REPORT R-440 OCTOBER 1969

CSL COORDINATED SCIENCE LABORATORY

ON A ROOT-DISTANCE RELATION FOR ARITHMETIC CODES

R. T. CHIEN
S. J. HONG

UNIVERSITY OF ILLINOIS – URBANA, ILLINOIS

ON A ROOT-DISTANCE RELATION FOR ARITHMETIC CODES

R. T. Chien and S. J. Hong
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois

This work was supported in part by the Joint Services Electronics Program (U.S. Army, U.S. Navy, and U.S. Air Force) under Contract DAAB-07-67-C-0199, and in part by the National Science Foundation under Grant No. GK-2339.

Other CSL Reports in Information Science include:

☐ 1. Kasami, Tadao, "An Efficient Recognition and Syntax-Analysis Algorithm for Context-Free Languages," March, 1966, R-257.

☐ 2. Barrows, J. T., Jr., "A Topological Technique for Analysis of Active Networks," August, 1965, R-266.

☐ 3. Barrows, J. T., Jr., "A New Method for Constructing Multiple Error Correcting Linear Residue Codes," January, 1966, R-277.

☐ 4. Lum, Vincent, "A Theorem on the Minimum Distance of BCH Codes over GF(q)," March, 1966, R-281.

☐ 5. Preparata, Franco P., "Convolutional Transformations of Binary Sequences: Boolean Functions and Their Resynchronizing Properties," March, 1966, R-283.

☐ 6. Kasami, Tadao, "Weight Distribution Formula for Some Class of Cyclic Codes," April, 1966, R-285.

☐ 7. Kasami, Tadao, "A Note on Computing Time for Recognition of Languages Generated by Linear Grammars," April, 1966, R-287.

☐ 8. Lum, Vincent, "On Bose-Chaudhuri-Hocquenghem Codes over GF(q)," July, 1966, R-306.

☐ 9. Bahl, Lalit Rai, "Matrix Switches and Error Correcting Codes from Block Designs," August, 1966, Thesis, R-314.

☐ 10. Kasami, Tadao, "Weight Distributions of Bose-Chaudhuri-Hocquenghem Codes," August, 1966, Thesis, R-317.

☐ 11. Preparata, F. P., Metze, G., and Chien, R. T., "On the Connection Assignment Problem of Diagnosable Systems," October, 1966, R-322.

☐ 12. Chien, R. T. and Preparata, F. P., "Topological Structures of Information Retrieval Systems," October, 1966, R-325.

☐ 13. Heller, James Ernest, "Decoding Procedures for Convolutional Codes," November, 1966, R-327.

☐ 14. Lum, Vincent and Chien, R. T., "On the Minimum Distance of Bose-Chaudhuri-Hocquenghem Codes," November, 1966, R-328.

CSL Reports (continued)

☐ 15. Hsu, Hsung Tsao, "Error Correcting Codes for Compound Channels," December, 1966, R-331.

☐ 16. Hong, Se June, "On Minimum Distance of Multiple Error Correcting Arithmetic Codes," January, 1967, R-336.

☐ 17. Gaddess, Terry G., "A Study of an Error Detecting Parallel Adder," January, 1967, M.S. Thesis, R-337.

☐ 18. Preparata, Franco P., "Binary Sequence Convolutional Mapping: The Channel Capacity of a Non-Feedback Decoding Scheme, March, 1967, R-345.

☐ 19. Preparata, F. P. and Chien, R. T., "On Clustering Techniques of Citation Graphs," May, 1967, R-349.

☐ 20. Lipovski, Gerald J., "Compatibility and Row-Column Minimization of Sequential Machines," May, 1967, R-355.

☐ 21. Lipovski, Gerald J., "An Improved Method of Finding all Largest Combinable Classes," August, 1967, R-362.

☐ 22. Chow, David K., "A Geometric Approach to Coding Theory with Application to Information Retrieval," October, 1967, R-368.

☐ 23. Tracey, Robert J., "Lattice Coding for Continuous Channels," December, 1967, R-371.

☐ 24. Preparata, Franco P., "A Study of Nordstrom-Robinson Optimum Code," April, 1968, R-375.

