ESD ACCESSION LIST
TRI Call No. 72785
Copy No. 1 of 2 cys.
TRI FILE COPY

ESD-TR-71-78

ESD RECORD COPY
RETURN TO
SCIENTIFIC & TECHNICAL INFORMATION DIVISION
(TRI), Building 1210

MTP-115

Kth ORDER NEAR-ORTHOGONAL CODES

Irving S. Reed

MARCH 1971

Prepared for

DEPUTY FOR PLANNING AND TECHNOLOGY
ELECTRONIC SYSTEMS DIVISION
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
L. G. Hanscom Field, Bedford, Massachusetts

This document has been approved for public release and sale; its distribution is unlimited.

Project 600G
Prepared by
THE MITRE CORPORATION
Bedford, Massachusetts
Contract F19(628)-68-C-0365

AD720822

When U.S. Government drawings, specifications, or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise, as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

Do not return this copy. Retain or destroy.

ESD-TR-71-78

MTP-115

Kth ORDER NEAR-ORTHOGONAL CODES

Irving S. Reed

MARCH 1971

Prepared for

DEPUTY FOR PLANNING AND TECHNOLOGY
ELECTRONIC SYSTEMS DIVISION
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
L. G. Hanscom Field, Bedford, Massachusetts

This document has been approved for public release and sale; its distribution is unlimited.

Project 600G
Prepared by
THE MITRE CORPORATION
Bedford, Massachusetts
Contract F19(628)-68-C-0365

FOREWORD

This report has been prepared under contract F19(628)-C-0365, by Irving S. Reed, consultant to The MITRE Corporation, Bedford, Massachusetts.

REVIEW AND APPROVAL

Publication of this technical report does not constitute Air Force approval of the report's findings or conclusions. It is published only for the exchange and stimulation of ideas.

KENNETH H. KRONLUND, Lt Col, USAF
UCNI/PLRACTA Program Manager
Communications Development Division
Deputy for Planning and Technology

ABSTRACT

Certain near-orthogonal codes have recently been used in multiple-shift keying communication systems. The codes generally considered for this application are the first order Reed-Solomon (RS) codes. The purpose of this paper is to extend this class of codes. It is shown that codes can be developed with the property that no two members of the code overlap in more than k frequency-time slots. It is also shown that certain subsets of these codes are synchronizable. The optimum k^{th} order near-orthogonal synchronizable codes are certain subsets of RS codes with a maximum distance $d = n-k$, where n is the number of code symbols.

THE AUTHOR

Irving S. Reed of Technology Service Corporation, Santa Monica, California, is a Consultant to The MITRE Corporation.

TABLE OF CONTENTS

		Page
SECTION I	INTRODUCTION	1
SECTION II	SOME MAXIMUM k^{th} ORDER NEAR-ORTHOGONAL CODES	3
	THEOREM 1	3
SECTION III	SYNCHRONIZABLE k^{th} ORDER NEAR-ORTHOGONAL CODES	4
	THEOREM 2	6
	THEOREM 3	8
	REFERENCES	10

SECTION I

INTRODUCTION

Recently, certain near-orthogonal codes have been proposed and used for multiple frequency shift keying (FSK) communications systems; e.g., see Reference [1]. The codes most generally considered for this application are the first order Reed-Solomon (RS) codes. These codes have the property that no two members of the code overlap in more than one symbol or frequency-time (FT) slot, and as a consequence, are very nearly orthogonal.

The purpose of this paper is first to show that the above class of codes can be extended to a code with the property that no two members of the code overlap in more than k frequency-time slots. These codes will be called k^{th} order near-orthogonal codes. Finally, it will be shown that certain subsets of kth order near-orthogonal codes can be generated in such a manner that no two words of a subset under different time delays or translations overlap in more than k symbols. The latter property means that these codes can be detected asynchronously with a bank of matched filters (either coherently or noncoherently). It is in this sense that these subsets constitute a self-synchronizable class of codes. The latter codes are closely related to what Gilbert, in Reference [2], called cyclically-permutable error-correcting codes. His attention was restricted to certain binary error-correcting codes, namely, the cyclic Hamming code of N binary digits. In this paper, more general symbol error-correcting codes are considered where the number of symbols, e.g. frequency slots, is some power of a prime number.

