Some long rate one-half binary convolutional codes with an optimum distance profile

Johannesson, Rolf

Published in:
IEEE Transactions on Information Theory

1976

Link to publication

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
where $O$ is the $M$-by-$M$ cyclic permutation matrix (28) and $A(i)$ is defined in (4).

Let us first consider the case $M = 2^a - 1$. Define the following $M$-by-$M$ matrices:

$$Q = \begin{pmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \epsilon & \epsilon^2 & \epsilon^3 & \cdots & \epsilon^{2^a-1} \\
1 & \epsilon & \epsilon^2 & \epsilon^3 & \cdots & \epsilon^{2^a-1} \\
1 & \epsilon^2 & \epsilon^4 & \epsilon^6 & \cdots & \epsilon^{2^a} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \epsilon^{m-1} & \epsilon^{m-1} & \cdots & \cdots & \cdots \\
1 & \epsilon^{m-1} & \epsilon^{m-1} & \cdots & \cdots & \cdots \\
\end{pmatrix} \quad (A.2)$$

$$T = \text{diag} \left(1, \left(\frac{1}{j-j}\right), \ldots, \left(\frac{1}{j-j}\right)\right) \quad (A.3)$$

and

$$B = M \text{ diag} \left(1, 2, 2, \ldots, 2\right) \quad (A.4)$$

where

$$\epsilon = \exp \frac{2\pi}{M}, \quad i = \exp -\frac{2\pi}{M}. \quad (A.5)$$

We have

$$P = B^{-1/2}TQ. \quad (A.6)$$

**Proof:** By direct computation, it is easy to show that

$$QOQT = M \text{ diag} \left(1, \left(\frac{0}{\epsilon^h}ight), \left(\frac{0}{\epsilon^{2^h}}\right), \ldots, \left(\frac{0}{\epsilon^{2^h-1}}\right)\right). \quad (A.7)$$

Since $T$ and $QOQT$ exhibit a quasidiagonal form, to compute $T(QOQT)^T$ it is sufficient to consider only the product

$$\left(\begin{array}{c}
1 \\
\epsilon \\
\epsilon^2 \\
\vdots \\
\epsilon^{2^a-1} \\
\end{array}\right) \left(\begin{array}{c}
1 \\
\epsilon^h \\
\epsilon^{2^h} \\
\vdots \\
\epsilon^{2^h-1} \\
\end{array}\right) = \left(\begin{array}{cc}
2 \cos \frac{2\pi}{M} & 2 \sin \frac{2\pi}{M} \\
-2 \sin \frac{2\pi}{M} & 2 \cos \frac{2\pi}{M} \\
\end{array}\right) \quad (A.8)$$

Thus

$$TQOQT^T = M \text{ diag} \left(1, \left(\frac{2 \cos \frac{2\pi}{M}}{M}\right), \left(\frac{2 \sin \frac{2\pi}{M}}{M}\right), \ldots, \left(\frac{2 \cos \frac{2\pi}{M}}{M}\right), \left(\frac{2 \sin \frac{2\pi}{M}}{M}\right)\right) \quad (A.9)$$

Premultiplying and postmultiplying (A.9) by $B^{-1/2}$ and taking into account (A.6), we see that (A.1) holds true. Hence, we have only to show that $P$ is orthogonal. By direct computation, we get

$$(TQ)(TQ)^T - B$$

so that

$$(B^{-1/2}TQ)(B^{-1/2}TQ)^T = I$$

and $P = B^{-1/2}TQ$ is orthogonal. Q.E.D.

