GPO PRICE $ ______

CFSTI PRICE(S) $ ______

Hard copy (HC) 2.00

Microfiche (MF) .50

ff 653 July 65

FACILITY FORM 602

N67 10884
(ACCESSION NUMBER)

30
(PAGES)

CR-79745
(NASA CR OR TMX OR AD NUMBER)

(THRU)

1
(CODE)

07
(CATEGORY)

RAND RESEARCH
BRIEF
THE RAND CORPORATION
1700 Main St. · Santa Monica · Calif.

September 1966 RB-5131

RM-5131-NASA, A Class of Codes for Multiple-Access Satellite Communication Systems, P. M. Spira, RAND Memorandum, September 1966, 33 pp.

PURPOSE: To describe mathematically a specific method for allocating time and frequency in communication satellite systems that use time-frequency multiplexing for random multiple access.

SCOPE: Algorithms are shown for constructing low-interference address codes for such systems, for various sizes of time-frequency matrices and address lengths. In these codes, the number of addresses, or code words, containing a given chip is KM/N, where K is the number of words, M is the number of chips in an address, and N is the number of chips in the time-frequency matrix. The ratio can be made as large as desired while, at the same time, M remains fixed. This is done by increasing N, which amounts to an increase in system bandwidth, and/or an increase in the time length of the matrix. As N increases, the maximum number of addresses also rises. Hence, since N is a measure of the total data rate of the system, the increase in size of the time-frequency matrix does not necessarily cause wasted bandwidth.

In practice, KM/N will be limited by considerations entirely divorced from the mathematics of code construction. Some of these factors include the duty cycle of an address, system noise, and the manner of detecting a message. Thus the requirement that any two addresses have, at most, one common chip (which drastically curbs the incidence of serious interference) will not usually be the factor that limits the number of system users.

Because consideration is confined to the mathematics of time and frequency assignments, no attempt has been made to extend the discussion to problems of establishing and monitoring circuits or of actual system design.

BACKGROUND: This is part of RAND's research for the National Aeronautics and Space Administration on communication satellite multiple-access techniques. See also RM-4298-NASA, Multiple-Access Techniques for Communication Satellites: I. Survey of the Problem, September 1964.

AG

NASr-21(02)

MEMORANDUM
RM-5131-NASA
SEPTEMBER 1966

A CLASS OF CODES FOR MULTIPLE-ACCESS SATELLITE COMMUNICATION SYSTEMS

P. M. Spira

This research is sponsored by the National Aeronautics and Space Administration under Contract No. NASr-21. This report does not necessarily represent the views of the National Aeronautics and Space Administration.

The RAND Corporation
1700 MAIN ST. • SANTA MONICA • CALIFORNIA • 90406

Published by The RAND Corporation

PREFACE

This Memorandum is part of RAND's continuing study of multiple-access techniques for communications satellites for the National Aeronautics and Space Administration. It presents a method of allocating time and frequency in systems employing time-frequency multiplexing which may prove useful for systems in which a user can transmit at any time without consulting a central controller--so-called random access systems.

Only the mathematics of time and frequency assignments are discussed in this Memorandum. It is not concerned with problems of establishing and monitoring circuits or of actual system design.

SUMMARY

In recent years the problem of providing multiple access to a communication satellite has been extensively studied, and various modulation methods have been proposed to fit different system requirements. One attractive method for random multiple access is time-frequency multiplexing. Large numbers of users are accommodated by allowing time-frequency assignments to overlap. However, it is also necessary to limit interference levels in any practical system.

In this Memorandum, a specific method of constructing addresses from a time-frequency matrix is developed which applies to many matrix sizes and many address lengths. As many addresses as possible are constructed so that no two of them have more than one chip in common. At the same time, for a fixed address length, the number of addresses containing a given chip can be made arbitrarily large and will, in fact, be almost exactly proportional to the number of chips in the time-frequency matrix.