☐ 25. Preparata, Franco P., "A Class of Optimum Nonlinear Double-Error-Correcting Codes," July, 1968, R-389.

☐ 26. Kisylia, Andrew Philip, "An Associative Processor for Information Retrieval," August, 1968, R-390.

☐ 27. Beach, Edward J., "A Study of a Feedback Time-Sharing System," September, 1968, R-391.

☐ 28. Weston, P., and Taylor, S. M., "Cylinders: A Data Structure Concept Based on Rings," September, 1968, R-393.

☐ 29. Bahl, Lalit Rai, "Correction of Single and Multiple Bursts of Error," October, 1968, R-397.

CSL Reports (continued)

☐ 30. Carroll, D. E., Chien, R. T., Kelley, K. C., Preparata, F. P., Reynolds, P., Ray, S. R. and Stahl, F. A., "An Interactive Document Retrieval System," December, 1968, R-398.

☐ 31. Biss, Kenneth, "Syntactic Analysis for the R2 System," December, 1968, R-399.

☐ 32. Tzeng, Kenneth Kai Ming, "On Iterative Decoding of BCH Codes and Decoding Beyond the BCH Bound," January, 1969, R-404.

☐ 33. Kelley, K. C., Ray, S. R. and Stahl, F. A., "ISL-A String Manipulating Language," February, 1969, R-407.

☐ 34. Lombardi, Daniel Joseph, "Context Modeling in a Cognitive Memory," February, 1969, R-408.

☐ 35. Chien, R. T., Hong, S. J. and Preparata, F. P., "Some Results in the Theory of Arithmetic Codes," May, 1969, R-417.

☐ 36. Hong, Se June, "On Bounds and Implementation of Arithmetic Codes," October, 1969, R-437.

☐ 37. Chien, R. T. and Hong, S. J., "Error Correction in High Speed Arithmetic," October, 1969, R-438.

For copies of these reports please complete this form and send to

Professor R. T. Chien
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois 61801

My name and address is ______________________________

____

____

____

ON A ROOT-DISTANCE RELATION FOR ARITHMETIC CODES

Arithmetic codes are of the form AN where A is a fixed integer called the generator and N = 0, 1, ..., B-1. B is the number of code words. An error pattern E is called t-fold if the arithmetic weight of E is t, that is at least t non-zero (± 1) coefficients are needed to express E in modified binary form allowing ± 1 or 0 as valid coefficients. The arithmetic distance between two integers I_1 and I_2 is defined as the arithmetic weight $W(|I_1-I_2|)$. It is well known that this distance function is metric and the minimum distance of an AN code is the weight of the minimum weight nonzero codeword. The arithmetic code corrects errors up to t if the minimum distance, $d_m \geq 2t+1$. The parallelism between arithmetic codes and polynomial codes does not end here. The complete analogy between single error correcting Brown codes [1] and single error correcting Hamming codes, and many other similarities have been observed and summarized by Massey in 1964 [2].

In 1966, Barrows [3] and Mandelbaum [4] simultaneously discovered a class of multiple error correcting arithmetic codes. These codes are since generalized by Chien, Hong and Preparata [5,6] and Chang and Tsao-Wu [7] to include a larger spectrum of codes between the two extremes. Brown codes are analogous to Hamming Codes and Barrows-Mandelbaum codes are analogous to maximal Length-Sequence Codes [8]. These codes have the form $A = (2^e-1)/B$ where e is the exponent of 2 modulo B. When B has 2 as its primitive root, the minimum distance becomes $dm = [\frac{B+1}{3}]$, which was first proven by Barrows [3]. For the composite B's the minimum distance is to be found by the procedures described by Chien, Hong and Preparata [6].

The fact that these codes are cyclic immediately poses a question, what is the analogy between these codes and cyclic polynomial codes such as BCH codes [8]? We answer this question with a conjecture on the root-distance relationship in arithmetic codes. First, notice that $AB = 2^n-1$ for some n which is the length of the code. To be an error correcting code ($d_m \geq 3$), it is well known that the exponent of 2 modulo A must be n. A BCH code has generator g(x) for which the exponent of x modulo g(x) equals n, the code length. The BCH theorem states that the minimum distance generated by g(x) is $d_m >$ the number of consecutive roots of g(x).