Consider briefly the nature of codes. Assume each symbol (each discrete frequency) of the code can be identified with an element of a Galois (finite) field $GF(q)$ where $q = p^m$ and p is a prime number. A word $\underline{f}$ of a code E is a vector (sequence) where its n components are elements

from GF (q); i.e., $\underline{f} = (f_1, f_2, \ldots f_n)$ where $f_k \epsilon GF(q)$ for $k = 1, 2, \ldots, n$. The norm or weight $\|\underline{f}\|$ of word $\underline{f}$ is defined as the number of non-zero components of $\underline{f}$.

If two vectors $\underline{f}$ and $\underline{g}$ overlap at k components, their algebraic difference $\underline{f} - \underline{g}$ has zeros in the corresponding k components, and vice versa. Hence, the norm or weight of $\underline{f} - \underline{g}$, i.e., $\|\underline{f} - \underline{g}\|$, is exactly the number of components of vectors $\underline{f}$ and $\underline{g}$ which differ. $\|\underline{f} - \underline{g}\|$ is called the generalized Hamming distance, or simply distance between codes $\underline{f}$ and $\underline{g}$.

Suppose code E is a linear vector space. That is, if $\underline{f}, \underline{g} \epsilon E$ and $\alpha \epsilon GF(p)$, then $(\underline{f} - \underline{g}) \epsilon E$ and $\alpha \underline{f} \epsilon E$. If E is a vector space, then the minimum distance d between any two vectors of E is the minimum weight or norm of any of its words.

This follows from the relation

$$d = \min_{\underline{f}, \underline{g} \epsilon E} \|\underline{f} - \underline{g}\| = \min_{\underline{h} \epsilon E} \|h\|.$$

From the above discussion, if d is the minimum distance between any two vectors of a code, E, the maximum number of overlaps between any two code words, is given by $k = n-d$ where n is the dimension (or number of components) of the code. The search for k^{th} order near orthogonal codes is ended. Any linear code, E, with minimum distance $d = n - k$, is a kth order near-orthogonal code. Most efficient near-orthogonal linear codes will be discussed in the next section.

SECTION II

SOME MAXIMUM k^{th} ORDER NEAR-ORTHOGONAL CODES

Suppose E is a code of length n, and d is the minimum distance between any two code words of E. E is called a maximum error-correcting code if the code has exactly $n - d + 1$ information symbols. For a given minimum distance d, a maximum code, E, has the greatest possible number of words, namely, q^{n-d+1} words (see the generalized Plotkin bound due to Peterson, Theorem 4.3 of Reference [3].

Since the maximum number of overlaps of a code, E, is $k = n-d$, the <u>largest</u> k^{th} order near-orthogonal code is a maximum error-correcting code with exactly $k + 1$ information symbols. This maximum code has a dictionary size of q^{k+1} where q is the mth power of a prime number p.

Now restrict code E to be a linear code. Forney, in Section 2.3 of Reference [4] defines generalized Reed-Solomon (RS) codes and shows that every RS code is a maximum error-correction code. Therefore, the following theorem is true.

THEOREM 1

Every RS code, E, of length n, with minimum distance d, between code words is a maximum k^{th} order near-orthogonal code where $k = n - d$, i.e., E is the largest dictionary in which any two words overlap in no more than k places. Code E has exactly q^{k+1} elements where $q = p^m$ and p is a prime.

In the next section, we use this theorem to develop synchronizable k^{th} order near-orthogonal codes.

SECTION III

SYNCHRONIZABLE k^{th} ORDER NEAR-ORTHOGONAL CODES

We develope synchronizable codes from the polynominal codes of Reed and Solomon (see Reference [4] and [5], Section 2.3.4). Let the Galois field of the code be $GF(q) = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-2}, \alpha^{q-1} = 1\}$ where α is a generator of the field. Define the following set of basis vectors:

$$\begin{aligned}
\underline{e}_0 &= (1, 1, \ldots 1) \\
\underline{e}_1 &= (\alpha, \alpha^2, \ldots \alpha^{q-1}) \\
\underline{e}_2 &= (\alpha^2, \alpha^4, \ldots \alpha^{2(q-1)}) \\
&\vdots \\
\underline{e}_k &= (\alpha^k, \alpha^{2k}, \ldots \alpha^{k(q-1)}).
\end{aligned}$$

This set is easily shown to be a linearly-independent set of vectors by the properties of Vandermonde determinants. Let code E be the $k+1$-dimensional vector space

$$E = \left\{(x_0 \underline{e}_0 + x_1 \underline{e}_1 + \ldots x_k \underline{e}_k) \,\middle|\, x_0, x_1, \ldots x_k \in GF(q)\right\} .$$

Code E is an RS code with maximum distance $d = n-k$ (see Section 2.3.4 of Reference [4], where $n = q-1$. Hence, by Theorem 1, E is a maximum k^{th} order near-orthogonal code.

