WEIGHT DISTRIBUTIONS OF SOME CLASSES OF BINARY CYCLIC CODES

Carlos R.P. Hartmann  
*Syracuse University*, chartman@syr.edu

J. R. Riek Jr.  
*Syracuse University*

Ralph J. Longobardi

Follow this and additional works at: [https://surface.syr.edu/eecs_techreports](https://surface.syr.edu/eecs_techreports)

Part of the Computer Sciences Commons

Recommended Citation  
[https://surface.syr.edu/eecs_techreports/20](https://surface.syr.edu/eecs_techreports/20)

This Report is brought to you for free and open access by the College of Engineering and Computer Science at SURFACE. It has been accepted for inclusion in Electrical Engineering and Computer Science - Technical Reports by an authorized administrator of SURFACE. For more information, please contact surface@syr.edu.
WEIGHT DISTRIBUTIONS OF SOME
CLASSES OF BINARY CYCLIC CODES

MARCH 1974

C. R. P. Hartmann
J. R. Riek, Jr.
R. J. Longobardi

SYSTEMS AND INFORMATION SCIENCE
SYRACUSE UNIVERSITY
WEIGHT DISTRIBUTIONS OF SOME CLASSES
OF BINARY CYCLIC CODES

by

C. R. P. Hartmann
J. R. Riek, Jr.
R. J. Longobardi

Abstract: Let $h_1(x)h_2(x)$ be the parity check polynomial of a binary cyclic code. This article presents a formula for decomposing words in the code as sums of multiples of words in the codes whose parity check polynomials are $h_1(x)$ and $h_2(x)$. This decomposition provides information about the weight distribution of the code.

This work was supported by National Science Foundation Grants GK-37449 and GK-34915.
Let \( h_1(x)h_2(x) \) be the parity check polynomial of a binary cyclic code, where the degrees of \( h_1(x) \) and \( h_2(x) \) are \( m_1 \) and \( m_2 \), and the exponents of \( h_1(x) \) and \( h_2(x) \) are \( n_1 \) and \( n_2 \) respectively. The generalization of what follows to more than two factors is straightforward and will not be considered here.

Let the code length be \( n = \text{l.c.m.} (n_1, n_2) = \frac{n_1 n_2}{d} \), where \( d = \text{g.c.d.} (n_1, n_2) \). Then \( g(x) = \frac{x^n+1}{h(x)} \) and each codeword \( v(x) \) can be written \( v(x) = m(x)g(x) \), where \( m(x) \) is a message polynomial of degree at most \((m_1 + m_2) - 1\). Since \( \text{g.c.d.} (h_1(x), h_2(x)) = 1 \), we may write each message polynomial \( m(x) \) as

\[
m(x) = a(x)h_1(x) + b(x)h_2(x)
\]

for some choice of \( a(x) \) and \( b(x) \). The representation is made unique by requiring that \( \deg a(x) < m_2 \) and \( \deg b(x) < m_1 \). Next let \( g_1(x) = \frac{x^n+1}{h_1(x)} \) and \( g_2(x) = \frac{x^n+1}{h_2(x)} \). We now substitute to obtain

\[
v(x) = m(x)g(x) = [a(x)h_1(x) + b(x)h_2(x)] \frac{x^n+1}{h(x)}
\]

\[
= a(x)g_2(x) \left( \frac{x^n+1}{x^{n_2}+1} \right) + b(x)g_1(x) \left( \frac{x^n+1}{x^{n_1}+1} \right)
\]

\[
= v_2(x) \left[ x^{\left( \frac{n_2}{d} - 1\right)} + \ldots + x^{n_2+1} \right] + v_1(x) \left[ x^{\left( \frac{n_1}{d} - 1\right)} + \ldots + x^{n_1+1} \right]
\]

\[
= v_2^*(x) + v_1^*(x),
\]

where \( v_2(x) = a(x)g_2(x) \) and \( v_1(x) = b(x)g_1(x) \). Note that \( \deg v_2(x) < n_2 \) and \( \deg v_1(x) < n_1 \).
Define $I = \{x^i : x^i \text{ has a non-zero coefficient in both } v_1^*(x) \text{ and } v_2^*(x)\}$. Then $I$ is just the intersection of $v_1^*(x)$ and $v_2^*(x)$. We have now proved the following theorem concerning $w(v)$, the weight of $v(x)$.

