On the Number of Information Symbols in Difference-Set Cyclic Codes

By R. L. GRAHAM and JESSIE MACWILLIAMS

(Manuscript received April 28, 1966)

The concept of a difference-set cyclic code has been described previously. It was shown that such a code is almost as powerful as a Bose-Chaudhuri code and considerably simpler to implement. It is the purpose of this paper to determine some of the more important properties of this code and its dual code (cf. Sec. IV). It may be pointed out that the problems we consider are equivalent to determining certain properties of incidence matrices associated with a class of balanced incomplete block designs formed from simple difference sets.

I. INTRODUCTION

The concept of a difference-set cyclic code has been described by E. J. Weldon, Jr. in the preceding paper.[1] In Ref. 1 it is shown that such a code is almost as powerful as a Bose-Chaudhuri code and considerably simpler to implement. It is the purpose of this paper to determine some of the more important properties of this code and its dual code (cf. Sec. IV). It may be pointed out that the problems we consider are equivalent to determining certain properties of incidence matrices of Desarguesian planes.

II. SIMPLE DIFFERENCE SETS AND ASSOCIATED CYCLIC CODES

A simple difference set S is a collection of l integers $\{d_1, \cdots, d_l\}$ modulo n such that every $a \not\equiv 0 \pmod{n}$ can be *uniquely* expressed in the form

$$d_i - d_j \equiv a \pmod{n},$$

for some d_i, d_j in S. Of course, $n = l(l-1) + 1$. If $\theta(x)$ (the difference-set polynomial) is defined by

$$\theta(x) = \sum_{i=1}^{l} x^{d_i},$$

then it follows that

$$\theta(x)\theta(x^{-1}) = l + \sum_{i=1}^{n-1} x^i \pmod{(x^n - 1)}.$$

This may be written

$$\theta(x)\theta(x^{-1}) = (l - 1) + (x^n - 1)/(x - 1) \pmod{(x^n - 1)}.$$

Changing to arithmetic over the finite field $GF(p)$, where p is a prime that divides $l - 1$, we have

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

This means that $\theta(x)$ has a nontrivial highest common factor $h(x)$ in common with $x^n - 1$ over $GF(p)$.

Let R be the ring of polynomials modulo $x^n - 1$ over $GF(p)$. The ideal $R \cdot \theta(x)$ is the same ideal as $R \cdot h(x)$ and is a proper ideal in R, and, in fact a cyclic code (see Ref. 5, Section 8.1). The dimension of this code is $(n - \deg h(x))$.*

The only known simple difference sets are obtained by a construction due to Singer.[2] For this construction, n must be of the form $p^{2s} + p^s + 1$. Hence, $l - 1 = p^s$, which determines the finite field one must use. For $p = 2$ and $1 \leqq s \leqq 5$, the dimension of $R \cdot \theta(x)$ was found by E. J. Weldon, Jr. to be $3^s + 1$. In this paper it is shown that in general the dimension of $R \cdot \theta(x)$ is $\binom{p+1}{2}^s + 1$.

III. AN EQUIVALENT PROBLEM

Let $n = p^{2s} + p^s + 1$, $r = p^s - 1$. $\{d_1, d_2, \cdots, d_l\}$ is a Singer difference set modulo n, and $\theta(x)$ the difference-set polynomial. In this section all arithmetic will be in $GF(p)$ (addition and multiplication mod p) unless otherwise specified.

The degree of $h(x)$ is the number of zeros of $x^n - 1$ which are also zeros of $\theta(x)$. Hence, the following odd-sounding theorem is relevant.

Theorem 1: The number of nth *roots of unity (over* $GF(p)$*) which are not zeros of* $\theta(x)$ *is the number of integers* t, $1 \leqq t \leqq n$, *such that for some* j, $1 \leqq j \leqq t - 1$, *the binomial coefficient* $\binom{tr}{jr}$ *is not zero (mod* p*).*

* This roundabout approach is usual in coding theory. Appendix B contains a direct proof that the dimension of $R \cdot \theta(x)$ is the number of zeros of $x^n - 1$ which are not zeros of $\theta(x)$.

