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

Interim Engineering Report

REDUNDANCY IN RESIDUE NUMBER SYSTEMS

T. R. N. Rao

ORA Project 04879

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

February 1963

TABLE OF CONTENTS

NOTATIONS

$< m_1, m_2, \ldots, m_n >$ = least common multiple of the integers $m_1, m_2, \ldots, m_n$

Z_M = integers modulo M
= $\{0, 1, 2, \ldots, M-1\}$

$|X|_{m_i}$ = residue of X with respect to modulo m_i

or $X \equiv x_i \bmod m_i$
$0 \leq x_i < m_i$

$(m_1, m_2, m_3, \ldots, m_n)$ = the greatest common divisor of the integers $m_1, m_2, \ldots m_n$

$X \mid Y$ = X divides Y

$X \nmid Y$ = X does not divide Y

SUMMARY

This paper investigates the conditions for a finite, redundant residue system using the moduli $m_1, m_2, \ldots m_n$ to represent integers modulo M. It is proved that for a general residue system (without any restriction on moduli) it is necessary and sufficient that M be a proper divisor of the product of moduli in order that the system be redundant and weighted. It is also proved that for a residue system if $M = < m_1, m_2, \ldots m_n >$ there exist exactly d sets of digit weights for the system where d is called the factor of redundancy and is given as

$$d = \frac{m_1 m_2 \ldots m_n}{< m_1, m_2, \ldots, m_n >} = \frac{\overbrace{\prod_{i=1}^{n} m_i}}{M}$$

I. INTRODUCTION

There has been a great deal of interest in the problem of residue number systems. In spite of the advantage of not having carry propagation in addition, residue systems pose considerable difficulty in the determination of sign, magnitude and division. Much of the work has been done on only the case of residue number systems with moduli pairwise relatively prime. Such a system is non-redundant and has the algebraic structure of an R-space,[1] or can be given the structure of a Z-module.[2] For a more general case of a non-redundant weighted number system, there is significant work on the necessary and sufficient conditions on the permissible digit weights of non-redundant weighted systems by H. L. Garner.[3] It was shown that the ρ matrix representation of the digit weights modulo the corresponding modulus $|\rho_i|_{m_j}$ can be arranged to have a lower diagonal form, with the diagonal elements relatively prime to the corresponding modulus, only when it is a mixed base system.

Redundancy in number systems can be introduced in several ways. However, if a redundant system is linear[4] and homogeneous, then it is possible that we can obtain the conditions on the digit weights. Very commonly we obtain a redundant weighted system by choosing a weighted system N of cardinality larger than M and forming a map $\phi : N \to Z_M$. The notation here is the same as in the earlier technical note,[4] where N is a system of representation, satisfying:

(1) $N = D_1 \times D_2 \times \cdots \times D_n$

$D_i = \{0, 1, 2, \ldots m_i - 1\}$, D_i is called the ith digit set and m_i the ith modulus.

any element $x \in N$ is of the form $(x_1, x_2 \ldots x_n)$ where $x_i \in D_i$

(2) (i) N is closed under the operation addition

$$x, y \in N \rightarrow x + y \in N .$$

(ii) $0 = (0, 0, \ldots, 0) \in N$ such that $x + 0 = 0 + x = x, \quad x \in N$

(3) a mapping $\omega : N \rightarrow Z_M$

such that $\omega(x + y) = | \omega(x) + \omega(y) |_M$

we recall the definition of a weighted system from the Technical Report,[4] as a number system whose weighing function ω is linear and homogeneous.

