THE UNIVERSITY OF MICHIGAN
COLLEGE OF ENGINEERING
Department of Electrical Engineering
Information Systems Laboratory

Technical Note

LINEAR NUMBER SYSTEMS

Richard F. Arnold

ORA Project 04879-8-T

under contract with:

UNITED STATES AIR FORCE
AERONAUTICAL SYSTEMS DIVISION
CONTRACT NO. AF 33(657)-7811
WRIGHT-PATTERSON AIR FORCE BASE, OHIO

administered through:

OFFICE OF RESEARCH ADMINISTRATION ANN ARBOR

October 1962

TABLE OF CONTENTS

SUMMARY

This paper presents a treatment of linear, computer number systems using the theory of finitely generated modules over the integers. The theory succeeds in characterizing certain properties of number systems relating to the structure of addition and carry propagation. There is some discussion of redundant number systems and their possible importance in computational speed. An appendix contains Le Veque's proof of the key theorem necessary to obtain necessary and sufficient conditions for non-redundant, linear number systems.

1. INTRODUCTION

This paper presents the basic development of a theory of linear number systems based on the theory of modules over a principal ideal domain. A sufficient amount of background information is given together with examples of codes covered in this class. Moreover, some considerations are briefly discussed which relate this theory to practical computer design.

2. ALGEBRAIC PRELIMINARIES

It is assumed that the reader is familiar with the concepts of group, ring, field and vector space.

Definition: Let R be a commutative ring with identity, and M an abelean group. M is said to have the structure of a finitely generated R-module if there is given a map $R \times M \to M$ called scalar multiplication satisfying the following axioms:

(1) $(a + b)x = ax + bx$ $\quad x \in M$ $\quad a,b \in R$

(2) $a(x + y) = ax + ay$ $\quad x,y \in M$ $\quad a \in R$

(3) $ab(x) = a(bx)$ $\quad x \in M$ $\quad a,b \in R$

(4) $1x = x$ $\quad x \in M$ $\quad 1 \in R$

(5) There exists a finite set of elements $\{x_1 \ldots x_k\}$ $x_i \in M$ such that for each $y \in M$, there exist scalars $\{a_1 \ldots a_k\}$ and $\sum_{i=1}^{k} a_i x_i = y$. Such a set is called a set of generators of M.

The notion of an R-module is a generalization of that of vector space. The

generalization takes two directions:

(a) The "scalars" of a module need only be a ring whereas a vector space is always defined over a field.

(b) A module may not have a basis. That is to say it may not satisfy the following strengthened form of axiom 5, which holds for vector spaces.

(5F) There exists a finite set of elements $\{x_1 \ldots x_k\}$ $x_i \in M$ such that for each $y \in M$ there exist unique scalars $\{q_1 \ldots q_k\}$ and $\sum_{i=1}^{k} a_i x_i = y$. Such a set is called a basis of M.

The difference between a set of generators and a basis is that given the latter, each element of the module is expressable in only one way as a linear combination of basis elements. An R-module having a basis is said to be free.

A map ϕ from an R-module M to an R-module N is called a homomorphism if:

(1) $\phi(x + y) = \phi(x) + \phi(y)$ $\qquad x,y \in M$

(2) $a\phi(x) = \phi(ax)$ $\qquad x \in M \quad a \in R$

Much of one's intuition about vector space homomorphisms carries over to modules, however one must be careful to note which theorems assume the existence of a basis. The interested reader should study Vol. II of Jacobson's "Linear Algebra."

3. NUMBER SYSTEMS

In this section, we develop the notion of a non-redundant linear number system characterized by the internal structure of the system and an interpretation function which is compatible with this structure. From this definition it will be shown that a non-redundant number system can be given the structure

of a module in a very natural way.

Definition: A finite set X of m elements is called a digit iff there is a distinguished element called zero, and a partially defined function $s:X \to X$ called "successor" satisfying the axioms.

(1) The domain of definition of s has cardinality (m-1)

(2) For $n > 0$, $s^n(x) \neq x$ $\qquad x \in X$

(3) $s(x) = s(y) \to x = y$

We write the elements of X as $\{0, 1, 2, \ldots, (m-1)\}$ and define an internal addition and subtraction wherever it is compatible with the successor function.