In order to develop a synchronizable code from E, define the following cyclic permutation ρ of an element $\underline{v} = (v_1, v_2, \ldots v_{q-1})$ of E as

$$\rho\ (v_1, v_2, \ldots v_{q-1}) = (v_2, v_3, \ldots v_{q-1}, v_1).$$

Consider now the action of the jth cyclic permutation ρ^j on an element $\underline{x} = x_0 \underline{e}_0 + x_1 \underline{e}_1 + \ldots x_k \underline{e}_k$ of E. Evidently,

$$\rho^j \underline{x} = x_0 \rho^j \underline{e}_0 + x_1 \rho^j \underline{e}_1 + \ldots x_k \rho^j \underline{e}_k. \qquad (1)$$

From this it is easy to see that the action of ρ^j on the basis vectors is as follows:

$$\begin{aligned} \rho^j \underline{e}_0 &= \underline{e}_0 \\ \rho^j \underline{e}_1 &= \alpha^j \underline{e}_1 \\ \rho^j \underline{e}_2 &= \alpha^{2j} \underline{e}_2 \\ \vdots \quad & \quad \vdots \\ \rho^k \underline{e}_k &= \alpha^{kj} \underline{e}_k \end{aligned} \qquad (2)$$

Thus Equation (1) becomes

$$\rho^j \underline{x} = x_0 \underline{e}_0 + \alpha^j x_1 \underline{e}_1 + \ldots \alpha^{kj} x_k \underline{e}_k,$$

which is an element of E for all $j = 1, 2, \ldots q-1$ and $\underline{x} \in E$.

Suppose $\underline{x}$ and $\underline{y}$ are elements of E. $\underline{x}$ is said to be ρ-equivalent to $\underline{x}$, written $\underline{x} \sim \underline{y}$, if there is an integer j such that $\underline{x} = \rho^j \underline{y}$. Obviously, ρ-equivalence is an equivalence relation which splits E into a disjoint class of sets, P, where the elements of each set are ρ-equivalent. If one chooses one element from each ρ-equivalent set of class P, and puts them in a set E', E' clearly has the property that the cyclic shifts of no two words of E' will overlap or correlate in more than k places. We have the following theorem.

THEOREM 2

If an E' is formed by picking a single element from each ρ-equivalent set, the cyclic shift of the words of E' overlap in no more than k-places. Code E' has

$$\frac{1}{q-1} \sum_{d \mid (q-1)} \phi(d)\, q^{1 + [k/d]}$$

elements where d is a divisor of q-1, ϕ (d) is the Euler ϕ function, and the symbol [x] denotes the greatest integer less than or equal to x.

To count the number of elements in E', we resort to Polya's counting formula in the form for a cyclic group (see Reference [6]). The number of ρ-equivalent classes in code E under the operations of the cyclic permutations group, $G = \{\rho, \rho^2 \ldots \rho^{q-1} = 1\}$ is

$$C = \frac{1}{q-1} \sum_{d \mid q-1} I(\rho^d)\, \phi\left(\frac{q-1}{d}\right)$$

where summation is over the divisors of (q-1), ϕ is Euler's function, and $I(\rho^d)$ is the number of elements of E left fixed by the cyclic permutation ρ^d of d steps. To evaluate $I(\rho^d)$, suppose $d \mid (q-1)$ and $\underline{x} = (x_0 \underline{e}_0 + x_{i_1} \underline{e}_{i_1} + \ldots x_{i_\ell} \underline{e}_{i_\ell})$ is an element of E left fixed by ρ^d, i.e. $\rho^d \underline{x} = \underline{x}$. By Equations (1) and (2), this is true if and only if i_j is a multiple of $(q-1)/d$, the order of group element ρ^d, for $j = 1, 2, \ldots \ell$. In other words, $\underline{x}$ is left fixed by ρ^d if and only if $\underline{x}$ lies in the subspace of E generated by basis vectors $\underline{e}_0, \underline{e}_{i_1}, \underline{e}_{i_2}, \ldots \underline{e}_{i_\ell}$ where i_j is a multiple