II. REDUNDANCY IN WEIGHTED SYSTEMS

In redundant systems, N representing $Z_M (M < \prod_{i=1}^{n} m_i)$; $\phi : N \rightarrow Z_M$ can be written sometimes more conveniently as a composition of two mappings ψ and f

such that $\phi = \psi f$

$$\psi : N \rightarrow Z_{\pi m_i}$$

$$f : Z_{\pi m_i} \rightarrow Z_M$$

ψ is a non-redundant (1-1) transformation and is linear and homogeneous. N representing $Z_{\pi m_i}$ will be a non-redundant, linear, homogeneous function. It is sufficient that f is a ring homomorphism, and the same arithmetic structure as in the non-redundant case can be retained in the redundant system also. In that case, the ρ_i of the non-redundant system of digit weights remain virtually the same as the digit weights of the redundant system except that

$|\rho_i|_M$ replaces ρ_i.

If there are no arithmetic restrictions placed on the redundant system (i.e., for example, if carry propagation to both left and right is permitted), then f need not be linear. Some of these notions can be understood from the results obtained below.

RESIDUE SYSTEM

Lemma 1. For a residue system N with moduli $m_1, m_2, \ldots, m_n$, we have:

$\rho_1, \rho_2, \ldots, \rho_n \in Z_M$ are the digit weights if and only if

$$\left.\begin{array}{ll} (1) & \rho_i m_i = 0 \pmod M \\ (2) & \sum_{i}^{n} \rho_i = 1 \pmod M \end{array}\right\} (*)$$

Proof. Let $\rho_1, \rho_2, \ldots, \rho_n$ be the digit weights, and if ϕ is the weight function

$$\phi(1, 0, 0, \ldots, 0) = \rho_1$$

$$\phi(0, \ldots, \underset{\substack{\uparrow \\ \text{ith place}}}{1}, \ldots 0) = \rho_i$$

Adding $(0, 0, \ldots, 1, \ldots, 0) m_i$ times, we have

$$\phi(0,0,\ldots,m_i,0,\ldots,0) = 0 = |m_i \rho_i|_M = 0 \quad \text{for} \quad i=1,2,n$$

Since $1 \equiv 1 \bmod m_i$ for $i = 1,2,\ldots,n$

$$\phi(1,1,1,\ldots,1) = 1$$

$$\phi(1,1,\ldots,1) = \left|\sum_{i}^{n} \rho_i\right|_M = 1$$

Assume $\rho_i \in Z_M$ such that

$$\rho_i m_i \equiv 0 \pmod{M} \qquad i = 1,2,\ldots,n$$

$$\sum \rho_i \equiv 1 \pmod{M}$$

for any $X \in Z_M$ let $X = x_i \bmod m_i$

Claim: $x = |\rho_i x_i|_M$

$$X \equiv x_i \bmod m_i \qquad i = 1,2,\ldots,n$$

$$X = k_i m_i + x_i \qquad \text{for some integers } k_i$$

$$X\rho_1 = k_1 m_1 \rho_1 + x_1 \rho_1$$

$$X\rho_2 = k_2 m_2 \rho_2 + x_2 \rho_2$$

$$\vdots$$

$$X\rho_n = k_n m_n \rho_n + x_n \rho_n$$

Adding

$$|X(\rho_1 + \rho_2 + \ldots + \rho_n)|_M \equiv \left| \sum_{i=1}^{n} k_i m_i \rho_i + \sum_{i=1}^{n} x_i \rho_i \right|_M$$

$$X \left| \sum P_i \right|_M = \left| \sum_{i=1}^{n} x_i \rho_i \right|_M$$

$$X = \left| \sum_{i=1}^{n} x_i \rho_i \right|_M$$

$\therefore$ $\rho_1, \rho_2, \ldots\ldots, \rho_n$ are a set of digit weights of the system N.

By using the lemma we may be able to check whether any set of numbers can be called the digit weights if the set satisfies the two conditions of (*).

NOTE: In a more general case of a residue system, (1,1,...,1) may not represent $1 \in Z_M$. Here the conditions (*) are modified by a new set of conditions (**) given below:

$$\left.\begin{aligned} m_i \rho_i &\equiv 0 \bmod M, \quad i = 1,2,\ldots,n \\ (\rho_1,\rho_2,\ldots,P_n,M) &= 1 \end{aligned}\right\} \quad (**)$$

It is easy to prove that for such a system the following Lemma 2 can be substituted for the earlier one.

