ESTI FILE COPY

ESD-TDR-64-348

Group Report 1964-37

E. Weiss

Partial Fractions and Error-Correcting Codes

6 July 1964

Prepared under Electronic Systems Division Contract AF 19(628)-500 by

Lincoln Laboratory
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Lexington, Massachusetts

AD602982

The work reported in this document was performed at Lincoln Laboratory, a center for research operated by Massachusetts Institute of Technology, with the support of the U.S. Air Force under Contract AF 19(628)-500.

48

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

LINCOLN LABORATORY

PARTIAL FRACTIONS AND ERROR-CORRECTING CODES

E. WEISS

Group 66

GROUP REPORT 1964-37

6 JULY 1964

LEXINGTON MASSACHUSETTS

Abstract

In this note we show how partial fractions may be used to derive the properties of linear recursive sequences and, in particular, of Bose-Chaudhuri codes. One of the novel features of this method is a new and transparent proof of the basic result of Mattson-Solomon.

Accepted for the Air Force
Franklin C. Hudson, Deputy Chief
Air Force Lincoln Laboratory Office

Partial Fractions and Error-Correcting Codes

There have appeared several expositions of the theory of Bose-Chaudhuri codes—see, for example, references [2], [3], [5] and [6]. Perhaps the most interesting version, in that it leads to the deepest results, is due to Mattson and Solomon [4]. The distinctive feature of their approach arises from the representation of each code vector as the set of values taken on by a certain polynomial at certain roots of unity; in this way the weight of a vector is related to the number of roots of a polynomial.

In this note we show how partial fractions may be used to derive the properties of linear recursive sequences and, in particular, of Bose-Chaudhuri codes. One of the novel features of this method is a new and transparent proof of the basic result of Mattson-Solomon.

We shall work over the two-element field $F = \{0, 1\}$. Essentially, all our remarks will carry over to the case of an arbitrary finite field, but the details of the carry-over will be left to the reader. If x is an indeterminate over F, then $F[x]$ denotes the ring of all polynomials $f(x) = c_o + c_1x + c_2x^2 + \cdots + c_nx^n$ with coefficients in F. We let $F\langle x\rangle$ denote the ring of formal power series with coefficients in F. In other words, an element of $F\langle x\rangle$ is of form

$$a(x) = a_o + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots = \sum_{i=o}^{\infty} a_i x^i \qquad a_i \in F \tag{1}$$

and if, in addition, $b(x) = \sum_{i=o}^{\infty} b_i x^i \in F\langle x \rangle$ then

$$a(x) + b(x) = \sum_{o}^{\infty} (a_i + b_i) x^i \tag{2}$$

and the n^{th} term of the product $a(x)b(x)$ is

$$(a(x)\, b(x))_n = \left(\sum_{j=o}^{n} a_j b_{n-j} \right) x^n \tag{3}$$

We shall also identify $F\langle x \rangle$ with $V_{\infty}(F)$, the set of all infinite sequences from F under the obvious correspondence

$$a_o + a_1 x + a_2 x^2 + \cdots \longleftrightarrow (a_o, a_1, a_2, \cdots) \tag{4}$$

In particular, the vector space $V_{\infty}(F)$ thus has the structure of a ring.

Suppose that $f(x) = c_o + c_1 x + \cdots + c_n x^n \in F[x]$ has $c_o = c_n = 1$ and that $a(x) = \sum_{o}^{\infty} a_i x^i \in F\langle x \rangle$. We say that $a(x)$ is <u>linear recursive for f</u> when the following relation holds:

$$a_i = c_1 a_{i-1} + c_2 a_{i-2} + \cdots + c_n a_{i-n} \qquad \text{for all } i \geq n \tag{5}$$

These conditions may also be rewritten as

$$c_o a_i + c_1 a_{i-1} + \cdots + c_n a_{i-n} = 0 \qquad \text{for all } i \geq n \tag{6}$$

The set of all elements of $F\langle x\rangle$ which are linearly recursive for f is denoted by $G(f)$.