The effect of requiring that any address contain at most one chip from each column of the matrix is examined. When the number of columns is equal to the address length each address has exactly one chip from any column. This requirement reduces the number of allowable addresses, but the reduction has no practical significance.

ACKNOWLEDGMENTS

The development of these ideas was greatly aided by discussions with E. Bedrosian and C.R. Lindholm of The RAND Corporation and with J. Spencer, a graduate student in mathematics at Harvard University and a member of the graduate student summer program at The RAND Corporation.

CONTENTS

I. INTRODUCTION

In recent years the problem of providing multiple access to a communication satellite has been extensively studied,(1-3) and various modulation schemes have been advanced to fit varying system requirements. One modulation method which has been proposed is time-frequency multiplexing,(4,5) which appears especially attractive for random multiple access. In a system employing this type of modulation, an area in time-frequency space is divided into contiguous equidimensional rectangular segments comprising the elements of a matrix (see Fig. 1). Each element is occupied by a basic waveform, e.g., a sinusoidal pulse, in such a way that the waveforms (commonly called the chips of the matrix) are pairwise orthogonal. Also, each chip will usually have the same energy.

In a given system addresses will be formed from the chips of the matrix and each address will consist of the same number of chips. The various transmitter-receiver pairs using the satellite will each be assigned one or more of these addresses. A given chip will, in general, appear in many addresses, but much of the utility of this type of multiple access depends upon constructing the addresses in such a way as to minimize interference, and to allow a large number of system users. In some cases it is desirable to transmit continuously; this requires an address having exactly one chip from each column of the matrix and poses an additional constraint.

This Memorandum describes a method of constructing sets of addresses for a time-frequency multiplex system which exhibits many desirable properties. Minimal interference is guaranteed by demanding that any