The purpose of this section is to prove Theorem 1. Several preliminary steps are needed.

Let ν be a primitive nrth root of unity over $GF(p)$; $\omega = \nu^n$ is a primitive rth root of unity, $\zeta = \nu^r$ is a primitive nth root of unity. The first n powers of ζ are the zeros of $x^n - 1$; the degree of the highest common factor of $\theta(x)$ and $x^n - 1$ is the number of integers $t \leqq n$ for which $\theta(\zeta^t) = 0$.

The powers of ω generate $GF(p^s)$, and, since $nr = p^{3s} - 1$, the powers of ν generate $GF(p^{3s})$. Since $GF(p^{3s}) \supset GF(p^s)$, any linear combination $\sum_{i,j} \omega^i \nu^j$ is again a power of ν.

To construct a Singer difference set modulo n, one picks two arbitrary distinct integers d_1, d_2 (less than n), forms all linear combinations $\omega^i \nu^{d_1} + \omega^j \nu^{d_2} = \nu^b$, and replaces ν^b by $\omega^{h_f} \nu^{d_f}$ $(d_f \leqq n)$ by using $\nu^n = \omega$ (cf., Ref. 2). The distinct exponents of ν which are obtained in this way form a Singer difference set.* Since $\omega^h(\omega^i \nu^{d_1} + \omega^j \nu^{d_2}) = \omega^{h_f + h} \nu^{d_f}$, each exponent d_f will be produced r times; we can get each one exactly once by using the equations

$$\begin{aligned} \nu^{d_1} + \nu^{d_2} &= \omega^{h_3} \nu^{d_3}, \\ \omega \nu^{d_1} + \nu^{d_2} &= \omega^{h_4} \nu^{d_4}, \\ &\cdots \\ \omega^{r-1} \nu^{d_1} + \nu^{d_2} &= \omega^{h_l} \nu^{d_l}, \end{aligned} \tag{1}$$

where

$$l = p^s + 1 = r + 2.$$

Lemma 1: ζ^t *is a zero of* $\theta(x)$ *if and only if*

$$\sum_{j=1}^{t-1} \binom{tr}{jr} \zeta^{(d_1 - d_2) j} = 0.$$

Proof: Raising (1) to the power tr gives the set of equations

$$\begin{aligned} (\nu^{d_1} + \nu^{d_2})^{tr} &= (\omega^{h_3} \nu^{d_3})^{tr} = (\nu^{d_3})^{tr} = \zeta^{t d_3} \\ (\omega \nu^{d_1} + \nu^{d_2})^{tr} &= (\nu^{d_4})^{tr} = \zeta^{t d_4} \\ &\cdots \\ (\omega^{r-1} \nu^{d_1} + \nu^{d_2})^{tr} &= (\nu^{d_l})^{tr} = \zeta^{t d_l}. \end{aligned}$$

---

* An example is given in the appendix.

Thus,

$$\theta(\zeta^t) = \sum_{i=1}^{l} (\zeta^t)^{d_i} = 0$$

if and only if

$$(\nu^{d_1})^{tr} + (\nu^{d_2})^{tr} + \sum_{i=0}^{r-1} (\omega^i \nu^{d_1} + \nu^{d_2})^{tr} = 0.$$

This may be rewritten as

$$(r+1)(\nu^{d_1})^{tr} + (r+1)(\nu^{d_2})^{tr} + \sum_{i=0}^{r-1} \sum_{h=1}^{tr-1} \binom{tr}{h} \nu^{\sigma_h} \omega^{ih},$$

where

$$\sigma_h = d_1 h + d_2(tr - h).$$

Since $r + 1 = p^s$ the first two terms are zero; the remainder is

$$\sum_{h=1}^{tr-1} \binom{tr}{h} \nu^{\sigma_h} \sum_{i=0}^{r-1} (\omega^h)^i.$$

Now,

$$\sum_{i=0}^{r-1} (\omega^h)^i = \begin{cases} 0 & \text{if} \quad h \not\equiv 0 \bmod r, \\ r & \text{if} \quad h = jr. \end{cases}$$

In particular (for $t = 1$) ζ is a zero of $\theta(x)$. Since

$$r \equiv -1 \bmod p, \quad \nu^r = \zeta, \quad \text{and} \quad \sigma_{jr} = (d_1 - d_2)jr + tr\, d_2,$$

the expression for $\theta(\zeta^t)$ becomes

$$-\nu^{tr d_2} \sum_{j=1}^{t-1} \binom{tr}{jr} \zeta^{j(d_1 - d_2)},$$

which proves the lemma.

