Further Results on Quadratic Permutation Polynomial-Based Interleavers for Turbo Codes

Eirik Rosnes, Senior Member, IEEE

Abstract—An interleaver is a critical component for the channel coding performance of turbo codes. Algebraic constructions are of particular interest because they admit analytical designs and simple, practical hardware implementation. Also, the recently proposed quadratic permutation polynomial (QPP) based interleavers by Sun and Takeshita (IEEE Trans. Inf. Theory, Jan. 2005) provide excellent performance for short-to-medium block lengths, and have been selected for the 3GPP LTE standard. In this work, we derive some upper bounds on the best achievable minimum distance \(d_{\text{min}}\) of QPP-based conventional binary turbo codes (with tailbiting termination, or dual termination when the interleaver length \(N\) is sufficiently large) that are tight for larger block sizes. In particular, we show that the minimum distance is at most \(2^\left(\nu+1\right)\), independent of the interleaver length, when the QPP has a QPP inverse, where \(\nu\) is the degree of the primitive feedback and monic feedforward polynomials. However, allowing the QPP to have a larger degree inverse may give strictly larger minimum distances (and lower multiplicities). In particular, we provide several QPPs with an inverse degree of at least three for some of the 3GPP LTE interleaver lengths giving a \(d_{\text{min}}\) with the 3GPP LTE constituent encoders which is strictly larger than 50. For instance, we have found a QPP for \(N = 6016\) which gives an estimated \(d_{\text{min}}\) of 57. Furthermore, we provide the exact minimum distance and the corresponding multiplicity for all 3GPP LTE turbo codes (with dual termination) which shows that the best minimum distance is 51. Finally, we compute the best achievable minimum distance with QPP interleavers for all 3GPP LTE interleaver lengths \(N \leq 4096\), and compare the minimum distance with the one we get when using the 3GPP LTE polynomials.

I. INTRODUCTION

Turbo codes have gained considerable attention since their introduction by Berrou et al. in 1993 [1] due to their near-capacity performance and low decoding complexity. The conventional turbo code is a parallel concatenation of two identical recursive systematic convolutional encoders separated by a pseudo-random interleaver.

Interleavers for conventional binary turbo codes [2–10] have been extensively investigated. The dithered relative prime (DRP) interleavers [9, 10] and the almost regular permutation interleavers [4] are considered among the best classes of interleavers. Recently, Sun and Takeshita [2] suggested the use of permutation polynomial (PP) based interleavers over integer rings. In particular, quadratic polynomials were emphasized. A useful property of this class of interleavers is that they are fully algebraic and admit the computation of analytical upper bounds on the best achievable minimum distance \(d_{\text{min}}\). The use of higher degree PPs was recently considered by Takeshita in [11], and a simple coefficient test for cubic PPs was provided in [12].

The decoding of turbo codes is performed by an iterative process in which the so-called extrinsic information is exchanged between sub-blocks of the iterative decoder. There are typically two (or more) sub-blocks in an iterative turbo decoder, each implementing a soft-input soft-output decoding algorithm of a convolutional code. The parallel processing of iterative decoding of turbo codes is of interest for high-speed decoders, and this requires that the interleaver satisfies additional properties. In particular, to avoid memory contentions in parallelized decoding, the interleaver should be contention-free [4, 13, 14]. In this regard, algebraically constructed interleavers have some advantages compared to random constructions. For instance, in [3], Takeshita showed that all PPs generate maximum contention-free interleavers, i.e., every factor of the interleaver length becomes a possible degree of parallel processing of the decoder. Thus, this class of interleavers is very interesting from an implementation point of view, and quadratic permutation polynomial (QPP) interleavers were indeed recently selected for the turbo codes in the 3GPP LTE standard [15].

This work is a continuation of [16], in which the \(d_{\text{min}}\) of conventional binary turbo codes with QPP interleavers was considered in detail. In particular, in [16], large tables of optimum (in terms of the induced \(d_{\text{min}}\), and its corresponding multiplicity) QPPs for conventional binary turbo codes with 8-state and 16-state constituent encoders were presented for short interleaver lengths. In this work, however, we consider the minimum distance properties with longer QPP interleavers. In particular, we present several upper bounds on the best possible \(d_{\text{min}}\) with QPP interleavers and compute the exact minimum distance of all 3GPP LTE turbo codes (with dual termination [17]) for all possible lengths. Estimating the minimum distance of 3GPP LTE turbo codes has recently been addressed by several authors, see, for instance, [18, 19]. However, the exact minimum distance has only been computed for short interleaver lengths \(N \leq 104\) [19].

The remainder of this paper is organized as follows. QPPs over integer rings and some of their properties are reviewed in Section II. Section III provides upper bounds on the optimum minimum distance for QPP-based turbo codes. A table providing the exact minimum distance and its corresponding multiplicity for all 3GPP LTE turbo codes (with dual termination) is presented in Section IV. In Section V, we present the results of an exhaustive computer search over the entire class of QPP interleavers. In particular, the best achievable minimum distance for all 3GPP LTE interleaver lengths \(N \leq 4096\) and for several selected larger interleaver lengths is prov...
lengths, is provided. The results are compared to those with the 3GPP LTE polynomials. Furthermore, we provide a table of several improved QPPs (compared to the ones selected for the 3GPP LTE standard) for medium-to-large interleaver lengths. Conclusions and a discussion of future work are given in Section VI.

II. QPPs OVER INTEGER RINGS

In this section, we establish notation and restate the criterion for existence of QPPs over integer rings. The interested reader is referred to [2, 20] for further details. Given an integer \( N \geq 2 \), a polynomial \( f(x) = f_1x + f_2x^2 \) \((\mod N)\), where \( f_1 \) and \( f_2 \) are nonnegative integers, is said to be a QPP over the ring of integers \( \mathbb{Z}_N \) when \( f(x) \) permutes \( \{0, 1, 2, \ldots, N-1\} \) [2].

In this paper, let the set of primes be \( \mathcal{P} = \{2, 3, 5, 7, \ldots\} \).

Then an integer \( N \) can be factored as \( N = \prod_{p \in \mathcal{P}} p^{n_{p,N}} \), where \( n_{N,p} \geq 1 \) for a finite number of \( p \)'s and \( n_{N,p} = 0 \) otherwise. For example, if \( N = 3888 \neq 2^3 \times 3^5 \) we have \( n_{3888,2} = 4 \) and \( n_{3888,3} = 5 \). For a quadratic polynomial \( f(x) \equiv f_1x + f_2x^2 \) \((\mod N)\), we will abuse the previous notation by writing \( f_1 = \prod_{p \in \mathcal{P}} p^{n_{p,N}} \), i.e., the exponents of the prime factors of \( f \) will be written as \( n_{p,N} \) instead of the more cumbersome \( n_{p,N} \).

Let us denote \( a \) divides \( b \) by \( a \mid b \) and by \( a \nmid b \) otherwise. The greatest common divisor of \( a \) and \( b \) is denoted by \( \gcd(a,b) \).

The necessary and sufficient condition for a quadratic polynomial \( f(x) \) to be a PP is given in the following proposition.

Proposition 1 ([2, 20]): Let \( N = \prod_{p \in \mathcal{P}} p^{n_{p,N}} \). The necessary and sufficient condition for a quadratic polynomial \( f(x) = f_1x + f_2x^2 \) \((\mod N)\) to be a PP can be divided into two cases.

1) Either \( 2 \mid N \) or \( 4 \mid N \) (i.e., \( n_{N,2} \neq 1 \))
   \[ \gcd(f_1, N) = 1 \text{ and } f_2 = \prod_{p \in \mathcal{P}} p^{n_{p,N}}, n_{F,p} \geq 1, \forall p \text{ such that } n_{N,p} \geq 1. \]

2) \( 2 \nmid N \) and \( 4 \nmid N \) (i.e., \( n_{N,2} = 1 \))
   \[ f_1 + f_2 \text{ is odd, } \gcd(f_1, N) = 1, \text{ and } f_2 = \prod_{p \in \mathcal{P}} p^{n_{p,N}}, n_{F,p} \geq 1, \forall p \text{ such that } p \neq 2 \text{ and } n_{N,p} \geq 1. \]

For example, if \( N = 256 \), then we determine from case 1) of Proposition 1 that \( f_1 \in \{1, 3, 5, \ldots, 255\} \) (set of numbers relatively prime to \( N \)) and \( f_2 \in \{2, 4, 6, \ldots, 254\} \) (set of numbers that contains 2 as a factor). This gives us 128 \times 127 = 16256 possible pairs of coefficients \( f_1 \) and \( f_2 \) that make \( f(x) \) a PP.