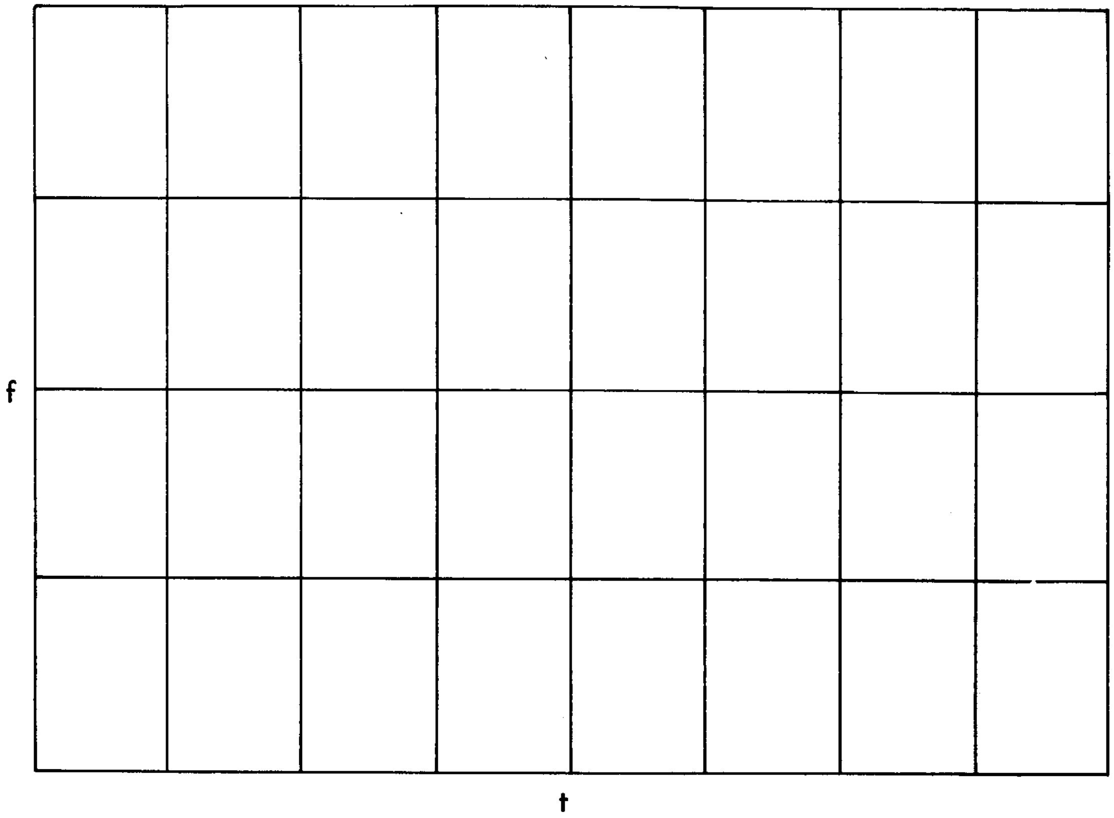

Fig. 1—A time frequency matrix for r = 4, s = 8

two addresses have at most one common chip, and by the symmetry of the construction to facilitate analysis of system performance. In addition, it is also possible to satisfy the requirement of continuous transmission without losing the ability to accommodate large numbers of users.

II. LATIN SQUARES

The construction of the codes in this Memorandum is based upon the theory of Latin squares. A Latin square of order n is an n x n matrix of n symbols, e.g., the integers between 1 and n arranged so that each of them appears once in each row and once in each column. Thus,

$$S = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix}$$

is a Latin square of order 5. Given two Latin squares S and S′ of order n, the array of their ordered pairs can be formed

$$(S,S') = \begin{bmatrix} (s_{11},s'_{11}) & (s_{12},s'_{12}) & \cdots & (s_{1n},s'_{1n}) \\ (s_{21},s'_{21}) & \cdot \quad \cdot & \cdot \quad \cdot & (s_{2n},s'_{2n}) \\ \vdots & \cdot \quad \cdot & \cdot \quad \cdot & \cdot \\ (s_{n1},s'_{n1}) & \cdot \quad \cdot & \cdot \quad \cdot & (s_{nn},s'_{nn}) \end{bmatrix}$$

The squares are said to be orthogonal if each of the n^2 possible ordered pairs appears exactly once in the array. For example, if

$$S = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$$

and

$$S' = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$$

then

$$(S,S') = \begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix}$$

so S and S' are orthogonal. A well-known fact based on Galois field theory(6) is that if n is a power of a prime, then there is a set of n - 1 pairwise orthogonal Latin squares of order n.(7) To construct them for $GF(p^k)$, the field of p^k elements, let

$$GF(p^k) = \{f_o = 0,\ f_1 = 1,\ f_2,\ \ldots,\ f_{(p^k-1)}\}$$

where 0 is the additive identity and 1 is the multiplicative identity. The j^{th} Latin square will be(8)

$$S_j = \begin{bmatrix} 0 & 1 & \cdots\cdots & f_{(p^k-1)} \\ f_j & f_j+1 & f_j+f_2 & f_j+f_{(p^k-1)} \\ f_jf_2 & f_jf_2+1 & \cdots\cdots & f_jf_2+f_{(p^k-1)} \\ & \cdots\cdots & \cdots\cdots & \cdot \\ f_jf_{(p^k-1)} & f_jf_{(p^k-1)}+1 & \cdots & f_jf_{(p^k-1)}+f_{(p^k-1)} \end{bmatrix}$$

To observe that any two of them, for instance S_j and S_m, are orthogonal, assume that an ordered pair (f_r,f_s) occurs twice in (S_j,S_m), e.g., in the α^{th} row and the β^{th} column and in the γ^{th} row and the δ^{th} column. Then

$$f_r = f_j f_{\alpha-1} + f_{\beta-1} = f_j f_{\gamma-1} + f_{\delta-1}$$

$$f_s = f_m f_{\alpha-1} + f_{\beta-1} = f_m f_{\gamma-1} + f_{\delta-1}$$

Thus

$$f_{\alpha-1}(f_j - f_m) = f_{\gamma-1}(f_j - f_m)$$

But, since $j \neq m$, this means that $\alpha = \gamma$, which in turn implies that $\beta = \delta$. Thus the squares are orthogonal. The application of these ideas to the construction of actual codes will be illustrated in the next section.