Lemma 2:

$$\sum_{j=1}^{t-1} \binom{tr}{jr} \zeta^{(d_1 - d_2)j} = 0$$

if and only if

$$\binom{tr}{jr} \equiv 0 \pmod p \quad \textit{for} \quad j = 1, \cdots, t-1.$$

Proof: The difference set $\{d_1, d_2, \cdots, d_l\}$ may be obtained by picking

any two distinct d_i, d_j contained in it, and applying the construction previously described to ν^{d_i}, ν^{d_j}. By the definition of a difference set we may choose $d_i - d_j$ to be any number $1, 2, \cdots, n-1$. Thus, $\theta(\zeta^t) = 0$ implies

$$\sum_{j=1}^{t-1} \binom{tr}{jr} \zeta^{uj} = 0 \quad \text{for} \quad u = 1, 2, \cdots, n-1,$$

and the equation

$$\sum_{j=1}^{t-1} \binom{tr}{jr} x^j = 0$$

will have $(n-1)$ nonzero roots. Since $t \leqq n$ this is impossible unless all the coefficients are zero. This proves the lemma.

The experimental evidence (for $p = 2$, $1 \leqq s \leqq 5$) showed that the number of ζ^t which are *not* zeros of $\theta(x)$ is $3^s + 1$. We guess (it turns out correctly) that "+1" corresponds to $t = n$,—ζ^n is not a zero of $\theta(x)$, since $\theta(1) \equiv 1 \pmod{p}$—, and that it will be simpler to count binominal coefficients which are not divisible by p. The information contained in Lemmas 1 and 2 is rephrased in the form of Theorem 1.

The following corollary is immediate.

Corollary 1: The degree of the highest common factor (over GF(p)) of $\theta(x)$ and $x^n - 1$ is the same for every Singer difference set.

IV. A THEOREM ON BINOMIAL COEFFICIENTS

In this section, we change to ordinary arithmetic (instead of mod p) and count the number of integers t which satisfy the conditions of Theorem 1. In particular, our goal is to establish

Theorem 2: The number of t, $1 \leqq t \leqq p^{2s} + p^s$, for which

$$\binom{tr}{jr} \not\equiv 0 \pmod{p} \tag{2}$$

for $r = p^s - 1$ and some j, $1 \leqq j < t$, is just $\binom{p+1}{2}^s$.

The proof of this result will depend upon several lemmas. We first need some notation. Let $P_p(u)$ denote the greatest power of p which divides u. If u is written to the base p, i.e.,

$$u = \sum_{i=1}^{h} u_i p^i, \qquad 0 \leqq u_i < p,$$

for some h, then $D(u)$ will denote* the sum of the "digits" of u, i.e.,

$$D(u) = \sum_{i=1}^{h} u_i .$$

As usual, we let $[u]$ represent the greatest integer not exceeding u.

Lemma 3:

$$\binom{u+v}{u} \not\equiv 0 \pmod{p}$$

if and only if

$$u_j + v_j \leqq p - 1, \qquad j = 0, 1, 2, \cdots .$$

Proof: It is well known that

$$P_p(m!) = \sum_{i=1}^{\infty} \left[\frac{m}{p^i}\right]$$

(the upper limit ∞ is convenient, but not necessary). Since

$$P_p\left(\binom{u+v}{u}\right) = P_p((u+v)!) - P_p(u!) - P_p(v!),$$

we have

$$P_p\left(\binom{u+v}{u}\right) = 0$$

if and only if

$$\sum_{i=1}^{\infty} \left[\frac{u+v}{p^i}\right] = \sum_{i=1}^{\infty} \left[\frac{u}{p^i}\right] + \sum_{i=1}^{\infty} \left[\frac{v}{p^i}\right]. \tag{3}$$