(1) $x + 0 = 0 + x = x$ $\qquad x \in X$

(2) If $x + y$ and $s(x + y)$ are defined
then $x + s(y) = s(x) + y = s(x + y)$ $\qquad x,y \in X$

(3) If $x + y = z$ then $z - y = x$ $\qquad x,y,z \in X$

Notice that addition of two elements whose "sum" in the ordinary sense exceeds (m-1) is not defined.

Let $Y = X_1 \times X_2 \times \ldots X_k$ be the cartesian product of k digits. Y has cardinality $M = \prod_{i=1}^{k} m_i$ (the m_i are not necessarily the same). A partial addition on Y is inherited from the partial addition in the digits.

$$(x_1 \ldots x_k) + (y_1 \ldots y_k) = (x_1 + y_1, \ldots, x_k + y_k)$$

for $(x_1 \ldots x_k), (y_1 \ldots y_k) \in Y$

if $x_i + y_i$ is defined for all i.

Y is called a non-redundant linear number system if a function $\phi:Y \to Z/M$ from Y into the ring of integers modulo M which is 1-1, onto and is compati-

ble with the partial addition in Y.

$$\phi(y + z) = \phi(y) + \phi(z) \qquad y,z \in Y \qquad \text{if } y + z \text{ is defined.}$$

Notice that ϕ is determined if its value is given for each of the elements $e_i = (0, 0, \ldots, 1_i, 0, 0)$. The numbers $\phi(e_i)$ in Z/M are called weights.

The fact that ϕ is 1-1 onto allows the addition in Y to be extended to arbitrary pairs of elements of Y so that ϕ becomes an isomorphism.

Y now has the structure of an abelean group. It becomes a Z/M - module by using the ring multiplication in the obvious way.

$$ay = \phi^{-1}(a\phi(y)) \qquad a \in Z/M \qquad y \in Y$$

Consider the free Z/M - module F on R generators $\{t_1 \ldots t_k\}$. This is just the set of all linear forms in the t_i with coefficients from Z/M. With respect to $\{t_i\}$ as a basis, the elements of F may be taken as k-tuples of elements of Z/M. The set $\{e_i\}$ $e_i = (0, 0, \ldots 1_i, 0, \ldots 0) \in Y$ may be taken as a set of generators for Y. A homomorphism $\psi: F \to Y$ is defined from the free module F to the number system Y by mapping t_i into e_i. Since $\{t_i\}$ is a basis for F, it may be mapped arbitrarily into any Z/M - module. and such a mapping determines the homomorphism.

$$\psi(\Sigma \alpha_i t_i) = \Sigma \alpha_i e_i$$

ψ is onto because $\{e_i\}$ is a set of generators. Let $H \subset F$ be the kernel of ψ, i.e.,

$$H = \{h: h \in F \text{ and } \psi(h) = 0\}$$

so

$$F/H \cong Y$$

H is a submodule of F, and it can be shown (Jacobson Vol. II, pp. 77-78) that if F is free, so is H.

The construction given above is usually made for the purpose of showing that every finitely generated module is isomorphic to the quotient of two free modules. Our purpose is quite different. It will be shown that the above characterization yields interesting information about the structure of addition in Y when "digit overflow" occurs.

It will be convenient to represent the free submodule H as a matrix. The generators of H appear as rows in this matrix $[h_{ij}]$. Although H is unique, a set of generators for H is usually not. The big advantage of writing H as a matrix is that it enables us to concisely express the manner in which <u>all</u> sets of generators of a particular H may be obtained.

We denote by G_ℓ the set of invertible ℓ by ℓ matrices with elements from R. If $[h_{ij}]$ is a matrix of generators for H, then we can show that $y[h_{ij}]$ is also when $y \in G_\ell$. Let some $a \in F$ be in H. Then we know that since $[h_{ij}]$ is a set of generators, there exists a set of coefficients $\{\alpha_i\}$ such that

$$(\alpha_1 \ldots \alpha_\ell) \begin{bmatrix} h_{11} \ldots h_{1k} \\ h_{\ell 1} \ldots h_{\ell k} \end{bmatrix} = (a_1 \ldots a_k) = a$$

The set of coefficients with respect to the new set of generators $y[h_{ij}]$ will then be $\alpha(y^{-1})$. y^{-1} must exist since y was required to be invertible and

$$(\alpha(y^{-1})y\ [h_{ij}] \;=\; \alpha[h_{ij}] \;=\; a$$

Examples

(A) Let Y be the consistently based radix 7 system of three digits. This system represents the integers modulo $7^3 = 343$. $Y = X \times X \times X$, each X having modulus 7, and ϕ is defined by giving its values on $\{e_i\}$

$$\begin{array}{lll} \phi(e_0) = 1 & & \\ \phi(e_1) = 7 & e_i = (0 \ldots 1_i \ldots 0) & \\ \phi(e_2) = 49 & & \end{array}$$

where the symbols on the right side of the equations represent elements in Z_{343}.