III. A CLASS OF CODES

Recall that a time-frequency matrix is an r by s matrix of contiguous rectangular cells in time-frequency space, each having the same dimensions (see Fig. 1). The cells are numbered from 1 to N, where

$$N = rs$$

It is desired to form a code in which each word consists of M out of the N cells and in which there are K words. Each code word will be an address of a system user. In general, each cell will appear in many different addresses. Thus

$$KM > N$$

It is desirable that available time-frequency space be shared by as many users as possible, i.e., that

$$\frac{KM}{N}$$

be large, while at the same time it is desirable that any two addresses have minimal overlap. If, in addition, each cell is used in the same number of addresses, then the calculation of system performance is greatly simplified. These last two requirements are stated as a coding problem and the class of codes constructed will allow arbitrarily high ratios of KM to N.

Problem: Assume there are N elements from which it is desired to form a code consisting of K code words, each formed from M elements out of the N. It is further required that:

1. Each of the N elements appears in the same number of code words.

2. No two code words contain more than one common element.

Then for given values of M and N, what values of K are possible? In particular, what is the largest possible value of K? The size of this maximal code will be denoted by $K_{max}(N,M)$. Any code satisfying the above two requirements will be called acceptable.

Two important special cases of acceptable codes will be those with words which have at most one element from each column of the time-frequency matrix, and those with words which have exactly one element from each column of the matrix. This latter will be continuous transmission or cw codes, which greatly simplify system implementation.

In the next section, it will be shown if $p = q^k$, where q is the prime > 1 and $k \geq 1$, and if $M = p$ and $N = p^n$, where $n \geq 1$, that:

1. $$K_{max}(p^n,p) = p^{n-1} \frac{p^n - 1}{p - 1}$$

2. If the time-frequency matrix is of the size $p^{n-k} \times p^k$, for $0 \leq k \leq n$, then an acceptable code of size

$$K = p^{n-1} \frac{p^n - p^{n-k}}{p - 1}$$

can be found, the words of which have at most one element from any given column of the matrix. In particular, if the matrix is of size $p^{n-1} \times p$, there is a cw code in which each word has exactly one element from each column of size

$$K = p^{2n-2}$$

3. If

$$a = 0 \text{ or } 1$$

and

$$b = 0, 1, \ldots, p$$

then acceptable codes exist for

$$K = ap^{n-1} + bp^{n-1} \frac{p^{n-2} - 1}{p - 1}$$

4. Acceptable codes can be found for

$$K = cp^{n-1} + dp^{n}$$

where a and b are as before and

$$c = 0 \text{ or } 1$$

$$d = a + b \frac{p^{n-2} - 1}{p - 1}$$

The proofs are rigorous but are also algorithmic. In addition, concrete examples of code construction are provided.

IV. EXISTENCE AND CONSTRUCTION OF ACCEPTABLE CODES

Now the existence of acceptable codes for the previously enumerated values of K will be demonstrated and exemplary codes will be constructed.

Remark: If q is a prime and $p = q^k$ for $k \geq 1$, then

$$K_{max}(p^2, p) = p(p+1)$$

Proof: Arrange the p^2 elements in a p x p matrix

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1p} \\ a_{21} & \cdot\;\cdot\;\cdot\;\cdot\;\cdot & & a_{2p} \\ & \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot & & \\ a_{p1} & \cdot\;\cdot\;\cdot\;\cdot\;\cdot & & a_{pp} \end{bmatrix}$$

