

## QPP Interleavers with Dispersion Maximization

Lucian Trifina, Ana-Mirela Rotopănescu, Lucian Ghercă, Bogdan Lupu<sup>1</sup>

**Abstract - Four types of QPP (Quadratic Permutation Polynomial) interleavers for turbo codes that maximize the dispersion are proposed. These interleavers lead to superior performances, compared to the interleavers proposed by Takeshita for some lengths and some component codes of turbo codes.**

**Keywords:** QPP interleaver, dispersion, turbo codes.

### I. INTRODUCTION

Polynomial interleavers are the most recent published interleavers having the following advantages [1]: remarkable performance, perfect algebraically structure and efficient implementation (high speed and little memory requirements).

A QPP interleaver of length  $L$  is defined in [1], [2], [3], [4] as:

$$\pi(x) = (q_0 + q_1x + q_2x^2) \bmod L, x \in \overline{0, L-1} \quad (1)$$

where  $q_1, q_2$  are chosen so that the quadratic polynomial from (1) is a permutation polynomial and  $q_0$  determines only a shift of the permutation elements. We note the set  $\square_L = \{0, 1, \dots, L-1\}$ . Then

the permutation function is  $\pi: \square_L \rightarrow \square_L$ .

The randomizing analysis of these interleavers was made with nonlinearity degree [1]. This is achieved by measuring the number of distinct orbits (a set of points) of the action of an isometry group on the interleaver code, that is, on the points  $(x, \pi(x))$ . It is demonstrated that the nonlinearity degree of a QPP interleaver is given by the relation:

$$\zeta = L / \text{gcd}(2q_2, L) \quad (2)$$

“gcd” meaning „greatest common divisor”.

The refined nonlinearity degree  $\zeta'$  is given by the number of distinct elements of set  $\{q_2x^2 \bmod L, x=0, 1, \dots, \zeta-1\}$ .

Takeshita states in [1] that the first spectral line with high multiplicity in distances spectrum of a turbo code with a QPP interleaver is very close to the degree of shift invariance  $\varepsilon$ , defined as the size of the orbits. The relation between  $\varepsilon$  and  $\zeta$  is the following:

$$\zeta = L / \varepsilon \quad (3)$$

Spread factor ( $D$  parameter) is defined by relation:

$$D = \min_{\substack{i \neq j \\ i, j \in \square_L}} \{\delta_L(p_i, p_j)\}, \quad (4)$$

where  $\delta_L(p_i, p_j)$  is Lee metric between the points

$$p_i = (i, \pi(i)) \text{ and } p_j = (j, \pi(j)) \text{ [5]:}$$

$$\delta_L(p_i, p_j) = |i - j|_L + |\pi(i) - \pi(j)|_L. \quad (5)$$

The notation  $|i - j|_L$  means:

$$|i - j|_L = \min\{(i - j) \bmod L, (j - i) \bmod L\}. \quad (6)$$

[1] gives the quadratic polynomials which have the largest spread ( $D$  parameter) and also which maximize  $\Omega'$  metric defined as:

$$\Omega' = \zeta' \cdot \ln(D), \quad (7)$$

where  $\zeta'$  was previously defined.

An older definition of spread is given through  $S$  parameter [6], which is the maximum value of  $S$  so that:  $(\forall) i \neq j$ , with  $i, j \in \square_L$ , the next inequalities are maintained:

$$|i - j| \leq S \Rightarrow |\pi(i) - \pi(j)| > S \quad (8)$$

To avoid the edge effects of trellis termination the corner merit is maximized. The corner merit is defined by relation:

$$C = \min_{x \in \square_L} \delta((L-1, L-1), (x, \pi(x))), \quad (9)$$

where  $\delta(p_i, p_j)$  is given by relation:

$$\delta(p_i, p_j) = |i - j| + |\pi(i) - \pi(j)|. \quad (10)$$

In this paper the randomizing analysis is made using the QPP interleaver dispersion.