Our first observation provides a simple characterization of $G(f)$, namely,

<u>Proposition 1</u>: $G(f) = \{ \frac{g(x)}{f(x)} \mid g(x) \in F[x], \ \deg g < \deg f\}$

<u>Proof</u>: Consider $a(x) \in F\langle x\rangle$. Since the coefficient of x^i in $a(x)f(x)$ for $i \geq n$ is $\sum_{j=o}^{n} c_j a_{i-j}$, it follows from (6) that

$$a(x) \in G(f) \Longleftrightarrow a(x)f(x) \text{ is a polynomial of degree } < n = \deg f(x)$$

$$\Longleftrightarrow a(x) = \frac{g(x)}{f(x)}, \ g(x) \in F[x], \ \deg g < \deg f .$$

<u>Corollary 1</u>: $G(f)$ is a vector space of dimension $n = \deg f$ over F.

<u>Corollary 2</u>: If $f_1 \mid f_2$ then $G(f_1) \subset G(f_2)$; moreover equality holds if and only if $f_1 = f_2$.

<u>Corollary 3</u>: If f_1 and f_2 are relatively prime then

$$G(f_1 f_2) = G(f_1) + G(f_2)$$

<u>Proof</u>: In virtue of Corollary 2,

$$G(f_1) + G(f_2) \subset G(f_1 f_2)$$

Suppose then that $a \in G(f_1f_2)$, and put $n_i = \deg f_i$, $i = 1, 2$. Thus we have $a = g/f_1f_2$ with $\deg g < n_1 + n_2$. We assert that

$$\frac{g}{f_1f_2} = \frac{g_1}{f_1} + \frac{g_2}{f_2} \quad \text{with } \deg g_i < n_i \qquad i = 1, 2 \tag{7}$$

and we give a constructive proof of this fact. Since $(f_1, f_2) = 1$ there exist polynomials k_1, k_2 such that $k_1f_1 + k_2f_2 = 1$. Therefore, $gk_1f_1 + gk_2f_2 = g$, and by the Euclidean algorithm we may write

$$gk_1 = tf_2 + g_2 \qquad \deg g_2 < n_2 = \deg f_2 \quad .$$

In other words,

$$g = g_2f_1 + (gk_2 + tf_1)f_2$$

Since g and g_2f_1 have degree $< n_1 + n_2$, it follows that $g_1 = gk_2 + tf_1$, has degree $< n_1$. These are the desired g_1 and g_2. Thus, a $a \in G(f_1) + G(f_2)$, and the proof is complete.

Corollary 4: For arbitrary f_1 and f_2 of degrees n_1 and n_2 respectively, let $d = \gcd(f_1, f_2)$ and $m = \operatorname{lcm}(f_1, f_2)$; then $G(f_1) \cap G(f_2) = G(d)$ and $G(f_1) + G(f_2) = G(m)$.

Proof: Choose polynomials k_1, k_2 such that $k_1f_1 + k_2f_2 = d$. Then

$$G(f_1) \cap G(f_2) \subset G(k_1f_1) \cap G(k_2f_2) \subset G(d) \subset G(f_1) \cap G(f_2) \tag{8}$$

where the non-trivial inclusion may be proved as follows. Suppose $a \in G(f_1f_1) \cap G(k_2f_2)$ — so $a = \dfrac{g_1}{k_1f_1} = \dfrac{g_2}{k_2f_2}$ with $\deg g_i < \deg k_if_i$, $i = 1, 2$.