It is shown in [11] that some QPPs \( f(x) = f_1x + f_2x^2 \) \((\mod N)\) such that \( f_2 \neq 0 \) \((\mod N)\) degenerate to a linear permutation polynomial (LPP), i.e., there is an LPP equivalent to the QPP generating the same permutation over the integer ring \( \mathbb{Z}_N \). QPPs that do not degenerate to an LPP are called irredcuble QPPs. The following proposition from [11] can be used to check if a QPP is irreducible.

Proposition 2 ([11]): A QPP \( f(x) = f_1x + f_2x^2 \) \((\mod N)\) is irreducible if and only if \( N/\gcd(2f_2, N) \neq 1 \).

Combining Propositions 1 and 2 we conclude that if the length \( N \) can written as the product of distinct prime numbers, then either there are no QPPs for this length or all QPPs are equivalent to LPPs.

Proposition 3 ([21]): Let \( N = \prod_{p \in \mathcal{P}} p^{n_{p,N}} \leq 2^{50} \), \( f(k) = \prod_{l=2}^{2k-2} l \), and \( f(x) \) a PP. Decompose \( f(k) \) into prime factors and denote the exponent of the prime factor \( p \) as \( n_{p,f(k)} \). Then, \( f(x) \) has \( \prod_{k=1}^{L} \gcd(k, N) \) inverse polynomials with the least degree \( L \) if and only if there is a smallest integer \( L \) such that

\[
\max \left( \frac{\gcd(N^2-2n_{p,f(k)+1})}{L}, 1 \right), \text{ if } n_{N,2} > 1 \text{ and } p = 2
\]

\[
0, \text{ if } n_{N,2} \leq 1 \text{ and } p = 2
\]

\[
\max \left( \frac{\gcd(N^p-2n_{p,f(k)+1})}{L}, 1 \right), \text{ if } n_{N,p} > 0 \text{ and } p \neq 2
\]

\[
0, \text{ if } n_{N,p} = 0 \text{ and } p \neq 2.
\]

Example 1: Let \( N = 5504 = 2^7 \times 43 \). With \( L = 3 \) in Proposition 3, \( \phi(L+1) = \phi(4) = 120 = 2^3 \times 3 \times 5 \), and we get

\[
n_{F,p} \geq \begin{cases} 2, & \text{if } p = 2 \\ 1, & \text{if } p = 43 \\ 0, & \text{otherwise}\end{cases}
\]

III. UPPER BOUNDS ON THE OPTIMUM \( d_{\min} \)

In this section, we report several upper bounds on the optimum \( d_{\min} \) for QPP-based conventional binary turbo codes of nominal rate 1/3. These upper bounds can be used in the selection of good interleaver lengths with QPP interleavers, and also to efficiently reject bad QPP candidates in a computer search.

In general, let \( f(x) = f_1x + f_2x^2 \) \((\mod N)\) denote a QPP and \( g(x) = g_1x + \cdots + g_Lx^L \) an inverse polynomial of degree \( L \). We assume tailbiting termination of the upper and lower constituent encoders throughout this section, but we remark that the derived upper bounds can be shown to hold with dual termination as well, i.e., the upper and lower constituent encoders are forced to begin and end in the zero state, when \( N \) is sufficiently large. Details are provided at the end of the section. We start by deriving some partial upper bounds (i.e., upper bounds that apply for specific interleaver lengths \( N \)) without constraints on an inverse polynomial.

A. Partial Upper Bounds on the \( d_{\min} \)

In this section, we derive partial upper bounds (i.e., upper bounds that apply for some values of the interleaver length \( N \)) on the \( d_{\min} \) that holds for any QPP, i.e., there are no constraints on the degree of an inverse polynomial.

Theorem 1: The minimum distance of a conventional binary turbo code (of nominal rate 1/3) with feedback polynomial \( 1 + D^2 + D^3 \) and feedforward polynomial \( 1 + D + D^3 \), is upper-bounded by \( 38 + 12l \), where \( l \) is some nonnegative integer, for all interleaver lengths \( N \) that satisfy

\[
n_{N,p} \leq \begin{cases} \frac{l+4}{2}, & \text{if } p = 2 \\ 2, & \text{if } p = 7 \\ 1, & \text{otherwise}\end{cases}
\]

when using QPP interleavers.

Proof: In Fig. 1, an input-weight 6 codeword is shown. The upper constituent codeword contains 3 input-weight 2 fundamental paths, while the lower constituent codeword contains
2 input-weight 3 fundamental paths. The interleaving of the systematic 1-positions is indicated by arrows and the 6 first letters of the English alphabet. The actual pattern in Fig. 1 is a codeword if

\[ f(g(x + b) + a) \equiv f(g(x) + a) + b \pmod{N} \]  
\[ f(g(x + c) + a) \equiv f(g(x) + a) + c \pmod{N} \]  

where \( x \in \mathbb{Z}_N \) denotes the first systematic 1-position (labeled by “A” in Fig. 1) in the lower constituent codeword. For the input-weight 3 fundamental paths in the lower constituent codeword, the index differences between the second and first systematic 1-positions and the third and first systematic 1-positions are denoted by \( b \) and \( c \), respectively. For the input-weight 2 fundamental paths in the upper constituent codeword, the index difference between the final and first systematic 1-positions is denoted by \( a \). The two congruences in (2) and (3) are equivalent, with \( x = 0 \), to

\[ 2baf_2(g_1 + bg_2 + \cdots + b^{L-1}g_L) \equiv 0 \pmod{N} \]  
\[ 2caf_2(g_1 + cg_2 + \cdots + c^{L-1}g_L) \equiv 0 \pmod{N} \]  

where \( L \) is the degree of an inverse polynomial. These two congruences are satisfied if both \( 2baf_2 \equiv 0 \pmod{N} \) and \( 2caf_2 \equiv 0 \pmod{N} \). Choose \( a = 2^l \cdot 7 \), where \( l \) is some nonnegative integer, and \( b = 8 \) and \( c = 12 \), from which it follows that the two congruences reduce to \( 2^{l+4} \cdot 7 \cdot f_2 = 0 \pmod{N} \) and \( 2^{l+3} \cdot 21 \cdot f_2 = 0 \pmod{N} \), and the result follows from Proposition 1 and the fact that the Hamming weight of the codeword in Fig. 1 is (at most) 38 + 12l.

**Theorem 2:** The minimum distance of a conventional binary turbo code (of nominal rate 1/3) with feedback polynomial \( 1 + D^2 + D^3 \) and feedforward polynomial and \( 1 + D + D^3 \), is upper-bounded by 51 for all interleaver lengths \( N \) that satisfy

\[ n_{N,p} \leq \begin{cases} 6, & \text{if } p = 2 \\ 2, & \text{if } p = 3 \\ 1, & \text{otherwise} \end{cases} \]

when using QPP interleavers.

**Proof:** In Fig. 2, an input-weight 9 codeword is shown. Both the upper and lower constituent codewords contain 3 input-weight 3 fundamental paths. The interleaving of the systematic 1-positions is indicated by arrows and the 9 first letters of the English alphabet. The actual pattern in Fig. 2 is a codeword if

\[ f(g(x) + b) + b \equiv f(g(x) + b) + b \pmod{N} \]  
\[ f(g(x) + b) + c \equiv f(g(x) + c) + b \pmod{N} \]  
\[ f(g(x) + c) + b \equiv f(g(x) + b) + c \pmod{N} \]  
\[ f(g(x) + c) + c \equiv f(g(x) + c) + c \pmod{N} \]  

where \( x \in \mathbb{Z}_N \) denotes the first systematic 1-position (labeled by “A” in Fig. 2) of the first fundamental path in the lower constituent codeword. The index differences between the second and first and the final and first systematic 1-positions of all the fundamental paths in both the upper and lower constituent codewords are denoted by \( b \) and \( c \), respectively. The congruences in (6) to (9) are equivalent, with \( x = 0 \), to

\[ 2b^2f_2(g_1 + bg_2 + \cdots + b^{L-1}g_L) \equiv 0 \pmod{N} \]  
\[ 2bcf_2(g_1 + cg_2 + \cdots + c^{L-1}g_L) \equiv 0 \pmod{N} \]  
\[ 2bcf_2(g_1 + bg_2 + \cdots + b^{L-1}g_L) \equiv 0 \pmod{N} \]  
\[ 2c^2f_2(g_1 + cg_2 + \cdots + c^{L-1}g_L) \equiv 0 \pmod{N} \].