Lemma 2. $\rho_1,\rho_2,\ldots\rho_n$ is a set of digit weights for the residue system N with moduli $m_1,m_2,\ldots,m_n$.

$$\left.\begin{aligned} m_i \rho_i &\equiv 0 \bmod M \\ (\rho_1,\rho_2,\ldots,P_n,M) &= 1 \end{aligned}\right\} \quad (**)$$

The following theorems are for residue systems which have a representation $(1,1,\ldots,1)$ for 1, and so use Lemma 1. However, they can all be proved equally well by using Lemma 2.

Theorem 1. A necessary and sufficient condition that a congruence $\sum_{i=1}^{n} k_i \frac{M}{m_i} \equiv 1 \pmod M$ where $M = < m_1,m_2\ldots m_n >$ is solvable for $k_1,\ldots,k_n$ is that $(M/m_1, M/m_2,\ldots M/m_n, M) = 1$.

Then there are exactly d sets of solutions to $k_1, k_2,\ldots,k_n$, such that

$$0 \leq k_i \leq m_i - 1$$

and

$$d = \frac{m_1 m_2 \ldots m_n}{M}$$

Proof. Let

$$(m_1, m_2) = d_{12}, \qquad M_{12} = \frac{m_1 m_2}{d_{12}}$$

$$(M_{12}, m_3) = d_{13}, \qquad M_{13} = \frac{m_1 m_2 m_3}{d_{12} d_{13}}$$

$$(M_{13}, m_4) = d_{14}, \qquad m_{14} = \frac{m_1 m_2 m_3}{d_{12} d_{13} d_{14}}$$

$$(M_{1,n-1}, m_n) = d_{1n}, \qquad M = M_{1n} = \frac{m_1 m_2 \ldots m_n}{d_{12} d_{13} \ldots d_{1n}}$$

d in the theorem is now obtained by

$$d = \frac{m_1 m_2 \ldots m_3}{M} = d_{12} d_{13} \ldots d_{1n} .$$

The first part of the theorem stating the necessary and sufficient condition for solvability is well established and proved in most of the textbooks on number theory.[5] However, we will show that

$$(M/m_1, M/m_2, \ldots, M/m_n, M) = 1$$

Let

$$(M/m_1, M/m_2, \ldots, M/m_n, M) = d$$

then

$$(M/(m_1 d), M/(m_2 d), \ldots, M/(m_n d), M/d) = 1$$

$$(\tfrac{M}{d}/m_1, \tfrac{M}{d}/m_2, \ldots, \tfrac{M}{d}/m_n, M/d) = 1$$

So

$$m_i \mid M/d \qquad \text{for } i = 1,2,\ldots n .$$

$\therefore$ M/d is a common multiple of $m_1, m_2, \ldots, m_n$.

The least common multiple, M divides all common multiples of $m_1, m_2, \ldots, m_n$

$$\therefore \quad M \left| \frac{M}{d} \right.$$

which is impossible unless d = 1. We have proved

$$(M/m_i,\ M/m_2,\ \ldots,\ M/m_n,\ M) \ = \ 1$$

$$\sum_{i=1}^{n} k_i \frac{M}{m_i} \ = \ 1 \bmod M$$

$$k_i \frac{M}{m_1} + k_2 \frac{M}{m_2} + \ldots + k_n \frac{M}{m_n} \ = \ 1 (\bmod M)$$

