

ALGEBRAIC STRUCTURE AND WEIGHT DISTRIBUTION
OF BINARY CYCLIC CODES

by

J.-M. Goethals
M.B.L.E.
Laboratoire de Recherches
Bruxelles 7, Belgium

Institute of Statistics Mimeo Series No. 484.4

August 1966

Presented at the NATO Summer School on
Combinatorial Methods in Coding and
Information Theory, Royan, France
August 26 - September 8, 1965

Organized by:

The Department of Statistics
University of North Carolina
and
The Institute of Statistics
University of Paris

This research was supported by the Air Force
Office of Scientific Research Contract No.
AF-AFOSR-760-65.

DEPARTMENT OF STATISTICS
UNIVERSITY OF NORTH CAROLINA
Chapel Hill, N. C.

Algebraic structure and weight distribution
of binary cyclic codes

Introduction

Some algebraic properties of cyclic codes are presented which are useful in the analysis of their weight distribution. Some ideas developed here are found in two recent papers by Mc Williams [1] and Nili [2].

Results on computer analysis of weight distributions in binary cyclic codes are also given. The analysis is exhaustive for all odd block length up to 43. It is to be noted that most of these results have been recently obtained by Kilman Goldman and Smola [5], without any simplification in the analysis, with the aid of a very powerful computer.

1. Algebraic structure of cyclic codes

1.1. A cyclic code over a finite field $GF(q)$ may be considered as an ideal in the ring of polynomial residue classes modulo (x^n-1) over $GF(q)$. The monic polynomial $g(x)$ of minimum degree in such an ideal is known to be a divisor of (x^n-1) and is called "generator" of the ideal. If r denotes its degree, then the dimension of the ideal is given by

$$k = n - r \quad (1)$$

which is also the degree of the reciprocal factor of $g(x)$, i.e.

$$h(x) = (x^n-1)/g(x) \quad (2)$$

Let us denote by

- A : a cyclic code (n,k) over $GF(q)$, generated by $g(x)$.
 $A[h(x)]$: the ring of polynomial residue classes modulo $h(x)$, given by (2).

Assuming n and q to be relatively prime, the polynomials $g(x)$ and $h(x)$ are then relatively prime, and there exist polynomials $m(x)$ and $n(x)$ such that

$$m(x) \cdot g(x) + n(x) \cdot h(x) = 1 \quad (3)$$

with $m(x)$ and $n(x)$ relatively prime to $h(x)$ and $g(x)$, respectively.

As a well known result in the theory of rings and ideals^(*), there is a complete isomorphism between A and $A[h(x)]$. This isomorphism is characterized as follows.

The element

$$e(x) = m(x) \cdot g(x) \quad (4)$$

being a multiple of $g(x)$, is a vector of the code A and has the following properties:

^(*) See f.i. ref. 3 or 4

$$e(x) \equiv 1 \pmod{h(x)} \quad (5)$$

$$e^2(x) \equiv e(x) \pmod{(x^n-1)} \quad (6)$$

i.e. $e(x)$ is an unit in $A[h(x)]$ and idempotent in A .

Now let

$$v(x) = a(x) \cdot e(x) \quad (7)$$

be a vector of the code A , with $a(x)$ an element of $A[h(x)]$. It is easy to see that the correspondence

$$a(x) \text{ in } A[h(x)] \rightarrow v(x) \text{ in } A \quad (8)$$

is actually an isomorphism.

1.2. When the polynomial $h(x)$ of degree k is irreducible, the ring $A[h(x)]$ is known to be a field, namely the Galois field $GF(q^k)$. The multiplicative group of this field is known to be cyclic, i.e. there exists an element $\alpha(x)$ called "primitive" such that

$$1, \alpha(x), \alpha^2(x), \dots, \alpha^{q^k-2}(x) \quad (9)$$

are all the distinct non-zero elements of $GF(q^k)$.

As a consequence, all the elements of the code A may be represented as

$$\alpha^i(x) \cdot e(x), \quad (i = 0, 1, 2, \dots, q^k-2) \quad (10)$$

i.e. may be generated by successive multiplications by $\alpha(x)$.

Let n' be the exponent to which $h(x)$ belongs, i.e. the least integer such that $x^{n'}-1$ be divisible by $h(x)$. Then, necessarily n' divides q^k-1 , i.e.

$$q^k-1 = n' \cdot m \quad (11)$$

and $\alpha^m(x)$ must be of order n' , i.e. must be a primitive root of $(x^{n'}-1)$.

Let us write

$$\alpha^m(x) \equiv x^j \pmod{h(x)} \quad (12)$$

where j is relatively prime to n' , and m is the least integer such that (12) holds, since otherwise $\alpha(x)$ would not be a primitive root.