But it is always true that

$$[x + y] \geqq [x] + [y] ,$$

so that (3) holds if and only if

$$\left[\frac{u+v}{p^i}\right] = \left[\frac{u}{p_i}\right] + \left[\frac{v}{p^i}\right], \qquad i = 1, 2, 3, \cdots . \tag{4}$$

Noting that, in general, $[x/p^i]$ is just one of the "digits" in the representation of x to the base p, we see that (4) is exactly the condition that,

* We should more accurately denote this by $D_p(u)$ but since p is fixed in this argument, no confusion will arise.

for each j, the jth digit in the representation of $u + v$ to the base p is just the sum of the jth digits of u and v. Hence, (4) holds if and only if

$$u_j + v_j \leqq p - 1, \qquad j = 0, 1, 2, \cdots,$$

and the lemma is proved.

We note as a

Corollary:

$$D(u + v) \leqq D(u) + D(v)$$

with equality if and only if

$$u_j + v_j \leqq p - 1, \qquad j = 0, 1, 2, \cdots.$$

We recall that the numbers of particular interest are

$$u = jr, \qquad v = tr - jr,$$

where

$$r = p^s - 1 = \sum_{i=0}^{s-1} wp^i \qquad (\text{where } w = p - 1).$$

Lemma 4:

$$D(tr) = sw \quad \textit{for} \quad 1 \leqq t \leqq r.$$

Proof: Set

$$t = \sum_{i=1}^{s-1} a_i p^i + a_0,$$

where we may take $a_0 \neq 0$, since $D(p^x u) = D(u)$. Now,

$$a_0 r = (a_0 - 1)p^s + \sum_{i=1}^{s-1} wp^i + (p - a_0).$$

Consequently,

$$\begin{aligned} tr &= (p^s - 1) \sum_{i=1}^{s-1} a_i p^i + a_0 r \\ &= \sum_{i=1}^{s-1} a_i p^{i+s} - \sum_{i=1}^{s-1} a_i p^i + (a_0 - 1)p^s + \sum_{i=1}^{s-1} wp^i + (p - a_0) \\ &= \sum_{i=1}^{s-1} a_i p^{i+s} + (a_0 - 1)p^s + \sum_{i=1}^{s-1} (w - a_i)p^i + (p - a_0). \end{aligned}$$

Thus,

$$D(tr) = \sum_{i=1}^{s-1} a_i + (a_0 - 1) + (s-1)w - \sum_{i=1}^{s-1} a_i + (p - a_0)$$

$$= sw \qquad \text{for} \qquad 1 \leqq t \leqq r = p^s - 1,$$

which proves the lemma.

Note that if $1 < t < n$, there is a 1 to 1 correspondence between t such that $D(tr) = u$ and t such that $D(tr) = 3sw - n$. For

$$0 < (p^{3s} - 1) - tr = (n - t)r$$

and clearly

$$D((n - t)r) = 3sw - D(tr).$$

Lemma 5:

$$sw \leqq D(tr) \leqq 2sw, \quad \text{for} \quad 1 \leqq t < n.$$

Proof: We show that $D(tr) \leqq 2sw$; the other inequality is then immediate by the preceding remark.

Since $t \leqq p^{2s} + p^s$ we have either

$$t = p^{2s} + \sum_{i=0}^{s-1} a_i p^i$$

or

$$t = p^s \sum_{i=0}^{s-1} b_i p^i + \sum_{i=0}^{s-1} a_i p^i.$$

In either case, let t_1 denote the first summand and t_2 denote the second summand (so that $t = t_1 + t_2$).

By Lemma 4

$$D(t_1 r) = D(t_2 r) = sw.$$

Hence,

$$D(tr) = D(t_1 r + t_2 r) \leqq D(t_1 r) + D(t_2 r) = 2sw$$

and the lemma is proved.