The dispersion of an interleaver is given by the number of distinct displacement vectors  $(\Delta_x, \Delta_y)$  [7]:

$$\Gamma = \left| \{(\Delta_x, \Delta_y) \in Z^2 \mid \Delta_x = j - i, \Delta_y = \pi(j) - \pi(i), 0 \leq i < j \leq L-1\} \right|. \quad (11)$$

The normalized dispersion is the value of  $\Gamma$  normalized to its maximum value, i.e.:

$$\gamma = \frac{2\Gamma}{L(L-1)} \quad (12)$$

The dispersion of an interleaver influences the multiplicities of the low weight code words, therefore a high dispersion is desirable. This desideratum was described in [8], [9] through the proposal of some interleavers with a high dispersion.

<sup>1</sup>Electronics and Telecommunications Faculty, Telecommunications Department, Bd. Carol I, no. 11, Iasi, Romania, e-mail luciant@zeta.etc.tuiasi.ro

This paper is structured as follows: in section II, four QPP interleavers are proposed that aim the maximization of the dispersion; section III presents the simulation results for the proposed interleavers for two lengths (128 and 512) compared to those proposed by Takeshita in [1]. Section IV summarizes the main results of the paper.

## II. QPP INTERLEAVERS WITH DISPERSION MAXIMIZATION

In this section we consider the dispersion parameter into consideration to further improve the performance of the interleavers given in [1]. The goal is to select interleavers with maximized dispersion following the criteria:

a) Among the interleavers with maximum spread ( $D$  parameter) the ones with maximum dispersion having the coefficient  $q_0=0$  are chosen, meaning maximum spread maximum dispersion (noted with MS-QPP-MG, where G is for Gamma, i.e. dispersion);

b) From the interleavers with maximum spread and dispersion, firstly there are selected the ones for which the corner merit is maximized through  $q_0$  coefficient. Secondly, only the interleavers with the  $q_0$  coefficients that maximize the dispersion are kept from the ones selected at the first step, that is maximum spread – maximum dispersion – maximum corner merit – maximum dispersion (noted with MS-QPP-MG-MC-MG);

c) Among the interleavers with the best  $\Omega'$  parameter, the ones with the largest dispersion are selected, for which the corner merit is maximized through the  $q_0$  coefficient, keeping then only the  $q_0$  coefficients that maximize the dispersion from the ones previously calculated, similar to interleavers in b), meaning maximum  $\Omega'$  – maximum dispersion – maximum corner merit – maximum dispersion (noted with  $\Omega'^2$ -QPP-MG-MC-MG).

d) A search that maximizes the  $S$  parameter and the dispersion, followed by the maximization of the corner merit factor and then again the dispersion for the  $q_0$  coefficient is proposed, meaning the maximum  $S$  parameter – maximum dispersion – maximum corner merit – maximum dispersion, noted with MSP-QPP-MG-MC-MG. The  $S$  parameter defined in [6] for the interleaver proposed by Takeshita does not necessarily have the maximum value.

Tables 1, 2 and 3 give the polynomials that are irreducible to polynomials of first degree (i.e. with nonlinearity degree  $\zeta > 1$ ), determined following the above description for different lengths of interleavers. Table 1 shows the value of the dispersion for QPP interleavers obtained following the instructions in section b) in two cases: with  $q_0=0$  and with  $q_0$  resulted after corner merit factor maximization. It also shows the maximum spread factor  $D$ , the initial nonlinear degree ( $\zeta$ ) and the refined one ( $\zeta'$ ). If more polynomials of the same type are found, we choose firstly the ones with the smallest  $q_1$  and then the ones with the smallest  $q_2$ . The choice of  $q_0$  is made by the

dispersion maximization after corner merit for all the polynomials with determined  $q_0=0$ . Again, if more than one value is found, the smallest one is chosen.

Table 2 gives the polynomials searched as shown in section c), together with its spread factor  $D$  and the initial nonlinear degree ( $\zeta$ ) and the refined one ( $\zeta'$ ).

Table 3 shows the polynomials with maximized  $S$  parameter, as shown in section d), together with its spread factor  $D$  and the initial nonlinear degree ( $\zeta$ ) and the refined one ( $\zeta'$ ).

