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

Technical Note

FINITE, NON-REDUNDANT NUMBER SYSTEM WEIGHTS

Harvey L. Garner

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

May 1962

FINITE, NON-REDUNDANT NUMBER SYSTEM WEIGHTS

In this paper the necessary and sufficient conditions for a finite number system to be non-redundant, complete and weighted are given in terms of permissible digit weights. The arithmetic of any given number system follows directly if the digit weights are given.

Definition. A finite, weighted, non-redundant number system N is defined as a finite set of n-tuples of the form $(x_1,\ldots,x_n)$ isomorphic to the finite group G_M. The elements of the G_M are the integers from zero to M-1. The mapping between G_M and N is defined by the congruence relationship

$$\sum_{i=1}^{n} x_i \rho_i \equiv g \bmod M \qquad (1)$$

where

$$g \in G_M,\ (x_1,\ldots,x_n) \in N;$$

$$x_i \in G_{m_i},\ i = 1,\ldots,n;$$

The elements of G_{m_i} are the integers $0, 1,\ldots,m_i-1$. M is called the modulus of the number system; ρ_i is the weight of the ith digit; x_i is the ith digit symbol; and m_i is called the digit modulus or digit base. If $m_1 = m_2 = \ldots = m_n$ the number system is termed a consistently based number system. Otherwise, the number system is termed non-consistently based or a mixed base number system.

Definition. In a redundant weighted number system there must exist at least one case where two or more elements of N are related by Eq. (1) to a single element of G_M. (Redundancy may be introduced by the choice of digit weights or by choosing $M < \prod_{i=1}^{n} m_i$).

<u>Definition</u>. A number system is incomplete if there exists at least one element of G_M not related by Eq. (1) to an element of N.

A number system is always redundant if $M < \prod_{i=1}^{n} m_i$ and is always incomplete if $M > \prod_{i=1}^{n} m_i$. In the remaining discussion we shall be concerned only with the case where $M = \prod_{i=1}^{n} m_i$ and the question of redundancy will depend upon the choice of digit weights.

<u>Definition</u>. A set of numbers is called a complete residue system modulo m

a. If $i \neq j$, $a_i \not\equiv a_j \bmod m$.

b. If a is any integer there is an index i with $1 \leqslant i \leqslant m$ for which $a \equiv a_i \bmod m$.

By this definition G_M is a complete residue system modulo M and x_i is a complete residue system modulo m_i.

<u>Lemma 1</u>. If $M = \prod_{i=1}^{n} m_i$ then a number system is redundant if, and only if, it is incomplete.

<u>Lemma 2</u>. If the weight ρ_i is such that $(\rho_i, M) = d_i$, then $\rho_i = k_i d_i$ where $(k_i, \frac{M}{d_i}) = 1$ and the m_i elements of G_M related to $x_i \rho_i$ by Eq. (1) are integers of the form $|x_i k_i d_i|_M$.

Proof: Setting all x's except x_i to zero in Eq. (1) yields

$$x_i \rho_i \equiv g \bmod M.$$

If $(\rho_i, M) = d_i$ then $d_i | g$. Hence $g = k_i d_i = \rho$ for $x_i = 1$ and $(k_i, \frac{M}{d_i}) = 1$ otherwise $(\rho_i, M) \neq d_i$

For any $x_i \epsilon G_{m_i}$

$$x_i k_i d_i = x_i \rho_i \equiv g \bmod M$$

so $g = |x_i k_i d_i|_M$.

Lemma 3. If $d_i = (\rho_i, M) = \frac{M}{m_i}$ and $(k_i, \frac{M}{d_i}) = (k_i, m_i) = 1$ then the set of elements generated by $|x_i k_i \frac{M}{m_i}|_M$ as x_i assumes all possible values of G_{m_i} is an additive subgroup of G_M of order m_i. Furthermore, there exists a one-to-one mapping between the elements $|x_i k_i \frac{M}{m_i}|_M$ and the elements of G_{m_i}.