The construction of $P$ when $M = 2^a$ is similar, provided that the $M$-by-$M$ matrices $Q,T,$ and $B$ are defined as follows:

$$Q = \begin{pmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & -1 & -1 & \cdots & -1 \\
1 & \epsilon & \epsilon^2 & \epsilon^3 & \cdots & \epsilon^{2^a-1} \\
1 & \epsilon & \epsilon^2 & \epsilon^3 & \cdots & \epsilon^{2^a-1} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \epsilon^2 & \epsilon^4 & \epsilon^6 & \cdots & \epsilon^{2^a} \\
1 & \epsilon^2 & \epsilon^4 & \epsilon^6 & \cdots & \epsilon^{2^a} \\
\end{pmatrix}$$

$$T = \text{diag} \left(\frac{1}{j-j}, \left(\frac{1}{j-j}\right), \ldots, \left(\frac{1}{j-j}\right)\right) \quad (A.3)$$

$$B = M \text{ diag} \left(1, \left(\frac{1}{j-j}\right), \ldots, \left(\frac{1}{j-j}\right)\right) \quad (A.4)$$

**REFERENCES**


Some Long Rate One-Half Binary Convolutional Codes with an Optimum Distance Profile

ROLLF JOHANNESSEON, MEMBER, IEEE

**Abstract**—This correspondence gives a tabulation of long systematic, and long quick-look-in (QLI) nonsystematic, rate $R = \frac{1}{2}$ binary convolutional codes with an optimum distance profile (ODP). These codes appear attractive for use with sequential decoders.

In this correspondence we report the results of computer searches for long rate $R = \frac{1}{2}$ fixed convolutional encoders (FCE's) with an optimum distance profile (ODP codes), i.e., with a distance profile equal to or superior to that of any other code with a rate of $\frac{1}{2}$. Some Long Rate One-Half Binary Convolutional Codes with an Optimum Distance Profile

**REFERENCES**


Table I

<table>
<thead>
<tr>
<th>M</th>
<th>o(2)</th>
<th>d_M</th>
<th># paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>0101234567890</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>37</td>
<td>0101234567890</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>38</td>
<td>0101234567890</td>
<td>15</td>
<td>31</td>
</tr>
<tr>
<td>39</td>
<td>1001234567890</td>
<td>15</td>
<td>12</td>
</tr>
<tr>
<td>40</td>
<td>01101234567890</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>41</td>
<td>10101234567890</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>42</td>
<td>01101234567890</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>43</td>
<td>01101234567890</td>
<td>16</td>
<td>5</td>
</tr>
<tr>
<td>44</td>
<td>01101234567890</td>
<td>16</td>
<td>5</td>
</tr>
<tr>
<td>45</td>
<td>10101234567890</td>
<td>17</td>
<td>13</td>
</tr>
<tr>
<td>46</td>
<td>01101234567890</td>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>47</td>
<td>01101234567890</td>
<td>18</td>
<td>16</td>
</tr>
<tr>
<td>48</td>
<td>01101234567890</td>
<td>18</td>
<td>10</td>
</tr>
<tr>
<td>49</td>
<td>01101234567890</td>
<td>18</td>
<td>2</td>
</tr>
<tr>
<td>50</td>
<td>01101234567890</td>
<td>19</td>
<td>7</td>
</tr>
<tr>
<td>51</td>
<td>01101234567890</td>
<td>19</td>
<td>2</td>
</tr>
<tr>
<td>52</td>
<td>01101234567890</td>
<td>19</td>
<td>7</td>
</tr>
<tr>
<td>53</td>
<td>01101234567890</td>
<td>20</td>
<td>60</td>
</tr>
<tr>
<td>54</td>
<td>01101234567890</td>
<td>20</td>
<td>10</td>
</tr>
</tbody>
</table>

Table II

<table>
<thead>
<tr>
<th>M</th>
<th>o(1)</th>
<th>o(2)</th>
<th>d_M</th>
<th># paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>25</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>26</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>27</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>28</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>16</td>
<td>2</td>
</tr>
<tr>
<td>29</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>30</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>31</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>14</td>
<td>5</td>
</tr>
<tr>
<td>32</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>15</td>
<td>2</td>
</tr>
<tr>
<td>33</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>34</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>35</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>36</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>18</td>
<td>18</td>
</tr>
<tr>
<td>37</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>38</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>39</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>40</td>
<td>0101234567890</td>
<td>0101234567890</td>
<td>20</td>
<td>10</td>
</tr>
</tbody>
</table>

IEEE TRANSACTIONS ON INFORMATION THEORY, SEPTEMBER 1976

Fig. 1. Minimum distance d_M for some rate 1/2 convolutional codes. — d_M for ODP codes; - - - - d_M for codes of Bussgang (0 ≤ M ≤ 15), Lin–Lyne (18 ≤ M ≤ 20), and Forney (21 ≤ M ≤ 48); --- d_M for systematic Costello A1 codes; x - x - x - x - d_M for Massey–Costello QLI codes (0 ≤ M ≤ 47); - - - - Gilbert bound.