Table 1: MS-QPP-MG-MC-MG Interleavers

$L$	$q_0$	$\pi(x)$	$\gamma$ (with $q_0=0$ )	$\gamma$ (with $q_0>0$ )	$D^{\max}$ ( $L$ )	$\zeta$	$\zeta'$
40	38	$19x+30x^2$	0.13846	0.12308	4	2	2
80	77	$31x+60x^2$	0.07215	0.07152	10	2	2
128	119	$49x+96x^2$	0.04552	0.04503	16	2	2
160	149	$21x+40x^2$	0.03656	0.03616	16	2	2
256	245	$81x+160x^2$	0.04136	0.04136	16	4	3
320	309	$21x+200x^2$	0.03327	0.03321	20	4	3
400	377	$183x+300x^2$	0.01483	0.01476	20	2	2
408	387	$155x+306x^2$	0.01454	0.01447	24	2	2
512	496	$31x+64x^2$	0.02100	0.02095	32	4	3
640	624	$39x+400x^2$	0.01686	0.01680	32	4	3
752	727	$285x+564x^2$	0.00792	0.00789	32	2	2
800	775	$143x+560x^2$	0.02058	0.02052	32	5	5
1024	1005	$333x+768x^2$	0.00583	0.00582	34	2	2

Table 2:  $\Omega'^2$ -QPP-MG-MC-MG Interleavers

$L$	$q_0$	$\pi(x)$	$\gamma$ (with $q_0=0$ )	$\gamma$ (with $q_0>0$ )	$D$	$\zeta$	$\zeta'$
40	38	$19x+30x^2$	0.13846	0.12308	4	2	2
80	77	$31x+60x^2$	0.07215	0.07152	10	2	2
128	122	$57x+80x^2$	0.08046	0.08009	8	4	3
160	142	$31x+140x^2$	0.06502	0.06337	10	4	3
256	245	$81x+160x^2$	0.04136	0.04136	16	4	3
320	309	$21x+200x^2$	0.03327	0.03321	20	4	3
400	375	$7x+280x^2$	0.04056	0.04031	16	5	5
408	387	$155x+306x^2$	0.01454	0.01447	24	2	2
512	480	$79x+352x^2$	0.04035	0.04020	16	8	4
640	89	$181x+360x^2$	0.03247	0.03243	20	8	4
752	714	$353x+470x^2$	0.01440	0.01435	26	4	3
800	775	$143x+560x^2$	0.02058	0.02052	32	5	5
1024	992	$223x+960x^2$	0.02051	0.02046	32	8	4

Table 3: MSP-QPP-MG-MC-MG Interleavers

$L$	$q_0$	$\pi(x)$	$\gamma$ (with $q_0=0$ )	$\gamma$ (with $q_0>0$ )	$S$	$D$	$\zeta$	$\zeta'$
40	37	$17x+30x^2$	0.13846	0.13718	2	4	2	2
80	77	$31x+60x^2$	0.07215	0.07152	6	10	2	2
128	119	$49x+96x^2$	0.04552	0.04503	7	16	2	2
160	151	$31x+40x^2$	0.03664	0.03601	8	10	2	2
256	232	$29x+64x^2$	0.02304	0.02279	10	12	2	2
320	307	$43x+80x^2$	0.01850	0.01836	12	14	2	2
400	377	$183x+300x^2$	0.01483	0.01476	14	20	2	2
408	387	$155x+306x^2$	0.01454	0.01447	15	24	2	2
512	497	$235x+384x^2$	0.01160	0.01155	18	26	2	2
640	616	$77x+160x^2$	0.00930	0.00927	22	28	2	2
752	727	$285x+564x^2$	0.00792	0.00789	23	32	2	2
800	769	$303x+600x^2$	0.00745	0.00742	23	32	2	2
1024	1000	$125x+256x^2$	0.00583	0.00581	23	32	2	2

## III. NUMERIC RESULTS

The interleaves proposed in this paper are compared to those in [1] by computing the distances spectrums. The interleavers of length 128 and 512 are obtained by means of methods described in section III. The

post-interleaver trellis termination method [6], [11] has been used. The total weights of information sequences which lead to specific distances are also computed. The component codes of turbo codes are those used in [1]: the code with 8 states and generator matrix (in octal form)  $G=[1, 15/13]$ , and the code with 16 states with  $G=[1, 35/23]$ .