For the given constituent encoders, we can choose \( b = 8 \) and \( c = 12 \), from which it follows that we require \( 3 \cdot 2^5f_2 = 0 \pmod{N} \), and the result follows from Proposition 1 and the fact that the Hamming weight of the codeword in Fig. 2 is (at most) 51 when \( b = 8 \) and \( c = 12 \).

In Fig. 3, an input-weight 4 codeword is shown. The upper and lower constituent codewords both contain 2 input-weight 2 fundamental paths. The interleaving of the systematic 1-positions is indicated by arrows and the 4 first letters of the English alphabet. To make the pattern in Fig. 3 a codeword, we need to make sure that \( f(g(x) + a) + b \equiv f(g(x) + c) + d \pmod{N} \), where \( x \in \mathbb{Z}_N \) denotes the first systematic 1-position (labeled by “A” in Fig. 3) of the first fundamental path in the lower constituent codeword. The index differences between the final and first systematic 1-positions of the first and second fundamental paths in the lower constituent codeword are denoted by \( a \) and \( d \), respectively. The corresponding index
differences for the upper constituent codeword are denoted by $c$ and $b$, respectively. With a primitive feedback polynomial of degree $\nu$, $a$, $b$, $c$, and $d$ are all multiples of $2^\nu - 1$. The Hamming weight of the codeword in Fig. 3 is (at most) $12 + 2^{\nu - 1}(|a| + |b| + |c| + |d|)/(2^\nu - 1)$. The congruence $f(g(x + a) + b) \equiv f(g(x) + c) + d \ (\text{mod } N)$ is equivalent, with $x = 0$, to

$$\left( b^2 - c^2 \right) f_2 + (b - c) f_1 + a - d + 2abf_2 (g_1 + ag_2 + \cdots + aL^{-1}g_L) \equiv 0 \pmod{N}. \quad (10)$$

If we choose $c = b$ and $d = a$, we get $2abf_2 (g_1 + ag_2 + \cdots + aL^{-1}g_L) \equiv 0 \pmod{N}$. Furthermore, let $a = (2^\nu - 1)a'$ and $b = (2^\nu - 1)b'$.

In Table I, we list in the second column the congruence in (10) with different values of the pair $(|a'|, |b'|)$ (different rows correspond to different values of the pair $(|a|, |b|)$). The third column contains simplified congruences corresponding to the congruences in the second column, in the sense that if a congruence in the third column is satisfied, then also the corresponding congruence in the second column is satisfied. The last column contains an upper bound on the weight of the corresponding codeword in the turbo code.

We will now consider the special case of $\nu = 3$ in more detail. Using Proposition 1 and the congruences in Table I, we get the conditions on $N$ and the corresponding upper bounds in Table II. When we assume that the QPP has a quadratic inverse, we can use [20, Theorem 3.6] (or Proposition 3 with $L = 2$) to relax the conditions on $N$ in Table II for the same upper bounds on the $d_{\text{min}}$. For instance, the congruence in the fifth row and third column of Table I (with $\nu = 3$) is satisfied if $n_{F,2} + 3 \geq n_{N,2}$, $n_{F,7} + 2 \geq n_{N,7}$, and $n_{F,p} \geq n_{N,p}$, $p \neq 2, 7$. Using [20, Theorem 3.6] (or Proposition 3 with $L = 2$), it follows that the two inequalities above are satisfied for all values of $f_2$ if

$$n_{N,2} \leq \begin{cases} 3 + \max \left( \frac{n_{N,2} - 2}{2} , 1 \right) , & \text{if } n_{N,2} > 1 \\ 3 , & \text{if } n_{N,2} = 0, 1 \end{cases}$$

$$n_{N,3} \leq \begin{cases} \max \left( \frac{n_{N,3} - 1}{2} , 1 \right) , & \text{if } n_{N,3} > 0 \\ 0 , & \text{if } n_{N,3} = 0 \end{cases}$$

$$n_{N,7} \leq 2 + \left[ \frac{n_{N,7}}{2} \right]$$

$$n_{N,p} \leq \left[ \frac{n_{N,p}}{2} \right] , \quad \text{if } p \neq 2, 3, 7$$

which reduces to

$$n_{N,p} \leq \begin{cases} 5 , & \text{if } p = 2, 7 \\ 1 , & \text{otherwise} \end{cases}$$

In a similar fashion, we can use the congruences in the other rows in Table I together with [20, Theorem 3.6] (or Proposition 3 with $L = 2$) to derive other conditions on $N$ for various upper bounds on the optimum minimum distance when the QPP has a quadratic inverse. The conditions and the corresponding upper bounds are summarized in Table III.

### B. General Upper Bound With a Quadratic Inverse

In this section, we provide a general (i.e., independent of $N$) upper bound on the $d_{\text{min}}$ of turbo codes when an inverse polynomial is of degree two, i.e., the inverse permutation is a QPP. In the following, let $g(x) = g_1x + g_2x^2 \pmod{N}$ denote the inverse of $f(x)$.

**Theorem 3:** The minimum distance of a conventional binary turbo code (of nominal rate $1/3$) using primitive feedback and monic feedforward polynomials of degree $\nu$ and QPPs with a quadratic inverse, is upper-bounded by $2(2^{\nu + 1} + 9)$.

**Proof:** In Fig. 4, an input-weight 6 codeword is shown. The upper and lower constituent codewords contain 3 input-weight 2 fundamental paths each. The interleaving of the systematic 1-positions is indicated by arrows and the 6 first letters of the English alphabet. To make the pattern in Fig. 4 a codeword, we need to make sure that $f(g(f(x) + a) + 2a) \equiv f(g(f(x) + a + 2a) + a) \pmod{N}$, where $x \in \mathbb{Z}_N$ is the leftmost systematic 1-position (labeled by “A” in Fig. 4) in the upper constituent codeword. The index difference between the final and first systematic 1-positions of the first and third fundamental paths in both the upper and lower constituent codewords is denoted by $a$. The corresponding index difference for the second (i.e., middle) fundamental path (in both constituent codewords) is $2a$. Since the feedback polynomial is primitive, we can choose $a = 2^\nu - 1$, and with a monic feedforward polynomial of degree $\nu$, the parity weight of the first and third fundamental paths in both constituent codewords in Fig. 4 is $2 + 2^\nu - 1$. The corresponding parity weight for the second (i.e., middle) fundamental path (in both constituent codewords) is $2 + 2^\nu$. Now, the congruence above is equivalent to

$$4 \cdot a^3 \cdot f_2 g_2 (1 + 2f_1 + 2a f_2 + 4xf_2) \equiv 0 \pmod{N}$$

which again is equivalent to

$$4 \cdot a^3 \cdot f_2 g_2 (1 + 2f_1 + 2a f_2) \equiv 0 \pmod{N} \quad (11)$$

since $4f_2^2 g_2 \equiv 0 \pmod{N}$. This follows from [20, Theorem 3.5] which states that $12f_2 g_2 \equiv 0 \pmod{N}$. The Hamming weight of the codeword in Fig. 4 is (at most) $2(2^{\nu + 1} + 9)$, where equality holds if the fundamental paths do not interfere with each other as in Fig. 4.

From [20, Theorem 3.5] we know that $12f_2 g_2 \equiv 0 \pmod{N}$, and it follows that $4f_2 g_2 \equiv 0 \pmod{N}$ if 27 is not a divisor of $N$. Thus, the congruence in (11) holds for all QPPs with a quadratic inverse, for a given value of $N$, if 27 is not a divisor of $N$.