F is the free Z_{343} module on three generators with $(343)^3$ elements. If the generators of Y are ordered from the right to left in the conventional manner, then a set of generators for H is given by:

$$\begin{bmatrix} 0 & 1 & 336 \\ 1 & 336 & 0 \end{bmatrix} \quad \text{which could also be written} \quad \begin{bmatrix} 0 & 1 & -7 \\ 1 & -7 & 0 \end{bmatrix}.$$

Another basis is obtained by taking

$$y = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \quad \text{so } y\ [h_{ij}] = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 0 & 1 & -7 \\ 1 & -7 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -6 & -7 \\ 2 & -14 & 0 \end{bmatrix}.$$

What is F/H? The elements of F/H are cosets of elements of F, two elements of F being in the same coset if they differ by an element in H.

For example, (3, 2, 1), (1, 15, 8) and (6, 28, 15) all are mapped by ψ into the code element (3, 2, 1) which is, in turn, mapped by ϕ into

$$3 \cdot 7^2 + 2 \cdot 7 + 1 = 162 \text{ of } Z_{343}$$

(B) Let Y be the 3-digit residue number system having moduli 2,3 and 5. Let

$$\phi(e_1) = 15$$

$$\phi(e_2) = 10$$

$$\phi(e_3) = 6$$

F is the free Z_{30} module on 3 generators and a basis for H is

$$\begin{bmatrix} 2 & 3 & 5 \\ 4 & 3 & 5 \end{bmatrix}$$

The interesting properties of the residue number system follow from the property that H has a set of generators:

$$\begin{vmatrix} 2 & 0 & \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{vmatrix}$$

The intimate connections between F, H and a number system Y should now be clear. Given any number system Y, used to represent the elements of a ring, computation in that number system is accomplished by passing first to F, doing the computation and returning to Y. In order to characterize this process more exactly, it is necessary to introduce the notion of an equivalence map.

Definition: Let $(S,\sim)$ be a system consisting of a set S and an equivalence

relation "~" on S. Let $\rho: S \to S$ be a function from S into S. ρ is called an equivalence map if

$$\rho(s) \sim s \qquad s \in S$$

The equivalence relation in mind is that induced by the coset decomposition of F by ψ. We shall define

$$s \sim t \Leftrightarrow \psi(s) = \psi(t)$$

It is now clear that the equivalence maps on F must map each element into an element differing from it by an element of H.

Let us define the set $C \subset F$ $\sum \alpha_i t_i \in C \Leftrightarrow 0 \leq \alpha_i < m_i$. The elements of C are a full set of representatives for F/H. C "looks" like Y, however it is important to keep them distinct because addition is defined differently in the two sets. Let two maps λ and $\psi|C$ be defined in the obvious way:

$$\lambda: Y \to C \qquad \lambda(\sum \alpha_i e_i) = \sum \alpha_i t_i$$

$$\psi|C: C \to Y \qquad \psi|C(\sum \alpha_i t_i) = \sum \alpha_i e_i$$

The computation of the sum of two numbers in Y may now be described as follows.

1. Given $x, y \in Y$, they are interpreted as elements in F. i.e., we take $\lambda(x)$ and $\lambda(y)$.
2. $\lambda(x)$ and $\lambda(y)$ are added in F. Because F is free, this may be done digitwise $\lambda(x) + \lambda(y)$.
3. A sequence of equivalence maps $\{\rho_1, \rho_2 \ldots \rho_n\}$ is applied to

$(\lambda(x) + \lambda(y))$. i.e., we take $\rho_n\rho_{n-1} \cdots \rho_i(\lambda(x) + \lambda(y))$.

The sequence of ρ_i's are subject to the following restriction.

Let $C+C = \{f : f \in F$ and $c_1, c_2 \in C \quad f = c_1 + c_2\}$

Then $\rho_n\rho_{n-1} \cdots \rho_1(C+C) \subseteq C$. This insures that the image of any sum obtained after applying the e' j's will be in C.