From the definition of $d_{12}, \ldots, d_{1n}$ we have

$$\left(\frac{M}{m_1},\ \frac{M}{m_2},\ \ldots,\ \frac{M}{m_{n-1}},\ M \right)$$

$$= \left(\frac{m_2 \,..\, m_n}{d_{12}..d_{1n}},\ \frac{m_1 m_3 \,\ldots\, m_n}{d_{12}d_{13}..d_{1n}},\ \ldots,\ \frac{m_1 m_2 \,\ldots\, m_{n-2} m_n}{d_{12}d_{13} \,..\, d_{1n}} \right)$$

using the formulas (1), (2) and (3) given below

(1) If $(m_1, m_2) = d_{12}$ then $\left(\frac{m_2}{d_{12}}, \frac{m_1}{d_{12}} \right) = 1$

(2) $\left(\frac{a}{t}, \frac{b}{t} \right) = \left(\frac{a,b}{t} \right)$; $(ta, tb) = t(a,b)$

(3) $(x_1, x_2, \ldots x_n) = \left(\ldots \left(\left((x_1, x_2), x_3 \right), x_4 \right), \ldots, x_n \right)$

We have

$$\left(\frac{m_2 \,\ldots\, m_n}{d_{12}\ldots d_{1n}},\ \frac{m_1 m_3 \,\ldots\, m_n}{d_{12} \,\ldots\, d_{1n}} \right) = \frac{m_3 \,\ldots\, m_n}{d_{13} \,\ldots\, d_{1n}}$$

$$\left(\frac{m_3 \,\ldots\, m_n}{d_{13}\ldots d_{1n}},\ \frac{m_1 m_2 m_4 \,\ldots\, m_n}{d_{12}d_{13} \,\ldots\, d_{1n}} \right) = \frac{m_4 \,\ldots\, m_n}{d_{14} \,\ldots\, d_{1n}}$$

because

$$\left(\frac{M_{12}}{d_{13}}, \frac{m_3}{d_{13}}\right) = 1; \qquad (M_{12}, m_3) = d_{13}; \qquad \frac{m_1 m_2}{d_{12}} = M_{12}$$

Continuing the process, we get

$$\left(\frac{m_{n-1}\, m_n}{d_{1,n-1} d_{1n}}, \frac{m_1 m_2 \cdots m_{n-2} m_n}{d_{12} d_{13} \cdots d_{1n}}\right) = \frac{m_n}{d_{1n}}$$

because

$$\left(\frac{m_{n-1}}{d_{1,n-1}}, \frac{M_{1,n-1}}{d_{1,n-1}}\right) = 1$$

$$\therefore \left(\frac{M}{m_1}, \frac{M}{m_2} \cdots \frac{M}{m_{n-1}}, M\right) = \frac{m_n}{d_{1n}}$$

$$k_1 \frac{M}{m_1} + k_2 \frac{M}{m_2} +, \ldots, + k_{n-1} \frac{M}{m_{n-1}} + k_n \frac{M}{m_n} \equiv 1 (\text{mod } M)$$

From the above two equations and from

$$\left(\frac{M}{m_1}, \frac{M}{m_2}, \ldots, \frac{M}{m_n}, M\right) = 1$$

we have

$$\left(\frac{M}{m_n}, \frac{m_n}{d_{1n}}\right) = 1$$

and

$$k_n \frac{M}{m_n} \equiv 1 (\text{mod } m_n/d_{1n})$$

k_n has exactly one solution mod m_n/d_{1n}; however, it has d_{1n} solutions mod m_n or $0 \leq k_n \leq m_{n-1}$. Now substituting for k_n one of the $d_{1,n}$ possible values we obtain a congruence in n-1 variables

$$k_1 \frac{M}{m_1} + k_2 \frac{M}{m_2} + k_{n-1} \frac{M}{m_{n-1}} \equiv \left(1 - k_n \frac{M}{m_n}\right) \pmod{M} .$$

This equation is divisible on both sides by

$$\frac{m_n}{d_{1n}} ,$$

and dividing thus we have

$$k_1 \frac{M_{1,n-1}}{m_1} + k_2 \frac{M_{1,n-1}}{m_2} \ldots + k_{n-1} \frac{M_{1,n-1}}{m_{n-1}} = C_{n-1} \pmod{M_{1,n-1}} .$$