As a consequence of (12)

$$\alpha^m(x) \cdot e(x) \equiv x^j \cdot e(x) \pmod{(x^n-1)} \quad (13)$$

and more generally

$$\alpha^{m+i}(x) \cdot e(x) = x^j \alpha^i(x) \cdot e(x) \pmod{(x^n-1)} \quad (14)$$

which shows that $\alpha^i(x) \cdot e(x)$ for $i \geq m$ are simply shifted repetitions of the first m ones. It has been proved (*) that all vectors in such a code have the same cycle length n , so that the weight distribution of the code is simply given by n times the weight distribution among the m vectors

$$e(x), \alpha(x) \cdot e(x), \alpha^2(x) \cdot e(x), \dots, \alpha^{m-1}(x) \cdot e(x) \quad (15)$$

1.3. In the general case where $h(x)$ is the product of several irreducible factors

$$h(x) = h_1(x) \cdot h_2(x) \dots h_s(x) \quad (16)$$

of respective degrees k_1, k_2, \dots, k_s , it has been shown (**) that A is the direct sum

$$A = A_1 \dot{+} A_2 \dot{+} \dots \dot{+} A_s \quad (17)$$

of the ideals A_i generated by

$$g_i(x) = (x^n-1)/h_i(x) \quad (18)$$

The ideals A_i and their idempotents $e_i(x)$ are called primitive, since they cannot be decomposed into the direct sum of some subideals; they are known to be isomorphic to a field. Furthermore, they are mutually orthogonal, i.e. for every $v_i(x)$ in A_i , and $v_j(x)$ in A_j

$$v_i(x) \cdot v_j(x) \equiv 0 \pmod{(x^n-1)} \quad (19)$$

(*) See ref. 1, proposition IX.

(**) See ref. 1, lemma 2.12; we use the term "direct sum" rather than "union" as it is called there.

as it may be seen from (18).

It is easy to see that A contains every subsum

$$A_{i_1} + A_{i_2} + \dots + A_{i_r} \quad (20)$$

with

$$i_1, i_2, \dots, i_r \in \{1, 2, \dots, s\}$$

i.e. $(2^s - 1)$ different subideals, A included.

The idempotent of A is given by

$$e(x) = e_1(x) + e_2(x) + \dots + e_s(x) \quad (21)$$

where $e_i(x)$ is the idempotent of A_i , since from

$$\begin{aligned} e_i &\equiv 1 \pmod{h_i(x)} \\ &\equiv 0 \pmod{h_j(x)} \end{aligned} \quad (22)$$

it follows that (21) is congruent to 1 modulo $h_i(x)$ for $i = 1, 2, \dots, s$, and thus modulo $h(x)$.

We now show that the set G of elements of A that are contained in none of the subideals (20) form a multiplicative group whose order is given by

$$(q^{k_1} - 1) (q^{k_2} - 1) \dots (q^{k_s} - 1) \quad (23)$$

First, these elements are all of the form

$$v = v_1 + v_2 + \dots + v_s \quad (24)$$

where v_i is a non zero element of A_i , and since there are $(q^{k_i} - 1)$ non zero elements in A_i , their number is given by (23).

Now, since A_i is a field, every non zero element v_i of A_i has an inverse v_i^{-1} in A_i such that

$$v_i v_i^{-1} = e_i \quad (25)$$

and thus

$$v^{-1} = v_1^{-1} + v_2^{-1} + \dots + v_s^{-1} \quad (26)$$

is an element of G such that

$$\begin{aligned} v.v^{-1} &= v_1 v_1^{-1} + v_2 v_2^{-1} + \dots + v_s v_s^{-1} \\ &= e_1 + e_2 + \dots + e_s \\ &= e \end{aligned} \quad (27)$$

so that G is actually a group.

It is easy to show that all the elements of G have the same cycle length n' , where n' is the least common multiple of the exponents to which the $h_i(x)$ belong.

By hypothesis, n' is the least integer such that $(x^{n'} - 1)$ is divisible by (16), so that it is impossible to have for $v(x)$ in G , and $n'' < n'$

$$(x^{n''} - 1).v(x) \equiv 0 \pmod{(x^{n'} - 1)}$$

since otherwise either $v(x)$ would be in a subideal, or $(x^{n''} - 1)$ would be divisible by (16).

It is now easy to see that $x.e(x)$ generates a subgroup $H_{n'}$ of order n' in G , and that the factor group $G/H_{n'}$ contains all the cycle representatives of G . This group turns out to be in general non cyclic so that a "system of

generators" is needed in order to generate the whole set of cycle representatives in a multiplicative way, similar to that used in (10).