4. $\rho_n\rho_{n-1} \cdots \rho_1(\lambda(x) + \lambda(y))$ is interpreted back in Y. i.e., we take

$$\psi|C\ [\rho_n\rho_{n-1} \cdots \rho_1\ (\lambda(x) + \lambda(y))]$$

What is the significance of this four-step process? Steps 1 and 4 are formal only, having been introduced to keep the mathematics straight. What has really happened is that additions in Y may be replaced by the two Steps 2 and 3. Step 2 is addition in the free module and therefore the sum in any position is a function only of the values of the summands in those two positions. The equivalence map of Step 3 may again be decomposed into component maps which are easily computed.

Referring back to Example A, the equivalence maps used are easily identified, and in this case it is conventional to call them carry propagations.

$$\rho_1[(\alpha_1,\alpha_2,\alpha_3))] = (\alpha_1,\alpha_2,\alpha_3) \qquad \text{if } 0 \leq \alpha_3 < 7$$

$$= (\alpha_1,\alpha_2,\alpha_3) + (0, 1, -7) \qquad \text{otherwise}$$

$$\rho_2[(\alpha_1,\alpha_2,\alpha_3)] = (\alpha_1,\alpha_2,\alpha_3) \qquad \text{if } 0 \leq \alpha_2 < 7$$

$$= (\alpha_1,\alpha_2,\alpha_3) + (1, -7, 0) \qquad \text{otherwise}$$

$$\rho_3[(\alpha_1,\alpha_2,\alpha_3)] = (\alpha_1,\alpha_2,\alpha_3) \qquad \text{if } 0 \leq \alpha_3 < 7$$

$$= (\alpha\ ,\alpha\ ,\alpha\ ) + (-7, 0, 0) \qquad \text{otherwise}$$

It is clear that $\rho_3\rho_2\rho_1$ applied to the sum in F of any two canonical representatives will again yield a canonical representative.

For Example B, the equivalence maps used were

$$\rho_1[(\alpha_1,\alpha_2,\alpha_3)] = (\alpha_1,\alpha_2,\alpha_3) \quad \text{if } 0 \leq \alpha_3 < 5$$
$$= (\alpha_1,\alpha_2,\alpha_3) + (0, 0, -5) \quad \text{otherwise}$$
$$\rho_2[(\alpha_1,\alpha_2,\alpha_3)] = (\alpha_1,\alpha_2,\alpha_3) \quad \text{if } 0 \leq \alpha_2 \; 3$$
$$= (\alpha_1,\alpha_2,\alpha_3) + (0, -3, 0) \quad \text{otherwise}$$
$$\rho_3[(\alpha_1,\alpha_2,\alpha_3)] = (\alpha_1,\alpha_2,\alpha_3) \quad \text{if } 0 \leq \alpha_1 < 2$$
$$= (\alpha_1,\alpha_2,\alpha_3) + (-2, 0, 0) \quad \text{otherwise}$$

Enlarging on a comment made earlier, we assert that every equivalence map on F may be described in the following way.

1. F is partitioned into classes $\{F_1,F_2 \ldots F_n\}$.
2. There are designated a set of elements of H $\{h_1 \ldots h_n\}$.
3. $\rho(f) = f + h_i \Leftrightarrow f \epsilon F_i$.

The equivalence maps described in the examples were expressed as the composition of equivalence maps where the partitions on F were into two classes.

Notice that in both cases the class determination for each component equivalence map was determined by examining only one digit. Such a map will be called an elementary equivalence map. We shall show next that, in "general," the canonical map always decomposes into exactly k elementary maps. This is done by showing that the matrix $[h_{ij}]$ may always be put in the form

$$\begin{bmatrix} -m_1 & C_{12} & \cdots & C_{1k} \\ 0 & -m_2 & \cdots & C_{2k} \\ \cdot & & \ddots & \\ \cdot & & & \\ \cdot & & & \\ 0 & & 0 & -m_k \end{bmatrix}$$

It then follows that the maps

$$\{\rho_i\ (\alpha_1 \ldots \alpha_i \ldots \alpha_k) = (\alpha_1 \ldots \alpha_i \ldots \alpha_k) + \left[\frac{\alpha_i}{m_i}\right] (h_{i1} \ldots h_{ik})\}$$

are such that $\rho_k\ \rho_{k-1} \ldots \rho_1$ satisfies the requirement of reducing all elements of F to canonical form.

To show that such a triangular form is possible requires the use of a somewhat difficult theorem about non-redundant number systems. The theorem is stated here and proved in the appendix.