Therefore,

$$a = \frac{g_1 + g_2}{k_1f_1 + k_2f_2} = \frac{g_1 + g_2}{d}$$

and it remains to show that $\deg(g_1 + g_2) < \deg d$. But

$$\begin{aligned}\deg(g_1 + g_2) &= \deg(g_1k_2f_2 + g_2k_2f_2) - \deg k_2f_2 \\ &= \deg(g_2k_1f_1 + g_2k_2f_2) - \deg k_2f_2 \\ &= \deg(k_1f_1 + k_2f_2) - \deg k_2f_2 + \deg g_2 \\ &= \deg d - (\deg k_2f_2 - \deg d) \\ &< \deg d \ .\end{aligned}$$

Since $G(f_1) + G(f_2) \subset G(m)$, it suffices to prove that these vector spaces have the same dimension, and in view of the above this follows from

$$\dim(G(f_1) + G(f_2)) + \dim(G(f_1) \cap G(f_2)) = \dim G(f_1) + \dim G(f_2) \ .$$

This completes the proof.

Corollary 5: $G(f_1) \cap G(f_2) \subset G(f_1 + f_2)$

Proof: Trivial, since $d \mid (f_1 + f_2)$. Of course, $f_1 + f_2$ has no constant term, so $G(f_1 + f_2)$ should be defined by dividing $f_1 + f_2$ by the power of x which will yield a constant term equal to 1.

Corollary 6: If f_1 and f_2 are relatively prime then

$$G(f_1 f_2) = G(f_1) \oplus G(f_2) \qquad \text{direct sum}$$

Let us define a linear transformation, called translation, of $F\langle x\rangle$.

For $a = \sum_{0}^{\infty} a_i x^i \in F\langle x\rangle$, put $aT = \sum_{0}^{\infty} a_{i+1} x^i$.

Proposition 2: $G(f)$ is translation invariant; in other words, if $a \in G(f)$ then $aT \in G(f)$.

Proof: If $a = g/f$ and we let g_o denote the constant term of g then (since $g_o = a_o$)

$$aT = \frac{\frac{g}{f} - g_o}{x} = \frac{\left(\frac{g - fg_o}{x}\right)}{f}, \quad \deg \frac{(g - fg_o)}{x} < \deg f . \tag{9}$$

Let Ω denote a fixed algebraic closure of F, so that $f(x)$ has n roots $\beta_1, \ldots, \beta_n$ in Ω. For convenience and because this is the most interesting situation, we shall assume henceforth that f(x) has distinct roots. Since every element of Ω is a root of unity, there exists a smallest integer m with the property that $(\beta_i)^m = 1$ for $i = 1, \ldots, m$. In other words, m is the unique smallest integer such that $f(x) \mid (x^m + 1)$. Note that m is odd—for if $m = 2k$ $f(x) \mid (x^{2k} + 1) = (x^k + 1)^2 \Longrightarrow f(x) \mid (x^k + 1)$. If we put

$$f^*(x) = \frac{x^m + 1}{f(x)} \tag{10}$$

then $a(x) = \frac{g(x)}{f(x)} \in G(f) \subset G(x^m + 1)$ can be written in the form

$$a(x) = \frac{g(x)\, f^*(x)}{x^m + 1} \qquad \deg(gf^*) < m \tag{11}$$

Now, for an element $a(x) \in F\langle x\rangle$ it follows from

$$\frac{1}{1+x^m} = 1 + x^m + x^{2m} + x^{3m} + \cdots \tag{12}$$

that $a(x)$ has m as a period $\Longleftrightarrow$ $a(x)(1+x^m)$ is a polynomial of degree $< m$ $\Longleftrightarrow$ $a(x) \in G(x^m + 1)$. We have therefore:

<u>Proposition 3</u>: Let m be the smallest integer such that $f(x) \mid (x^m + 1)$; then every element of $G(f)$ has m as a period and, in fact, m is the smallest common period of the elements of $G(f)$.