In Fig. 5, another input-weight 6 codeword is depicted. The upper and lower constituent codewords contain 3 input-weight...
TABLE I

Summary of conditions that make the pattern in Fig. 3 a codeword.

| (|a'|,|b'|) | Equation (10) with c = b and d = a | Simplified congruence | Weight |
|---|---|---|---|
| (1,1) | (2ν − 1)² · 2f₂((2ν − 1)g₂ + · · · + (±(2ν − 1))L−1g_L) ≡ 0 | (2ν − 1)² · 2f₂ ≡ 0 | 12 + 2ν+1 |
| (1,2) | (2ν − 1)² · 2²f₂((2ν − 1)g₂ + · · · + (±(2ν − 1))L−1g_L) ≡ 0 | (2ν − 1)² · 2²f₂ ≡ 0 | 12 + 3 · 2ν |
| (2,1) | (2ν − 1)² · 2f₂((2ν − 1)g₂ + · · · + (±(2ν − 1))L−1g_L) ≡ 0 | (2ν − 1)² · 2f₂ ≡ 0 | 12 + 3 · 2ν |
| (2,2) | (2ν − 1)² · 2²f₂((2ν − 1)g₂ + · · · + (±(2ν − 1))L−1g_L) ≡ 0 | (2ν − 1)² · 2²f₂ ≡ 0 | 12 + 2ν+2 |
| (1,3) | (2ν − 1)² · 2 · 3f₂((2ν − 1)g₂ + · · · + (±(2ν − 1))L−1g_L) ≡ 0 | (2ν − 1)² · 2 · 3f₂ ≡ 0 | 12 + 2ν+2 |
| (3,1) | (2ν − 1)² · 2 · 3f₂((2ν − 1)g₂ + · · · + (±(2ν − 1))L−1g_L) ≡ 0 | (2ν − 1)² · 2 · 3f₂ ≡ 0 | 12 + 2ν+2 |

TABLE II

Summary of conditions on N (derived using the congruences in Table I) for various upper bounds on the optimum minimum distance when ν = 3.

| n_{N,2} | n_{N,3} | n_{N,7} | n_{N,p} ≠ 2, 3, 7 | Upper bound | Row from Table I |
|---|---|---|---|---|---|
| ≤ 2 | ≤ 1 | ≤ 3 | ≤ 1 | 28 | 2 |
| ≤ 3 | ≤ 1 | ≤ 3 | ≤ 1 | 36 | 3 and 4 |
| ≤ 4 | ≤ 1 | ≤ 3 | ≤ 1 | 44 | 5 |
| ≤ 2 | ≤ 2 | ≤ 3 | ≤ 1 | 44 | 6 and 7 |

TABLE III

Summary of conditions on N (derived using the congruences in Table I) for various upper bounds on the optimum minimum distance when ν = 3 and the inverse degree is two.

| n_{N,2} | n_{N,3} | n_{N,7} | n_{N,p} ≠ 2, 3, 7 | Upper bound | Row from Table I |
|---|---|---|---|---|---|
| ≤ 2 | ≤ 1 | ≤ 5 | ≤ 1 | 28 | 2 |
| ≤ 3 | ≤ 1 | ≤ 5 | ≤ 1 | 36 | 3 and 4 |
| ≤ 5 | ≤ 1 | ≤ 5 | ≤ 1 | 44 | 5 |
| ≤ 2 | ≤ 2 | ≤ 5 | ≤ 1 | 44 | 6 and 7 |

Fig. 5. An input-weight 6 critical codeword for QPP-based interleavers.

2 fundamental paths each. The interleaving of the systematic 1-positions is indicated by arrows and the 6 first letters of the English alphabet. To make this pattern a codeword, \(f(g(f(x) + 2a) − a) \equiv f(g(f(x) + a) + a) − 2a + a \pmod{N}\), where \(x \in \mathbb{Z}_N\) is the leftmost systematic 1-position (labeled by “A” in Fig. 5) in the upper constituent codeword. The index difference between the final and first systematic 1-positions of the first and third fundamental paths in the upper constituent codeword, and of the second and third fundamental paths in the lower constituent codeword is denoted by \(a\). The corresponding index difference for the second fundamental path in the upper constituent codeword, and for the first fundamental path in the lower constituent codeword is 2a. Now, the congruence above is equivalent to
\[
4 \cdot a^3 \cdot f_2 g_2 (1 - 2f_1 - 2a f_2 - 4x f_2) \equiv 0 \pmod{N}
\]
which again is equivalent to
\[
4 \cdot a^3 \cdot f_2 g_2 (1 - 2f_1 - 2af_2) \equiv 0 \pmod{N}
\]
since \(4f_2^2 g_2 \equiv 0 \pmod{N}\). This follows from [20, Theorem 3.5] which states that \(12f_2 g_2 \equiv 0 \pmod{N}\). As for the codeword in Fig. 4, the Hamming weight of the codeword in Fig. 5 is (at most) \(2(2^{ν+1} + 9)\). Assume \(27|N\). Then, \(f_2 = 3 \cdot c\), for some integer \(c\), since \(3|f_2\). Furthermore, \(f_1 = 1 + 3 \cdot k\) or \(2 + 3 \cdot k\), for some integer \(k\), since \(gcd(f_1, f_2, N) = 1\). If \(f_1 = 1 + 3 \cdot k\), then the congruence in (11) reduces to \(4 \cdot a^3 \cdot f_2 g_2 (1 + 2(2 + 3 \cdot k) + 2a \cdot 3 \cdot c) \equiv 12 \cdot a^3 \cdot f_2 g_2 (1 + 2 + 2a \cdot 3 \cdot c) \equiv 0 \pmod{N}\), which is always true, since \(12f_2 g_2 \equiv 0 \pmod{N}\) [20, Theorem 3.5]. Furthermore, if \(f_1 = 2 + 3 \cdot k\), then the congruence in (12) reduces to \(4 \cdot a^3 \cdot f_2 g_2 (1 - 2(2 + 3 \cdot k) - 2a \cdot 3 \cdot c) \equiv 12 \cdot a^3 \cdot f_2 g_2 (1 - 2 - 2a \cdot 3 \cdot c) \equiv 0 \pmod{N}\), which is always true, since \(12f_2 g_2 \equiv 0 \pmod{N}\) [20, Theorem 3.5]. Thus, there is an upper bound of \(2(2^{ν+1} + 9)\) on the \(d_{min}\) for QPPs with a quadratic inverse for all values of \(N\).

We emphasize that Theorem 3 applies for all interleaver lengths \(N\) and is achievable, at least for \(ν = 3\), for a range
of $N$-values (see Fig 8). Thus, for $\nu = 3$, to achieve a $d_{min}$ strictly larger than $2(2^{\nu+1} + 9) = 50$, the degree of an inverse permutation should be at least three.

Example 2: For $N = 5504 = 2^7 \times 43$, it follows from Theorem 3 (with $\nu = 3$) that the $d_{min}$ is at most 50 when the QPP has a quadratic inverse. Furthermore, using the condition in (1) in Example 1 for the QPP to have an inverse cubic, we observe that the condition $3 \cdot 2^5 f_2 \equiv 0 \pmod{N}$ from the proof of Theorem 2 is always satisfied, which means that to achieve a $d_{min}$ (with the 3GPP LTE encoders) strictly larger than 51, the degree of an inverse polynomial has to be at least four.

C. Partial Upper Bounds With a Quadratic Inverse

Theorem 4: The minimum distance of a conventional binary turbo code (of nominal rate 1/3) with feedback polynomial $1 + D^2 + D^3$ and feedforward polynomial $1 + D + D^3$, is upper-bounded by $38 + 12l$, where $l$ is some nonnegative integer, for all interleaver lengths $N$ that satisfy

$$n_{N,p} \leq \begin{cases} 2l + 5, & \text{if } p = 2 \\ 3, & \text{if } p = 7 \\ 1, & \text{otherwise} \end{cases}$$

when using QPP interleavers with a quadratic inverse.