Theorem: If Y is a non-redundant linear system, representing Z/M, then there exists a digit X_i such that

$$M \mid m_i \phi(e_i) .$$

It can then be shown that the set of elements $\{m_i t_i\}$ in F are a triangular set of generators with respect to some ordering of the digits.

Proof: The conclusion follows from an induction argument on the number of digits. It is obviously true for K = 1.

For aribtrary k, by the previous theorem it is known that for some i, $M \mid m_i \phi(e_i)$ or equivalently, $m_i \phi(e_i) \equiv 0 \bmod M$. It follows that $(0, 0 \ldots 0, m_i) \in H$ if the digits are reordered so that the digit satisfy-

ing the theorem is last.

Dividing the congruence by m_i, we get $\phi(e_k) \equiv 0 \bmod M/m_i$. Therefore any two elements of Y differing only in position k are congruent modulo M/m_i. From this it follows that the elements of the form $(y_1 \ldots y_{k-1}, 0)$ must map 1-1 into Z_M/m_k when ϕ is composed with the obvious map from Z_M into Z_M/m_k.

Using the induction hypothesis on this reduced code, the elements $\{m_i t_i\}$ $1 \leq i \leq (k-1)$ form a triangular set of generators of $H_{(k-1)}$

$$\begin{bmatrix} m_i & C_{12} & C_{13} & \cdots & C_{1,k-1} \\ 0 & m_2 & & & \\ \vdots & & & & \\ 0 & \cdots & 0 & \cdots & m_{k-1} \end{bmatrix}$$

Each row is congruent to 0 modulo M/m_k and thus congruent to a multiple of M/m_k modulo M. However, all multiples of M/m_k may be written as multiples of t_k, so by taking appropriate multiples of t_k and subtracting them from the rows of the $H_{(k-1)}$, a matrix of elements in H_k is formed.

$$\begin{bmatrix} m_1 & C_{1,2} & \cdots & C_{1,k-1} & - X_{1,k} \\ 0 & m_2 & & C_{2,k-1} & - X_{2,k} \\ \vdots & & & & \\ 0 & \cdots & 0 & m_{k-1} & - X_{k-1,\,k} \end{bmatrix}$$

This matrix is now augmented by appending $(0, \ldots 0, m_k)$.

The resulting matrix may be shown to <u>generate</u> H by noting that the

equivalence map mentioned at the beginning of this section reduces any element in F to one in C and uses only multiples of the rows of the matrix.

We have constructed a free module F, a kernel H, and a canonical set of representatives C for a non-redundant linear number system Y. In order to achieve more generality, a definition of a (possibly redundant) linear number system is given entirely in terms of F, H, and C.

Definition: Let F be a free module on k generators, and H a submodule such that F/H is finite. Let $C \subset F$ be such that its intersection with each equivalence class of F/H is non-empty. Let ρ be an equivalence map with respect to F/H such that $\rho(C+C) \subset C$. Then C is called a linear number system.

Notice that this definition is given entirely without reference to a map from C onto Z_M for some M.

The non-redundant number systems as defined previously certainly qualify. That this is a non-trivial generalization can be seen from the following well-known example.

(C) "One's Compliment" System

Let F be the free Z - module on five generators and H the submodule generated by the following elements.

h_1	-2	0	0	0	1
h_2	1	-2	0	0	0
h_3	0	1	-2	0	0
h_4	0	0	1	-2	0
h_5	0	0	0	1	-2

C is the set of those elements of the form $\sum \alpha_i e_i$ $0 \leq \alpha_i < 2$.

Let

$$\rho_i(\alpha_1 \ldots \alpha_i \ldots \alpha_5) = (\alpha_1 \ldots \alpha_i \ldots \alpha_5) \text{ if } 0 \leq \alpha_i < 2$$

$$= (\alpha_1 \ldots \alpha_i \ldots \alpha_5) + h_i \text{ otherwise}$$

Then

$$\rho = (\rho_1 \rho_2 \rho_3 \rho_4 \rho_5)^2$$

The "squaring" is necessary because of the "end around carry."

It is well known that this number system represents Z_{31}. Although C has 32 elements in it, F/H has only 31. It is the structure of F/H that determines which Z_M may be represented.

To characterize the structure of F/H it is necessary to introduce more module theory. Rather tnan repeat this development the reader is referred to Chapter 3 of Jacobson. The result of interest is:

Theorem: If R is a principal ideal domain, any finitely generated R module is a direct sum of cyclic modules.