2. Computer analysis of weight distributions in binary cyclic codes

The ideas developed in section 1 have been used in the analysis of weight distributions in several binary cyclic codes. For an ideal A such as (17), the program generates the cycle representatives of the group G of regular elements for each subideal (20). Further reduction in the amount of computation has been obtained using the fact that squaring is a weight preserving operation over the binary field, so that the cycle representatives may be divided into automorphism classes, each class containing elements that are obtained from each other by squaring. Only one element from each class need to be considered.

An exhaustive analysis has been done of all inequivalent binary cyclic codes of odd block length up to 43. For codes of dimension k greater than $(n-1)/2$, the weight distribution has been obtained directly from the null code using Mc Williams formula (*).

These results together with some additional results for block length greater than 43, are given in section 3. For each block length n , the irreducible factors of x^n-1 , given in octal form, are labelled $f_1, f_3, f_5 \dots$ according to the following rule: one of the primitive polynomials is labelled f_1 ; then another polynomial is labelled f_j if, α being a root of f_1 , j is the smallest power of α such that α^j is a root of f_j . The polynomial $f_0 = 1+x$ is not mentioned. The code (n,k) labelled $f_{i_1} f_{i_2} \dots f_{i_m}$ is generated by

(*) See ref. 6

$$g = (x^n - 1) / f_i f_j \dots f_m$$

and has only even weight vectors; the code $(n, k+1)$ generated by g/f_0 is not mentioned, since it has the same even weight vectors as the one generated by g and, in addition, the odd weight vectors obtained by adding the all-one vector.

3. Numerical results

3.1. Polynomials

| n | f_1 | f_3 | f_5 | f_7 | f_9 | f_{11} | f_{13} | f_{15} |
|----|---------|---------|---------|-------|---------|----------|----------|----------|
| 7 | 13 | 15 | | | | | | |
| 9 | 111 | 007 | | | | | | |
| 15 | 23 | 37 | 07 | 31 | | | | |
| 17 | 727 | 471 | | | | | | |
| 21 | 127 | 015 | 165 | 007 | 013 | | | |
| 23 | 5343 | | 6165 | | | | | |
| 25 | 4102041 | | 0000037 | | | | | |
| 27 | 1001001 | 0000111 | | | 0000007 | | | |
| 31 | 45 | 75 | 67 | 57 | | 73 | | 51 |
| 33 | 3043 | 3777 | 2251 | | | 0007 | | |
| 35 | 16475 | 13627 | 00013 | 00037 | | | | 00015 |
| 39 | 17075 | 17777 | | 13617 | | | 00007 | |
| 41 | 6647133 | 5747175 | | | | | | |
| 43 | 52225 | 47771 | | 64213 | | | | |