Now we look at the roots of X^n-1 in the complex field. A primitive n^{th} root of unity in this case would be $\alpha = e^{\frac{2\pi}{n}i}$. We have

$$X^n-1 = \prod_{i=1}^{n} (x-\alpha^i) \qquad (1)$$

A cyclotomic polynomial Qh(x) is defined as

$$Q_h(x) = \prod_{(i,h)=1} (x-\beta^i) \qquad (2)$$

where β is a primitive h th root of unity. It is well known [see for instance Ref. 9] that a cyclotomic polynomial has all integer coefficients and

$$X^n-1 = \prod_{h|n} Q_h(x) \qquad (3)$$

Hence for all $h|x$, $Q_h(x)$'s are unrepeated factors of X^n-1. Each $Q_h(x)$ contains a set of disjoint n^{th} roots of unity as its roots, i.e.,

$$Q_h(x) = \prod_{i \in I_h} (x-\alpha^i) \qquad (4)$$

where
$$I_n = \{ i \mid 1 \leq i \leq n,\ (i,n) = \tfrac{n}{h} \} \qquad (5)$$

As we replace x with 2 in the above equations, we have $A_n = Q_h(2) = \prod_{i \in I_h} (2-\alpha^i)$, the integer factors of 2^n-1. Each A_h may or may not be a prime, but has a definite relation with the n^{th} roots of unity given by Eq. (5). Any further decomposition of A_h preserving the root relationship is impossible because $Q_h(x)$ is always irreducible in the field of rationals [10].

Table 1. A_h

Q_h	A_h	h	A_h	h	A_h	h	A_h
1	1	7	127	13	8191	20	5·41
2	3	8	17	14	43	21	7·337
3	7	9	73	15	151	22	683
4	5	10	11	16	257	24	241
5	31	11	23·89	17	131071	30	331
6	3	12	13	18	3·19	36	37·109

Dickson [11] has shown that $A_h \neq A_k$ for all $h \neq k$ except $A_2 = A_6 = 3$ and that every A_h (except A_6) has the exponent of 2 modulo A_h equal to h. Now for given A a divisor of 2^n-1, we find the number of <u>positively consecutive roots</u> as follows. First, choose only those A_h's in A which are clearly the A_h, and then count the number of the longest consecutive roots using Eq. (5). This is best illustrated by an example: n = 18 has A_2, A_3, A_6, A_9 and A_{18}. Among them, ambiguous A_h's are $A_2 = A_3 = 3$ and $A_{18} = 3 \cdot 19$.

roots:	α^i; i=	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Factors:	A_h=	3·19	73	3	73	3·19	7	3·19	73	3	73	3·19	7	3·19	73	3	73	3·19

$A = 3 \cdot 19 \cdot 73$ → positive factors $\{73\}$ → 1 consecutive roots

$A = 3^3 \cdot 19 \cdot 7$ → positive factors $\{3, 3, 3 \cdot 19, 7\}$ → 3 consecutive roots

$A = 19 \cdot 73$ → positive factors $\{73\}$ → 1 consecutive root

<u>Conjecture</u>: If A has d positively consecutive roots, $d_m(A) \geq d+1$.

We define <u>weakly consecutive roots</u> of A as the following. In case some A_k divides A_h and $A_k \neq A_h$, the factor of A_h is recognized as A_h even in the absence of A_k. Again the illustration with n = 18;

$A = 3 \cdot 19 \cdot 73$ → weak factors $\{3 \cdot 19, 73\}$ → 2 consecutive roots

$A = 3^2 \cdot 73$ → weak factors $\{3, 3, 73\}$ → 3 consecutive roots

$A = 3 \cdot 3 \cdot 19$ → weak factors $\{3 \cdot 19\}$ → 1 consecutive root

It is empirically discovered that if A has d weakly consecutive roots, $dm \geq d+1$ for all A's up to length n = 36 with only two exceptions. (See the * entry in the table 2) Table 2 shows the exhaustive proof of the above statement. This is achieved by listing all possible A's of different weakly consecutive roots without any superflows non-recognized factors. If any A has non-recognized factors, obviously $d_m(A) \geq d_m(A')$

where A' is without those non-recognized factors (Example $A = 3\cdot 3\cdot 19$, $A' = 3\cdot 19$). Also, for a given A, one can easily verify that the number of positively consecutive roots is less than or equal to the number of weakly consecutive roots. Hence, table 2 also provides an empirical proof for the conjecture except for the two starred exceptions. The proof for these two cases are as follows.