The method of computing the orders of the various cyclic submodules follows from the canonical form construction for matrices with elements from a principal ideal domain. By elementary row and column operations, one reduces the matrix of generators of H to canonical form. This canonical form does not give an alternative set of generators for H since the elementary transformations may change the basis of F. It does preserve the abstract structure of F/H. The lower right-hand diagonal element gives the order of the largest cyclic submodule and therefore the maximum value of M such that a homomorphism from C onto Z_M exists. This process is partially carried out

for the above example.

$$\begin{bmatrix} -2 & 0 & 0 & 0 & 1 \\ 1 & -2 & 0 & 0 & 0 \\ 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 & -2 \end{bmatrix} \backsim \begin{bmatrix} 1 & -6 & 0 & 0 & 1 \\ 1 & -2 & 0 & 0 & 0 \\ 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 & -2 \end{bmatrix}$$

by adding three times the second row to the first row,

$$\sim \begin{bmatrix} 1 & -6 & 0 & 0 & 1 \\ 0 & 4 & 0 & 0 & -1 \\ 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 & -2 \end{bmatrix} \backsim \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & -1 \\ 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 & -2 \end{bmatrix}$$

by another row and then a column operation.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 6 & 0 & -1 \\ 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 & -2 \end{bmatrix} \backsim \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & -8 & 0 & 1 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 & -2 \end{bmatrix} \backsim \cdots \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 31 \end{bmatrix}$$

It is always possible to represent the ring of integers modulo as a divisor of the order of the maximal cyclic submodule.

The notion of equivalence of matrices used above is not appropriate if

we are interested in obtaining a "good" set of generators of H. By "good," we mean a set which lends itself to the construction of easily computed equivalence maps. The appropriate reduced [set] of elementary operations is all the row operations plus column permutations since the ordering of the digits is arbitrary.

A trivial example of a code whose structure is not cyclic is obtained by letting F have two generators and

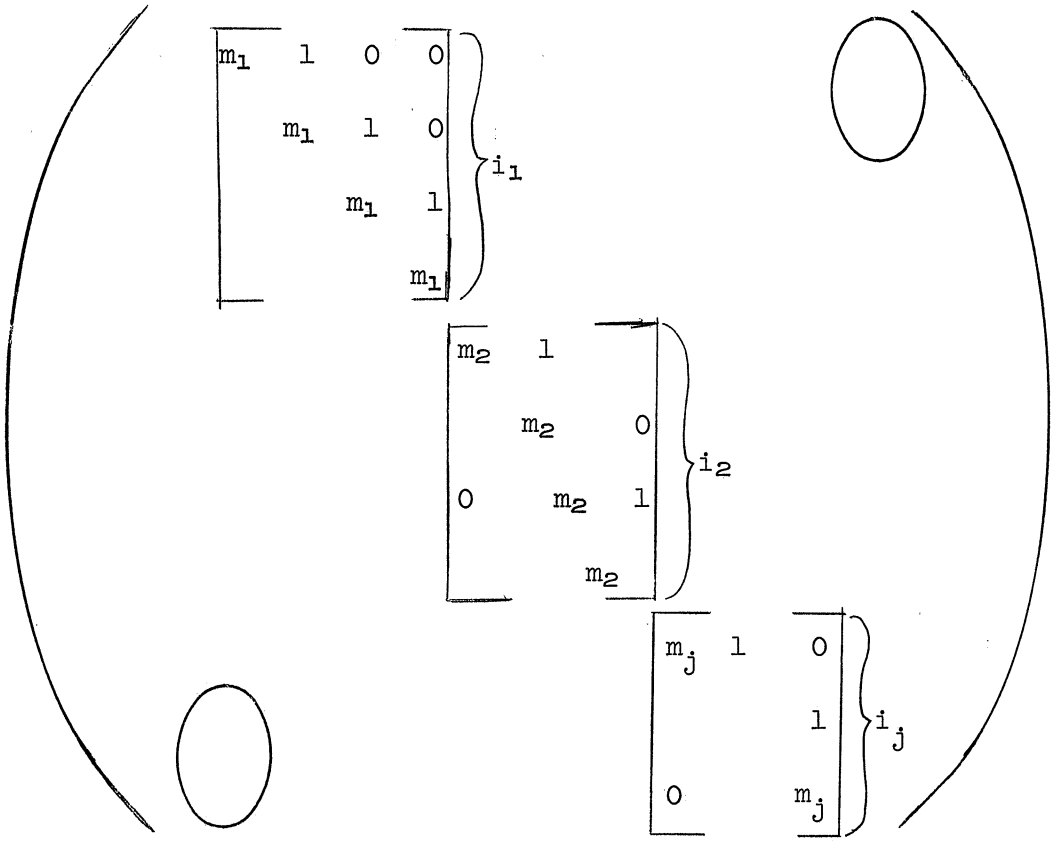
$$H = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$$

H is already in canonical form and F/H is the direct sum of two cyclic modules of order three.