Proof: The proof is based on the codeword in Fig 1. In the case that an inverse polynomial is of degree two, the congruences in (4) and (5) reduce (with $L = 2$, $a = 2^l \cdot 7$, $b = 8$, and $c = 12$) to $2^l \cdot 112 f_2 (g_1 + 8g_2) \equiv 0 \pmod{N}$ and $2^l \cdot 168 f_2 (g_1 + 12g_2) \equiv 2^l \cdot 168 f_2 g_1 \equiv 0 \pmod{N}$ [20, Theorem 3.5]. Furthermore, if $2^l \cdot 168 f_2 g_1 \equiv 0 \pmod{N}$, then $2^l \cdot 112 f_2 g_1 + 224 \cdot 12 f_2 g_2 = 2^l (3 \cdot 112 f_2 (g_1 + 8g_2)) \equiv 0 \pmod{N}$ [20, Theorem 3.5], from which it follows that $2^l \cdot 112 f_2 (g_1 + 8g_2) \equiv 0 \pmod{N}$ if $N$ is not a divisor of $N$. The congruence $2^l \cdot 168 f_2 g_1 \equiv 0 \pmod{N}$ is satisfied for all valid values of $g_1$ and $f_2$ if $n_{f,2} + l + 3 \geq n_{f,2}, n_{f,3} + 1 \geq n_{f,3}, n_{f,7} + 1 \geq n_{f,7},$ and $n_{f,4} \geq n_{f,4}, p \neq 2, 3, 7$. Using [20, Theorem 3.6] (or Proposition 3 with $L = 2$), it follows that the congruences are satisfied for all valid values of $f_2$, for a given value of $N$, if the following conditions are satisfied.

$$n_{N,2} \leq \begin{cases} l + 3 + \max \left( \left[ \frac{n_{N,2} - 2}{2} \right], 1 \right), & \text{if } n_{N,2} > 0 \\ l + 3, & \text{if } n_{N,2} = 0,1 \end{cases}$$

$$n_{N,3} \leq \begin{cases} 1 + \max \left( \left[ \frac{n_{N,3} - 1}{2} \right], 1 \right), & \text{if } n_{N,3} > 0 \\ 1, & \text{if } n_{N,3} = 0 \end{cases}$$

$$n_{N,7} \leq 1 + \left[ \frac{n_{N,7}}{2} \right]$$

$$n_{N,p} \leq \left[ \frac{n_{N,p}}{2} \right],$$

which reduce (when we use the fact that 9 should not be a divisor of $N$) to (13). The Hamming weight of the codeword in Fig 1 is (at most) $38 + 12l$, and the result follows.

We remark that Theorem 4 is only useful when $l = 0$, since the $d_{min}$ upper bound is at least 50 when $l \geq 1$. This is the case since Theorem 3 (with $\nu = 3$) gives a general upper bound of 50.

D. Partial Upper Bounds With an Inverse Degree of Three

Theorem 5: The minimum distance of a conventional binary turbo code (of nominal rate 1/3) with feedback polynomial $1 + D^2 + D^3$ and feedforward polynomial $1 + D + D^3$, is upper-bounded by $38 + 12l$, where $l$ is some nonnegative integer, for all interleaver lengths $N$ that satisfy

$$n_{N,p} \leq \begin{cases} \left[ \frac{3}{2} \right] + 4, & \text{if } p = 2 \\ 2, & \text{if } p = 7 \\ 1, & \text{otherwise} \end{cases}$$

when using QPP interleavers with a cubic inverse.

Proof: The result can be proved using the same arguments as in the proof of Theorem 4, but using Proposition 3 with $L = 3$ instead of [20, Theorem 3.6] (or Proposition 3 with $L = 2$). In particular, we require that

$$n_{N,2} \leq \begin{cases} l + 3 + \max \left( \left[ \frac{n_{N,2} - 3 - 1}{3} \right], 1 \right), & \text{if } n_{N,2} > 1 \\ l + 3, & \text{if } n_{N,2} \leq 1 \end{cases}$$

$$n_{N,3} \leq \begin{cases} 1 + \max \left( \left[ \frac{n_{N,3} - 1}{3} \right], 1 \right), & \text{if } n_{N,3} > 0 \\ 1, & \text{if } n_{N,3} = 0 \end{cases}$$

$$n_{N,5} \leq \begin{cases} \max \left( \left[ \frac{n_{N,5} - 1}{3} \right], 1 \right), & \text{if } n_{N,5} > 0 \\ 0, & \text{if } n_{N,5} = 0 \end{cases}$$

$$n_{N,7} \leq 1 + \left[ \frac{n_{N,7}}{3} \right]$$

$$n_{N,p} \leq \left[ \frac{n_{N,p}}{3} \right],$$

which gives the upper bound in (14).

Theorem 6: The minimum distance of a conventional binary turbo code (of nominal rate 1/3) using primitive feedback and monic feedforward polynomials of degree $\nu$ and QPPs with an inverse degree of three, is upper-bounded by $2(2^{\nu+1} + 9)$ for all interleaver lengths $N$ that satisfy

$$n_{N,p} \leq \begin{cases} 4, & \text{if } p = 2 \\ \left[ \frac{9n_{N,p} - 1}{2} \right] + 2, & \text{if } p = 3, 5 \\ \left[ \frac{9n_{N,p} - 1}{2} \right] + 2, & \text{otherwise.} \end{cases}$$

Proof: By repeating the first part of the proof of Theorem 3 with $g(x) = g_1 x + g_2 x^2 + g_3 x^3$, the congruence in (11) (with $x = 0$) is generalized to

$$4a^3 f_2 (g_2 (1 + 2f_1 + 2a f_2) + 3a^2 a (1 + f_1 + a f_2)^2) \equiv 0 \pmod{N}.$$
period turbo codes are quasi-cyclic (with tailbiting termination) with
up the computation, we have used the fact that the 3GPP LTE
paths in Fig. 4 may wrap around at the end of the trellis. Since
\(D\) is a constituent codeword. For a given value of
follows.

\[ n_{N,2} \leq \begin{cases} 3 + \max \left( \left\lfloor \frac{n_{N,2}-3}{3} \right\rfloor, 1 \right), & \text{if } n_{N,2} > 1 \\ 3, & \text{if } n_{N,2} \leq 1 \end{cases} \]

\[ n_{N,3} \leq \begin{cases} 1 + 3n_{2v-1,3} + \max \left( \left\lfloor \frac{n_{N,3}-1}{3} \right\rfloor, 1 \right), & \text{if } n_{N,3} > 0 \\ 1 + 3n_{2v-1,3}, & \text{if } n_{N,3} = 0 \end{cases} \]

\[ n_{N,5} \leq \begin{cases} 1 + 3n_{2v-1,5} + \max \left( \left\lfloor \frac{n_{N,5}-1}{3} \right\rfloor, 1 \right), & \text{if } n_{N,5} > 0 \\ 1 + 3n_{2v-1,5}, & \text{if } n_{N,5} = 0 \end{cases} \]

\[ n_{N,p} \leq 1 + 3n_{2v-1,p} + \left\lfloor \frac{n_{N,p}}{3} \right\rfloor, \quad \text{if } p \neq 2, 3, 5 \]

which simplifies to the result in (15).

E. Upper Bounds With Dual Termination

We remark that the upper bounds on the \(d_{\min}\) derived above
can be shown to hold with dual termination as well as long as
\(N\) is sufficient large. As an example, we consider the upper
bound of Theorem 3, which holds with dual termination when
\(N \geq 2^{v+3} - 7\). The argument is as follows.

The bound in Theorem 3 is based on the upper and lower
constituent codewords in Figs. 4 and 5. For details, see the
proof of Theorem 3. Now, consider the codeword in Fig. 4. Let
\(x \in \mathbb{Z}_N\) denote the leftmost systematic 1-position in the upper
constituent codeword. For a given value of \(x\), the fundamental
paths in Fig. 4 may wrap around at the end of the trellis. Since
all the systematic 1-positions are determined by the value of \(x\),
there will be exactly \(L_i - 1\) values for \(x\) that will make the \(i\)th,
\(i = 0, \ldots, Q - 1\), fundamental path wrap around at the end of
the trellis, where \(L_i\) is the length of the \(i\)th fundamental path
and \(Q\) is the total number of fundamental paths in the upper
and lower constituent codewords. By repeating the argument,
we get that there will be at most \(L - Q\) values for \(x\) that will
make at least one of the fundamental paths wrap around at the
end of the trellis, where \(L = \sum_{i=0}^{Q-1} L_i\), and we get the
condition \(N - (L - Q) \geq 1\), which simplifies to \(N \geq 2^{v+3} - 7\),
since, for the codeword in Fig. 4, \(Q = 6\) and \(L = 8 \cdot 2^v - 2\).

Note that the argument above can be repeated for the codeword in Fig. 5, and we get exactly the same lower bound on \(N\). Thus, if \(N \geq 2^{v+3} - 7\), there will exist at least one value for \(x\) such that none of the fundamental paths in Figs. 4
and 5 will wrap around at the end of the trellis, and the result
follows.