of $(q-1)/d$ for $j = 1, 2, \ldots, \ell$ and $1 \leq \ell \leq k$. But the number of integers $\leq k$ which are multiples of $q-1/d$ is given exactly by $[k/(q-1)/d] = [dk/(q-1)]$ where $[x]$ denotes the integer part of x. Thus, the number of elements in the subspace of E left fixed by ρ^d is given by $I(\rho^d) = q^{1+[dk/(q-1)]}$ and the theorem follows.

Now we wish to find a code with the following two properties: (1) the cyclic shift of two code words overlap in no more than k places, and (2) a code word coincides with a cyclic shift of the same code word in no more than k places. Note some further properties of cyclic shifts of a word in E. The period of $\underline{x} \in E$ under cyclic shift is the least integer m, such that $\rho^m \underline{x} = \underline{x}$. By Equation (2), the period of the basis vector $\underline{e}_j$ for $(j = 0, 1, \ldots, k)$ is the least integer m such that $(\alpha^j)^m = 1$. Thus, the period p_j of $\underline{e}_j$ is the same as the order of element $\alpha^j \in GF(q)$, and $p_j = q + 1/(j, q-1)$ where $(j, q-1)$ denotes the greatest common divisor of integers j and $q-1$. If $\underline{x} \in E$, it can be represented uniquely in the form $\underline{x} = \underline{x}_{i_1} \underline{e}_{i_1} + x_{i_2} \underline{e}_{i_2} + \ldots x_{i_\ell}$ where $0 \leq i_1 < i_2 < \ldots i_\ell \leq k$, $x_{i_j} \neq 0$ and $x_{i_j} \in GF(q)$ for $(j = 1, 2, \ldots \ell)$. If $\underline{x}$ has the latter form, by Equations (1) and (2) and the above facts, the period of $\underline{x}$ is the least common multiple of the periods of $\underline{e}_{i_1}$, $\underline{e}_{i_2}, \ldots \underline{e}_{i_n}$, namely, $[p_{i_1}, p_{i_2}, \ldots p_{i_\ell}]$, where $p_{i_j} = q-1/(i_j, q-1)$ for $(j = 1, 2, \ldots, \ell)$.

Now consider the set

$$E_1 = \{\underline{x} \in E \mid \underline{x} \text{ has least period } q-1\}$$

Since $E_1 \subset E$, E_1 is still a kth order near-orthogonal code. However, if

is no longer a linear vector space. Note again that if $\underline{x} \in E_1$, that $\rho^j \underline{x} \in E_1$. Thus, ρ-equivalence will split E_1 in a disjoint class P_1 of ρ-equivalent sets. If one again forms a set E'_1 in exactly the same manner in which E' was formed from E, we have the following theorem.

THEOREM 3

Let E'_1 be formed from E_1 by choosing one element from each ρ-equivalent set. E'_1 has the property that the cyclic shifts of any two elements overlap in no more than k places. Code E'_1 also has the property that the cyclic shift, say, $\rho^j \underline{x}$ of an element $\underline{x}$, coincides with $\underline{x}$ in no more than k places. The number of elements in E'_1 is at least $[q^{k+1} - q^{\tau(k, q-1)}] / (q-1)$ where $\tau(k, q-1)$ is the number of integers, less than $k+1$, which are not relatively prime to $q-1$.

Code E'_1 is the synchronizable k^{th} order near-orthogonal code we have been seeking. The theorem will be proved when the lower bound on the number of elements in E'_1 is established. Consider another subset, E_2 of E_1, also with the property that all vectors of E_2 have least period $q-1$. In particular, let E_2 be any linear combination of basis vectors in E which includes at least one basis vector of period $q-1$. Evidently, E_2 is a subset of E_1. The number of elements in E_2 is the number of elements in E minus the number of elements in the vector space generated by all basis vectors which have period less than $q-1$. The number of such basis vectors is exactly the number $\tau(k, q-1)$ of integers less than $k+1$ which are not relatively prime to $q-1$. Now form a set E'_2 from E_2, exactly in the manner E'_1 was formed from E_1. Clearly, $E'_2 \subset E'_1$ and the number of elements in E'_2 is the number of

elements in E_2 divided by the number of possible cyclic shifts, $q-1$. Evidently Theorem 3 is true.