Enumerate a set of p - 1 pairwise orthogonal Latin squares of order p, composed of integers 1, 2, •••, p. Pick any of the Latin squares, e.g., S, where

$$S = \begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1p} \\ s_{21} & \cdot\;\cdot\;\cdot\;\cdot\;\cdot & & s_{2p} \\ & \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot & & \\ s_{p1} & \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot & & s_{pp} \end{bmatrix}$$

and form code words $W_1, W_2, \cdots, W_p$, each word being a set of p elements of S according to the rule:

$$a_{ij} \in W_m \text{ if and only if } s_{ij} = m$$

i.e., the m^{th} word contains the elements of A which are in the same location of the matrix A as m is in the Latin square S. This will result in p code words which will be disjoint sets of p elements each. Now the same is done for each of the p - 1 Latin squares obtaining p(p-1) words. It has been seen that any two words derived from the same square are disjoint. Now consider two words derived from different squares, e.g., W_u from S and W_v from S'. They will have exactly one element of A in common, since the ordered pair (u, v) will appear in one place of (S, S'), the array of ordered pairs defined in Section II. Thus, the set of p(p-1) words has the property that any two contain at most one common element. To this set can be added the p rows and p columns of A, since in no Latin square does any element appear twice in any row or in any column. Thus, an acceptable code of p(p+1) words has been constructed, showing that

$$K_{max}(p^2, p) \geq p(p+1)$$

This will be proven to be an upper bound. If any element is chosen from A and it is desired to form as many words as possible using it with each other element at most once, then, since there are p - 1 places left to fill and p^2 - 1 elements left to fill them with, there are at most

$$\frac{p^2 - 1}{p - 1} = p + 1$$

words containing the given element. If each of the p^2 elements is contained in this many words, then the sum of the lengths of all words in the code is

$$p^2(p+1)$$

But since there are p elements per word

$$K_{max}(p^2, p) \leq p(p+1)$$

Therefore

$$K_{max}(p^2, p) = p(p+1)$$

To illustrate this remark, a code having 20 words will be found for

$$M = 4$$

$$N = 16$$

First the three orthogonal Latin squares will be found. The addition and multiplication tables for GF(4) are

+	0	1	x	1+x
0	0	1	x	1+x
1	1	0	1+x	x
x	x	1+x	0	1
1+x	1+x	x	1	0

	0	1	x	1+x
0	0	0	0	0
1	0	1	x	1+x
x	0	x	1+x	1
1+x	0	1+x	1	x

Using as a correspondence of GF(4) with {1, 2, 3, 4}

$$0 \Leftrightarrow 1$$

$$1 \Leftrightarrow 2$$

$$x \Leftrightarrow 3$$

$$1+x \Leftrightarrow 4$$

the Latin squares are

$$\begin{bmatrix} 0 & 1 & x & 1+x \\ 1 & 0 & 1+x & x \\ x & 1+x & 0 & 1 \\ 1+x & x & 1 & 0 \end{bmatrix} \Leftrightarrow \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & x & 1+x \\ x & 1+x & 0 & 1 \\ 1+x & x & 1 & 0 \\ 1 & 0 & 1+x & x \end{bmatrix} \Leftrightarrow \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & x & 1+x \\ 1+x & x & 1 & 0 \\ 1 & 0 & 1+x & x \\ x & 1+x & 0 & 1 \end{bmatrix} \Leftrightarrow \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$

Letting

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix}$$

the 20 code words are (1, 2, 3, 4), (5, 6, 7, 8), (9, 10, 11, 12), (13, 14, 15, 16), (1, 5, 9, 13), (2, 6, 10, 14), (3, 7, 11, 15), (4, 8, 12, 16), (1, 6, 11, 16), (2, 5, 12, 15), (3, 8, 9, 14), (4, 7, 10, 13), (1, 7, 12, 14), (2, 8, 11, 13), (3, 5, 10, 16), (4, 6, 9, 15), (1, 8, 10, 15), (2, 7, 9, 16), (3, 6, 12, 13), and (4, 5, 11, 14).

This result is not very useful for the application proposed here, but the generalization provided by the following theorem is. It should be noted that it is equivalent to the existence of an incomplete balanced block design with parameters

$$v = p^n$$

$$b = p^{n-1} \frac{p^n - 1}{p - 1}$$

$$r = \frac{p^n - 1}{p - 1}$$

$$k = p$$

$$\lambda = 1$$

Though this design is known,(9) the following proof presupposes no knowledge of projective geometry, while illustrating actual application of the result.