Proof: If $x_i k_i \frac{M}{m_i} \equiv g \bmod M$

then $x_i k_i \equiv g' \bmod m_i$

and $g' = |x_i k_i|_{m_i}$

g' is a complete residue system modulo m_i because $(k_i m_i) = 1$ and $x_i \epsilon G_{m_i}$. Hence if $(\rho_i, M) = \frac{M}{m_i}$ then the elements of G_M associated with $x_i \rho_i$ are

$$0, \frac{M}{m_i}, 2\frac{M}{m_i}, \ldots (m_i - 1)\frac{M}{m_i}$$

These elements form an additive subgroup of order m_i.

Theorem I. Sufficient conditions for the weights of a non-redundant weighted number system are:

$$(\rho_1, M) = \frac{M}{m_1}$$

$$\left(\rho_2, \frac{M}{m_1}\right) = \frac{M}{m_1 m_2}$$

$$\vdots$$

$$\left(\rho_q, \frac{M}{\prod_{i=1}^{q-1} m_i}\right) = \frac{M}{\prod_{i=1}^{q} m_i}$$

$$\vdots$$

$$(\rho_n, m_n) = 1$$

The ordering $m_1, \ldots, m_n$ is arbitrary.

Proof: If $(\rho_1, M) = \frac{M}{m_1}$ then it follows from Lemma 3 that the elements of G_M generated by $x_1\rho_1$, $x_1 \epsilon G_{m_1}$, form a complete subgroup of G_M of order m_1. This subgroup is designated H_{m_1} and consists of elements $0, \frac{M}{m_1}, \ldots, (m_1-1)\frac{M}{m_1}$. Now $(\rho_2, \frac{M}{m_1}) = \frac{M}{m_1 m_2}$ so the elements generated by $x_2\rho_2$ satisfy the equation

$$x_2\rho_2 \equiv z \frac{M}{m_1 m_2} \bmod \frac{M}{m_1}$$

where $z = 0, 1, \ldots m_2 - 1.$

The elements of G_M represented by

$$x_1\rho_1 + x_2\rho_2$$

are all elements divisible by $\frac{M}{m_1 m_2}$. In other words, $x_1\rho_1+x_2\rho_2$ generates the subgroup of G_M of order m_1m_2. Thus $x_1\rho_1+x_2\rho_2+x_3\rho_3$ is seen to generate the subgroup of G_M of order $m_1m_2m_3$ consisting of all elements of G_M divisible by $\frac{M}{m_1m_2m_3}$. Since there is a finite number of digits, the process will terminate and $x_1\rho_1+ \ldots +x_n\rho_n$ will generate the subgroup of G_M of order $m_1 \ldots m_n = M$ which is G_M.

Lemma 4. If $(\rho_i,M) = d_i$ where $d_i > \frac{M}{m_i}$ and $(k_i, \frac{M}{d_i}) = 1$ then the set of elements generated by $|x_ik_id_i|_M$ as x_i assumes all values of G_{m_i} is a subgroup of G_M of order $\frac{M}{d_i}$. There does not exist a one-to-one mapping between the elements $|x_ik_id_i|_M$ and the elements of G_{m_i}, because two or more elements of G_{m_i} are associated with the same element $|x_ik_id_i|_M$.

Proof: Given $x_ik_id_i \equiv g \bmod M$

and $(\rho_i,M) = (kd_i,M) = d_i$

then $x_ik \equiv g' \bmod \frac{M}{d_i}$

or $|x_ik|_{\frac{M}{d_i}} = g'$

where $x_i \in G_{m_i} - 1$ and $(k_i, \frac{M}{d_i}) = 1$

If $d_i < \frac{M}{m_i}$ then $\frac{M}{d_i} < m_i$

and g' has only $\frac{M}{d_i}$ different values. $g' = 0, 1, 2, \ldots, \frac{M}{d_i} - 1$.

Hence $g = 0, d_i, 2d_i, \ldots M-d_i$

which is an additive subgroup of G of order $\frac{M}{d_i}$. Since $\frac{M}{d_i} < m_i$ there is not a one-to-one mapping between the elements $|x_ik\rho_i|_M$ and G_{m_i}.

Theorem II. If there exists some $(\rho_i, M) = d_i$ where $d_i > \frac{M}{m_i}$ then the number system is redundant.