3.2. Codes

| Codes | Polynomials | Weights | | | | | | | | | | |
|---------|----------------------|---------|---|-----|------|------|-------|------|------|-----|----|----|
| | | 0 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 |
| (7,3) | f_1 | 1 | 0 | 7 | | | | | | | | |
| (9,6) | f_1 | 1 | 9 | 27 | 27 | | | | | | | |
| (9,2) | f_3 | 1 | 0 | 0 | 3 | | | | | | | |
| (15,4) | f_1 | 1 | 0 | 0 | 0 | 15 | | | | | | |
| (15,4) | f_3 | 1 | 0 | 0 | 10 | 0 | 0 | 5 | | | | |
| (15,2) | f_5 | 1 | 0 | 0 | 0 | 0 | 3 | 0 | | | | |
| (15,6) | f_1, f_5 | 1 | 0 | 0 | 30 | 15 | 18 | 0 | | | | |
| (15,6) | f_3, f_5 | 1 | 0 | 0 | 25 | 30 | 3 | 5 | | | | |
| (15,8) | f_1, f_3 | 1 | 0 | 15 | 100 | 75 | 60 | 5 | | | | |
| (15,8) | f_1, f_7 | 1 | 0 | 30 | 60 | 105 | 60 | 0 | | | | |
| (15,10) | f_1, f_3, f_5 | 1 | 0 | 105 | 280 | 435 | 168 | 35 | | | | |
| (17,8) | f_1 | 1 | 0 | 0 | 68 | 85 | 68 | 34 | 0 | | | |
| (21,6) | f_1 | 1 | 0 | 0 | 0 | 21 | 0 | 42 | 0 | 0 | 0 | |
| (21,3) | f_3 | 1 | 0 | 0 | 0 | 0 | 0 | 7 | 0 | 0 | 0 | |
| (21,2) | f_7 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | |
| (21,5) | f_3, f_7 | 1 | 0 | 0 | 0 | 0 | 21 | 7 | 3 | 0 | 0 | |
| (21,8) | f_1, f_7 | 1 | 0 | 0 | 21 | 21 | 126 | 42 | 45 | 0 | 0 | |
| (21,9) | f_7, f_3 | 1 | 0 | 0 | 0 | 210 | 0 | 280 | 0 | 21 | 0 | |
| (21,9) | f_1, f_9 | 1 | 0 | 21 | 0 | 147 | 0 | 343 | 0 | 0 | 0 | |
| (21,8) | f_3, f_7, f_9 | 1 | 0 | 0 | 21 | 21 | 105 | 98 | 3 | 0 | 7 | |
| (21,11) | f_1, f_3, f_7 | 1 | 0 | 0 | 168 | 210 | 1008 | 280 | 360 | 21 | 0 | |
| (21,11) | f_1, f_7, f_9 | 1 | 0 | 21 | 0 | 297 | 343 | 1071 | 147 | 147 | 21 | |
| (21,12) | f_1, f_3, f_9 | 1 | 0 | 21 | 189 | 903 | 1197 | 1295 | 399 | 84 | 7 | |
| (21,12) | f_1, f_5 | 1 | 0 | 63 | 210 | 735 | 1260 | 1281 | 546 | 0 | 0 | |
| (21,14) | f_1, f_3, f_7, f_9 | 1 | 0 | 84 | 924 | 2982 | 5796 | 4340 | 1956 | 273 | 28 | |
| (21,15) | f_1, f_5, f_3 | 1 | 0 | 210 | 1638 | 6468 | 10878 | 9310 | 3570 | 651 | 42 | |
| (23,11) | f_1 | 1 | 0 | 0 | 0 | 506 | 0 | 1288 | 0 | 253 | 0 | |
| (21,6) | f_3, f_9 | 1 | 0 | 0 | 21 | 0 | 0 | 35 | 0 | 0 | 7 | |

| Codes | Polynomials | Weights | | | | | | |
|---------|------------------------------|---------|----|------|-------|---------|---------|---------|
| | | 0 | 2 | 4 | 6 | 8 | 10 | 12 |
| (25,4) | f_5 | 1 | 0 | 0 | 0 | 0 | 10 | 0 |
| (25,20) | f_1 | 1 | 50 | 1025 | 11000 | 65250 | 207500 | 326250 |
| (27,2) | f_9 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| (27,6) | f_3 | 1 | 0 | 0 | 9 | 0 | 0 | 27 |
| (27,8) | f_3, f_9 | 1 | 0 | 0 | 36 | 0 | 0 | 126 |
| (27,18) | f_1 | 1 | 27 | 324 | 2268 | 10206 | 30618 | 61236 |
| (31,5) | f_1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| (31,10) | f_1, f_3 | 1 | 0 | 0 | 0 | 0 | 0 | 310 |
| (31,10) | f_1, f_5 | 1 | 0 | 0 | 0 | 0 | 0 | 310 |
| (31,10) | f_1, f_{15} | 1 | 0 | 0 | 0 | 0 | 31 | 155 |
| (31,15) | f_1, f_3, f_5 | 1 | 0 | 0 | 0 | 465 | 0 | 8680 |
| (31,15) | f_1, f_5, f_7 | 1 | 0 | 0 | 0 | 465 | 0 | 8680 |
| (31,15) | f_1, f_3, f_{15} | 1 | 0 | 0 | 31 | 310 | 1116 | 4340 |
| (31,15) | f_1, f_3, f_7 | 1 | 0 | 0 | 0 | 310 | 1271 | 4340 |
| (31,20) | f_1, f_3, f_5, f_{15} | 1 | 0 | 0 | 806 | 7905 | 41602 | 142600 |
| (31,20) | f_1, f_3, f_5, f_7 | 1 | 0 | 0 | 806 | 7905 | 41602 | 142600 |
| (31,20) | f_1, f_3, f_7, f_{15} | 1 | 0 | 0 | 837 | 7595 | 42997 | 138880 |
| (31,25) | $f_1, f_3, f_5, f_7, f_{11}$ | 1 | 0 | 1085 | 22568 | 247.845 | 1383096 | 4414865 |
| (33,10) | f_1 | 1 | 0 | 0 | 0 | 0 | 0 | 165 |
| (33,10) | f_3 | 1 | 0 | 0 | 55 | 0 | 0 | 330 |
| (33,2) | f_{11} | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| (33,12) | f_1, f_{11} | 1 | 0 | 0 | 0 | 0 | 165 | 396 |
| (33,12) | f_3, f_{11} | 1 | 0 | 0 | 55 | 0 | 0 | 363 |
| (33,20) | f_1, f_3 | 1 | 0 | 0 | 220 | 3795 | 21615 | 87648 |
| (33,20) | f_1, f_5 | 1 | 0 | 165 | 990 | 6930 | 27720 | 84546 |
| (33,22) | f_1, f_3, f_{11} | 1 | 0 | 0 | 1276 | 13200 | 90453 | 347457 |