We recall now that in Theorem 2 we are considering integers t which satisfy (2). By Lemma 3, this is equivalent to finding j and t, with $1 \leqq j < t < n$, such that

$$D(tr) = D(jr) + D((t - j)r).$$

But Lemma 5 implies

$$2sw \geqq D(tr) = D(jr) + D((t-j)r) \geqq sw + sw = 2sw.$$

Hence, we must have

$$D(tr) = 2sw, \qquad D(jr) = D((t-j)r) = sw.$$

On the other hand, suppose for some u, $1 \leqq u < n$, we have

$$D(ur) = 2sw.$$

Let h denote $P_p(u)$ and set $u = p^h u'$. As in Lemma 5, set

$$u' = u_1' + u_2',$$

where $u_2' \leqq r$ and $D(u_2' r) = sw$. Since

$$D(u'r) = D(ur) = 2sw$$

then we must have $D(u_1' r) = sw$. Thus for $j = p^h u_2'$,

$$\binom{ur}{jr} \not\equiv 0 \pmod{p}.$$

We can summarize this discussion in

Lemma 6: The number of t which satisfy (2) is exactly the number of t for which

$$D(tr) = 2sw.$$

By a previous remark, this is just the number of t such that

$$D(tr) = sw.$$

This problem is equivalent to finding the number of u, $1 \leqq u < p^{3s} - 1$, such that

$$D(u) = sw \quad \text{and} \quad u \equiv 0 \pmod{r}. \tag{5}$$

We state the result in

Lemma 7: The number of integers u which satisfy (5) is $\binom{p+1}{2}^s$.

Proof: Write u in the form

$$u = \sum_{i=0}^{s-1} a_i p^i + p^s \sum_{i=0}^{s-1} b_i p^i + p^{2s} \sum_{i=0}^{s-1} c_i p^i$$

$$= A + p^s B + p^{2s} C,$$

where

$$0 \leqq A, B, C \leqq r = p^s - 1.$$

Then

$$u = A + B + C + (p^s - 1)B + (p^{2s} - 1)C$$

and so we have

$$u \equiv 0 \pmod{r}$$

if and only if

$$A + B + C = 0 \pmod{r}.$$

Since $u > 0$, then by Lemma 5,

$$D(A + B + C) \geqq sw.$$

But

$$D(A + B + C) \leqq D(A) + D(B) + D(C) = D(u) = sw$$

by the corollary to Lemma 3. Hence, we must have

$$D(A + B + C) = sw = D(A) + D(B) + D(C).$$

This implies that

$$a_i + b_i + c_i \leqq w, \qquad i = 0, 1, \cdots, s - 1,$$

and consequently

$$A + B + C \leqq r.$$

However, the requirement that r divides u implies

$$A + B + C = r,$$

so the only possibility left is

$$a_i + b_i + c_i = w, \qquad i = 0, 1, \cdots, s - 1.$$

Since the number of ways (cf. Ref. 4, 6.6) of obtaining w as the ordered sum of three nonnegative integers is $\binom{w+2}{2} = \binom{p+1}{2}$ then the total number of choices for A, B, and C (and hence for u) is just $\binom{p+1}{2}^s$. This completes the proof of Lemma 7.

By combining the preceding lemmas, Theorem 2 is proved.

V. CODING THEORY

It has been shown[1] that the minimum distance of the dual code of the cyclic code $R \cdot \theta(x)$ is at least $p^s + 2$. It is now easy to show that the minimum distance of $R \cdot \theta(x)$ itself is $p^s + 1$.

Since $R \cdot \theta(x)$ contains $\theta(x)$, $p^s + 1$ is an upper bound for its minimum distance; it suffices to show that it is also a lower bound.