Whenever H is of the form:

$$H = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}$$

partitioning F/H into $F_1/H_1 \oplus F_2/H_2$, the largest cyclic submodule will have order less than or equal to the least common multiple of the orders of F_1/H_1 and F_2/H_2. The equality will hold when F_1/H_1 and F_2/H_2 are themselves cyclic. For a non-redundant system, it must be that the orders of F_1/H_1 and F_2/H_2 are relatively prime. Repeated application of the above, in the non-redundant case using only prime moduli, yields the following form:



This is as "sparse" a matrix as possible for any given set of moduli. Conventional consistently weighted codes and residue codes are special cases where $j = 1$ and $i_j = 1$ respectively.

Before continuing this discussion, another example of a redundant code is given to demonstrate the reduction of the free addition portion of computation at the expense of increased complexity of the canonical transformation.

(D) Let F be the free Z - module on eight generators and H, the subgroup spanned by

$$\begin{bmatrix} -2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Notice that H is simply the submodule similar to that of example C with an additional generator, the last row. The addition of this row results in the order of F/H being 17 instead of 255. Let the canonical set be $(\alpha_7 \ldots \alpha_0)$ $0 \leq \alpha_i < 2$, i.e., of order 255. The following feature of C may be observed. Every coset of F/H has a representative in C which has at most two α_i whose value is one. If $\phi: F/H \to Z_{17}$ is given by $\phi(\alpha_7 \ldots \alpha_0) = (\sum \alpha_i 2^i) \bmod 17$, then a set of representatives with this property is

0	(0	0	0	0	0	0	0	0)
1	(0	0	0	0	0	0	0	0)
2	(0	0	0	0	0	0	1	0)
3	(0	0	0	1	0	1	0	0)
4	(0	0	0	0	0	1	0	0)
5	(0	0	0	0	0	1	0	1)
6	(0	0	1	0	1	0	0	0)
7	(1	0	1	0	0	0	0	0)
8	(0	0	0	0	1	0	0	0)
9	(1	0	0	0	0	0	0	0)
10	(0	0	0	0	1	0	1	0)
11	(1	0	0	0	0	0	1	0)
12	(0	1	0	1	0	0	0	0)
13	(0	1	0	0	0	0	0	0)
14	(0	1	0	0	0	0	0	1)
15	(0	0	1	0	0	0	0	0)
16	(0	0	0	1	0	0	0	0)

Notice also that no representative in this set has adjacent "ones." Let this special subset of C be designated C*. For the sum of two elements x, y $\in$ C* it is clear that the part of the equivalence map ordinarily corresponding to carry propagations is quite simple, since carries can propagate, at most, one stage. On the other hand, unless the image of C*+C* under ρ is again in C*, this property will not be preserved. In other words, the canonical set of interest is really C*, but we may choose to represent it as elements of C. For this particular example, the equivalence map necessary to insure $\rho(C^*+C^*) \subset C^*$ appears to be not terribly complicated, but sufficiently more so than ordinary carry propagation-type maps to make the code impractical.

4. CONCLUSION

In evaluating a code, one must consider how easy the other arithmetic operations are to do. To a great extent, the difficulty of doing integer multiplication follows in a monotonic manner that of doing additions. This results from the fact that the codes are linear and one generally does multiplication by employing the distributive law and summing a set of products. Division is somewhat more complicated and is best considered in the context of magnitude control.

The main calculations of interest to computer users are after all, not in any ring Z_M, but in a field, usually either the real or complex numbers.