| Codes | Polynomials | Weights | | | |
|---------|------------------------------|---------|---------|---------|---------|
| | | 14 | 16 | 18 | 20 |
| (25,4) | f_5 | 0 | 0 | 0 | 5 |
| (25,20) | f_1 | 275000 | 128125 | 31250 | 3125 |
| (27,2) | f_9 | 0 | 0 | 3 | 0 |
| (27,6) | f_3 | 0 | 0 | 27 | 0 |
| (27,8) | f_3, f_9 | 0 | 0 | 84 | 0 |
| (27,18) | f_1 | 78732 | 59049 | 19683 | 0 |
| (31,5) | f_1 | 0 | 31 | 0 | 0 |
| (31,10) | f_1, f_3 | 0 | 527 | 0 | 186 |
| (31,10) | f_1, f_5 | 0 | 527 | 0 | 186 |
| (31,10) | f_1, f_{15} | 310 | 217 | 155 | 155 |
| (31,15) | f_1, f_3, f_5 | 0 | 18259 | 0 | 5208 |
| (31,15) | f_1, f_5, f_7 | 0 | 18259 | 0 | 5208 |
| (31,15) | f_1, f_3, f_{15} | 8370 | 9393 | 5580 | 2852 |
| (31,15) | f_1, f_3, f_7 | 8060 | 9393 | 5890 | 2852 |
| (31,20) | f_1, f_3, f_5, f_{15} | 251100 | 301971 | 195300 | 85560 |
| (31,20) | f_1, f_3, f_5, f_7 | 251100 | 301971 | 195300 | 85560 |
| (31,20) | f_1, f_3, f_7, f_{15} | 257610 | 294159 | 201910 | 81840 |
| (31,25) | $f_1, f_3, f_5, f_7, f_{11}$ | 8280720 | 9398115 | 6440560 | 2648919 |
| (33,10) | f_1 | 165 | 165 | 330 | 165 |
| (33,10) | f_3 | 0 | 0 | 462 | 0 |
| (33,2) | f_{11} | 0 | 0 | 0 | 0 |
| (33,12) | f_1, f_{11} | 495 | 1155 | 1155 | 528 |
| (33,12) | f_3, f_{11} | 495 | 1386 | 1452 | 165 |
| (33,20) | f_1, f_3 | 199815 | 284031 | 253902 | 139920 |
| (33,20) | f_1, f_5 | 180180 | 270765 | 270600 | 162393 |
| (33,22) | f_1, f_3, f_{11} | 797775 | 1140777 | 1013298 | 557898 |

| Codes | Polynomials | Weights | | | | | |
|---------|------------------------------|---------|-------|------|-----|----|----|
| | | 22 | 24 | 26 | 28 | 30 | 32 |
| (25,4) | f_5 | 0 | | | | | |
| (25,20) | f_1 | 0 | | | | | |
| (27,2) | f_9 | 0 | 0 | | | | |
| (27,6) | f_3 | 0 | 0 | | | | |
| (27,8) | f_3, f_9 | 0 | 9 | | | | |
| (27,18) | f_1 | 0 | 0 | | | | |
| (31,5) | f_1 | 0 | 0 | 0 | 0 | | |
| (31,10) | f_1, f_3 | 0 | 0 | 0 | 0 | | |
| (31,10) | f_1, f_5 | 0 | 0 | 0 | 0 | | |
| (31,10) | f_1, f_{15} | 0 | 0 | 0 | 0 | | |
| (31,15) | f_1, f_3, f_5 | 0 | 155 | 0 | 0 | | |
| (31,15) | f_1, f_5, f_7 | 0 | 155 | 0 | 0 | | |
| (31,15) | f_1, f_3, f_{15} | 775 | 0 | 0 | 0 | | |
| (31,15) | f_1, f_3, f_7 | 620 | 0 | 31 | 0 | | |
| (31,20) | f_1, f_3, f_5, f_{15} | 18910 | 2635 | 186 | 0 | | |
| (31,20) | f_1, f_3, f_5, f_7 | 18910 | 2635 | 186 | 0 | | |
| (31,20) | f_1, f_3, f_7, f_{15} | 20305 | 2325 | 217 | 0 | | |
| (31,25) | $f_1, f_3, f_5, f_7, f_{11}$ | 628680 | 82615 | 5208 | 155 | | |
| (33,10) | f_1 | 33 | 0 | 0 | 0 | 0 | |
| (33,10) | f_3 | 0 | 165 | 0 | 0 | 11 | |
| (33,2) | f_{11} | 3 | 0 | 0 | 0 | 0 | |
| (33,12) | f_1, f_{11} | 201 | 0 | 0 | 0 | 0 | |
| (33,12) | f_3, f_{11} | 3 | 165 | 0 | 0 | 11 | |
| (33,20) | f_1, f_3 | 47058 | 9405 | 1155 | 0 | 11 | |
| (33,20) | f_1, f_5 | 44286 | 0 | 0 | 0 | 0 | |
| (33,22) | f_1, f_3, f_{11} | 190842 | 36630 | 4521 | 165 | 11 | |