Thus d > d_j implies that the “early growth” of d_j with j greater than that of d_j with j. (It could, of course, happen that for sufficiently large j, d_j < d_j.)

Systematic ODP codes are already known for M ≤ 35 [1]. Newly found systematic ODP codes are listed in Table I for 36 ≤ M ≤ 60. The code generators are given in an octal form according to the convention in [1]. In cases where the optimum code is not unique, ties were resolved using the number of low-weight paths as a further optimality criterion.

Massey and Costello [3] introduced a class of quick-look-in (QLI) nonsystematic codes in which the two generators differ only in the second position. In Table II, we list newly found QLI codes for 24 ≤ M ≤ 60. For M ≤ 23 such codes are already known [1].

The excellence as regards d_M for the ODP codes can be seen from Fig. 1 in which we have plotted d_M for these codes; the best of the systematic codes found by Bussgang [4], Lin–Lyne [5], and Forney [6]: Costello's Algorithm A1 systematic codes [9]; and Massey–Costello's QLI codes [2], [3]. The codes are also compared with the Gilbert bound [2], [4]. We notice that the newly found codes have d_M equal to or superior to that of any previously known code with the same memory.

REFERENCES


Some Two-Weight Codes with Composite Parity-Check Polynomials

TOR HELLESETH

Abstract—The Hamming weight enumerator polynomials of some two-weight codes are presented. The codes have parity-check polynomials which are products of two irreducible polynomials.

I. INTRODUCTION

Let \( \psi \) be a primitive element of \( GF(q^n) \). Let \( h_d(x) = \psi^d \) denote the minimum polynomial of \( \psi^d \). Then \( h_d(x) \) is a primitive polynomial if and only if \( \gcd(d, q^n - 1) = 1 \).

It is well known that codes which have primitive parity-check polynomials are equidistant in the Hamming metric. In Kjelgaard and Oganesyan, Yagdzyan, and Tairoyan [3], some other cyclic equidistant codes are found. From the papers of Semakov and Zinov’ev [4] and Semakov, Zinov’ev, and Zaitsev [5], it can be concluded that every equidistant cyclic code has an irreducible parity-check polynomial.

Here we study codes that have parity-check polynomials which are the product of two irreducible polynomials. Since the codes do not have an irreducible parity-check polynomial, at least two nonzero Hamming weights must occur in the codewords. We present here a family of nonbinary cyclic codes with composite parity-check polynomials such that only two nonzero weights occur.

Some of the codes have parity-check polynomials which are a product of two primitive polynomials of the same degree. The complete weight enumerator of such codes has been studied indirectly by studying the cross-correlation function between two maximal-length linear sequences. In Helleseh [1], it is proved that, for \( q = p^n \), where \( p \) is a prime and \( n = 1 \), at least three different nonzero weights occur in the complete weight enumerator. In particular, if we consider instead the Hamming weight enumerator, it is possible to achieve only two nonzero weights.

II. THE TWO-WEIGHT CODES

Let \( \deg h(x) \) denote the degree of \( h(x) \) and let \( \deg h(x) \) denote the least positive integer \( r \) such that \( h(x) \) divides \( x^r - 1 \).

Lemma: Let \( \gcd(k, N_1) = \gcd(k, N_2) = \gcd(t, N_2) = 1 \), where \( N_1 \) and \( N_2 \) divide \( q - 1 \). Let \( d_1 = (q^k - 1)/N_1 + 1 \) and \( d_2 = (q^k - 1)/N_2 + 1 \). We then have that

i) \( \deg h_{d_1}(x) = \deg h_{d_2}(x) = k \);

ii) \( \deg h_{d_1}(x) = (q^k - 1)/\gcd(d_1, N_1) \), \( \deg h_{d_2}(x) = (q^k - 1)/\gcd(d_2, N_2) \);

iii) let \( d_i = q^k d_i \) (mod \( q^k - 1 \)), for all \( i \geq 0 \); let \( h(x) = h_{d_1}(x) h_{d_2}(x) \), then \( \deg h(x) = (q^k - 1)/\gcd(d_1, d_2, N_1, N_2) \).