Proof: This theorem follows directly from Lemma 4 and the definition of a redundant number system. If

$$(\rho_i, M) = d_i, \; d_i > \frac{M}{m_i}$$

then two different values of $x_i \epsilon G_{m_i}$ correspond to the same element of G_M and the number system is redundant.

Lemma 5. If $(\rho_i, M) = d_i$ where $d_i < \frac{M}{m_i}$, $x_i \epsilon G_{m_i}$ and $(k_i, \frac{M}{d_i}) = 1$, then the set of elements generated by $|x_i k_i d_i|_M$ as x_i assumes all values of G_{m_i} is not a complete subgroup of G_M but is a particular set of m_i elements selected from the subgroup of G_M of order $\frac{M}{d_i}$.

Proof: If $d_i < \frac{M}{m_i}$ then $m_i < \frac{M}{d_i}$, then

$$|x_i k_i d_i|_{\frac{M}{d_i}} = g'$$

defines a set of m_i elements because $x_i \epsilon G_{m_i}$ and $(k_i, \frac{M}{d_i}) = 1$. The set of elements $|x_i k_i|_{\frac{M}{d_i}}$ is a particular subset of m_i elements from $\frac{G_M}{d_i}$. The set of elements $|x_i k_i d_i|_M = g$ is a particular subset of m_i elements selected from the subgroup of G_M of order $\frac{M}{d_i} > m_i$ because $g'd = g$.

Lemma 6. Let S_1 be the incomplete subgroup generated by $|x_i k_i d_i|_M$ where $(\rho_i, M) = d_i$, $x_i \epsilon G_{m_i}$, $d_i = \frac{M}{a_i} < \frac{M}{m_i}$ and $(k, a_i) = 1$. The complete subgroup H is of order a_i while S_1, the incomplete subgroup, is of order m_i. There exists a set of elements S_2 which is to be used to complete the subgroup H by the following operation:

$$h = |u + v|_M \qquad \begin{matrix} h \in H \\ u \in S_1 \\ v \in S_2 \end{matrix}$$

H can be completed non-redundantly if, and only if, $(a_i, m_i) = m_i$ and the only element common to S_1 and S_2 is zero.

Proof: If S_2 contains an element other than zero which is common to S_1 there would exist a redundant representation for that element. Every element of S_2 which combines with an element of S_1 to give an element of H combines with every element of S_1 to yield m_i elements of H. If q distinct elements of S_2 are used, then qm_i elements of H are generated. If the subgroup is to be generated complete and non-redundant, then $qm_i = a_i$ and $(m_i, a_i) = m_i$.

Lemma 7.* The necessary and sufficient condition for the solvability of the general equation

$$\sum_{i=1}^{n} x_i \rho_i \equiv C \bmod M$$

$$x_1 \in G_M \qquad i = 1, \ldots, n$$

is that

$$(\rho_1, \ldots, \rho_n, M) | C$$

Theorem III. If for all i, $d_i < \frac{M}{m_i}$ where $\rho_i = k_i d_i$ and $(k_i, \frac{M}{d_i}) = 1$ then the number system is incomplete and hence redundant.

*This is a standard theorem of number theory. See page 33 Le Veque, Topics in Number Theory, Addison Wesley, 1956.

Proof: Let $d_1 = (\rho_1, M) = \frac{M}{a_1} < \frac{M}{m_1}$ and $(k_1, a_1) = 1$. It follows from Lemma 5 that $|x_1\rho_1|_M$ generates m_1 elements of H_{a_1} (H_{a_1} is the subgroup of G_M of order a_1). Specifically, the elements are:

$$\left|\frac{0Mk_1}{a_1}\right|_M, \quad \ldots \quad , \left|\frac{(m_1 - 1)\, Mk_1}{a_1}\right|_M .$$

So

$$x_1 \frac{Mk_1}{a_1} \equiv z \bmod \frac{m_1 M}{a_1}$$

$$x_1 k_1 \equiv z' \bmod m_1.$$

Lemma 6 shows that $(m_1, a_1) = m_1$. We are given that $(k_1, a_1) = 1$. So $a_1 = q_1 m_1$ and $(k_1, q_1 m_1) = 1$. It follows that $(k_1, m_1) = 1$. Therefore, $z' = 0, 1, \ldots, m_1 - 1$. The elements needed to complete H_{a_1} are

$$0, \frac{m_1 M}{a_1}, \ldots, \left(\frac{a_1}{m_1} - 1\right) \frac{m_1 M}{a_1}$$