| Codes | Polynomials | Weights | | | | | | |
|---------|-------------------------|---------|-----|-------|--------|---------|---------|----------|
| | | 0 | 4 | 6 | 8 | 10 | 12 | 14 |
| (35,3) | f_5 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| (35,4) | f_7 | 1 | 0 | 0 | 0 | 0 | 0 | 10 |
| (35,6) | f_5, f_{25} | 1 | 0 | 0 | 0 | 21 | 0 | 0 |
| (35,7) | f_5, f_7 | 1 | 0 | 0 | 0 | 0 | 0 | 10 |
| (35,10) | f_5, f_7, f_{15} | 1 | 0 | 0 | 0 | 56 | 0 | 10 |
| (35,12) | f_1 | 1 | 0 | 0 | 70 | 0 | 420 | 0 |
| (35,15) | f_1, f_5 | 1 | 0 | 0 | 70 | 0 | 3255 | 0 |
| (35,15) | f_1, f_{15} | 1 | 35 | 0 | 490 | 0 | 3430 | 0 |
| (35,16) | f_1, f_7 | 1 | 0 | 70 | 70 | 1260 | 1925 | 9460 |
| (35,18) | f_1, f_5, f_{15} | 1 | 35 | 0 | 490 | 1701 | 14770 | 33075 |
| (35,19) | f_1, f_5, f_7 | 1 | 0 | 70 | 525 | 6930 | 19180 | 88700 |
| (35,19) | f_1, f_7, f_{15} | 1 | 35 | 490 | 490 | 10430 | 15435 | 74980 |
| (35,22) | f_1, f_5, f_7, f_{15} | 1 | 35 | 595 | 4200 | 48426 | 198485 | 577825 |
| (35,24) | f_1, f_3 | 1 | 210 | 2100 | 25655 | 175140 | 801220 | 2275560 |
| (35,27) | f_1, f_3, f_5 | 1 | 665 | 13020 | 182525 | 1426880 | 6538805 | 18123420 |
| (39,12) | f_1 | 1 | 0 | 0 | 0 | 0 | 156 | 0 |
| (39,12) | f_3 | 1 | 0 | 78 | 0 | 0 | 715 | 0 |
| (39,14) | f_1, f_{13} | 1 | 0 | 0 | 0 | 117 | 156 | 1404 |
| (39,14) | f_3, f_{13} | 1 | 0 | 78 | 0 | 0 | 715 | 39 |
| (39,24) | f_1, f_7 | 1 | 234 | 1716 | 15015 | 77220 | 314028 | 936936 |
| (39,24) | f_1, f_3 | 1 | 0 | 234 | 3393 | 40404 | 233935 | 933894 |
| (39,26) | f_1, f_3, f_{13} | 1 | 0 | 819 | 15327 | 153075 | 964171 | 3652623 |
| (41,20) | f_1 | 1 | 0 | 0 | 0 | 1312 | 7585 | 33210 |
| (43,14) | f_1 | 1 | 0 | 0 | 0 | 0 | 0 | 344 |
| (43,28) | f_1, f_3 | 1 | 0 | 301 | 9116 | 117691 | 931294 | 4792909 |