By Theorems 1 and 2, ζ^t is a zero of $\theta(z)$ if $D(tr) = sw$ (this is, of course, only a sufficient condition). By Lemma 4, the $p^s - 1$ numbers $t = 1, 2, \cdots, p^s - 1$ have the property that $D(tr) = sw$; clearly $t = p^s$ also has this property. Thus there are at least p^s consecutive powers of ζ which are zeros of $\theta(x)$. By the usual proof of the Bose-Chaudhuri bound* (See Ref. 5, Section 9.1) the minimum distance of $R \cdot \theta(x)$ is at least $p^s + 1$.

Theorem 2′ is a summary of known results about difference-set cyclic codes.

Theorem 2′: Let $d_1, d_2, \cdots, d_l$ be a Singer difference-set modulo n, where $n = p^{2s} + p^s + 1$. Set

$$\theta(x) = \sum_{i=1}^{l} x^{d_i}.$$

Let R be the ring of polynomials modulo $x^n - 1$ over $GF(p)$. Then $R \cdot \theta(x)$ is a cyclic code of dimension $\binom{p+1}{2}^s + 1$, and minimum distance $p^s + 1$.

It has been shown that for every Singer difference-set modulo n, there exists a set of integers t such that ζ^t is a zero of the difference-set polynomial. The set of such t is the same for every difference set, but this of course does not mean that every $\theta(x)$ has the same zeros in common with $x^n - 1$. The difference set is constructed by means of a primitive nrth root of unity ν; ν determines the choice of ζ, and a different choice may or may not lead to a different set of zeros for $\theta(x)$.

APPENDIX A

Example

Take $p = 2$, $s = 2$, $n = 2^4 + 2^2 + 1 = 21$, $nr = 2^6 - 1 = 63$. The polynomial $x^6 + x + 1$ is an irreducible factor of $x^{63} + 1$ over $GF(2)$

* The proof applies although $R \cdot \theta(x)$ is not necessarily a BCH code.

[see Ref. 6, p. 309, polynomial f_{10}]. In this case, ω is a cube root of unity and the above polynomial factors over $GF(4)$ into

$$(x^3 + x^2 + \omega^2 x + \omega)(x^3 + x^2 + \omega x + \omega^2).$$

We take a zero of the first polynomial for ν, and for purposes of calculation it is convenient to express it as

$$\nu = \begin{bmatrix} 1 & 1 & 0 \\ \omega^2 & 0 & 1 \\ \omega & 0 & 0 \end{bmatrix}.$$

It is readily checked that the characteristic equation of this matrix is $x^3 + x^2 + \omega^2 x + \omega$. A table of the relevant powers of ν follows.

$$\nu = \begin{bmatrix} 1 & 1 & 0 \\ \omega^2 & 0 & 1 \\ \omega & 0 & 0 \end{bmatrix} \quad \nu^2 = \begin{bmatrix} \omega & 1 & 1 \\ 1 & \omega^2 & 0 \\ \omega & \omega & 0 \end{bmatrix} \quad \nu^3 = \begin{bmatrix} \omega^2 & \omega & 1 \\ \omega^2 & 1 & \omega^2 \\ \omega^2 & \omega & \omega \end{bmatrix}$$

$$\nu^6 = \begin{bmatrix} 0 & 1 & 0 \\ \omega^2 & 1 & 1 \\ \omega & 0 & 1 \end{bmatrix} \quad \nu^{12} = \begin{bmatrix} \omega^2 & 1 & 1 \\ 1 & \omega & 0 \\ \omega & \omega & 1 \end{bmatrix}$$

$$\nu^7 = \begin{bmatrix} \omega^2 & 0 & 1 \\ \omega & \omega^2 & 1 \\ 0 & \omega & 0 \end{bmatrix} \quad \nu^{14} = \begin{bmatrix} \omega & \omega & \omega^2 \\ 0 & 0 & 1 \\ \omega^2 & 1 & \omega \end{bmatrix}$$

Take $d_1 = 3$, $d_2 = 6$.

