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

Johannesson, Rolf

Published in:
IEEE Transactions on Information Theory

Published: 1976-01-01

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 \( M \times M \) cyclic permutation matrix (28) and \( A(i) \) is defined in (4).

Let us first consider the case \( M = 2^e - 1 \). Define the following \( M \times M \) matrices:

\[
Q = \begin{pmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \epsilon & \epsilon^2 & \epsilon^3 & \cdots & \epsilon^{(2^e-1)} \\
1 & \epsilon^2 & \epsilon^4 & \epsilon^6 & \cdots & \epsilon^{2(2^e-1)} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \epsilon^{(-1)} & \cdots & \cdots & \cdots & 1 \\
1 & \epsilon & \cdots & \cdots & \cdots & 1
\end{pmatrix}
\]

(A.2)

\[
T = \text{diag} \left( 1, \left(\frac{1}{j-j}\right), \cdots, \left(\frac{1}{j-j}\right) \right)
\]

(A.3)

and

\[
B = M \text{ diag} (1,2,2,\cdots,2)
\]

where

\[
\epsilon = \exp \frac{2\pi}{M} \quad i = \exp -\frac{2\pi}{M}
\]

We have

\[
P = B^{-1/2}TQ.
\]

(A.6)

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

\[
QOQT = M \text{ diag} \left( 1, \left(\frac{0}{\epsilon \cdots 0}\right), \left(\frac{0}{\epsilon^2 \cdots 0}\right), \cdots, \left(\frac{0}{\epsilon^{(-1)} \cdots 0}\right) \right)
\]

(A.7)

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

\[
\left(\frac{1}{j-j}\right) \left(\frac{0}{\epsilon^h \cdots 0}\right) \left(\frac{1}{j-j}\right)
\]

Thus

\[
TQOQT = M \text{ diag} \left( 1, \left(\frac{2 \cos \frac{2\pi}{M} \hbar}{2 \sin \frac{2\pi}{M} \hbar}\right) \ldots \right)
\]

(A.8)

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

\[
(B^{-1/2}T)(B^{-1/2}T)^T = I
\]

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

The construction of \( P \) when \( M = 2^e \) is similar, provided that the \( M \times M \) matrices \( Q, T, \) and \( B \) are defined as follows:

\[
Q = \begin{pmatrix}
1 & 1 & 1 & \cdots & 1 \\
\epsilon & \epsilon^2 & \epsilon^3 & \cdots & \epsilon^{(2^e-1)} \\
\epsilon^2 & \epsilon^4 & \epsilon^6 & \cdots & \epsilon^{2(2^e-1)} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
\epsilon^{(-1)} & \cdots & \cdots & \cdots & \cdots & \epsilon \\
1 & \epsilon & \cdots & \cdots & \cdots & 1
\end{pmatrix}
\]

\[
T = \text{diag} \left( 1, \left(\frac{j-j}{j-j}\right), \cdots, \left(\frac{j-j}{j-j}\right) \right)
\]

\[
B = M \text{ diag} (1,1,2,2,\cdots,2)
\]

References


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

ROLF JOHANNESSEN, 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 some other code with

Manuscript received September 2, 1975; revised January 26, 1976. This work was supported in part by the National Aeronautics and Space Administration under NASA Grant NGR 50025 at the University of Notre Dame in liaison with the Communications and Navigation Division of the Goddard Space Flight Center and in part by the Swedish Board of Technical Development under Grant 75-4165.

The author is with the Department of Automata and General Systems Sciences, University of Lund, Lund, Sweden.
IEEE TRANSACTIONS ON INFORMATION THEORY, SEPTEMBER 1976