| Codes | Polynomials | Weights | | | | |
|---------|-------------------------|----------|----------|----------|----------|----------|
| | | 16 | 18 | 20 | 22 | 24 |
| (35,3) | f_5 | 0 | 0 | 7 | 0 | 0 |
| (35,4) | f_7 | 0 | 0 | 0 | 0 | 0 |
| (35,6) | f_5, f_{15} | 0 | 0 | 35 | 0 | 0 |
| (35,7) | f_5, f_7 | 35 | 70 | 7 | 0 | 0 |
| (35,10) | f_5, f_7, f_{15} | 385 | 350 | 105 | 105 | 0 |
| (35,12) | f_1 | 1505 | 0 | 2100 | 0 | 0 |
| (35,15) | f_1, f_5 | 15365 | 0 | 12502 | 0 | 1540 |
| (35,15) | f_1, f_{15} | 12005 | 0 | 16807 | 0 | 0 |
| (35,16) | f_1, f_7 | 12845 | 23520 | 8330 | 6230 | 1260 |
| (35,18) | f_1, f_5, f_{15} | 67445 | 59010 | 58415 | 19670 | 6160 |
| (35,19) | f_1, f_5, f_7 | 92715 | 172900 | 74592 | 56350 | 9415 |
| (35,19) | f_1, f_7, f_{15} | 102900 | 188860 | 66297 | 49490 | 10430 |
| (35,22) | f_1, f_5, f_7, f_{15} | 964320 | 1146460 | 762125 | 372645 | 100660 |
| (35,24) | f_1, f_3 | 3993535 | 4412520 | 3153570 | 1449700 | 412265 |
| (35,27) | f_1, f_3, f_5 | 31688755 | 35460320 | 25403707 | 11510100 | 3258255 |
| (39,12) | f_1 | 1053 | 0 | 2028 | 0 | 858 |
| (39,12) | f_3 | 0 | 1716 | 0 | 0 | 1287 |
| (39,14) | f_1, f_{13} | 1053 | 5070 | 2028 | 5148 | 858 |
| (39,14) | f_3, f_{13} | 858 | 5577 | 5148 | 2145 | 1521 |
| (39,24) | f_1, f_7 | 2111967 | 3517800 | 4222218 | 3454308 | 1727193 |
| (39,24) | f_1, f_3 | 2269683 | 3862872 | 4138719 | 3167190 | 1509027 |
| (39,26) | f_1, f_3, f_{13} | 9275877 | 15112383 | 16955367 | 12353913 | 6192069 |
| (41,20) | f_1 | 97539 | 195160 | 255266 | 232060 | 146370 |
| (43,14) | f_1 | 1204 | 2107 | 3311 | 3999 | 3311 |
| (43,28) | f_1, f_3 | 16184770 | 37106979 | 58671522 | 64182703 | 48849892 |

| Codes | Polynomials | Weights | | | | | |
|---------|-------------------------|----------|---------|---------|--------|-------|------|
| | | 26 | 28 | 30 | 32 | 34 | 36 |
| (35,3) | f_5 | 0 | 0 | 0 | 0 | | |
| (35,4) | f_7 | 0 | 5 | 0 | 0 | | |
| (35,6) | f_5, f_{15} | 0 | 0 | 7 | 0 | | |
| (35,7) | f_5, f_7 | 0 | 5 | 0 | 0 | | |
| (35,10) | f_5, f_7, f_{15} | 0 | 5 | 7 | 0 | | |
| (35,12) | f_1 | 0 | 0 | 0 | 0 | | |
| (35,15) | f_1, f_5 | 0 | 35 | 0 | 0 | | |
| (35,15) | f_1, f_{15} | 0 | 0 | 0 | 0 | | |
| (35,16) | f_1, f_7 | 420 | 145 | 0 | 0 | | |
| (35,18) | f_1, f_5, f_{15} | 1225 | 140 | 7 | 0 | | |
| (35,19) | f_1, f_5, f_7 | 2730 | 180 | 0 | 0 | | |
| (35,19) | f_1, f_7, f_{15} | 3430 | 985 | 0 | 35 | | |
| (35,22) | f_1, f_5, f_7, f_{15} | 16730 | 1755 | 7 | 35 | | |
| (36,24) | f_1, f_3 | 71540 | 4200 | 0 | 0 | | |
| (35,27) | f_1, f_3, f_5 | 556640 | 52535 | 2100 | 0 | | |
| (39,12) | f_1 | 0 | 0 | 0 | 0 | 0 | 0 |
| (39,12) | f_3 | 0 | 0 | 286 | 0 | 0 | 13 |
| (39,14) | f_1, f_{13} | 549 | 0 | 0 | 0 | 0 | 0 |
| (39,14) | f_3, f_{13} | 3 | 0 | 286 | 0 | 0 | 13 |
| (39,24) | f_1, f_7 | 398580 | 0 | 0 | 0 | 0 | 0 |
| (39,24) | f_1, f_3 | 502164 | 101829 | 12922 | 936 | 0 | 13 |
| (39,26) | f_1, f_3, f_{13} | 1966617 | 410241 | 52741 | 3510 | 117 | 13 |
| (41,20) | f_1 | 60024 | 16605 | 3034 | 410 | 0 | 0 |
| (43,14) | f_1 | 1505 | 301 | 301 | 0 | 0 | 0 |
| (43,28) | f_1, f_3 | 25735801 | 9224962 | 2240343 | 351869 | 32809 | 2494 |