IV. 3GPP LTE Turbo Codes

The turbo codes in the 3GPP LTE standard [15] use the
8-state constituent encoder with feedforward polynomial \(1 + D + D^3\) and feedback polynomial \(1 + D^2 + D^3\). We have
computed the exact \(d_{\min}\) and the corresponding multiplicity of the 3GPP LTE turbo codes (with dual termination) for all
interleaver lengths \(N\) using the algorithm from [22]. To speed-up the computation, we have used the fact that the 3GPP LTE
 turbo codes are quasi-cyclic (with tailbiting termination) with period \(N/\gcd(2f_2, N)\). The results with dual termination are
presented in Table IV. With dual termination both constituent
trellises are terminated to the zero state and all systematic
bits are included in the interleaver. Due to trellis termination
some of the systematic bits (twice the constraint length) are
redundant and these bits are in general not consecutive at the
end of the input block. We have also tailored a version of the
triple impulse method [9] which also explicitly checks for special low input-weight codewords. We ran the method
using all the 3GPP LTE QPPs of length at least 512. For all
lengths, this method found the exact \(d_{\min}\) and also the exact
multiplicity in all but the case of \(N = 1920\), where the
multiplicity was slightly underestimated. Finally, we remark
that the 3GPP LTE specification [15] uses a different trellis
termination technique, and thus the results in Table IV do not
strictly apply to the codes from the standard.

For the 3GPP LTE lengths

{496, 624, 656, 688, 752, 816, 848, 880, 912, 944, 976}
the results in Table IV together with the upper bound from
Theorem 1 (with \(l = 0\)) show that the 3GPP LTE interleavers
are \(d_{\min}\)-optimal, i.e., there are no QPPs that give a strictly
larger \(d_{\min}\), for these lengths.

In a similar fashion, for the 3GPP LTE lengths

{1696, 1760, 1952}
the results in Table IV together with the upper bound from
Theorem 1 (with \(l = 1\)) show that the 3GPP LTE interleavers
are \(d_{\min}\)-optimal for these lengths.

The 3GPP LTE lengths greater than 2048 that satisfy the
conditions of Theorem 2 are

{2112, 2240, 2368, 2496, 2624, 2752, 2880, 3008, 3264, 3392,
3520, 3648, 3776, 3904, 4032, 4160, 4288, 4416, 4544, 4672,
4928, 5056, 5312, 5440, 5568, 5696, 5824, 5952, 6080}.

From the results of Table IV, it follows that the 3GPP LTE
interleavers are \(d_{\min}\)-optimal for lengths

{4288, 4544, 5056, 5312, 5568, 6080}.

Finally, for the lengths

{1920, 2176, 2368, 2432, 2496, 2624, 2752, 3264, 3392, 3456,
3520, 3648, 3712, 3776, 3840, 3904, 3968, 4224, 4864, 5376,
5632, 5760, 5888, 6144}.

the 3GPP LTE QPPs have a quadratic inverse, and thus (from
Theorem 3 with \(\nu = 3\)) they are \(d_{\min}\)-optimal within the class of
QPPs with a quadratic inverse, since they give a \(d_{\min}\) of
50 (see Table IV).

V. COMPUTER SEARCH

In Fig. 6, the optimum \(d_{\min}\) within the class of all
irreducible QPPs (found by computer search) for 8-state
turbo codes is plotted versus the interleaver length \(N\).
In particular, we have considered the 3GPP LTE inter-
leaver lengths from 40 to 1008, i.e., the interleaver lengths
40, 48, \ldots, 512, 528, 544, \ldots, 1008. Note that in some cases,
a better \(d_{\min}\) may be achieved by using an LPP, i.e., a
reducible QPP, for small interleaver lengths [16], but the best
achievable minimum distance is upper-bounded by 27 over the
class of reducible QPPs [16]. For comparison, we also show
### TABLE IV

The exact minimum distance $d_{\text{min}}$ and its corresponding multiplicity $N_{d_{\text{min}}}$ of 3GPP LTE turbo codes (with dual termination).

| N   | $f(z)$          | $d_{\text{min}}$ | $N_{d_{\text{min}}}$ | N   | $f(z)$          | $d_{\text{min}}$ | $N_{d_{\text{min}}}$ | N   | $f(z)$          | $d_{\text{min}}$ | $N_{d_{\text{min}}}$ |
|-----|-----------------|------------------|-----------------------|-----|-----------------|------------------|-----------------------|-----|-----------------|------------------|-----------------------|
| 40  | $3z + 19z^2$    | 17               | 11                    | 36  | $19z + 42z^2$  | 24               | 23                    | 56  | $19z + 42z^2$  | 24               | 23                    |
| 48  | $7z + 12z^2$    | 17               | 16                    | 56  | $19z + 42z^2$  | 24               | 23                    | 72  | $7z + 18z^2$   | 23               | 51                    |
| 64  | $7z + 16z^2$    | 20               | 22                    | 80  | $11z + 20z^2$  | 25               | 103                   | 112 | $4z + 8z^2$   | 22               | 17                    |
| 64  | $7z + 16z^2$    | 20               | 22                    | 80  | $11z + 20z^2$  | 25               | 103                   | 112 | $4z + 8z^2$   | 22               | 17                    |
| 104 | $7z + 26z^2$    | 27               | 114                   | 120 | $103z + 90z^2$| 26               | 44                    | 128 | $15z + 32z^2$ | 21               | 51                    |
| 132 | $4z + 8z^2$     | 22               | 171                   | 136 | $9z + 14z^2$   | 28               | 103                   | 144 | $17z + 108z^2$| 30               | 205                   |
| 152 | $9z + 8z^2$     | 28               | 60                    | 160 | $21z + 120z^2$| 31               | 248                   | 168 | $101z + 84z^2$| 27               | 592                   |
| 176 | $21z + 44z^2$   | 28               | 71                    | 232 | $85z + 58z^2$  | 32               | 90                    | 240 | $29z + 60z^2$ | 25               | 101                   |
| 184 | $57z + 46z^2$   | 29               | 144                   | 248 | $33z + 62z^2$  | 35               | 212                   | 256 | $15z + 32z^2$ | 30               | 53                    |
| 192 | $23z + 48z^2$   | 31               | 148                   | 264 | $17z + 19z^2$  | 35               | 339                   | 272 | $33z + 68z^2$ | 36               | 1633                  |
| 200 | $12z + 50z^2$   | 31               | 81                    | 272 | $33z + 68z^2$  | 36               | 1633                  | 280 | $103z + 210z^2$| 22               | 126                   |
| 208 | $27z + 52z^2$   | 31               | 181                   | 288 | $9z + 18z^2$   | 36               | 1120                  | 296 | $19z + 74z^2$ | 35               | 260                   |
| 216 | $11z + 36z^2$   | 29               | 61                    | 304 | $37z + 76z^2$  | 36               | 1690                  | 312 | $19z + 78z^2$ | 36               | 1654                  |
| 224 | $27z + 56z^2$   | 22               | 99                    | 320 | $21z + 120z^2$ | 32               | 68                    | 328 | $21z + 120z^2$| 32               | 68                    |
| 232 | $85z + 58z^2$   | 32               | 92                    | 350 | $115z + 84z^2$ | 30               | 147                   | 364 | $17z + 19z^2$  | 35               | 339                   |
| 240 | $29z + 60z^2$   | 25               | 101                   | 364 | $17z + 19z^2$  | 35               | 339                   | 280 | $103z + 210z^2$| 22               | 126                   |
| 256 | $33z + 62z^2$   | 35               | 212                   | 288 | $9z + 18z^2$   | 36               | 1120                  | 296 | $19z + 74z^2$ | 35               | 260                   |
| 264 | $17z + 19z^2$   | 35               | 339                   | 304 | $37z + 76z^2$  | 36               | 1690                  | 312 | $19z + 78z^2$ | 36               | 1654                  |
| 272 | $33z + 68z^2$   | 36               | 1633                  | 320 | $21z + 120z^2$ | 32               | 68                    | 328 | $21z + 120z^2$| 32               | 68                    |
| 280 | $103z + 210z^2$ | 22               | 126                   | 350 | $115z + 84z^2$ | 30               | 147                   | 364 | $17z + 19z^2$  | 35               | 339                   |
| 288 | $19z + 74z^2$   | 35               | 260                   | 364 | $17z + 19z^2$  | 35               | 339                   | 280 | $103z + 210z^2$| 22               | 126                   |
| 304 | $37z + 76z^2$   | 36               | 1690                  | 312 | $19z + 78z^2$  | 36               | 1654                  | 320 | $21z + 120z^2$ | 32               | 68                    |
the results with optimized DRP interleavers [9, 23] and the results with the 3GPP LTE QPPs from Table IV. Note that the $d_{\text{min}}$ values with the DRP interleavers are only estimates for $N > 800$ [9, 23]. In the search, to quickly reject bad QPPs, we used the special version of the triple impulse method mentioned above. In the final stage, the best candidate QPPs were checked using the exhaustive algorithm from [22]. In Fig. 7, we show the corresponding results with larger interleaver lengths from 1024 to 4096. All 3GPP LTE interleaver lengths have been considered, i.e., the interleaver lengths 1024, 1056, . . ., 2048, 2112, . . ., 4096. In the search, all irreducible QPPs have been considered for all lengths. For comparison, we also show the results with optimized DRP interleavers up to length $N = 2560$ taken from [9, 23] (only estimates of the $d_{\text{min}}$ are provided in [9, 23]) and the results with the 3GPP LTE QPPs from Table IV.