The necessary and sufficient condition for the completion of the subgroup is the existence of $\frac{a_1}{m_1}$ n-tuples of the form $(0, x_2, \ldots, x_n)$ satisfying the following congruence:

$$\sum_{i=2}^{n} x_i \rho_i \equiv y \frac{m_1 M}{a_1} \bmod M$$

$$y = 0, 1, \ldots, \frac{a_1}{m_1} - 1. \qquad (2)$$

A similar condition exists for elements which are not members of the subgroup H_{a_1}

$$\sum_{i=2}^{n} x_i \rho_i \equiv y \bmod \frac{M}{a_1} \qquad y = 0, 1, \ldots, \frac{M}{a_1} - 1 \tag{3}$$

The proof of the theorem presented here demonstrates that the subgroup H_{a_1} can never be represented by the number system if for all i, $(\rho_i, \frac{M}{m_i}) < \frac{M}{m_i}$.

Some, but not all, of the x_i, $i = 2,\ldots,n$, which make up the n-tuples satisfying Eq. (2) may have the value zero for all values of y. To account for this the variable η_i is introduced. If $x_i = 0$ for all values of y then $\eta_i = 0$, otherwise $\eta_i = 1$.

It follows from Lemma 7 that the necessary condition for the solution of Eq. (2) is

$$(\eta_2\rho_2,\ldots,\eta_n\rho_n,M) \mid y \frac{Mm_1}{a_1}$$

for all $y = 0, 1,\ldots \frac{a_1}{m_1} - 1$.

Thus $$(\eta_2\rho_2,\ldots,\eta_n\rho_n,M) = \frac{Mm_1}{\delta a_1}$$

and Eq. (2) may be divided by $\frac{Mm_1}{\delta a_1}$ to yield

$$\sum_{i=2}^{n} x_i \rho_i \frac{\delta a_1}{Mm_1} \equiv \delta y \bmod \frac{\delta a_1}{m_1}$$

But every $\rho_i = k_i \frac{M}{a_i}$ so

$$\sum_{i=2}^{n} x_i k_i \frac{\delta a_1}{a_i m_1} \equiv \delta y \bmod \frac{\delta a_1}{m_1} \tag{5}$$

Division by δ yields

$$\sum_{i=2}^{n} x_i k_i \frac{a_1}{a_i m_1} \equiv y \bmod \frac{a_1}{m_1} \tag{6}$$

$$y = 0, 1, \ldots, \frac{a_1}{m_1} - 1$$

Equation (6) shows that $a_i m_1$ must divide $k_i a_1$ if $\eta_i = 1$ since $x_i \epsilon G_{m_i}$.

Suppose that there is only one $\eta_i = 1$. If $m_i > \frac{a_1}{m_1}$ then the number system is redundant. If $m_i < \frac{a_1}{m_1}$ then the number system is incomplete. If $a_1 = m_i m_1$ then $a_i m_1 \nmid k_i a_1$ since $(a_i, k_i) = 1$ and $m_i < a_i$. Thus the number system is not complete if only one $\eta_i = 1$. If more than one $\eta_i = 1$ then Eq. (6) must be reduced. A given weight in Eq. (6) for which $\eta_i = 1$ generates an incomplete subgroup of $\frac{G_{a_1}}{m_1}$. The complete subgroup is of order a_i while the incomplete subgroup is of order m_i. Except for the reduction of the order of the group this is the same condition considered at the start of the proof of this theorem. Thus the repetition of the process of removing the partially generated subgroup and stating the conditions necessary to complete the subgroup will lead eventually to a condition involving only one digit of the form $x_i k_i \frac{a_{i-r}}{a_i m_{i-r}} \equiv v \bmod \frac{a_{i-r}}{m_{i-r}}$. This cannot be satisfied.

<u>Theorem IV</u>. The conditions for weights given in Theorem I are necessary as well as sufficient.