As shown in table 4 the first 20 terms of distance spectra for interleavers of length 128 were determined. For the interleavers of length 512 present in table 5, the maximum computed distance has been limited to a maximum value of 45, knowing the fact that above this value the Garelo method [11] is time consuming. The minimum distance and the first spectral line with a high multiplicity are highlighted in the tables.

To underline the performances of the interleavers proposed in this paper, the simulated and asymptotic bit error rate (BER) and the frame error rate (FER) curves are given for an AWGN (Additive White Gaussian Noise) channel in the figures 1 and 2. For the 8 states code, the curves are obtained by simulation in 0-3 dB signal to noise ratios (SNR) domain while for the 3-4 dB domain, the asymptotic curves are obtained with distances spectra from tables 4. For the 16 states code, the curves are obtained by simulation in 0-2 dB SNR domain and continued by asymptotic curves in 2-3 dB SNR domain obtained with distances spectra from tables 5. On the same diagram were also drawn the curves of interleavers in [1].

Figure 1 illustrates the superior performances of some proposed interleavers of length 128 in the asymptotic curves domain for 8 states code, while figure 2 illustrates the superior performances of some proposed interleavers of length 512 in the asymptotic curves domain, as well as in the simulated domain. This behavior is explained by the fact that for smaller lengths, the difference between the simulated curves is noticeable only at large SNR values where error rates are small. For large lengths, due to the gain effect of the interleaver, the difference becomes noticeable at smaller SNR values.

Looking at tables 4 and 5 and at figures 1 and 2 we observe that the same interleavers, but with different component codes lead to different performances.

The maximization of the dispersion over that of the spread factor leads to easy benefits (the minimum distance is larger or the distance spectrum is better).

For length of 512 we obtained the same QPP interleaver as the one from [1]. The maximization of the corner merit leads to an improvement only for

length of 128.

The maximization of the dispersion over the  $\Omega'$  parameter leads to better performance, only for 16 states component code. However the maximization of corner merit doesn't bring more benefits. Therefore we also give the performance of the interleaver without the corner merit maximization.

The maximization of the  $S$  parameter, together with that of the dispersion, followed by the maximization of the corner merit factor, and again of the dispersion leads to the biggest minimum distance for the 16 states code of length 512. This could be due to fact that the obtained  $S$  parameter (18) is larger than the one of MS-QPP-MG-MC-MG interleaver (15). For length of 128 we obtained the same interleaver as in the case of the MS-QPP-MG-MC-MG interleaver.

The minimum distances for the obtained interleavers are smaller than the ones from [12], but there a dual termination was used. Also in contrast with [12] the interleavers proposed here are generic and not optimized for a specific component code.

#### IV. CONCLUSIONS

This paper analyzed the influence of dispersion on the performances of the QPP interleavers, when they are part of turbo codes.

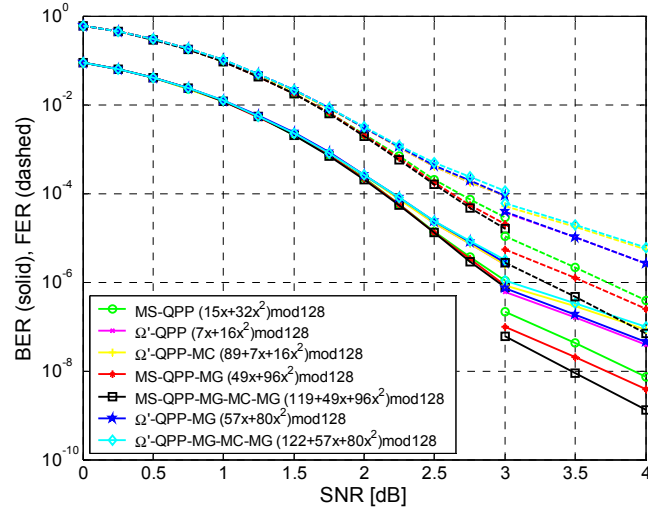
Unlike the maximization of the following parameters: the spread factor ( $D$  parameter),  $\Omega'$  parameter and corner merit, used by Takeshita in [1], we have performed additional searches including the dispersion maximization on four types of QPP interleavers. A number of QPP interleavers were also proposed, selected after the maximization of the  $S$  parameter, defined in [6].