It is of interest, though not in the main stream of the present discussion, to take a slightly different viewpoint. With the notation as before, for $a(x) \in G(f)$ we may refer to

$$a(x)(1+x^m) = a_o + a_1 x + \cdots + a_{m-1} x^{m-1}$$

as its <u>periodic part</u> and this determines an element in the residue class ring $R = F[x]/(x^m + 1)$. More precisely the map

$$a(x) \longrightarrow a(x)(x^m + 1) \tag{13}$$

is an isomorphism of $G(f)$ into R. Thus, we may view $G(f)$ as contained in R, and when this view is taken we have:

<u>Proposition 4</u>: $G(f)$ is the ideal Rf^* of R

<u>Proof</u>: In R $G(f) = \{ gf^* \mid \deg g < \deg f \} \subset Rf^*$. On the other hand, any polynomial g can be written as $g = kf + r$ with $\deg r < \deg f$. Since $ff^* = 0$

in R, it follows that $gf^* = rf^*$ — so $Rf^* = G(f)$.

Let us return to an arbitrary element of $G(f)$; it is of form $a(x) = g(x)/f(x)$. Since $\deg g < \deg f$ and $f(x) = (x+\beta_1)\cdots(x+\beta_n)$ we have a partial fraction decomposition (see [1])

$$a(x) = \frac{g(x)}{f(x)} = \frac{\alpha_1}{x+\beta_1} + \cdots + \frac{\alpha_n}{x+\beta_n} \tag{14}$$

The coefficients α_i are unique and come from the splitting field K of $f(x)$ over F. Now, expansion of (14) yields:

$$\frac{g(x)}{f(x)} = \sum_1^n \frac{\alpha_i}{x+\beta_i} = \sum_1^n \frac{\alpha_i}{\beta_i}\left(\frac{1}{1+\frac{x}{\beta_i}}\right)$$

$$= \sum_{i=1}^n \left\{\frac{\alpha_i}{\beta_i}\left[\sum_{j=o}^{\infty}\left(\frac{x}{\beta_i}\right)^j\right]\right\}$$

$$= \sum_{i=1}^n \sum_{j=o}^{\infty} \alpha_i \beta_i^{-(j+1)} x^j \tag{15}$$

Thus, the coefficients of $a(x)$ are given in terms of elements from K by

$$a_j = \sum_{i=1}^n \alpha_i \beta_i^{-(j+1)} \qquad j=0, 1, 2, \ldots \tag{16}$$

Fix a primitive m^{th} root of unity ζ, where m is as in Proposition 3.

Thus, there exist distinct integers r_j for $j = 1, \ldots, n$ such that

$$\beta_j^{-1} = \zeta^{r_j} \qquad 0 \leq r_j \leq m-1 \tag{17}$$

Upon reversal of notation in (16), we get

$$a_i = \sum_{j=1}^{n} \alpha_j \beta_j^{-(i+1)} = \sum_{j=1}^{n} (\alpha_j \zeta^{r_j})(\zeta^{i})^{r_j} \tag{18}$$

If we then put

$$P_a(x) = \sum_{j=1}^{n} (\alpha_j \zeta^{r_j}) x^{r_j} \tag{19}$$

then clearly

$$P_a(\zeta^i) = a_i \qquad i = 0, 1, 2, \ldots \tag{20}$$

We have proved (see [4])

<u>Proposition 5</u>: For each $a \in G(f)$ there exists a polynomial $P_a(x) \in K[x]$ with $\deg P_a(x) \leq \max\{r_j\}$ and such that $a_i = P_a(\zeta^i)$ for $i = 0, 1, 2, \ldots$.

If we had written $\beta_j = \zeta^{r_j}$ (with different r_j) instead of $\beta_j^{-1} = \zeta^{r_j}$, formula (18) would become

$$a_i = \sum_{j=1}^{n} (\alpha_j \zeta^{-r_j})(\zeta^{-i})^{r_j} \tag{21}$$

and the polynomial $\overline{P}_a(x) = \sum_{j=1}^{n} (\alpha_j \zeta^{-r_j}) x^j \in K[x]$ would satisfy

$P_a(\xi^{-i}) = a_i$, $i = 0, 1, 2, \ldots$. All this amounts solely to the use of the primitive m^{th} root of unity ξ^{-1} instead of ξ. The use of any other primitive m^{th} root of unity would give an analogous result, but with different values for r_j. When it is necessary to emphasize the dependence of r_j on ξ, we shall write them as $r_j(\xi)$.