(1) $n = 20$, $A = 3\cdot 31\cdot 5^2\cdot 41$ has 7 positively consecutive roots and the actual $d_m = 8 = 7+1$.

(2) $n = 36$, $A = 3^3\cdot 5\cdot 73\cdot 37\cdot 109$ has 6 positively consecutive roots and the actual $d_m = 8 > 6+1$.

The actual d_m's in the following table was obtained by the method described in [6].

Table 2

n	A	B	weak d+1	actual dm
8	5·17	3	4	4
	3·17	5	4	4
9	73	7	3	3
10	3·31	11	4	4
	11·31	3	5	5
12	3·3·5	7·13	3	3
	5·7	3·3·13	3	3
	7·13	3·3·5	3	3
	3·3·13	5·7	4	4
	3·3·5·7	13	4	4
	5·7·13	3·3	4	4
14	3·127	43	4	4
	43·127	3	7	7
15	151	7·31	3	3
	7·31	151	3	4
	31·151	7	5	5
16	3·257	5·17	4	4
	5·257	51	4	4
	17·257	3·5	4	4
	3·17·257	5	8	8
	5·17·257	3	8	8

Table 2 (continued)

n	A	B	weak d+1	actual d_m
18	3·19·73	3·3·7	3	3
	3·3·73	7·3·19	4	4
	7·3·19	3·3·73	4	4
	3·3·3·19·73	7	6	6
	7·3·19·73	3·3	6	6
	3·3·3·19·7	73	6	8
20	5·31	3·11·5·41	3	3
	5·11	3·31·5·41	3	3
	11·5·41	5·3·31	4	4
	31·5·41	5·3·11	4	4
	3·5·41	5·11·31	4	4
	5·11·31	3·5·41	4	4
	11·31·5·41	3·5	5	5
	3·31·5·41	5·11	8*	6
	5·11·31·5·41	3	10	10
	3·11·31·5·41	5	10	10
21	7·337	7·127	3	3
	7·127	7·337	3	4
	127·7·337	7	7	7
22	3·23·89	683	4	4
	23·89·683	3	11	11
24	13·241	3·3·5·7·17	3	3
	13·17	3·3·5·7·241	3	3
	3·3·17	5·7·13·241	3	3
	7·241	3·3·5·13·17	3	3
	7·17	3·3·5·13·241	3	3
	5·241	3·3·13·7·17	4	4
	3·3·241	5·13·7·17	4	4
	13·17·241	3·3·5·7	4	4
	7·17·241	3·3·5·13	4	4
	7·13·17	3·3·5·241	4	4
	5·7·241	3·3·13·17	5	5
	3·3·5·241	7·13·17	5	5
	3·3·13·241	5·7·17	6	6
	5·7·17·241	3·3·13	6	6
	7·13·17·241	3·3·5	6	6
	3·3·13·17·241	5·7	8	8
	3·3·5·7·17·241	13	8	8
	5·7·17·13·241	3·3	8	8
	3·3·7·13·17·241	5	12	12
25	601·1801	31	4	4
26	3·8191	2731	4	4
27	7·262567	73	6	6
	73·262567	7	9	9
28	5·43	3·127·29·113	3	3
	5·127	3·43·29·113	3	3
	43·29·113	3·5·127	4	4
	127·29·113	3·5·43	4	4