Now associate each code word of E'_2 with a frequency-time (FT) waveform. Let each Galois field symbol correspond with a pulse of different frequency and let each vector coordinate of a code word be associated with a time slot (pulse time). The set of such FT waveforms corresponding to code E'_1 have the following two desirable properties from the standpoint of waveform design:

1. Each word has an autocorrelation function with bounded sidelobes less than the energy of k pulses.
2. The cross-correlation of any two waveforms under different time delays or translations is always less than the energy of k pulses.

If the frequency bands, which correspond to the Galois field symbols, are contiguous, it is evident that the energy of each FT waveform is spread fairly uniformly over the band it occupies. This fact is important in spread spectrum applications.

REFERENCES

1. I.S. Reed and H. Blasbalg, Multipath Tolerant Ranging and Data Transfer Techniques for Air-To-Ground and Ground-To-Air Links, Proc. of IEEE, 38, 1, (1970), 422-430.

2. E.N. Gilbert, Cyclically Permutable Error-Correcting Codes, IEEE Trans on Info Theory, IT-9, 3 (1963).

3. W.W. Peterson, Error-Correcting Codes, MIT Press, and John Wiley and Sons, Inc., (1961).

4. G.D. Forney, Jr., Concatenated Codes, MIT Press, (1966).

5. I.S. Reed and G. Solomon, Polynomial Codes Over Certain Finite Fields, J.Soc. Indust. Appl. Math., 6, 2, (1960).

6. S. Golomb, A Mathmatical Theory of Discrete Classification, Information Theory, Fourth London Symposium, 1960, Butterworths, 88 Kingsway, London, (1961).

UNCLASSIFIED
Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)* The MITRE Corporation Bedford, Massachusetts 01730	2a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED 2b. GROUP

3. REPORT TITLE

Kth ORDER NEAR-ORTHOGONAL CODES

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*

5. AUTHOR(S) *(First name, middle initial, last name)*

Irving S. Reed

6. REPORT DATE MARCH 1971	7a. TOTAL NO. OF PAGES 15	7b. NO. OF REFS 6
8a. CONTRACT OR GRANT NO. F19(628)-68-C-0365 b. PROJECT NO. 600G c. d.	9a. ORIGINATOR'S REPORT NUMBER(S) ESD-TR-71-78 9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)* MTP-115	

10. DISTRIBUTION STATEMENT

This document has been approved for public release and sale; its distribution is unlimited.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY Electronic Systems Division, Air Force Systems Command, L. G. Hanscom Field, Bedford, Massachusetts

13. ABSTRACT

Certain near-orthogonal codes have recently been used in multiple-short keying communication systems. The codes generally considered for this application are the first order Reed-Solomon (RS) codes. The purpose of this paper is to extend this class of codes. It is shown that codes can be developed with the property that no two members of the code overlap in more than k frequency-time slots. It is also shown that certain subsets of these codes are synchronizable. The optimum k^{th} order near-orthogonal synchronizable codes are certain subsets of RS codes with a maximum distance $d = n-k$, where n is the number of code symbols.

DD FORM 1 NOV 65 1473

UNCLASSIFIED
Security Classification

UNCLASSIFIED
Security Classification

14. KEY WORDS	LINK A ROLE	LINK A WT	LINK B ROLE	LINK B WT	LINK C ROLE	LINK C WT
CODING THEORY						
COMMUNICATIONS SYSTEMS						
DATA TRANSMISSION						
FREQUENCY SHIFT KEYING (FSK)						
KTH ORDER NEAR-ORTHOGONAL CODES						
MULTIPLE-SHIFT KEYING						
NEAR-ORTHOGONAL CODES						
REED-SOLOMON (RS) CODES						
SYNCHRONIZABLE CODES						
TELECOMMUNICATIONS						

UNCLASSIFIED
Security Classification