Proof: By Theorem III, not all ρ_i can be such that $(\rho_i, M) < \frac{M}{m_i}$. By Theorem II, no ρ_i can be such that $(\rho_i, M) > \frac{M}{m_i}$. Therefore there exists at least one ρ_i such that $(\rho_i, M) = \frac{M}{m_i}$. Since order is of no consequence let $i = 1$. Then $(\rho_1, M) = \frac{M}{m_1}$ and $x_1\rho_1$ generates the subgroup of G of order m_1. The remaining n-1 digits must satisfy

$$\sum_{i=2}^{n} x_i\rho_i \equiv z \bmod \frac{M}{m_i}$$

$$z = 0, 1, \dots \frac{M}{m_i} - 1$$

Repetition of the above argument yields

$$\left(\rho_2, \frac{M}{m_1}\right) = \frac{M}{m_1 m_2}$$

Repetition of the argument until termination provides all of the conditions stated in Theorem I.

Theorem V. Given a non-redundant and complete weighted number system. The multiplication of weight ρ_q by a constant k'_q yields a non-redundant complete number system if and only if $(k'_q, m_q) = 1$.

Theorem VI. The number of distinct weights which may be assigned to the qth weight of a non-redundant, complete number system is

$$\psi(m_q) \prod_{i=1}^{q-1} m_i .$$

$\psi(x)$ is Euler's ψ function which is equal to the number of integers less than x and relatively prime to x. $\psi(x) = x \prod_{p|x} (1 - \frac{1}{p})$. (The notation $\prod_{p|x}$ indicates a product over all distinct primes which divide x.)

Example: $\psi(10) = 10(1 - \frac{1}{2})(1 - \frac{1}{5}) = 4$. For further details see Le Veque, pages 27-30.

Proof: If $k_q = 1$ then $\rho_q = \frac{M}{\prod_{i=1}^{q} m_i} = \prod_{i=q+1}^{n} m_i$.

All multiples of $\prod_{i=q+1}^{n} m_i$ for which $(k_q, m_q) = 1$ may be used as the qth digit weight. Multiples of $\prod_{i=q+1}^{n} m_i$ greater than or equal to M are congruent modulo M to a multiple less than M and must not be counted. The total number of multiples of $\prod_{i=q+1}^{n} m_i$ less than M is equal to $\frac{M}{\prod_{i=q+1}^{n} m_i} = \prod_{i=1}^{q} m_i$. The fraction of these multiples for which $(k_q, m_q) = 1$ is $\frac{\psi(m_q)}{m_q}$. Thus there are

$$\frac{\psi(m_q)}{m_q} \prod_{i=1}^{q} m_i = \psi(m_q) \prod_{i=1}^{q-1} m_i$$

distinct weights for the qth weight.

Corollary: The number of distinct weighted, non-redundant, n digit, number systems for a given ordering of the digit moduli is equal to

$$\prod_{q=1}^{n} \left\{ \psi(m_q) \prod_{i=1}^{q-1} m_i \right\}$$

Corollary: The number of distinct weighted, consistently based, non-redundant, n digit, number systems for base m is $m^x \psi(m)$ where $x = \frac{n(n-1)}{2}$.

Theorem VII. Every non-redundant complete number system with relatively prime moduli can be represented by a lower triangular matrix [W] where

$w_{ij} = |\rho_i|_{m_j}$.

(We shall consider the base moduli symbols $m_1, \ldots, m_n$ as variables. The set of base moduli $\mu_1, \ldots \mu_n$ are constants. There are n! different ways of assigning the base moduli constants to the base variables. There is a lower triangular W matrix for at least one of these assignments.)

Proof:

$$W = \begin{bmatrix} \left|\frac{k_1 M}{m_1}\right|_{m_1} & \left|\frac{k_1 M}{m_1}\right|_{m_2} & \cdots & \left|\frac{k_1 M}{m_1}\right|_{m_n} \\ \left|\frac{k_2 M}{m_1 m_2}\right|_{m_1} & \left|\frac{k_2 M}{m_1 m_2}\right|_{m_2} & \cdots & \left|\frac{k_2 M}{m_1 m_2}\right|_{m_n} \\ \vdots & & & \\ \left|\frac{k_n M}{m_1 \cdots m_n}\right|_{m_1} & \left|\frac{k_n M}{m_1 \cdots m_n}\right|_{n_2} & \cdots & \left|\frac{k_n M}{m_1 \cdots m_n}\right|_{m_n} \end{bmatrix}$$

where $(k_i, m_i) = 1 \qquad i = 1, \ldots, n$

W is a lower triangular matrix because:

1. No diagonal element is equal to zero. The qth diagonal element has the form

$$\left|\frac{k_q M}{m_1 \cdots m_q}\right|_{m_q} = \left|k_q m_{q+1} \cdots m_n\right|_{m_q}$$

$$\left|k_q m_{q+1} \cdots m_n\right|_{m_q} \neq 0 \text{ because } (k_q, m_q) = 1 \text{ and}$$

all base moduli are relatively prime by pairs.

2. In any row every element to the right of the diagonal element is equal to zero. Elements to the right of the diagonal in the qth row have the form

$$\left|\frac{k_q M}{m_1 \cdots m_q}\right|_{m_{q+k}} = \left|k_q m_{q+1} \cdots m_n\right|_{m_{q+t}}$$

where $t = 1, \ldots, n-q$

$$\left|k_q m_{q+1} \cdots m_n\right|_{m_{q+t}} = 0 \text{ for all } t = 1, \ldots, n-q.$$

Theorem VIII. The elements below the diagonal in the W matrix are not necessarily zero. w_{ij}, $i > j$ assumes m_j different values depending on the choice of k_i.

Proof: Elements to the left of the diagonal in the qth row have the form

$$\left| \frac{k_q M}{m_1 \cdots m_q} \right|_{m_{q-t}} = \left| k_q m_{q+1} \cdots m_n \right|_{m_{q-t}} = w_{q,q-t}$$

where $t = 1,\ldots,q-1$.

The only restriction on k_q is $(k_q,m_q) = 1$. The moduli are relatively prime so k_q can be equal to any moduli except m_q. $k_q = m_{q-t}$ for any $t = 1,\ldots,q-1$ yields $w_{q,q-t} = 0$. If $k_q \neq m_{q-t}$ then $w_{q,q-t} \neq 0$. Furthermore $|k_q m_{q+1} \cdots m_n|_{m_{q-t}}$ is a complete residue system modulo m_{q-t} so w_{ij}, $i > j$ may assume m_j different values.

Theorem IX. The diagonal element w_{qq} assumes only $\phi(m_q)$ different values such that $(w_{qq},m_q) = 1$.

Proof: Theorem VI shows that the number of distinct weights assignable to the qth weight is given by

$$\psi(m_q) \prod_{i=1}^{q-1} m_i$$

From Theorem VIII we know that the nondiagonal elements to the left of the diagonal in the q row have $\prod_{i=1}^{q-1} m_i$ different combinations since each w_{ij} may assume m_j different values and $i = 1,\ldots q-1$. Hence $\psi(m_q)$ different values may be assigned to the diagonal element.

Assume that $(w_{qq}, m_q) = d \neq 1$. Then $d \mid m_{q+1} \cdots m_n$ since $w_{qq} = |k_q m_{q+1} \cdots m_n|_{m_q}$ and $(k_q, m_q) = 1$. But $d \nmid m_{q+1} \cdots m_n$ because m_q is relatively prime to all the other moduli. Hence there is a contradiction and the assumption that $(w_{qq}, m_q) \neq 1$ is not valid.

Lemma 7. Repeated permutation of selected pairs of rows followed by the permutation of the same pair of columns will transform a lower triangular W matrice in the S matrix. The S matrix is associated with a standard ordering of the base moduli constants $\mu_1, \ldots, \mu_n$. Let r_i be the digit weight associated with μ_i, then $s_{ij} = |r_i|_{\mu_j}$.

$$S = \begin{bmatrix} |r_1|_{\mu_1} & |r_1|_{\mu_2} & \cdots & |r_1|_{\mu_n} \\ |r_2|_{\mu_1} & |r_2|_{\mu_2} & \cdots & |r_2|_{\mu_n} \\ \vdots & & & \vdots \\ |r_n|_{\mu_1} & |r_n|_{\mu_2} & \cdots & |r_n|_{\mu_n} \end{bmatrix}$$

Theorem X. In the S matrix symmetric elements cannot both be non-zero. This and the condition $(w_{qq}, m_q) = 1$ for the diagonal elements is necessary and sufficient for the construction of an S matrix associated with a finite, non-redundant, weighted number system for relatively prime base moduli.