The simulation results confirm that by extra dispersion maximization, superior performances are obtained compared to a number of interleavers proposed by Takeshita in [1]. Superior performances are obtained in the following cases: MS-QPP-MG-MC-MG and MS-QPP-MG interleavers of length 128 compared to MS-QPP interleaver for 8 states code and the one with 16 states and  $\Omega'$ -QPP-MG interleaver compared to  $\Omega'$ -QPP interleaver of length 512 for 16 states code, respectively. Additionally, the simulation results point out that the  $S$  parameter maximization leads to the best performances for certain lengths and component codes (for example, 8 states code and the interleaver of 128 length and 16 states code and the interleaver of 512 length).

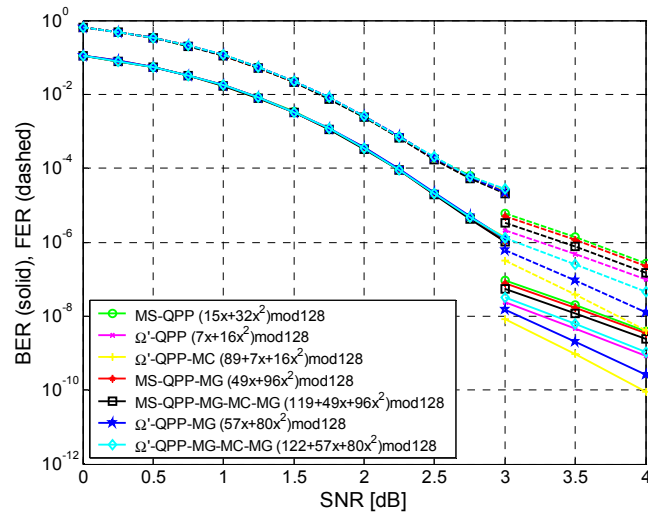
Table 4: Length  $L=128$

8-state																				
MS-QPP-MG $\pi(x)=49x+96x^2 \pmod{L} \epsilon=64$																				
$i$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$d_i$	<b>16</b>	18	19	20	21	22	23	24	<b>25</b>	26	27	28	29	30	31	32	33	34	35	36
$N_i$	<b>1</b>	1	1	1	2	2	6	7	<b>63</b>	17	29	89	52	234	464	472	857	1628	1963	2693
$w_i$	<b>2</b>	2	1	2	6	4	16	20	<b>197</b>	60	93	342	186	1220	2222	2538	4875	9784	11149	16790
MS-QPP-MG-MC-MG $\pi(x)=119+49x+96x^2 \pmod{L} \epsilon=64$																				
$i$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$d_i$	<b>18</b>	20	21	22	23	24	<b>25</b>	26	27	28	29	30	31	32	33	34	35	36	37	38
$N_i$	<b>1</b>	3	2	1	8	5	<b>63</b>	17	27	86	49	234	444	456	860	1604	1901	2612	5410	7674



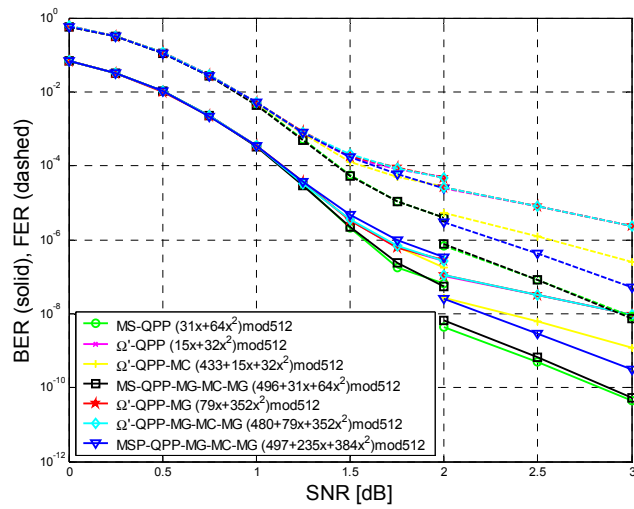


a)