It may be noted that for any $a(x) \in F\langle x \rangle$ with odd period, m say, we may write $a(x) = g(x)/x^m + 1$, and according to Proposition 5 there exists a polynomial whose value at ξ^i is a_i for all $i \geq 0$.

Now, let us look somewhat more carefully at formula (14); we shall also change notation in the process. Let σ denote the automorphism of Ω/F such that $\sigma(\xi) = \xi^2$ for all $\xi \in \Omega$; then for any finite extension E/F, σ is a generator of the Galois group of E/F. $f(x)$ is a polynomial of degree m with distinct roots which divides $x^m + 1$, m odd. The irreducible factorization of $x^m + 1$ is of form

$$x^m + 1 = (x + 1)\, f_1(x)\, f_2(x) \cdots f_s(x) \tag{22}$$

where each $f_i(x) \in F[x]$ is irreducible, and they are all distinct. The f_i may have different degrees, but it may be observed that when m is an odd prime they all have the same degree $\frac{m-1}{s}$.

Since $f(x) \mid (x^m + 1)$, it is of form (with re-ordering, if necessary)

$$f(x) = (x + 1)^{\delta}\, f_1(x) \cdots f_t(x) \qquad \delta = 0 \text{ or } 1,\ t \leq s \tag{23}$$

Denoting the degree of f_i by n_i, we may index the roots of f_i by

$\{\xi_i, \sigma\xi_i, \sigma^2\xi_i, \ldots, \sigma^{n_i-1}\xi_i\}$ $i = 1, \ldots, t$. In particular, the field $E_i = F(\xi_i)$ is the splitting field of $f_i(x)$ over F and its degree is n_i; K is the composite of all the E_i. Any element $a(x) = \frac{g(x)}{f(x)} \epsilon G(f)$ may be written uniquely (as in Corollary 3) in the form

$$a(x) = \frac{g_o(x)}{x+1} + \frac{g_1(x)}{f_1(x)} + \cdots + \frac{g_t(x)}{f_t(x)} \qquad g_i \epsilon F[x], \ \deg g_i < n_i \tag{24}$$

where, of course, $g_o(x)$ is a constant and is 0 when $x+1$ is not a factor of $f(x)$. By decomposing each term on the right we get a unique expression

$$a(x) = \frac{\eta_o}{x-1} + \frac{\eta_1}{x-\xi_1} + \frac{\eta_1^{(1)}}{x-\sigma\xi_1} + \cdots + \frac{\eta_1^{(n_1-1)}}{x-\sigma^{n_1-1}\xi_1} + \cdots + \frac{\eta_t}{x-\xi_t} + \cdots + \frac{\eta_t^{(n_t-1)}}{x-\sigma^{n_t-1}\xi} \tag{25}$$

where $\eta_o = 0$ or 1 and $\eta_i, \eta_i^{(j)} \epsilon E_i$. Now, extend σ to an automorphism of $\Omega\langle x\rangle$ by putting $\sigma x = x$; thus, for example, $\sigma(\frac{\eta}{x-\xi}) = \frac{\sigma\eta}{x-\sigma\xi}$. Apply, this extended σ to both sides of (25). The left side is unchanged (since $a(x) \epsilon F\langle x\rangle$), hence so is the right side. By uniqueness, we have then $\sigma\eta_i = \eta_i^{(1)}$, $i = 1, \ldots, t$. Repeating the process, yields $\sigma^j\eta_i = \eta_i^{(j)}$. If we let S_i denote the trace function from E_i to F (so that S_i is the operator $\sigma + \sigma^2 + \sigma^3 + \cdots + \sigma^{n_i}$) then:

$$a(x) = \frac{g(x)}{f(x)} = \frac{\eta_o}{x+1} + S_1\left(\frac{\eta_1}{x-\xi_1}\right) + \cdots + S_t\left(\frac{\eta_t}{x-\xi_1}\right) \tag{26}$$

