3-1974

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

WEIGHT DISTRIBUTIONS OF SOME CLASSES OF BINARY CYCLIC CODES

MARCH 1974

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

SYRACUSE UNIVERSITY SUOS CULTORES SCIENTIA CORONAT FOUNDED A·D·1870

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 $n = \text{l.c.m.}\ (n_1,n_2) = n_1n_2/d$, where $d = \text{g.c.d.}\ (n_1,n_2)$. Then $g(x) = (x^n+1)/h(x)$ 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 $g_1(x) = (x^{n_1}+1)/h_1(x)$ and $g_2(x) = (x^{n_2}+1)/h_2(x)$. We now substitute to obtain

$$\begin{aligned} v(x) &= m(x)g(x) = [a(x)h_1(x)+b(x)h_2(x)]\ (x^n+1)/h(x) \\ &= a(x)g_2(x)\ [(x^n+1)/(x^{n_2}+1)] + b(x)g_1(x)\ [(x^n+1)/(x^{n_1}+1)] \\ &= v_2(x)\ [x^{n_2(\frac{n_1}{d}-1)} + \ldots + x^{n_2}+1] + v_1(x)\ [x^{n_1(\frac{n_2}{d}-1)} + \ldots \\ &\qquad + x^{n_1}+1] \\ &= v_2^*(x) + v_1^*(x)\ , \end{aligned}$$

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 $I = \{x^i : x^i$ has a non-zero coefficient in both $v_1^*(x)$ 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 $v(x)$.

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

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

<u>Lemma</u>: $k_1 + \theta_1 n_1 = k_2 + \theta_2 n_2$ for $0 \le \theta_1 < \frac{n_2}{d}$, $0 \le \theta_2 < \frac{n_1}{d}$ iff

$k_1 - k_2 \equiv 0 \bmod d$.

<u>Proof</u>: Note that g.c.d. $(\frac{n_1}{d}, \frac{n_2}{d}) = 1$. 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 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 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 $h_1(x) = (x^{n_1}+1)/(x+1)$ 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 α^{i_j}, α a primitive n^{th} root of unity.

d_0: BCH minimum distance of the code.

d: actual minimum distance of the code.

(n,k)	h(x)	d_0	WEIGHT DISTRIBUTION										
			40	38	36	34	32	30	28	26	24	20	0
(63,12)	(1,31)	22		378	441	756	882	378	567	504	189		1
(63,12)	(1,23)	16			1134		1827		756		252	126	1
(63,12)	(1,13)	24	378				3087				630		1

Table 1. Weight distributions for selected (63,12) binary cyclic codes

			WEIGHT DISTRIBUTION													
(n,k)	h(x)	d_0	84	74	72	70	68	66	64	62	60	58	56	54	52	0
(127,14)	(1,63)	42		889	889	1016	2667	889	2032	2667	889	1778	1778	889		1
(127,14)	(3,63)	44	127		1778		3556		4699		3556		1778		889	1
(127,14)	(5,63)	52	127		1778		3556		4699		3556		1778		889	1
(127,14)	(7,63)	56			3556				8255				4572			1
(127,14)	(9,63)	48	127		1778		3556		4699		3556		1778		889	1
(127,14)	(11,63)	52			3556				8255				4572			1
(127,14)	(19,63)	48			3556				8255				4572			1
(127,14)	(21,63)	34			3556				8255				4572			1

Table 2. Weight distributions for selected (127,14) binary cyclic codes

(n,k)	h(x)	d_0	d
(63,8)	(1,21)	26	26
(63,12)	(1,9,27)	18	18
(63,14)	(1,7,21)	14	14
(63,26)	(1,3,9,15,21,27)	6	6

(n,k)	h(x)	d_0	d
(63,9)	(0,1,21)	21	21
(63,13)	(0,1,9,27)	9	9
(63,15)	(0,1,7,21)	7	7
(63,27)	(0,1,3,9,15,21,27)	3	3

Table 3. Minimum distance values for selected binary cyclic codes of length 63

BIBLIOGRAPHY

[1] T. Kasami, "Some lower bounds on the minimum weight of cyclic codes of composite length," IEEE Trans. Inform. Theory, vol. IT-14, pp. 814-818, Nov. 1968.

[2] R. R. Varshamov and G. M. Tenengolts, "On a class of cyclic codes" (in Russian), Problems of Cybernetics, vol. 22, pp. 157-166, Moscow, 1970.

[3] C. L. Chen, "Computer results on the minimum distance of some binary cyclic codes", IEEE Trans. Inform. Theory, vol. IT-16, pp. 359-360, May 1970.

[4] W. W. Peterson and E. J. Weldon, Jr., Error-Correcting Codes, Cambridge, Mass: The M.I.T. Press, 1972.

[5] E. R. Berlekamp, Algebraic Coding Theory, New York: McGraw-Hill Book Company, 1968.