Theorem 1: Let q be a prime and $p = q^k$ for $k \geq 1$, and let

$$M = p$$

$$N = p^n$$

Then

$$K_{max}(p^n, p) = p^{n-1} \frac{p^n - 1}{p - 1} \text{ for } n \geq 2$$

Proof: Induction on n will be used. For $n = 2$, apply the preceding remark. Now assume the theorem is true for $n \leq t - 1$, i.e., assume

$$K_{max}(p^{t-1}, p) = p^{t-2} \frac{p^{t-1} - 1}{p - 1}$$

Now $K_{max}(p^t, p)$ will be determined. Set

$$N = p^t$$

Arrange the elements in a $p^{t-1} \times p$ matrix

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1p} \\ a_{21} & \cdot & \cdot\ \cdot & a_{2p} \\ \cdot\ \cdot & \cdot\ \cdot & \cdot\ \cdot & \cdot \\ a_{(p^{t-1})1} & \cdot & \cdot\ \cdot & a_{(p^{t-1})p} \end{bmatrix}$$

Since there are p^{t-1} rows, the induction hypothesis implies that they can be used to form $K_{max}(p^{t-1}, p)$ $p \times p$ matrices such that no two matrices have more than one row in common, and such that each row is used in the same number of $p \times p$ matrices. Using the same argument as before, from each of these matrices, p^2 code words can be constructed such that no two words have more than one element in common without using rows as words. Since no two p x p matrices have more than one common row, any word from one matrix will have at most one element in common with any word from another matrix. Hence, this procedure will yield

$$p^2\, K_{max}(p^{t-1}, p)$$

words. To these, add the p^{t-1} rows of the p^{t-1} x p matrix. This will yield an acceptable code with

$$p^{t-1} + p^2\, K_{max}(p^{t-1}, p) = p^{t-1}\, \frac{p^t - 1}{p - 1}$$

words. Exactly the same reasoning used in the proof of the remark shows this number to be an upper bound for $K_{max}(p^t, p)$. Thus, the theorem is proved, i.e.,

$$K_{max}(p^n, p) = p^{n-1}\, \frac{p^n - 1}{p - 1}$$

To illustrate the application of the theorem let

$$p = 3$$

$$n = 3$$

There are 27 elements arranged as shown next:

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \\ 13 & 14 & 15 \\ 16 & 17 & 18 \\ 19 & 20 & 21 \\ 22 & 23 & 24 \\ 25 & 26 & 27 \end{bmatrix} = \begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ R_4 \\ R_5 \\ R_6 \\ R_7 \\ R_8 \\ R_9 \end{bmatrix}$$

To form the 3 x 3 matrices, treat the rows as elements of a 3 x 3 matrix

$$R = \begin{bmatrix} R_1 & R_2 & R_3 \\ R_4 & R_5 & R_6 \\ R_7 & R_8 & R_9 \end{bmatrix}$$

Two orthogonal Latin squares of order three are

$$S = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$$

and

$$S' = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$$

These dictate the rows of six of the 3 x 3 matrices. The rows and columns of R dictate the others. Thus there will be twelve 3 x 3 matrices with rows (R_1,R_2,R_3), (R_4,R_5,R_6), (R_7,R_8,R_9), (R_1,R_4,R_7), (R_2,R_5,R_8), (R_3,R_6,R_9), (R_1,R_4,R_7), (R_2,R_6,R_7), (R_3,R_4,R_8), (R_1,R_6,R_8), (R_2,R_4,R_9), and (R_3,R_5,R_7). For example, the fourth 3 x 3 matrix will be

$$(R_1,R_4,R_7) = \begin{bmatrix} 1 & 2 & 3 \\ 10 & 11 & 12 \\ 19 & 20 & 21 \end{bmatrix}$$

The $3^2 = 9$ words formed from it using its columns and the same Latin squares will be (1,10,19), (2,11,20), (3,12,21), (1,11,21), (2,12,19), (3,10,20), (1,12,20), (2,10,21), and (3,11,19). The rest of the 3 x 3 matrices are treated similarly, and the nine rows are added to the code, yielding

$$K_{max}(3^3, 3) = 117$$

words.