Table I

<table>
<thead>
<tr>
<th>M</th>
<th>(d_0(2))</th>
<th>(d_M)</th>
<th># paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>671415454704</td>
<td>14</td>
<td>5</td>
</tr>
<tr>
<td>37</td>
<td>671415454676</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>38</td>
<td>671415455564</td>
<td>15</td>
<td>31</td>
</tr>
<tr>
<td>39</td>
<td>740424020712</td>
<td>15</td>
<td>12</td>
</tr>
<tr>
<td>40</td>
<td>611415457371</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>41</td>
<td>740424020737</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>42</td>
<td>671415455564</td>
<td>16</td>
<td>31</td>
</tr>
<tr>
<td>43</td>
<td>740424020712</td>
<td>16</td>
<td>14</td>
</tr>
<tr>
<td>44</td>
<td>740424020712</td>
<td>16</td>
<td>5</td>
</tr>
<tr>
<td>45</td>
<td>740424020712</td>
<td>16</td>
<td>5</td>
</tr>
<tr>
<td>46</td>
<td>740424020746</td>
<td>17</td>
<td>39</td>
</tr>
<tr>
<td>47</td>
<td>740424020712</td>
<td>17</td>
<td>13</td>
</tr>
<tr>
<td>48</td>
<td>740424020712</td>
<td>17</td>
<td>4</td>
</tr>
<tr>
<td>49</td>
<td>740424020712</td>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>50</td>
<td>740424020712</td>
<td>18</td>
<td>38</td>
</tr>
<tr>
<td>51</td>
<td>740424020712</td>
<td>18</td>
<td>16</td>
</tr>
<tr>
<td>52</td>
<td>740424020712</td>
<td>18</td>
<td>7</td>
</tr>
<tr>
<td>53</td>
<td>740424020712</td>
<td>18</td>
<td>2</td>
</tr>
<tr>
<td>54</td>
<td>740424026636</td>
<td>19</td>
<td>13</td>
</tr>
<tr>
<td>55</td>
<td>740424026636</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>56</td>
<td>740424026636</td>
<td>19</td>
<td>7</td>
</tr>
<tr>
<td>57</td>
<td>740424026636</td>
<td>19</td>
<td>2</td>
</tr>
<tr>
<td>58</td>
<td>740424026636</td>
<td>20</td>
<td>60</td>
</tr>
<tr>
<td>59</td>
<td>740424026636</td>
<td>20</td>
<td>95</td>
</tr>
<tr>
<td>60</td>
<td>740424026636</td>
<td>20</td>
<td>10</td>
</tr>
</tbody>
</table>

Table II

<table>
<thead>
<tr>
<th>M</th>
<th>(d_0(1))</th>
<th>(d_0(2))</th>
<th>(d_M)</th>
<th># paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>740424174</td>
<td>740424174</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>25</td>
<td>740424175</td>
<td>740424175</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>26</td>
<td>740424173</td>
<td>740424173</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>27</td>
<td>740424172</td>
<td>740424172</td>
<td>10</td>
<td>23</td>
</tr>
<tr>
<td>28</td>
<td>740424171</td>
<td>740424171</td>
<td>12</td>
<td>8</td>
</tr>
<tr>
<td>29</td>
<td>740424171</td>
<td>740424171</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>30</td>
<td>7404242074</td>
<td>7404242074</td>
<td>14</td>
<td>13</td>
</tr>
<tr>
<td>31</td>
<td>7404242072</td>
<td>7404242072</td>
<td>13</td>
<td>15</td>
</tr>
<tr>
<td>32</td>
<td>7404242071</td>
<td>7404242071</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>33</td>
<td>7404242071</td>
<td>7404242071</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>34</td>
<td>7404242072</td>
<td>7404242072</td>
<td>14</td>
<td>34</td>
</tr>
<tr>
<td>35</td>
<td>7404242663</td>
<td>7404242663</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>36</td>
<td>7404242664</td>
<td>7404242664</td>
<td>14</td>
<td>5</td>
</tr>
<tr>
<td>37</td>
<td>7404242662</td>
<td>7404242662</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>38</td>
<td>7404242071</td>
<td>7404242071</td>
<td>15</td>
<td>31</td>
</tr>
<tr>
<td>39</td>
<td>7404242071</td>
<td>7404242071</td>
<td>15</td>
<td>12</td>
</tr>
<tr>
<td>40</td>
<td>7404242071</td>
<td>7404242071</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>41</td>
<td>7404242071</td>
<td>7404242071</td>
<td>15</td>
<td>5</td>
</tr>
<tr>
<td>42</td>
<td>7404242071</td>
<td>7404242071</td>
<td>16</td>
<td>31</td>
</tr>
<tr>
<td>43</td>
<td>7404242071</td>
<td>7404242071</td>
<td>16</td>
<td>14</td>
</tr>
<tr>
<td>44</td>
<td>7404242071</td>
<td>7404242071</td>
<td>16</td>
<td>7</td>
</tr>
<tr>
<td>45</td>
<td>7404242071</td>
<td>7404242071</td>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>46</td>
<td>7404242071</td>
<td>7404242071</td>
<td>17</td>
<td>39</td>
</tr>
<tr>
<td>47</td>
<td>7404242071</td>
<td>7404242071</td>
<td>17</td>
<td>13</td>
</tr>
<tr>
<td>48</td>
<td>7404242071</td>
<td>7404242071</td>
<td>17</td>
<td>4</td>
</tr>
<tr>
<td>49</td>
<td>7404242071</td>
<td>7404242071</td>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>50</td>
<td>7404242071</td>
<td>7404242071</td>
<td>18</td>
<td>38</td>
</tr>
</tbody>
</table>

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 [2]; and Massey–Costello 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.