Proof: Consider the symmetric elements of the W matrix w_{ij}, and w_{ji} where $j < i$. Since $w_{ij} = 0$ it follows that $w_{ij} = w_{ji}$ only if $w_{ji} = 0$. A permutation of the ith and jth rows followed by a permutation of the ith and jth columns simply interchanges w_{ij} and w_{ji}. A permutation of the ith and kth rows followed by a permutation of the ith and kth columns does not destroy the relationship between w_{ij} and w_{ji} since w_{ij} replaces w_{kj} and w_{ji} replaces w_{jk}.

Thus the permutation operations do not change the relationship between symmetric elements in the matrix. Every W matrix, and hence every S matrix, has at least $\frac{n(n-1)}{2}$ zero elements. In every n x n matrix, there are $\frac{n(n-1)}{2}$ symmetric elements. The specification of the diagonal elements and the $\frac{n(n-1)}{2}$ symmetric elements subject to the condition w_{ij} or $w_{ji} = 0$ and $w_{ij} \neq w_{ji}$ except when $w_{ij} = w_{ji} = 0$ define a non-redundant, finite, weighted number system for relatively prime moduli. That every such number system is so specified follows from the fact that the n! possible W matrices specify every possible non-redundant, finite, weighted number system at least once.

Theorem XI. For a given set of relatively prime moduli $\mu_1, \ldots, \mu_n$ there exists

$$Q = \prod_{k=1}^{n} \psi(\mu_k) \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\mu_i + \mu_j - 1)$$

distinct weighted, non-redundant, number systems. (Each number system is distinct in the sense that the set of weights $r_1, \ldots r_n$ is different for each number system.)

Examples:

$$\mu_1 = 2,\ \mu_2 = 3,\ Q = 8$$

$$\mu_1 = 2,\ \mu_2 = 3,\ \mu_3 = 5,\ Q = 1344.$$

Proof: Consider the S matrix: Each diagonal element s_{kk} can be assigned $\psi(m_j)$ different values. There are therefore $\prod_{k=1}^{n} \psi(m_k)$ different combinations of diagonal elements. The number of different values which can be assigned to the symmetric pair s_{ij}, s_{ji} is $\mu_i + \mu_j - 1$. The number of values that may be assigned to the $\frac{n(n-1)}{2}$ pairs of symmetric elements of the S matrix is obtained from enumeration of the elements in each column below the diagonal. Each element in the ith column is associated with μ_i. Each element below the diagonal has a corresponding symmetric element in the ith row. The modulus corresponding to this element depends on the position and is designated μ_j where $i < j \leqslant n$. Hence there are

$$\prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\mu_i + \mu_j - 1)$$

different combinations of element values for the non-diagonal elements. The total number of different combinations of element values for the matrix S is

$$Q = \prod_{j=1}^{n} \psi(\mu_j) \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\mu_i + \mu_j - 1)$$

Corollary: If all moduli are prime then

$$Q = \prod_{i=0}^{n-1} \prod_{j=i+1}^{n} (\mu_i + \mu_j - 1) \qquad \text{where } \mu_o = 0.$$

LIST OF SYMBOLS

G_M	the group of M integers 0, 1,...,M-1
G_{m_i}	the group of m_i integers 0, 1,...,m_i-1
H_{m_i}	a subgroup of G_M of order m_i
$x_i \epsilon G_{m_i}$	x_i an element of G_{m_i}
(ρ_i, M)	the greatest common divisor of ρ_i and M
$\lvert X\rvert_{m_i}$	is the least positive residue of X modulo m_i. This can be defined in terms of the greatest integer part. The symbol for the greatest integer part of $X \div m_i$ is $\left[\frac{X}{m_i}\right]$. Then $\lvert X\rvert_{m_i} = X - m_i\left[\frac{X}{m_i}\right]$.
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\psi(x)$	Euler's ψ function