Remark: If the time-frequency matrix is of size $p^{n-k} \times p^k$, where $0 \leq k \leq n$, then an acceptable code of size

$$K = \frac{p^{n-1}}{p - 1}(p^n - p^{n-k})$$

can be constructed, and any given word of this code will have at most one element from any column of the matrix. In particular, for k = 1, there is a code of size

$$K_{cw} = p^{2n-2}$$

in which every word has exactly one element from each column. This is the cw case.

Proof: If $k = 0$, the matrix has one column, and no words can be formed. This agrees with the above remark. If $k = n$, the code having $K_{max}(p^n, p)$ elements from Theorem 1 can be used, since each column has only one element, and this is the value given above in the case $k = n$. If $k = n - 1$, let each column correspond to a row of the $p^{n-1} \times p$ matrix in the proof of Theorem 1, and eliminate words consisting of a row. No other words will have two elements from the same column of the time-frequency matrix and there will be

$$K_{max}(p^n, p) - p^{n-1} = p^{n-1} \frac{p^n - p}{p - 1}$$

words left. For $1 \leq k \leq n - 2$, let each column correspond to p^{n-k-1} rows of the $p^{n-1} \times p$ matrix in Theorem 1. Use these rows to make $K_{max}(p^{n-k-1}, p)$ of the $p \times p$ matrices from before. Eliminate all words derived from these matrices. Thus, since there are p^k rows, eliminate

$$p^{k+2} K_{max}(p^{n-k-1}, p) = p^n \frac{p^{n-k-1} - 1}{p - 1}$$

words from the code of size $K_{max}(p^n, p)$, and in addition eliminate the p^{n-1} row words from the $p^{n-1} \times p$ matrix. There will be left a code of size

$$K_{max}(p^n, p) - p^n \frac{p^{n-k-2} - 1}{p - 1} - p^{n-1} = p^{n-1} \frac{p^n - p^{n-k}}{p - 1}$$

which proves the remark. Setting $k = 1$ demonstrates the existence of a code in which each word contains exactly one element from each column of the time-frequency matrix of size

$$K_{cw}(p^n, p) = p^{2n-2}$$

For the example following the proof of Theorem 1, if the time-frequency matrix is

$$\begin{bmatrix} 1 & 10 & 19 \\ 2 & 11 & 20 \\ 3 & 12 & 21 \\ 4 & 13 & 22 \\ 5 & 14 & 23 \\ 6 & 15 & 24 \\ 7 & 16 & 25 \\ 8 & 17 & 26 \\ 9 & 18 & 27 \end{bmatrix}$$

then a cw code of size

$$3^4 = 81$$

is obtained by eliminating the nine original row words and the words from matrices containing (R_1, R_2, R_3), (R_4, R_5, R_6), and (R_7, R_8, R_9).

Remark: Acceptable codes can be found having size

$$K = ap^{n-1} + bpK_{max}(p^{n-1}, p) = ap^{n-1} + bp^{n-1} \frac{p^{n-2} - 1}{p - 1}$$

where

$$a = 0 \text{ or } 1$$

$$b = 0, 1, \ldots, p$$

Proof: To construct such a code, if $a = 0$ do not use the rows of the $p^{n-1} \times p$ matrix. If $b < p$, use only b of the $p - 1$ orthogonal Latin squares of order p in determining words to be formed from the $p \times p$ matrices. Recall that since there are $K_{max}(p^{n-1}, p)$ of such matrices, this procedure will yield the $bpK_{max}(p^{n-1}, p)$ words. If $b = p$, use all $p - 1$ Latin squares, and in addition form words from the columns of each $p \times p$ matrix.