In Fig. 8, we compare the minimum distance for general optimum QPPs with the minimum distance for optimum QPPs with a quadratic inverse for the 3GPP LTE lengths from 736 to 4096 for 8-state turbo codes. From Fig. 8, we observe that the class of QPP-based interleavers with a quadratic inverse is in general inferior to the general class of QPP-based interleavers for larger block sizes. We remark that the interleaver length $N = 736$ is the first length among the 3GPP LTE lengths where the class of QPPs with a quadratic inverse is inferior to the general class of QPPs. For some lengths, the performance in the error floor region can be greatly improved by considering QPPs with no quadratic inverse. For instance, the optimum $d_{\text{min}}$ increases from 38 to 50 for the lengths $\{1376, 1504, 1632, 1696, 1760, 1824, 1888, 1952\}$. Note that among the lengths giving an optimum $d_{\text{min}}$ of 38 within the class of QPPs with a quadratic inverse, only the lengths 360, 432, 512, 896, 1008, 1344, and 1792 do not satisfy the condition in (13) with $l = 0$. There are in total 42 lengths that give an optimum $d_{\text{min}}$ of 38 within the class of QPPs with a quadratic inverse (when $N \leq 4096$).

Finally, we remark that a $d_{\text{min}}$-optimum QPP interleaver is not necessarily unique, in the sense that there will be several QPPs with the optimum minimum distance. In Table V, we list some $d_{\text{min}}$-optimum QPPs giving a $d_{\text{min}}$ of at most 50 for some specific short-to-medium block lengths. For each QPP we also list the exact number $N_{d_{\text{min}}}$ of minimum-weight codewords. We remark that these polynomials do not necessarily give the lowest multiplicity, but are also selected based on error rate performance through simulations.

### A. Improved QPPs

In this subsection, we present some improved QPPs (with respect to the induced turbo code $d_{\text{min}}$) compared to the ones selected for the 3GPP LTE standard.

**Example 3:** For $N = 5504 = 2^7 \times 43$, the $d_{\text{min}}$ is at most 55 over the entire class of QPPs. This follows from an exhaustive search over all QPPs with an inverse degree of at least four (see Example 2). Furthermore, the polynomial $f(x) = 21x + 1118x^2$ has an estimated $d_{\text{min}}$ of 55 with an estimated multiplicity of 507, using the triple impulse method.
TABLE V
SOME $d_{\text{min}}$-OPTIMUM QPPs FOR SOME PARTICULAR INTERLEAVER LENGTHS.

| $N$  | $f(x)$               | $f^{-1}(x)$               | $d_{\text{min}}$ | $N_{d_{\text{min}}}$ |
|------|----------------------|---------------------------|------------------|----------------------|
| 640  | $141x + 120x^2$      | $581x + 360x^2$           | 39               | 74                   |
| 768  | $25x + 240x^2$       | $555x + 144x^2$           | 39               | 90                   |
| 1024 | $245x + 448x^2$      | $861x + 832x^2$           | 45               | 486                  |
| 1504 | $49x + 658x^2$       | $353x + 470x^2 + 1128x^3$ | 50               | 3241                 |
| 2048 | $21x + 128x^2$       | $1853x + 1408x^2$         | 50               | 9198                 |

TABLE VI
ESTIMATED/EXACT MINIMUM DISTANCE AND ITS CORRESPONDING ESTIMATED/EXACT MULTIPLICITY FOR SOME IMPROVED QPPs WITH A POLYNOMIAL INVERSE OF DEGREE GREATER THAN TWO. EXACT RESULTS APPEAR IN BOLD.

| $N$  | $f(x)$               | $f^{-1}(x)$               | $d_{\text{min}}$ | $N_{d_{\text{min}}}$ |
|------|----------------------|---------------------------|------------------|----------------------|
| 2496 | $119x + 702x^2$      | $215x + 390x^2 + 2184x^3$ | 51               | 3034                 |
| 2624 | $125x + 1066x^2$     | $677x + 246x^2 + 2296x^3$ | 51               | 2556                 |
| 2752 | $21x + 430x^2$       | $557x + 1634x^2 + 344x^3$ | 51               | 2853                 |
| 2880 | $133x + 450x^2$      | $157x + 270x^2 + 1080x^3$ | 51               | 2986                 |
| 2944 | $21x + 1196x^2$      | $701x + 1380x^2 + 2208x^3$ | 51               | 3236                 |
| 3008 | $143x + 91x^2$       | $1951x + 470x^2 + 1128x^3$ | 51               | 2940                 |
| 3200 | $83x + 100x^2$       | $347x + 1300x^2 + 2400x^3$ | 51               | 3132                 |
| 3264 | $55x + 102x^2$       | $2359x + 2958x^2 + 2856x^3$ | 51               | 3396                 |
| 3392 | $81x + 106x^2$       | $513x + 2862x^2 + 2968x^3$ | 51               | 3324                 |
| 3456 | $91x + 108x^2$       | $1747x + 540x^2 + 864x^3$  | 51               | 3813                 |
| 3520 | $27x + 110x^2$       | $1923x + 2750x^2 + 3080x^3$ | 51               | 3452                 |
| 3648 | $43x + 114x^2$       | $403x + 1026x^2 + 2280x^3$  | 51               | 3580                 |
| 3712 | $55x + 116x^2$       | $135x + 2900x^2 + 2784x^3$ | 51               | 3644                 |
| 3776 | $1359x + 826x^2$     | $1151x + 354x^2 + 1416x^3$ | 51               | 3708                 |
| 3904 | $1283x + 854x^2$     | $2715x + 2806x^2 + 2440x^3$ | 51               | 3836                 |
| 3968 | $109x + 1054x^2$     | $1893x + 3162x^2 + 3720x^3 + 3720x^4$ | 52   | 242                  |
| 4736 | $61x + 666x^2$       | $1941x + 814x^2 + 1480x^3 + 4440x^4$ | 53   | 145                  |
| 5248 | $21x + 1886x^2$      | $2740x + 1066x^2 + 328x^3 + 328x^4$ | 53   | 161                  |
| 5504 | $21x + 1118x^2$      | $2621x + 5418x^2 + 3784x^3 + 3784x^4$ | 55   | 507                  |
| 6016 | $59x + 658x^2$       | $3059x + 4794x^2 + 3384x^3 + 5640x^4$ | 57   | 744                  |
| 6144 | $59x + 1680x^2$      | $2291x + 4560x^2 + 1536x^3$ | 51   | 94                   |

\*a The tabulated QPP is $d_{\text{min}}$-optimal for this length.
\*b The tabulated QPP is $d_{\text{min}}$-optimal for this length if the estimated $d_{\text{min}}$ given in the fourth column is the exact value. In any case, the estimated $d_{\text{min}}$ in the fourth column is an upper bound on the best possible $d_{\text{min}}$ with QPP interleavers for this length.
\*c The tabulated QPP is $d_{\text{min}}$-optimal for this length within the class of QPPs with an inverse degree of at most three.