n	A	B	weak d+1	actual d_m
	5·43·127	3·29·113	4	4
	3·29·113	5·43·127	4	4
	43·127·29·113	3·5	7	7
	Rest*	3	14	14
	Rest	5	14	14
30	331·151	3·3·11·7·31	3	3
	3·3·31	7·151·11·331	3	3
	7·11	9·31·151·331	3	3
	7·331	9·11·31·151	3	3
	3·3·151	7·11·31·331	4	4
	11·151	7·9·31·331	4	4
	31·331	7·9·11·151	4	4
	7·11·151	9·31·331	4	4
	7·11·331	9·31·151	4	4
	11·151·331	7·9·31	5	5
	7·31·331	9·11·151	5	6
	31·151·331	9·7·11	5	5
	3·3·31·151·11	7·331	6	6
	7·11·151·331	9·31	6	6
	7·11·31·331	9·151	6	7
	7·31·151·331	9·11	6	6
	3·3·151·331	7·11·31	6	6
	11·7·31·151·331	9	10	10
	3·3·31·151·331	7·11	10	10
	Rest	11	12	12
32	257·65537	3·5·17	4	4
	17·65537	3·5·257	4	4
	5·65537	3·17·257	4	4
	3·65537	5·17·257	4	4
	17·257·65537	3·5	8	8
	5·257·65537	3·17	8	8
	3·257·65537	5·17	8	8
	Rest	3	16	16
	Rest	5	16	16
33	599497	7·23·89	3	3
	7·23·89	599479	3	4
	Rest	7	11	11
34	3·131071	43691	4	4
	Rest	3	17	17
35	31·127	71·122921	3	4
	31·71·122921	127	5	5
	127·71·122921	7	7	7
36	37·109·3·19	5·7·3·3·13·73	3	3
	13·3·19	3·3·7·5·73·37·109	3	3
	13·73	5·3·3·7·3·19·37·109	3	4
	73·37·109	3·3·7·3·19·5·13	3	3
	5·73	3·3·7·3·19·13·37·109	3	3
	5·3·19	3·3·7·73·13·37·109	3	3
	3·19·13·37·109	3·3·7·5·73	4	4
	3·19·13·73	3·3·7·5·37·109	4	4

*"Rest" means $A = (2^n-1)/B$, i.e., all other factors

Table 2 (continued)

n	A	B	weak d+1	actual d_m
36	13·73·37·109	3·3·7·5·3	4	4
	3·3·37·109	5·13·7·73·3·19	4	4
	5·73·37·109	3·3·7·3·19·13	4	4
	5·3·19·73	3·3·7·13·37·109	4	4
	5·3·19·37·109	3·3·7·13·73	4	4
	7·37·109	3·3·5·13·3·19·73	4	4
	3·19·13·73·37·109	3·3·7·5	6	6
	3·3·73·37·109	7·3·19·5·13	6	6
	5·3·19·73·37·109	3·3·7·13	6	6
	7·3·19·37·109	3·3·73·5·13	6	6
	3·3·5·73·37·109	3·19·7·13	7*	6
	5·7·3·19·37·109	3·3·73·13	7	8
	13·7·3·19·37·109	3·3·5·73	7	8
	5·7·13·3·19·37·109	3·3·73	8	8
	3·3·73·13·37·109	5·7·3·19	8	8
	Rest	7·13	9	9
	Rest	3·3·13	9	9
	Rest	3·3·5	9	9
	Rest	5·7	12	12
	Rest	3·3	12	12
	Rest	5	18	18

We now prove the conjecture for a special case of two adjacent roots which should give actual $d_m \geq 3$. First a well known lemma.

Lemma 1 For code length n, $d_m(A) \geq 3$ if $e(A) = n$ and $2^{e/2}+1 \not\equiv 0 \mod A$.

Lemma 2 (See [11]) $e(A_h) = h$ except $h = 6$.

Theorem 1 If A clearly contains two weakly consecutive roots of unity, then $d_m(A) \geq 3$.

Proof Case 1) A is composed of a single A_h, i.e., $A = A_h$ for some h.

From the adjacency we have

$$\left.\begin{aligned} (i,n) &= \frac{n}{h} \\ (i+1,n) &= \frac{n}{h} \end{aligned}\right\} \quad \text{Can happen only if } h = n = \text{odd}$$

By lemmas 1 and 2, the theorem is true.