**Theorem:** $w(v) = \frac{n_1}{d} w(v_2) + \frac{n_2}{d} w(v_1) - 2|I|$.

Assuming that the weight distributions of the codes generated by $g_1(x)$ and $g_2(x)$ are known, the key to the weight of $v(x)$ lies in the ability to determine $|I|$. We proceed as follows.

Let $[j] = \{j, j+d, j+2d, \ldots\}$ for each $j = 0, 1, \ldots, d-1$. Then we define

$I_j^{(1)} = \{x^k : x^k \text{ has non-zero coefficient in } v_1(x) \text{ and } k \in [j]\}$

$I_j^{(2)} = \{x^k : x^k \text{ has non-zero coefficient in } v_2(x) \text{ and } k \in [j]\}$.

Now if $x_1$ has a non-zero coefficient in $v_1^*(x)$ and $x_2$ has a non-zero coefficient in $v_2^*(x)$, we wish to know under what conditions $x_1^{k_1} + \theta_1 n_1$ and $x_2^{k_2} + \theta_2 n_2$ for $0 \leq \theta_1 < \frac{n_2}{d}$ and $0 \leq \theta_2 < \frac{n_1}{d}$ will coincide.

**Lemma:** $k_1 + \theta_1 n_1 = k_2 + \theta_2 n_2$ for $0 \leq \theta_1 < \frac{n_2}{d}$, $0 \leq \theta_2 < \frac{n_1}{d}$ iff $k_1 - k_2 \equiv 0 \pmod{d}$.

**Proof:** Note that $\text{g.c.d.} \left(\frac{n_1}{d}, \frac{n_2}{d}\right) = 1$. Then $k_1 + \theta_1 n_1 = k_2 + \theta_2 n_2$ and $k_1 + \theta_1' n_1 = k_2 + \theta_2' n_2$ implies that $\theta_1 = \theta_1'$ and $\theta_2 = \theta_2'$. The lemma now follows. Q.E.D.
Thus for a particular choice of \( v_1(x) \) and \( v_2(x) \), the value of \( |I| \) is given by
\[
|I| = \sum_{j=0}^{d-1} |I_j^{(1)}||I_j^{(2)}|.
\]

Although approached from different points of view, special cases of the above theorem have already been obtained. They are listed below as corollaries.

**Corollary (Kasami [1]):** If \( \text{g.c.d.} (n_1,n_2) = 1 \), then
\[
w(v) = n_1 w(v_2) + n_2 w(v_1) - 2 w(v_1) w(v_2).
\]

**Corollary (Varshamov and Tenegolts [2]):** If \( \text{g.c.d.} (n_1,n_2) = 1 \), and \( h_1(x) \) and \( h_2(x) \) are primitive polynomials, the minimum distance of the code whose parity check polynomial is \( h_1(x)h_2(x) \) is
\[
2^{m_1+m_2-1} - 2^{m_1-1} - 2^{m_2-1}.
\]

We shall now describe two classes of codes to which the above theorem is easily applied.

Suppose \( h_1(x) \) and \( h_2(x) \) are primitive polynomials. Then the codes generated by \( g_1(x) \) and \( g_2(x) \) are maximum length sequence codes, where each codeword is a cyclic shift of the generator polynomial. Having found \( g_1(x) \) and \( g_2(x) \), the determination of \( I_j^{(1)} \) and \( I_j^{(2)} \) is quite simple. Numerical results are listed in Table 1 and Table 2.

Suppose \( h_1(x) = \frac{n_1+1}{x+1} \) and \( h_2(x) \) is primitive, where \( n_1 | n_2 \). Then \( g_1(x) = x+1 \) and the code generated by \( g_1(x) \) consists
of all words of even weight. Numerical results are listed in Table 3.

In the course of preparing this paper for publication, it was discovered that a (31,10) code with minimum distance 10 is missing from the Chen [3] tables in the back of Peterson and Weldon [4]. This code has a parity check polynomial which is the product of two primitive polynomials of degree six, one of which is the reciprocal of the other. However, this code is included in Table 16.1 of Berlekamp [5].

The following symbols are used to label the columns of the tables.