Since

$$\frac{\eta_i}{x-\xi_c} = \sum_{j=o}^{\infty} \left(\eta_i \xi_i^{-(j+1)}\right) x^j$$

we may write

$$\frac{g(x)}{f(x)} = \sum_{j=o}^{\infty} \eta_o x^j + \sum_{j=o}^{\infty} S_1(\eta_1 \xi_1^{-(j+1)})x^j + \cdots + \sum_{j=o}^{\infty} S_t(\beta_t \xi_t^{-(j+1)})x^j$$

The conclusion is then:

Proposition 6: Suppose that $f(x)$ has distinct roots, and let $\xi_1, \ldots, \xi_t$ be representatives of the different conjugate classes of its roots (i. e. the ξ_i are roots of the distinct irreducible factors f_i of f) and put $\xi_o = \eta_o = 1$, $E_o = F$, or $\xi_o = \eta_o = 0$, $E_o = (0)$ according as 1 is or is not a root of $f(x)$. Then given $a(x) \in G(f)$ there exist unique $\eta_i \in E_i = F(\xi_i)$, $i = 0, 1, \ldots, t$ such that

$$a_j = \eta_o + \sum_{i=1}^{t} S_i\left(\eta_i \xi_i^{-(j+1)}\right) \qquad j = 0, 1, 2, \ldots \tag{27}$$

By examining the proof of Proposition 6, we have the following immediate consequence.

Corollary 7: Let the hypotheses be as in Proposition 6; then there is an additive isomorphism between $G(f)$ and the additive groups of the formal direct sum $E_o \oplus E_1 \oplus \cdots \oplus E_t$—it is given by

$$\frac{g(x)}{f(x)} \longleftrightarrow (\eta_o, \eta_1, \ldots, \eta_t)$$

We have been fussing with the distinction between the cases where 1 is or is not a root of $f(x)$. In terms of knowledge of the codes $G(f)$ and their distance properties this distinction is inessential. To see this, suppose that 1 is not a root of $f(x)$ and that the mesh of $G(f)$ (meaning the minimum distance between elements of $G(f)$, or what is the same, the minimum weight of a non-zero element of $G(f)$) is $\geq d$, while the diameter of $G(f)$ (meaning the maximum distance between two elements of $G(f)$) is $\leq D$. Since $\dim G((x-1)f) = \dim G(f) + 1$, it follows that $(1, 1, \ldots, 1) \notin G(f)$. Let

$$\overline{G(f)} = \{ a + (1, 1, 1, \ldots, 1) \mid a \in G(f)\} \tag{28}$$

so that

$$G((x-1)f) = G(f) \cup \overline{G(f)} \qquad \text{disjoint} \tag{29}$$

Of course, this is just the coset decomposition of $G((x-1)f)$ with respect to the subgroup $G(f)$. We see then that

$$\text{mesh } G((x-1)f) \geq \min\{ d, m - D\} \tag{30}$$

where m is the period (i.e. the smallest integer such that $f(x) \mid x^m - 1$) or to be more precise

$$\text{mesh } G((x-1)f) = \min\{ \text{mesh } G(f),\ m - \text{diam } G(f)\} \tag{31}$$

Therefore, it will be necessary only to consider the situation where 1 is not a root of $f(x)$—since (31) relates the error-correcting properties of $(x-1)f(x)$ with those of $f(x)$. This assumption that 1 is not a root of $f(x)$ means that in formula (27) we have $\eta_o = 0$.