Repeating the same step

$$\left(\frac{M_{1,n-1}}{m_1}, \frac{M_{1,n-1}}{m_2} \ldots \frac{M_{1,n-1}}{m_{n-2}}, M_{1,n-1}\right) = \frac{m_{n-1}}{d_{1,n-1}}$$

we can show that k_{n-1} has exactly $d_{1,n-1}$ solutions modulo m_{n-1} and k_{n-2} has $d_{1,n-2}$ and so on. This proves that we have a total of

$$d_{1n} \cdot d_{1,n-1}\, d_{1n-2} \ldots d_{12} = d$$

solutions for $k_1, k_2, \ldots, k_n$. Such that $0 \leq k_i \leq m_i - 1$. Hence the theorem is proved.

From the above theorem we have

$$\sum k_i \frac{M}{m_i} \equiv 1 \pmod{M}$$

which has d sets of solutions for $k_1, \ldots, k_n$. Such that

$$k_i \in Z_{m_i}$$

Now applying the conditions on the digit weights of a residue system N with the operating moduli $m_1, m_2 \ldots m_n$

(1) $m_i \rho_i = 0 \bmod M$

$$(2)\quad \sum \rho_i \equiv 1 \bmod M \qquad \rho_i \in Z_M \qquad k_i \in Z_{m_i}$$

we have $\rho_i = k_i\, M/m_i$

$$\sum_{}^{n} \rho_i = \sum_{}^{n} k_i\, M/m_i \equiv 1 \bmod M$$

which has d sets of solutions for $k_1 \ldots k_n$, $0 \leq k_i \leq m_i$. Thus we have proved the theorem stated below.

Theorem 2. For a residue system N with moduli $m_1, m_2, \ldots m_n$ representing integers modulo M where $M = < m_1, m_2, \ldots, m_n >$, there are exactly

$$d = \frac{m_1 m_2 \ldots m_n}{M}$$

sets of digit weights.

EXAMPLE: Let us take a residue system N with moduli 6, 10, 21 representing Z_{210} which has

$$d = \frac{6 \cdot 10 \cdot 21}{210} = 6\ ; \quad m_1 = 6,\ m_2 = 10,\ m_3 = 21.$$

The six sets of digit weights are given below.

ρ_1	ρ_2	ρ_3
0	21	190
35	126	50
175	126	120
70	21	120
105	126	190
140	21	50

$\rho_1 + \rho_2 + \rho_3 \equiv 1 (\bmod 210)$

$m_1\rho_1 \equiv m_2\rho_2 \equiv m_3\rho_3 \equiv 0 (\bmod 210)$

Theorem 3. $m_1, m_2, \ldots, m_n$ are the moduli of a residue system N. N can represent integers modulo M, if and only if M is a divisor of $<m_1, m_2, \ldots, m_n>$.

Proof. If N is a residue system, then $\exists$ $\rho_1, \rho_2, \ldots, \rho_n \in Z_M$ such that

(1) $\rho_i m_i \equiv 0 \bmod M$

(2) $\sum_{1}^{n} \rho_i \equiv 1 \bmod M$

for any i if $(m_i, M) = 1$

$$\rho_i m_i \equiv 0 \bmod M$$

$$= k_i M$$

$$M \mid \rho_i m_i \qquad (M, m_i) = 1$$

$\therefore \quad M \mid \rho_i$

$\therefore \quad \rho_i = c_i M \qquad$ for some integer C_i

$\equiv 0 (\bmod M)$

This means for any modulo that is relatively prime to M its digit weight is zero. Such digits exist in the system as purely redundant digits. Assume there are r such bits where $0 \leq r < n$. If $r = n$ then $\rho_i = 0$ for $i = 1,2,\ldots n$ and $\sum \rho_i \equiv 0 (\bmod M)$ which contradicts condition (2).