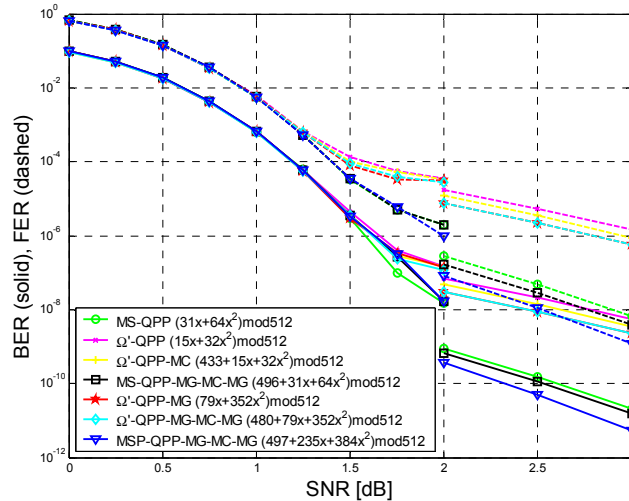


b)

Fig. 1. Simulated and asymptotic BER (FER) curves for interleavers of  $L=128$  length and code with a) 8 states; b) 16 states



a)



b)

Fig. 2. Simulated and asymptotic BER (FER) curves for interleavers of  $L=512$  length and code with a) 8 states; b) 16 states

## REFERENCES

- [1] Takeshita, Y. Oscar, "Permutation Polynomial Interleavers: An Algebraic-Geometric Perspective", *IEEE Transactions on Information Theory*, Vol. 53, No. 6, pp. 2116-2132, June 2007
- [2] Sun, Jing and Takeshita, Y. Oscar, "Interleavers for Turbo Codes Using Permutation Polynomial Over Integers Rings", *IEEE Transactions on Information Theory*, Vol. 51, No. 1, pp. 101-119, January 2005
- [3] Takeshita, Y. Oscar, "On Maximum Contention-Free Interleavers and Permutation Polynomials Over Integers Rings", *IEEE Transactions on Information Theory*, Vol. 52, No. 3, pp. 1249-1253, March 2006
- [4] Ryu, Jonghoon and Takeshita, Y. Oscar, "On Quadratic Inverses for Quadratic Permutation Polynomials Over Integers Rings", *IEEE Transactions on Information Theory*, Vol. 52, No. 3, pp. 1254-1260, March 2006
- [5] Lee, C.Y., "Some properties of nonbinary error-correcting codes", *IRE Transactions on Information Theory*, Vol. IT-4, No. 2, pp. 77-82, June 1958
- [6] Divsalar, D. and Pollara, F., "Turbo Codes for PCS Applications," *Proceedings of ICC 1995*, Seattle, WA., pp. 54-59, June 1995
- [7] Heegard, C. and Wicker, S. B., *Turbo Coding*, Kluwer Academic Publishers, Dordrecht, the Netherlands, 1999
- [8] Trifina, L., Munteanu, V. and Baltă, H., "New Types of Interleavers Based on the Welch-Costas Permutation", *Proceedings of the Second European Conference on the Use of Modern Information and Communication Technologies (ECUMICT) 2006*, Gent, Belgium, pp. 107-117, 30-31 March 2006
- [9] Trifina, L., Munteanu, V. and Tărniceriu, D., "Welch-Costas Interleaver with Cyclic Shifts on Groups of Elements", *Electronics Letters*, Vol. 42, No. 24, pp. 1413-1415, 23rd November 2006
- [10] Crozier, S., "New High-Spread High-Distance Interleavers for Turbo-Codes", *20th Biennial Symposium on Communications*, Kingston, Ontario, Canada, pp. 3-7, May 28-31, 2000
- [11] Garelo, R., Pierleoni, P. and Benedetto, S., "Computing the Free Distance of Turbo Codes and Serially Concatenated Codes with Interleavers: Algorithms and Applications", *IEEE Journal on Selected Areas in Communications*, Vol. 19, No. 5, pp. 800-812, May 2001
- [12] Rosnes, E. and Takeshita, Y. Oscar, "Optimum Distance Quadratic Permutation Polynomial-Based Interleavers for Turbo Codes," *Proc. 2006 IEEE International Symposium on Information Theory*, Seattle, July 9-14, 2006, pp. 1988-1992