Proof: i) Let \( \deg h_{d_1}(x) = m \). By definition, \( m \) is the least positive integer such that

\[ (q^{(q^k - 1)/N_1 + 1}x^{q^k - 1} - 1) = 1. \]

Therefore

\[ ((q^k - 1)/N_1 + 1)(q^m - 1) \equiv 0 \pmod{q^k - 1}. \]

Since \( N_1 \) divides \( q - 1 \), this means

\[ q^m - 1 \equiv 0 \pmod{q^k - 1}. \]

Hence \( m \geq k \) and, therefore, \( m = k \). The proof that \( \deg h_{d_2}(x) = k \) is similar.

ii) Since \( \gcd(d_i, q^k - 1) = \gcd(d_i, N_i) \), for \( i = 1,2 \), we have

\[ \deg h_{d_i}(x) = (q^k - 1)/\gcd(d_i, q^k - 1) = (q^k - 1)/\gcd(d_i, N_i). \]

iii) Since \( d_1 = q^k d_2 \) (mod \( q^k - 1 \)), for all \( i \geq 0 \), we have \( \gcd(h_{d_1}(x), h_{d_2}(x)) = 1 \). Hence

\[ \deg h(x) = \deg(h_{d_1}(x), h_{d_2}(x)). \]

We are now able to prove the main theorem.

Theorem: Let \( d_1 \) and \( d_2 \) be defined as in the lemma. Put \( N = \lcm(N_1, N_2) \). Suppose \( \gcd((d_1, q^k - 1)) \) and \( \gcd(d_2, q^k - 1)) = 1 \). Let \( V \) be the \( (q^k - 1)/2 \) cyclic code with parity-check polynomial \( h(x) = h_{d_1}(x) h_{d_2}(x) \). Then the weight enumerator polynomial of \( V \) is

\[ A(x) = 1 + (q^k - 1) \frac{N}{u} x^{(q^k - 1)/q^m - 1} + \left( q^{2k} - 1 - (q^k - 1) \frac{N}{u} \right) x^{(q^k - 1)/q^m}. \]

where

\[ u = \gcd(N, N_1 - t N_2/N). \]

Proof: By \( \text{iii) of the lemma} \), we have \( \deg h(x) = q^k - 1 \). Let \( a_1, a_2 \in GF(q^k) \). Let \( v(a_1, a_2) = (v_0, v_1, \ldots, v_{q^k - 2}) \) with

\[ v_0 = \text{tr}(a_1 \psi^{d_1} + a_2 \psi^{d_2}), \]

where

\[ \text{tr}(x) = \sum_{i=0}^{k-1} x^{q^i}. \]

We then have

\[ V = \{ v(a_1, a_2) \mid a_1, a_2 \in GF(q^k) \}. \]

Let \( j = N_2 + j_1 \), with \( 0 \leq j_2 < (q^k - 1)/N \) and \( 0 \leq j_1 < N \). Then

\[ v_j = \text{tr} \left( a_1 \psi^{d_1} + a_2 \psi^{d_2} \right) \]

since \( d_i = (N - 1)/N_i \) and \( N = (q^k - 1)/N_i + 1 \) if \( a \neq 0 \). Therefore

\[ v_{N_2+j_1} = \text{tr} \left( \psi^{d_1} + a_2 \psi^{d_1} - a_2 \psi^{d_1} \right). \]

Let \( T(a) = \{ (j, v_j) \} \). From Oganesyan, Yagdzyan, and Tairoyan [3, p. 220] we have

\[ T(a) = \begin{cases} 0, & \text{if } a = 0, \\ \left( q^{k-1}(q-1)/N \right), & \text{if } a \neq 0. \end{cases} \]

Let

\[ S(a_1, a_2) = |ij| a_1 \psi^{d_1} + a_2 \psi^{d_1} = 0, \quad 0 \leq j < N. \]