Example 4: For $N = 6016 = 2^7 \times 47$, the $d_{\text{min}}$ is at most 57 over the entire class of QPPs. This follows from an exhaustive search over all QPPs with an inverse degree of at least four; it follows from Proposition 3, the proof of Theorem 2, and Theorem 3 that it is sufficient to look at QPPs with an inverse degree of at least four. Furthermore, the polynomial $f(x) = 59x + 658x^2$ has an estimated $d_{\text{min}}$ of 57 with an estimated multiplicity of 744, using the triple impulse method. The QPP from the 3GPP LTE standard gives a $d_{\text{min}}$ of 51 with a much higher multiplicity of 6012.

In Table VI, we give some new QPPs for some 3GPP LTE interleaver lengths for which the estimated/exact $d_{\text{min}}$ is strictly larger than 50. Also, the corresponding estimated/exact multiplicity $N_{d_{\text{min}}}$ is given. The tabulated results (the $d_{\text{min}}$ and the corresponding multiplicity) are exact when they appear in bold. In the third column of the table, an inverse polynomial, denoted by $f^{-1}(x)$, is tabulated. Note that for $N = 6144$, we have found a QPP giving a $d_{\text{min}}$ of 51 with a very low multiplicity of 94, compared to the high multiplicity of 12179 for the 3GPP LTE turbo code. Also, for this length, the $d_{\text{min}}$ is 50 for the 3GPP LTE turbo code. Finally, we remark that the highest found $d_{\text{min}}$ is 51 when the QPP has an inverse polynomial of degree three.
VI. CONCLUSION AND FUTURE WORK

In this work, we have presented several upper bounds on the best achievable minimum distance with conventional binary turbo codes (with tailbiting termination, or dual termination when the interleaver length is sufficiently large) using QPP-based interleavers. We have verified by exhaustive computer search that the upper bounds are tight for larger interleaver lengths. One of the main results was a general upper bound of \(2(2^{\nu+1} + 9)\) on the minimum distance, independent of the interleaver length, when the QPP has a QPP inverse, where \(\nu\) is the degree of the primitive feedback and monic feedforward polynomials. Furthermore, by means of several examples, we showed that by allowing the QPP to have a larger degree inverse may give strictly larger minimum distances (and lower multiplicities). We also provided the exact minimum distance and the corresponding multiplicity for all 3GPP LTE turbo codes (with dual termination). Finally, we computed the best achievable minimum distance with QPP interleavers for the 3GPP LTE lengths \(N \leq 4096\) and compared the minimum distance with the one we get when using the 3GPP LTE polynomials.

Deriving a general, i.e., independent of \(N\) upper bound on the \(d_{\min}\) that holds for any interleaver length \(N\) without any constraints on the degree of an inverse polynomial is an important open problem. Even finding a general upper bound when an inverse polynomial has degree three would be interesting. As a final remark in this respect, we identified the polynomial \(39x + 760x^2 \mod 9728\) (inverse degree of three) with an estimated \(d_{\min}\) of 56, which again indicates that it is probably not a universal upper bound on the \(d_{\min}\) when the QPP has an inverse degree of three.

REFERENCES

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, “Near Shannon limit error-correcting coding and decoding: Turbo-codes,” in Proc. IEEE Int. Conf. Commun. (ICC), Geneva, Switzerland, May 1993, pp. 1064–1070.
[2] J. Sun and O. Y. Takeshita, “Interleavers for turbo codes using permutation polynomials over integer rings,” IEEE Trans. Inf. Theory, vol. 51, no. 1, pp. 101–119, Jan. 2005.
[3] O. Y. Takeshita, “On maximum contention-free interleavers and permutation polynomials over integer rings,” IEEE Trans. Inf. Theory, vol. 52, no. 3, pp. 1249–1253, Mar. 2006.
[4] C. Berrou, S. Kerouédan, Y. Saouter, C. Douillard, and M. Jézéquel, “Designing good permutations for turbo codes: Towards a single model,” in Proc. IEEE Int. Conf. Commun. (ICC), vol. 1, Paris, France, Jun. 2004, pp. 341–345.
[5] H. R. Sadjadpour, N. J. A. Sloane, M. Salehi, and G. Nebe, “Interleaver design for turbo codes,” IEEE J. Select. Areas Commun., vol. 19, no. 5, pp. 831–837, May 2001.
[6] O. Y. Takeshita and D. J. Costello, Jr., “New deterministic interleaver designs for turbo codes,” IEEE Trans. Inf. Theory, vol. 46, no. 6, pp. 1988–2006, Sep. 2000.
[7] S. Dolinar and D. Divsalar, “Weight distributions for turbo codes using random and nonrandom permutations,” Aug. 1995, TDA Progress Report 42-122, JPL, Pasadena, CA.
[8] D. Divsalar and F. Pollara, “Turbo codes for PCS applications,” in Proc. IEEE Int. Conf. Commun. (ICC), vol. 1, Seattle, WA, Jun. 1995, pp. 54–59.
[9] S. Crozier, P. Guinand, and A. Hunt, “Computing the minimum distance of turbo-codes using iterative decoding techniques,” in Proc. 22th Biennial Symp. Commun., Kingston, ON, Canada, May-Jun. 2004, pp. 306–308.
[10] S. Crozier and P. Guinand, “Distance upper bounds and true minimum distance results for turbo-codes designed with DRP interleavers,” in Proc. 3rd Int. Symp. on Turbo Codes & Related Topics, Brest, France, Sep. 2003, pp. 169–172.
[11] O. Y. Takeshita, “Permutation polynomial interleavers: An algebraic-geometric perspective,” IEEE Trans. Inf. Theory, vol. 53, no. 6, pp. 2116–2132, Jun. 2007.
[12] Y.-L. Chen, J. Ryu, and O. Y. Takeshita, “A simple coefficient test for cubic permutation polynomials over integer rings,” IEEE Commun. Lett., vol. 10, no. 7, pp. 549–551, Jul. 2006.
[13] A. Nimbalker, T. K. Blankenship, B. Classon, T. E. Fujita, and D. J. Costello, Jr., “Contention-free interleavers,” in Proc. IEEE Int. Symp. on Inf. Theory (ISIT), Chicago, IL, Jun.-Jul. 2004, p. 54.
[14] T. K. Blankenship, B. Classon, and V. Desai, “High-throughput turbo decoding techniques for 4G,” in Proc. Int. Conf. 3G Wireless and Beyond, San Francisco, CA, May 2002, pp. 137–142.
[15] “3rd generation partnership project; technical specification group radio access network; evolved universal terrestrial radio access (E-UTRA); multiplexing and channel coding (release 8),” Dec. 2008, 3GPP TS 36.212 v8.5.0.
[16] E. Rosnes and O. Y. Takeshita, “Optimum distance quadratic permutation-polynomial-based interleavers for turbo codes,” in Proc. IEEE Int. Symp. on Inf. Theory (ISIT), Seattle, WA, Jul. 2006, pp. 1988–1992.
[17] P. Guinand and J. Lodge, “Trellis termination for turbo encoders,” in Proc. 17th Biennial Symp. Commun., Kingston, ON, Canada, May-Jun. 1994, pp. 389–392.
[18] A. Nimbalker, Y. Blankenship, B. Classon, and T. K. Blankenship, “ARP and QPP interleavers for LTE turbo coding,” in Proc. IEEE Wireless Commun. and Networking Conf. (WCNC), Las Vegas, NV, Mar.-Apr. 2008, pp. 1032–1037.
[19] M. Punekar, F. Kienle, N. Wehn, A. Tanatmis, S. Ruzika, and H. W. Hamacher, “Calculating the minimum distance of linear block codes via integer programming,” in Proc. 6th Int. Symp. Turbo Codes & Iterative Information Processing, Brest, France, Sep. 2010, pp. 329–333.
[20] J. Ryu and O. Y. Takeshita, “On quadratic inverses for quadratic permutation polynomials over integer rings,” IEEE Trans. Inf. Theory, vol. 52, no. 3, pp. 1254–1260, Mar. 2006.
[21] J. Ryu, “Permutation polynomial based interleavers for turbo codes over integer rings: Theory and applications,” Ph.D. dissertation, Ohio State University, OH, Jun. 2007.
[22] E. Rosnes and O. Ytrehus, “Improved algorithms for the determination of turbo-code weight distributions,” IEEE Trans. Commun., vol. 53, no. 1, pp. 20–26, Jan. 2005.
[23] S. Crozier, P. Guinand, and A. Hunt, “Estimating the minimum distance of turbo-codes using double and triple impulse methods,” IEEE Commun. Lett., vol. 9, no. 7, pp. 631–633, Jul. 2005.