3.3. Additional results

1) Code (51,17); polynomial $h = f_1, f_5, f_0$

| <u>weights</u> | <u>number of vectors</u> |
|----------------|--------------------------|
| 16 and 35 | 30 x 51 |
| 20 and 31 | 160 x 51 |
| 24 and 27 | 504 x 51 |
| 28 and 23 | 480 x 51 |
| 32 and 19 | 111 x 51 |

2) Code (55,21); polynomial $h = f_1, f_0$

| <u>weights</u> | <u>number of vectors</u> |
|----------------|--------------------------|
| 16 and 39 | 70 x 55 |
| 20 and 35 | 1048 x 55 |
| 24 and 31 | 5296 x 55 |
| 28 and 27 | 8080 x 55 |
| 32 and 23 | 3947 x 55 |
| 36 and 19 | 600 x 55 |
| 40 and 15 | 24 x 55 |

3) Code (63,13); polynomial $h = f_1, f_5, f_0$

| <u>weights</u> | <u>number of vectors</u> |
|----------------|--------------------------|
| 24 and 39 | 10 x 63 |
| 32 and 31 | 49 x 63 |
| 40 and 23 | 6 x 63 |

4) Code (63,13); polynomial $h = f_1, f_3, f_0$

| <u>weights</u> | <u>number of vectors</u> |
|----------------|--------------------------------------|
| 24 and 39 | $3 \times 63 + 1 \times 21 = 210$ |
| 28 and 35 | $24 \times 63 = 1.512$ |
| 32 and 31 | $17 \times 63 = 1.071$ |
| 36 and 27 | $18 \times 63 + 2 \times 21 = 1.176$ |
| 40 and 23 | $2 \times 63 = 126$ |

5) Code (65,13); polynomial $h = f_1, f_0$

| <u>weights</u> | <u>number of vectors</u> |
|----------------|--------------------------|
| 26 and 39 | 6×65 |
| 28 and 37 | 7×65 |
| 30 and 35 | 12×65 |
| 32 and 33 | 12×65 |
| 34 and 31 | 6×65 |
| 36 and 29 | 9×65 |
| 38 and 27 | 8×65 |
| 40 and 25 | 3×65 |

6) Code (89,12); polynomial $h = f_1, f_0$

| <u>weights</u> | <u>number of vectors</u> |
|----------------|--------------------------|
| 40 and 49 | 11×89 |
| 48 and 41 | 11×89 |
| 56 and 33 | 1×89 |

7) Code (91,13); polynomial $h = f_1$

| <u>weights</u> | <u>number of vectors</u> |
|----------------|--------------------------|
| 36 and 55 | 4 x 91 |
| 40 and 51 | 6 x 91 |
| 44 and 47 | 12 x 91 |
| 48 and 43 | 15 x 91 |
| 52 and 39 | 8 x 91 |

8) Code (151,16); polynomial $h = f_1$

| <u>weights</u> | <u>number of vectors</u> |
|----------------|--------------------------|
| 60 and 91 | 3 x 151 |
| 64 and 87 | 5 x 151 |
| 68 and 83 | 30 x 151 |
| 72 and 79 | 65 x 151 |
| 76 and 75 | 39 x 151 |
| 80 and 71 | 30 x 151 |
| 84 and 67 | 40 x 151 |
| 88 and 63 | 5 x 151 |

References

- [1] J. Mc Williams, "The structure and properties of Binary Cyclic Alphabets", B.S.T.J. 44, 2, pp. 303-333; Feb. 1965.
- [2] H. Nili, "Matrixschaltungen zur Codierung und Decodierung von Gruppen-Code", A.E.U. 18, 9, pp. 555-565; Sept. 1964.
- [3] N. H. Mc Coy, Rings and Ideals, The Carus Math. Monographs n^o 8, M.A.A.; New York (1956).
- [4] B. L. van der Waerden, Modern Algebra (2 vol.), Fred. Ungar Pub. Co; New York (1949, 1950).
- [5] M. Kliman, H. D. Goldman, and H. Smola, "The Weight structure of some Bose-Chaudhuri Codes", (privately communicated).
- [6] J. Mc Williams, "A theorem on the distribution of weights in a systematic code," B.S.T.J. 42, 1, pp. 79-94; Jan. 1963.