Now, in order to make use of (27) it is advisable to assume that $t = 1$—in other words, that $f(x)$ is irreducible. Then, according to Corollary 7, $G(f)$ is additively isomorphic to $E_1 = F(\xi_1)$, and an element $\eta_1 \in E_1$ corresponds to the sequence with

$$a_j = S_1(\eta_1 \xi_1^{-(j+1)}) \qquad j = 0, 1, 2, \ldots \tag{32}$$

Since the trace is a homomorphism of E_1 onto F, it follows immediately that:

Corollary 8: Suppose that $f(x)$ is irreducible. For each j the j^{th} coordinates of the elements of $G(f)$ are half zeros and half ones.

Needless to say, this result can be derived in other ways also. Another standard fact which is an immediate consequence of (32) is:

Corollary 9: Suppose that $f(x)$ is a primitive polynomial of degree n, then every element of $G(f)$ (except the zero vector) has 2^{n-1} ones and $2^{n-1} - 1$ zeros.

Proof: ξ_1 is a primitive $2^n - 1^{th}$ root of unity, so $\{\eta_1 \xi_1^{-(j+1)}\}$ runs over all non-zero elements of the field E_1 (for $\eta_1 \neq 0$).

From our discussion, it is clear that (20) and (27) are equivalent as far as the properties of $a(x)$ in $G(f)$ are concerned. However, (20) is often more useful, since it gives an immediate bound for the weight of $a(x)$. More precisely, with ζ as in (17) let $\mathfrak{z}(\zeta) = \{1, \zeta, \ldots, \zeta^{m-1}\}$ be the multiplicative group generated by ζ. Then the polynomial $P_a(x)$ of (19) provides a function from $\mathfrak{z}(\zeta) \to F$. Now the weight of $a(x)$ can be expressed as

$$\| a(x) \| = \#\{ \xi \in \mathfrak{z}(\zeta) \mid P_a(\xi) = 1 \}$$

$$= m - \#\{ \mathfrak{z}(\zeta) \cap \ker P_a(x) \}$$

Now $\deg P_a(x) \leq \max\limits_j r_j$ so that $\ker P_a(x)$ has $\leq \max\limits_j r_j$ elements, and

$$\| a(x) \| \geq m - \max_j r_j$$

Of course, $P_a(x)$ has a very special form (essentially, it too can be expressed in terms of traces) and we hope to discuss such matters in a future note.

REFERENCES

1. G. Birkhoff and S. MacLane, "A Survey of Modern Algebra", MacMillan, New York (1957).

2. R. C. Bose and D. K. Ray-Chaudhuri, "On a Class of Error-Correcting Codes," Information and Control, 3, (1960).

3. D. Gorenstein and N. Zierler, "A Class of Error-Correcting Codes in p^m Symbols," J. Soc. Indust. Appl. Math, 9 (1961).

4. H. F. Mattson and G. Solomon, "A New Treatment of Bose-Chaudhuri Codes," J. Soc. Indust. Appl. Math, 9 (1961).

5. W. W. Peterson, "Error-Correcting Codes," MIT and Wiley, New York (1961).

6. E. Weiss, "Some Connections Between Linear Recursive Sequences and Error-Correcting Codes: Informal Lectures," Group Report 55-22, Lincoln Laboratory (1960).

DISTRIBUTION

Group 28

C. R. Arnold

Division 6

G. P. Dinneen
W. E. Morrow, Jr.

Group 62

B. Gold
K. L. Jordan, Jr.
I. L. Lebow
P. Rosen

Group 63

R. M. Lerner
J. Max
W. G. Schmidt
H. Sherman

Group 64

R. Price

Group 66

F. Belvin
R. G. Enticknap
T. J. Goblick, Jr.
J. R. Kinney
T. S. Pitcher
R. T. Prosser
B. Reiffen
W. L. Root
D. Snyder
E. Weiss
File (10)