Case 2) A is composed of A_{h_1} and A_{h_2} each contributing one root and perhaps some unrecognized factors, ie, $A = A_{h_1} \cdot A_{h_2} \cdot C$. From the adjacency we have,

$$\left.\begin{array}{r}(i,n) = \dfrac{n}{h_1} \\ \\ (i+1,n) = \dfrac{n}{h_2}\end{array}\right\} \rightarrow \left(\frac{n}{h_1}, \frac{n}{h_2}\right) = 1 \rightarrow LCM(h_1,h_2) = n$$

But $e(A_{h_1} \cdot A_{h_2})$ is divisible by

$$LCM(e(Ah_1), e(A_{h_2})) = LCM(h_1,h_2) = n$$

Thus $e(A)|n$ and $n|e(A)$, resulting $e(A) = n$. If n is odd the theorem follows. If n is even, $(2^n-1) = (2^{n/2}-1)(2^{n/2}+1)$; and every odd root is from $2^{n/2}+1$ and every even root is from $2^{n/2}-1$. Hence A_{h_1} and A_{h_2} can not both divide $2^{2/n}+1$ for $(2^{n/2}-1)$ and $(2^{n/2}+1)$ are relatively prime.

Q.E.D.

Unfortunately, this theorem does not lend itself for a generalization. For a general proof, the method introduced by Pierce [12] and the study on the coefficients of the cyclotonic polynomials by Lehmer [13] will be of invaluable help.

Mandelbaum [4] shows a simple extension of these codes as the following. If $e(B) = n$ and $A = (2^n-1)/B$ gives minimum distance d_m over the codelength n, then $A' = (2^{kn}-1)/B$ gives minimum distance kd_m over the code length kn. The conjecture we have shown is entirely compatible with this theorem. Consider n^{th} roots of unity occupied by B. There must be at least d_m-1 length gap which is equivalent to a gap of kd_m-1 in kn th roots of unity. Hence, by the conjecture the new minimum distance is kd_m.

From the empirical evidence and some facts we presented here, we conclude that the conjecture is very strong. For all practical purposes, now we can synthesize codes of given length and minimum distance by a simple root-distance relation. This gives the strong relation between the arithmetic code and the BCH code. The decoding technique using this approach should be the subject of further research.

References

[1] D. T. Brown, "Error Detecting and Correcting Binary Codes for Arithmetic Operations," IRE Trans. Vol. EC-9, 1960; pp. 333-337.

[2] J. L. Massey, "Survey of Residue Coding for Arithmetic Errors," International Computation Center Bulletin, UNESCO, Rome, Italy, Vol. 3, No. 4, Oct. 1964; pp. 195-209.

[3] J. T. Barrows, Jr., "A New Method for Constructing Multiple Error Correcting Linear Residue Codes," Report R-277, Coordinated Science Laboratory, Urbana, Illinois, January, 1966.

[4] D. Mandelbaum, "Arithmetic Codes with Large Distance," IEEE Trans. on Information Theory, Vol. IT-13, No. 2, April, 1967.

[5] R. T. Chien, S. J. Hong and F. P. Preparata, "Some Contribution to the Theory of Arithmetic Codes," Proceedings of the First Annual Hawaii International Conference on Systems Sciences, January, 1968.

[6] R. T. Chien, S. J. Hong and F. P. Preparata,"Some Results in the Theory of Arithmetic Codes," Submitted for publication in Information and Control, Report R-417, Coordinated Science Laboratory, Urbana, Illinois, May, 1969.

[7] S. H. Chang and N. T. Tsao-Wu, "Discussion on Arithmetic Codes with Large Distance," IEEE PGIT-14, January, 1968.

[8] W. W. Peterson, *Error Correcting Codes*, The MIT Press, Cambridge, Mass., 3rd Ed., July, 1965.

[9] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw Hill Book Company, New York, 1968; pp. 87-118.

[10] Van del Waerden, *Modern Algebra*, 3rd printing, Frederick Ungar Publishing Company, New York, 1964, pp. 111-115.

[11] L. E. Dickson, "On the Cyclotomic Function," American Math. Monthly, Vol. 12, 1905, pp. 86-89.

[12] T. A. Pierce, "The Numerical Factors of the Arithmetic Forms, $\pi(1+\alpha_i^m)$," Annals of Math., Vol. 18, Series 2, 1916, pp. 53-64.

