows:

$$\Delta_y = (q_1\Delta_x + q_2\Delta_x^2 + 2q_2\Delta_x x) \bmod L \tag{7}$$

For negative values, Δ_y is computed as

$$\Delta_y = (q_1\Delta_x + q_2\Delta_x^2 + 2q_2\Delta_x x) \bmod L - L \tag{8}$$

Since

$$\Delta_{y0} = (q_1\Delta_x + q_2\Delta_x^2) \bmod L \tag{9}$$

is constant for a fixed Δ_x, we should only find the number of distinct values in the set $\left\{(2q_2\Delta_x x) \bmod L | x = 0, \dots, L-1-\Delta_x\right\}$. We denote

$$\Delta_{y_1} = (2q_2\Delta_x)\%L \tag{10}$$

where

$$p\%L = \begin{cases} p \bmod L, \text{when } p \neq kL, \\ L, \text{when } p = kL. \end{cases} \tag{11}$$

So, the number of different values of (7) or (8) depends on the number of solutions of the congruence

$$\Delta_{y_1} \cdot x = \beta \bmod L, \text{with } \beta \text{ constant} \tag{12}$$

The solutions of this congruence are presented in theorem 2.8 given in [4]. The equation has $d = gcd(\Delta_{y_1}, L)$ solutions, if $d \mid \beta$ (i.e. d divides β).

If x_0 is a solution of equation 12, then $x_0 + L/d$, $x_0 + 2L/d$,..., $x_0 + (d-1)L/d$ are also solutions of this equation. Thus, the elements in the set $\left\{(2q_2\Delta_x x) \bmod L | x = 0, \dots, L-1-\Delta_x\right\}$ repeat with period L/d.

Since Δ_y is given by both (7) and (8), it means that an upper bound for the number of distinct values of Δ_y for constant Δ_x is equal to $min(2L/gcd(\Delta_{y_1}, L), L - \Delta_x)$ and an upper bound on the dispersion is:

$$\text{UB}(\Gamma) = \sum_{\Delta_x=1}^{L-1} min(2L/gcd(\Delta_{y_1}, L), L - \Delta_x) \tag{13}$$

The upper bound on the normalized dispersion, UB(γ), is calculated using Equation (6):

$$\text{UB}(\gamma) = \frac{2}{L(L-1)} \cdot \text{UB}(\Gamma) \tag{14}$$

For $\Delta_x = 1$, we have

$$\Delta_{y_1} = (2q_2)\%L = \begin{cases} 2q_2, \text{when } 2q_2 < L, \\ 2q_2 - L, \text{when } 2q_2 > L, \\ L, \text{when } 2q_2 = L. \end{cases} \tag{15}$$

Thus, in this case,

$$gcd(\Delta_{y_1}, L) = gcd(2q_2, L) \tag{16}$$

It follows that the connection between the upper bound of dispersion (13) and the nonlinearity degree in (4) is given by

$$\begin{aligned} \text{UB}(\Gamma) &= min(2 \cdot \zeta, L-1) + \\ &+ \sum_{\Delta_x=2}^{L-1} min(2L/gcd(\Delta_{y_1}, L), L - \Delta_x) \end{aligned} \tag{17}$$

The upper bound on normalized dispersion for the QPP interleaver given in Equation (14) for large lengths is calculated much easier than the normalized dispersion value, and is very close to it.

To highlight this aspect, Table 1 gives the real dispersion and its upper bound for interleavers with the largest spread (Largest Spread QPP) [1].

Table 2 also gives the real dispersion and its upper bound for QPP interleavers with the largest value of metric Ω' (Ω'-QPP) [1]. Only constant free polynomials were kept. Among polynomials repeated in both tables, only those in the second table were held.

From Tables 1 and 2 we notice the efficient approximation of the dispersion of a QPP interleaver with the proposed upper bound.

From Table 2 we notice that the dispersion of Ω'-QPP interleavers is very small, but higher than that of the largest spread interleavers. This happens because the metric Ω' takes into account the nonlinearity degree, which is also a measure of randomness.

However, the performance of Ω'-QPP interleavers for medium and large lengths is very good, as shown in [1] by simulations. This fact shows that the randomness of the interleaver is important.

Table 1 QPP Interleavers with the largest spread.

L	$\pi(x)$	γ	UB(γ)
128	$15x + 32x^2$	0.04540	0.04651
160	$19x + 40x^2$	0.03640	0.03726
400	$17x + 100x^2$	0.01474	0.01496
512	$31x + 64x^2$	0.02100	0.02137
640	$39x + 80x^2$	0.01683	0.01712
752	$31x + 188x^2$	0.00790	0.00797
1024	$123x + 256x^2$	0.00583	0.00586
1504	$183x + 376x^2$	0.00397	0.00399
1600	$49x + 100x^2$	0.01319	0.01339
2048	$63x + 128x^2$	0.01033	0.01047
2560	$79x + 160x^2$	0.00828	0.00838
3200	$79x + 800x^2$	0.00187	0.00187
4096	$173x + 1024x^2$	0.00146	0.00147
8192	$127x + 256x^2$	0.00515	0.00521

It should be noted that if we want to search QPP interleavers with good error-rate performance, we should maximize the UB$(\Gamma) \cdot \ln(D)$ product, with the parameter D under the same conditions as in [1]. Considering relations (17), (4) and (10), which indicate that UB(Γ) and ζ depend only on the length L and the coefficient q_2, maximizing this product for a certain length will lead to the same interleavers as those with the best $\Omega = \zeta \cdot \ln(D)$. Therefore, relation (17) shows the equivalence from this point of view of the upper bound of the dispersion and the degree of nonlinearity.