There are also other possible sizes of K, as the following theorem shows:

Theorem 2: Let $p = q^k$, where q is a prime, and $k \geq 1$. Then acceptable codes exist for

$$K = cp^{n-1} + dp^n$$

where, as before,

$$M = p$$

$$N = p^n$$

Here

$$c = 0, 1$$

$$d = a + b \frac{p^{n-2} - 1}{p - 1}$$

and a and b are as in the preceding remark.

Proof: As before, arrange the p^n elements into a matrix having p^{n-1} rows of p elements. By the last remark these rows can be used to form a set of

$$ap^{n-2} + bpK_{max}(p^{n-2}, p)$$

p x p matrices such that each row is used in the same number of matrices and no two matrices have more than one common row, where

$$a = 0, 1$$

$$b = 0, 1, \cdots, p$$

From each of these matrices, p^2 code words can be obtained using no words consisting of entire rows. Hence, acceptable codes exist for

$$K = ap^n + bp^3K_{max}(p^{n-2}, p)$$

$$= dp^n$$

The p^{n-1} rows can be added to these, if desired ($c = 1$), or not included ($c = 0$), proving the theorem.

V. CONCLUSIONS

Algorithms have been shown for constructing low interference address codes for a system employing time-frequency multiplexing for various sizes of time-frequency matrices and address lengths. In these codes the number of addresses containing a given chip is $\frac{KM}{N}$, which can be made as large as desired while, at the same time, M (the number of chips in an address) remains fixed. This is done by increasing N (the number of chips in the time-frequency matrix), which amounts to an increase in system bandwidth, and/or an increase in the time length of the matrix. Note that as N is increased, the maximum number of addresses also rises. In fact, for fixed M

$$K_{max}(N, M) \alpha N^2$$

almost exactly. Hence, since N is a measure of the total data rate of the system, the increase in size of the time-frequency matrix does not result in wasted bandwidth.

In practice, $\frac{KM}{N}$ will be limited by considerations entirely divorced from the mathematics of code construction. Some of these factors will be the duty cycle of an address, system noise, and the manner of detecting a message. Thus, perhaps the most important fact to note is that the requirement that any two addresses have at most one common chip, which drastically curbs the incidence of serious interference, will not usually be the factor which limits the number of system users.

REFERENCES

1. Bedrosian, E., N.E. Feldman, G. Northrop, and W. Sollfrey, Multiple Access Techniques for Communication Satellites: I. Survey of the Problem, The RAND Corporation, RM-4298-NASA, September 1964.

2. Reinhart, E. E., Multiple-Access Techniques for Communication Satellites: Analog Modulation, Frequency-Division Multiplexing, and Related Signal Processing Methods, The RAND Corporation, RM-5117-NASA (to be published).

3. Lindholm, C. R., Multiple-Access Techniques for Communication Satellites: Digital Modulation, Time-Division Multiplexing, and Related Signal Processing Methods, The RAND Corporation, RM-4997-NASA (to be published).

4. Schwartz, J. W., J. M. Aein, and J. Kaiser, "Modulation Techniques for Multiple Access to a Hard-Limiting Satellite Repeater," Proc. IEEE, Vol.54, No. 5, May 1966, pp. 763-777.

5. Lanning, H. E., "Random Multiple Access," Ninth National Communications Symposium, Western Periodicals Co., North Hollywood, California, 1963, pp. 169-174.

6. Herstein, I. N., Topics in Algebra, Blaisdell Publishing Company, New York, 1965, p. 316.

7. Ryser, H. J., Combinatorial Mathematics, The Mathematical Association of America, No. 14, John Wiley and Sons, Inc., 1963, p. 81.

8. Mann, H. B., Analysis and Design of Experiments, Dover Publications, New York, 1949, pp. 91-92.

9. Kaplansky, Irving, et al., Some Aspects of Analysis and Probability, John Wiley and Sons, Inc., New York, 1958, p. 90.