Fig. 1. Minimum distance \(d_M\) for some rate \(1/2\) convolutional codes. — \(d_M\) for ODP codes; - - - - - - \(d_M\) for mas for systematic Costello A1 codes; x - x - x - x - d_M for Massey–Costello QLI codes (0 \(\leq M \leq 47\)); - - - - - - Gilbert bound.

Thus \(d > d_j\) implies that the “early growth” of \(d_j\) with \(j\) is 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 \(M \leq 35\) [1]. Newly found systematic ODP codes are listed in Table I for \(M = 36 \leq M \leq 60\). 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 ODP QLI codes for \(24 \leq M \leq 50\). For \(M = 28\) such codes are already known [1].

The references 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 [2]; 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

[3] J. L. Massey and D. J. Costello, Jr., “Nonsystematic convolutional...
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 $GF(q^k)$. Let $h_d(x) \subseteq GF(q)[x]$ denote the minimum polynomial of $\psi^d$. Then $h_d(x)$ is a primitive polynomial if and only if $\gcd(d,q^k-1) = 1$.

It is well known that codes which have primitive parity-check polynomials are equivalent in the Hamming metric. In Kjærgaard [2] and Oganessian, Yagdzyan, and Taiaryan [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 products 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 Helleseth [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 $p h(x)$ denote the least positive integer $r$ such that $h(x)$ divides $x^r-1$.

**Lemma:** Let $\gcd(k,N_1) = \gcd(k,N_2) = \gcd(t,N_3) = 1$, where $N_1$ and $N_2$ divide $q-1$. Let $d_1 = (q^k-1)/N_1 + 1$ and $d_2 = t(q^k-1)/N_2 + 1$. Then we have that

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

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

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

**Proof:**

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

$$(q^k(q^k-1)/N_1+1)^{m-1} = 1.$$ 

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 $\gcd(d_1,q^k-1) = \gcd(d_1,N_1)$, for $i = 1, 2$, we have

$\per h_{d_1}(x) = (q^k-1)/\gcd(d_1,q^k-1) = (q^k-1)/\gcd(d_1,N_1).$

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

$\per h(x) = \lcm(\per h_{d_1}(x), \per h_{d_2}(x))$

$$= (q^k-1)/\gcd(d_1,N_1)\gcd(d_2,N_2).$$

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 $\gcd(d_1,d_2,N_1,N_2) = 1$. Let $V$ be the $(q^k + 1,2k)$ cyclic code with parity-check polynomial $h(x) = h_{d_1}(x)/h_{d_2}(x)$. Then the weight enumerator polynomial of $V$ is

$$A(z) = 1 + (q^k - 1)\frac{N}{u} z^{q^k-1-(q^k-1)/u/N} + \left(\frac{q^k - 1}{u} - (q^k - 1)\frac{N}{u}\right) z^{q^k-1}$$

where

$u = \gcd(N, N_1 - t N_3/N_2).$

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

$\nu_j = \tr_{q^k/q}^{1/2}(a_1 \psi^j + a_2 \psi^j),$

where

$\tr_{q^k/q}^{1/2}(x) = \sum_{i=0}^{q^k-1} x^i.$

We then have

$$V = \{v(a_1,a_2) | a_1,a_2 \subseteq GF(q^k)\}.$$

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

$\nu_j = \tr_{q^k/q}^{1/2}(a_1 \psi^{j(N_1+j_1)} + a_2 \psi^{j(N_2+j_1)})$

$$= \tr_{q^k/q}^{1/2}(a_1 \psi^{j(N_2+j_1)} + a_2 \psi^{j(N_2+j_1)}),$$

since $d_N = ((q^k - 1)/N_1 + 1)N = N$ (mod $q^k - 1$), for $i = 1,2$. Therefore

$\nu_{N_2+j_1} = \tr_{q^k/q}^{1/2}(\psi^{j(N_1+j_1)} + \psi^{j(N_2+j_1)}).$

Let $T(a) = \{|v| \mid \nu(v) \neq 0, 0 \leq j < (q^k-1)/N\}$. From Oganessian, Yagdzyan, and Taiaryan [3, p. 220] we have

$$T(a) = \{0, \text{ if } u = 0 \}

\quad \left(\frac{q^k-1}{u} - (q^k-1)/N, \text{ if } a \neq 0.\right)$$

Let

$$S(a_1,a_2) = \{|v| \mid a_1 \psi^{j_1} + a_2 \psi^{j_2} = 0, 0 \leq j_1 < N\}.$$