Now reordering the moduli so that the last r moduli

$$m_{n-r+1}, m_{n-r+2}, \ldots, m_n$$

are the ones that are relatively prime to M.

Let

$$(M, m_i) = d_i \qquad \text{for} \quad i = 1,2,\ldots, n-r$$

and

$$\frac{M}{d_i} = M_i'$$

$$d_i > 1 .$$

Then applying condition (1) we have

$$\rho_i m_i \equiv 0 (\text{mod } M)$$

$$= k_i M .$$

Dividing by d_i

$$\rho_i \frac{m_i}{d_i} = k_i \frac{M}{d_i}$$

Let $$\frac{m_i}{d_i} = m_i' ; \quad \frac{M}{d_i} = M_i'$$

such that

$$(m'_i, M'_i) = 1 .$$

$$\rho_i = \frac{k_i}{m'_i} M_i = c_i \frac{M}{d_i} \qquad \text{for some integer } c_i \qquad \text{for } i = 1,2,\ldots n-r.$$

Applying condition (2) we have

$$\sum_{1}^{n-r} c_i \frac{M}{d_i} - CM = 1 .$$

This equation has solutions for ρ_i if and only if

$$\left(\frac{M}{d_1}, \frac{M}{d_2}, \ldots \frac{M}{d_{n-r}}, M \right) = 1 .$$

This is possible only if

$$M = < d_1, d_2, \ldots d_{n-r} >$$

$$= < \frac{m_1}{m'_1}, \frac{m_2}{m'_2}, \ldots, \frac{m_{n-r}}{m'_{n-r}} >$$

which implies that

$$M \Big| < m_1, m_2, \ldots, m_{n-r} >$$

and also divides

$$< m_1, m_2, \ldots, m_n >$$

Now, if

$$M \mid < m_1, m_2, \ldots, m_n >$$

it is necessary to prove the following claim.

Claim. N represents Z_M. If we can show that $\exists\ \rho_1, \rho_2, \ldots, \rho_n$ such that

(1) $\sum \rho_i m_i = 0 \bmod M$

(2) $\sum_{i=1}^{n} \rho_i \equiv 1 \bmod M$, then we will have the proof completed.

We know that N with moduli $m_1, m_2, \ldots, m_n$ represents Z_t where $t = < m_1, m_2, \ldots, m_n >$. Let $\rho_1, \rho_2 \ldots \rho_n \in Z_t$ be the digit weights of the weight functions $\omega: N \to Z_t$. Since $M \mid t$ we have $\rho_i m_i = 0 \bmod t$

$$\rho_i m_i \equiv 0 (\bmod\ t) \Longrightarrow \rho_i m_i \equiv 0 (\bmod\ M)$$

$$\sum \rho_i \equiv 1 (\bmod\ t) \Longrightarrow \sum \rho_i \equiv 1 (\bmod\ M)$$

so $|\rho_1|_M, \ldots, |\rho_n|_M$ are the digit weights for the system $N \to Z_M$.

III. ACKNOWLEDGEMENTS

I am grateful to Professor H. L. Garner for his guidance, and to Mr. R. F. Arnold for useful discussions in this area.

REFERENCES

1. D. P. Rozenberg, The algebraic properties of the residue number systems. IBM No. 61-907-176.

2. R. F. Arnold, Linear number systems, Information Systems Lab., The Univ. of Mich., Tech. Note ORA, 04879-8-T, Oct., 1962.

3. H. L. Garner, Finite non-redundant number system weights, Information Systems Lab., The Univ. of Mich, Tech. Note ORA, 04879-2-T, May, 1962.

4. T.R.N. Rao, Computer number systems, linear and non-linear categories, Information Systems Lab., The Univ. of Mich., Tech. Note, ORA, 04879-6-T, September, 1962.

5. LeVeque, Theory of numbers, Vol. 1, Addison Wesley Publishing Co.