3. Conclusion

This paper addresses the algebraic QPP interleavers from the viewpoint of dispersion and nonlinearity degree.

An upper bound for the dispersion of QPP interleavers has been computed and its relationship with the nonlinearity degree was established. This upper bound is very close to the real dispersion for proposed interleavers and, as the nonlinearity degree, only depends on the q_2 coefficient and on the interleaver length. In this way the link between the dispersion and the nonlinearity degree for a QPP interleaver is shown.

The search of QPP interleavers by maximizing the UB$(\Gamma)\cdot\ln(D)$ metric is equivalent to maximizing the $\Omega = \zeta \cdot \ln(D)$ metric from [1], showing the equivalence from this point view of the upper bound of the dispersion and the degree of nonlinearity.

Acknowledgement

The authors would like to thank the anonymous reviewers for their helpful comments and suggestions.

Table 2 QPP Interleavers with the best Ω'.

L	$\pi(x)$	γ	UB(γ)
40	$x + 10x^2$	0.12308	0.14615
80	$9x + 20x^2$	0.07152	0.07405
128	$7x + 16x^2$	0.07948	0.08415
160	$9x + 20x^2$	0.06462	0.06761
256	$15x + 32x^2$	0.04133	0.04253
320	$19x + 40x^2$	0.03325	0.03409
400	$7x + 40x^2$	0.04051	0.04158
408	$25x + 102x^2$	0.01450	0.01467
512	$15x + 32x^2$	0.04022	0.04151
640	$19x + 40x^2$	0.03243	0.03328
752	$23x + 94x^2$	0.01437	0.01458
800	$17x + 80x^2$	0.02052	0.02090
1024	$31x + 64x^2$	0.02050	0.02088
1280	$39x + 80x^2$	0.01645	0.01672
1504	$23x + 94x^2$	0.01401	0.01424
1600	$17x + 80x^2$	0.01542	0.01568
2048	$31x + 64x^2$	0.02035	0.02074
2560	$39x + 80x^2$	0.01633	0.01662
3200	$17x + 80x^2$	0.01412	0.01437
4096	$31x + 64x^2$	0.02029	0.02071
5472	$77x + 114x^2$	0.00896	0.00914
8192	$31x + 64x^2$	0.02028	0.02070

References

[1] O.Y. Takeshita, "Polynomial Interleavers: An Algebraic-Geometric Perspective", IEEE Transactions on Information Theory **53**, 6 (2007).

[2] J. Sun and O.Y. Takeshita, "Interleavers for Turbo Codes Using Permutation Polynomial over Integers Rings", IEEE Transactions on Information Theory **51**, 1 (2005).

[3] O.Y. Takeshita, "On Maximum Contention-Free Interleavers and Permutation Polynomials Over Integers Rings", IEEE Transactions on Information Theory **52**, 3 (2006).

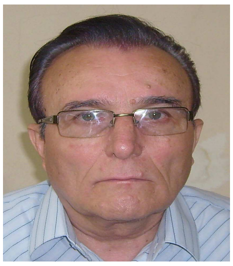
[4] J. Ryu and O.Y. Takeshita, "On Quadratic Inverses for Quadratic Permutation Polynomials Over Integers Rings", IEEE Transactions on Information Theory **52**, 3 (2006).

[5] C. Heegard and S.B. Wicker, Turbo Coding (Kluwer Academic Publishers, Dordrecht, the Netherlands, 1999).

Lucian Trifina was born in Falticeni, Romania in 1976. He obtained his B.Sc. degree in Electronics and Telecommunications engineering from the "Gheorghe Asachi" Technical University of Iasi, Romania, in 2002. He received his M.Sc. degree in Modern Techniques for Signal Processing from the "Gheorghe Asachi" Technical University of Iasi, Romania, in 2003. In October 2007 he received the Ph.D. degree, with the doctoral thesis "Turbo

Codes - Theoretical and Practical Aspects”. Currently he works at the Technical University Gh. Asachi of Iasi, Faculty of Electronics, Telecommunications and Information Technology, Telecommunications Department as a teaching assistant.

Daniela Tarniceriu was born in Iasi, Romania in 1960. She received the M.Sc. degree in 1983 in Electrical Engineering and the Ph.D. degree in Electronics and Telecommunications in 1997 from the Technical University “Gheorghe Asachi” of Iasi, Romania. In 1991 she joined the Communications Department of the Faculty of Electronics and Telecommunications of Iasi and received the title of Professor in 2000. From 2005 she was vice-dean of the Faculty and from 2008 she is the head of the Telecommunications Department. Her research interests currently include digital signal processing and coding theory with emphasis on turbo coding and wireless systems.



Valeriu Munteanu was born in Romania in 1941. He received the M.Sc. degree in 1965 in Electrical Engineering and the Ph.D. degree in Electronics and Telecommunications in 1972 from the “Gheorghe Asachi” Technical University of Iasi, Romania. In 1965 he joined the Communications Department of the Faculty of Electronics and Telecommunications, “Gheorghe Asachi” Technical University of Iasi and received the title of Professor in 1990. His research interests currently is Information Theory.