(n,k): n = code length, k = degree of the parity check polynomial.

h(x): parity check polynomial of the code. The tuple \((i_1, i_2, \ldots, i_n)\)

means \(h(x) = m_{i_1}(x) m_{i_2}(x) \ldots m_{i_n}(x)\) where \(m_{i_j}(x)\) is the minimal polynomial of \(\alpha^j\), \(\alpha\) a primitive \(n^{th}\) root of unity.

d_0: BCH minimum distance of the code.

d: actual minimum distance of the code.
<table>
<thead>
<tr>
<th>$(n,k)$</th>
<th>$h(x)$</th>
<th>$d_0$</th>
<th>40</th>
<th>38</th>
<th>36</th>
<th>34</th>
<th>32</th>
<th>30</th>
<th>28</th>
<th>26</th>
<th>24</th>
<th>20</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(63,12)$</td>
<td>$(1,31)$</td>
<td>22</td>
<td>378</td>
<td>441</td>
<td>756</td>
<td>882</td>
<td>378</td>
<td>567</td>
<td>504</td>
<td>189</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$(63,12)$</td>
<td>$(1,23)$</td>
<td>16</td>
<td>1134</td>
<td>1827</td>
<td>756</td>
<td>252</td>
<td>126</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$(63,12)$</td>
<td>$(1,13)$</td>
<td>24</td>
<td>378</td>
<td>3087</td>
<td>630</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Weight distributions for selected $(63,12)$ binary cyclic codes
<table>
<thead>
<tr>
<th>(n,k)</th>
<th>h(x)</th>
<th>d₀</th>
<th>84</th>
<th>74</th>
<th>72</th>
<th>70</th>
<th>68</th>
<th>66</th>
<th>64</th>
<th>62</th>
<th>60</th>
<th>58</th>
<th>56</th>
<th>54</th>
<th>52</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>(127,14)</td>
<td>(1,63)</td>
<td>42</td>
<td>889</td>
<td>889</td>
<td>1016</td>
<td>2667</td>
<td>889</td>
<td>2032</td>
<td>2667</td>
<td>889</td>
<td>1778</td>
<td>1778</td>
<td>889</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(127,14)</td>
<td>(3,63)</td>
<td>44</td>
<td>127</td>
<td>1778</td>
<td>3556</td>
<td>4699</td>
<td>3556</td>
<td>1778</td>
<td>889</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(127,14)</td>
<td>(5,63)</td>
<td>52</td>
<td>127</td>
<td>1778</td>
<td>3556</td>
<td>4699</td>
<td>3556</td>
<td>1778</td>
<td>889</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(127,14)</td>
<td>(7,63)</td>
<td>56</td>
<td>3556</td>
<td>8255</td>
<td>4572</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(127,14)</td>
<td>(9,63)</td>
<td>48</td>
<td>127</td>
<td>1778</td>
<td>3556</td>
<td>4699</td>
<td>3556</td>
<td>1778</td>
<td>889</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(127,14)</td>
<td>(11,63)</td>
<td>52</td>
<td>3556</td>
<td>8255</td>
<td>4572</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(127,14)</td>
<td>(19,63)</td>
<td>48</td>
<td>3556</td>
<td>8255</td>
<td>4572</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(127,14)</td>
<td>(21,63)</td>
<td>34</td>
<td>3556</td>
<td>8255</td>
<td>4572</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Weight distributions for selected (127,14) binary cyclic codes
Table 3. Minimum distance values for selected binary cyclic codes of length 63

<table>
<thead>
<tr>
<th>(n,k)</th>
<th>h(x)</th>
<th>d₀</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>(63,8)</td>
<td>(1,21)</td>
<td>26</td>
<td>26</td>
</tr>
<tr>
<td>(63,12)</td>
<td>(1,9,27)</td>
<td>18</td>
<td>18</td>
</tr>
<tr>
<td>(63,14)</td>
<td>(1,7,21)</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>(63,26)</td>
<td>(1,3,9,15,21,27)</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>(63,9)</td>
<td>(0,1,21)</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>(63,13)</td>
<td>(0,1,9,27)</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>(63,15)</td>
<td>(0,1,7,21)</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>(63,27)</td>
<td>(0,1,3,9,15,21,27)</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
BIBLIOGRAPHY