The area of numerical analysis has dealt extensively with this question of approximating a field. Unfortunately, it has primarily studied the effect on accuracy of algorithm variation somewhat independently of the number system being used. This has been possible because of the ease in handling scaling problems in consistently based systems. The fundamental nature of the scaling problem is best seen in the context of fractional multiplication. Multiplication of fractions where the fractions are represented by integers usually must involve a division. For example, in a binary machine one has

$$x_1 = n_1 \cdot 2^{-36} \qquad x_2 = n_2 \cdot 2^{-36}$$

then $x_1 x_2 = n_1 n_2 \cdot 2^{-72}$, but this must be expressed as $n_3\, 2^{-36}$ so $n_1 n_2$ must be divided by 2^{36}. In a binary machine this is accomplished by simply truncating the double length result in the middle and retaining the top half. The ability to divide by an arbitrary power of 2 by truncation is crucial,

and is not shared by all other linear number systems. Sign determination is seen to be a special case, where the divisor is M/2, so that the quotient is 0 or 1 depending on whether the given number is in the bottom or top half of the set of numbers. In our efforts to understand the nature of the residue number system, ways were found to reduce considerably the necessary number of sign determinations. All the techniques developed involved the necessity for Euclidean division by some large constant. Although any large constant would do, it is a property of the residue number system that division by any number other than the moduli is difficult and must be realized by successive divisions with moduli. Although by no means so difficult as to make the residue number system impractical, the operation of division by a large constant dominates design considerations for residue number arithmetic units, much as multiplication has dominated the design of conventional arithmetic units.

It is the above considerations that limit the utility of the characterization of linear number systems given in this paper. Previous work on this problem has been largely confined to the sign detection problem. The central difficulty has been the inability to discover abstract mathematical structures which adequately incorporate the physical operations involved in Euclidean division. The extent to which the module characterization may be useful is still unknown.

5. ACKNOWLEDGMENT

The development of this work rests substantially on the earlier work of Prof. H. L. Garner and D. P. Rozenburg. I also wish to thank T.R.N. Rao, Michael Harrison, and Henry Glover for many useful discussions in this area.

APPENDIX

Le VEQUE'S THEOREM

Le Veque's theorem was used to show the existence of a triangular form for non-redundant linear number systems.

Theorem: Let X be a non-redundant linear number system and $\phi: X \to Z/M$ defined as before. Then there exists a $1 \leq j' \leq n$ such that $m_{j'}\phi(e_{j'}) \equiv 0 \bmod M$.

Proof: Let X be mapped into the unit circle of the complex plane as follows:

$$\lambda: (x_1 \ldots x_n) \to e^{\left(\sum_{i=1}^{n} x_j w_j\right) 2\pi i/M} \qquad (x_1 \ldots x_n) \in X$$

Notice that it is not necessary to take $\left(\sum_{i=1}^{n} x_j w_j\right)$ modulo M since the kernel of $\lambda(\mathrm{Im}^{-1}(1))$ contains (M).

Now the sum of the M Mth roots of unity is always 0 since if P is a primative Mth root,

$$\sum_{j=0}^{M-1} P^j = \frac{P^M - 1}{P - 1} = 0$$

So

$$0 = \sum_{x \in X} e^{\left(\sum_j w_j x_j\right) 2\pi i/M}$$

$$= \sum_{x \in X} \prod_j e^{w_j x_j 2\pi i/M}$$

Since there is a product term for all combinations of values of x's, the above expression may be factored, i.e.,

$$0 = \prod_j \sum_{x_j=0}^{m_j-1} e^{w_j x_j 2\pi i/M}$$

Therefore, since we have a product of factors equal to zero, it must be that one of the factors is zero. For some j', we have

$$0 = \sum_{x_{j'}=0}^{m_{j'}-1} e^{w_{j'} x_{j'} 2\pi i/M}$$

$$= \sum_{x_{j'}=0}^{m_{j'}-1} \left(e^{w_{j'} 2\pi i/M}\right)^{x_{j'}}$$

Again using the identity

$$\frac{a^n - 1}{a - 1} = \sum_{i=0}^{n-1} a^n$$

we have

$$0 = \left[\left(e^{w_{j'} 2\pi i/M}\right)^{m_{j'}} - 1\right] \Big/ \left[e^{w_{j'} 2\pi i/M} - 1\right]$$

$$0 = \left(e^{w_{j'} 2\pi i/M}\right)^{m_{j'}} - 1$$

$$1 = \left(e^{w_{j'} 2\pi i/M}\right)^{m_{j'}} = e^{w_{j'} m_{j'} 2\pi i/M}$$

hence

$$M \mid w_{j'} m_{j'} \quad \text{or} \quad m_{j'} w_{j'} \equiv 0 \bmod M.$$