$$\nu^3 + \nu^6 = \begin{bmatrix} \omega^2 & \omega^2 & 1 \\ 0 & 0 & \omega \\ 1 & \omega & \omega^2 \end{bmatrix} = \omega\nu^{14}$$

$$\omega\nu^3 + \nu^6 = \begin{bmatrix} 1 & \omega & \omega \\ \omega & \omega^2 & 0 \\ \omega^2 & \omega^2 & \omega \end{bmatrix} = \omega\nu^{12}$$

$$\omega^2\nu^3 + \nu^6 = \begin{bmatrix} \omega & \omega & \omega^2 \\ 1 & \omega & \omega^2 \\ 0 & 1 & 0 \end{bmatrix} = \omega\nu^7.$$

Hence, 3, 6, 7, 12, 14 is a difference-set modulo 21. In this case, $r = 2^2 - 1 = 3$, and the appropriate values of t are 5, 10, 20, 19, 17, 13; 9, 18, 15. ($tr = 15, 30, 60$ etc.) It is readily checked that each tr has a digit sum (to base 2) of $2s = 4$.

APPENDIX B

Let $\theta(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. The ideal $R \cdot \theta(x)$ consists of all linear combinations over $GF(p)$ of the n polynomials $x^i\theta(x)$ (mod $(x^n - 1)$), $i = 0, 1, \cdots, n - 1$. Its dimension is therefore the rank over $GF(p)$ of the matrix

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}.$$

Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be the n zeros of $x^n - 1$ over $GF(p)$; they are all distinct since p does not divide n. Let Δ be the matrix

$$\Delta = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}.$$

Then

$$\det \Delta = \prod_{i<j\leqq n} (\alpha_i - \alpha_j) \neq 0,$$

and the rank of A is the same as the rank of $A\Delta$. Now,

$$A\Delta = \begin{vmatrix} \theta(\alpha_1) & \theta(\alpha_2) & \cdots & \theta(\alpha_n) \\ \alpha_1\theta(\alpha_1) & \alpha_2\theta(\alpha_2) & \cdots & \alpha_n\theta(\alpha_n) \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_1^{n-1}\theta(\alpha_1) & \alpha_2^{n-1}\theta(\alpha_2) & \cdots & \alpha_n^{n-1}\theta(\alpha_n) \end{vmatrix}.$$

Suppose the a_i are arranged so that $\theta(\alpha_i) \neq 0$, $i = 1, \cdots, t$, and $\theta(\alpha_i) = 0$ $i = t + 1, \cdots, n$. The last $n - t$ columns of $A\Delta$ contain only zeros, so that the rank of $A\Delta$ is $\leqq t$. The t by t matrix in the upper left hand corner of $A\Delta$ is

$$\begin{vmatrix} \theta(\alpha_1) & \theta(\alpha_2) & \cdots & \theta(\alpha_t) \\ \alpha_1\theta(\alpha_1) & \alpha_2\theta(\alpha_2) & \cdots & \alpha_t\theta(\alpha_t) \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_1^{t-1}\theta(\alpha_1) & \alpha_2^{t-1}\theta(\alpha_2) & \cdots & \alpha_t^{t-1}\theta(\alpha_t) \end{vmatrix},$$

and the determinant of this is

$$\theta(\alpha_1)\cdot\theta(\alpha_2) \cdots \theta(\alpha_t) \prod_{i<j\leqq t} (\alpha_i - \alpha_j) \neq 0.$$

Thus, the rank of $A\Delta$ (hence, the dimension of $R\cdot\theta(x)$) is exactly t.

REFERENCES

1. Weldon, E. J., Jr., Difference-Set Cyclic Codes. B.S.T.J. this issue, pp. 1045–1055.
2. Singer, J., A Theorem in Finite Projective Geometry and Some Applications to Number Theory, Trans., AMS *43*, 1938, pp. 377–385.
3. Evans, T. A. and Mann, H. B., On Simple Difference Sets, Sankhya, *11*, 1955, pp. 464–481.
4. Riordan, J., *An Introduction to Combinatorial Analysis*, John Wiley and Sons, 1958.
5. Peterson, W. W., *Error Correcting Codes*, M.I.T. Press, 1961.
6. MacWilliams, Jessie, The Structure and Properties of Binary Cyclic Alphabets, B.S.T.J., *44*, 1965, pp. 303–332.