[13] E. Lehmer, "On the Magnitude of the Coefficients of the Cyclotomic Polynomial," Bull. Am. Math. Soc., Vol. 42, 1936, pp. 389-392.

Distribution List as of 1 October, 1969

Dr A.A. Dougal
Asst Director (Research)
Ofc of Defense Res & Eng
Department of Defense
Washington, D.C. 20301

Office of Deputy Director
(Research and Information, Rm 3D1037)
Department of Defense
The Pentagon
Washington, D.C. 20301

Director, Advanced Research Projects
Agency
Department of Defense
Washington, D.C. 20301

Director for Materials Sciences
Advanced Research Projects Agency
Department of Defense
Washington, D.C. 20301

Headquarters
Defense Communications Agency (340)
Washington, D.C. 20305

Defense Documentation Center
Attn: DDC-TCA
Cameron Station
Alexandria, Virginia 22314 (50 Copies)

Director
National Security Agency
Attn: TDL
Fort George G. Meade, Maryland 20755

Weapons Systems Evaluation Group
Attn: Colonel Blaine O. Vogt
400 Army-Navy Drive
Arlington, Virginia 22202

Central Intelligence Agency
Attn: OCR/DD Publications
Washington, D.C. 20505

Hq USAF (AFRDD)
The Pentagon
Washington, D.C. 20330

Hq USAF (AFRDDG)
The Pentagon
Washington, D.C. 20330

Hq USAF (AFRDSD)
The Pentagon
Washington, D.C. 20330

Colonel E.P. Gaines, Jr.
ACDA/FO
1901 Pennsylvania Ave N.W.
Washington, D.C. 20451

Lt Col R.B. Kalisch (SREE)
Chief, Electronics Division
Directorate of Engineering Sciences
Air Force Office of Scientific Research
Arlington, Virginia 22209

Dr I.R. Mirman
AFSC (SCT)
Andrews Air Force Base, Maryland 20331

AFSC (SCTSE)
Andrews Air Force Base, Maryland 20331

Mr Morton M. Pavane, Chief
AFSC Scientific and Technical Liaison Office
26 Federal Plaza, Suite 1313
New York, New York 10007

Rome Air Development Center
Attn: Documents Library (EMTLD)
Griffiss Air Force Base, New York 13440

Mr H.E. Webb (EMMIIS)
Rome Air Development Center
Griffiss Air Force Base, New York 13440

Dr L.M. Hollingsworth
AFCRL (CRN)
L.G. Hanscom Field
Bedford, Massachusetts 01730

AFCRL (CRMPLR), Stop 29
AFCRL Research Library
L.G. Hanscom Field
Bedford, Massachusetts 01730

Hq ESD (ESTI)
L.G. Hanscom Field
Bedford, Massachusetts 01730 (2 copies)

Professor J. J. D'Azzo
Dept of Electrical Engineering
Air Force Institute of Technology
Wright-Patterson AFB, Ohio 45433

Dr H.V. Noble (CAVT)
Air Force Avionics Laboratory
Wright-Patterson AFB, Ohio 45433

Director
Air Force Avionics Laboratory
Wright-Patterson AFB, Ohio 45433

AFAL (AVTA/R.D. Larson
Wright-Patterson AFB, Ohio 45433

Director of Faculty Research
Department of the Air Force
U.S. Air Force Academy
Colorado Springs, Colorado 80840

Academy Library (DFSLB)
USAF Academy
Colorado Springs, Colorado 80840

Director
Aerospace Mechanics Division
Frank J. Seiler Research Laboratory (OAR)
USAF Academy
Colorado Springs Colorado 80840

Director, USAF PROJECT RAND
Via: Air Force Liaison Office
The RAND Corporation
Attn: Library D
1700 Main Street
Santa Monica, California 90045

Hq SAMSO (SMTTA/Lt Nelson)
AF Unit Post Office
Los Angeles, California 90045

Det 6, Hq OAR
Air Force Unit Post Office
Los Angeles, California 90045

AUL3T-9663
Maxwell AFB, Alabama 36112

AFETR Technical Library
(ETV,MU-135)
Patrick AFB,Florida 32925

ADTC (ADBPS-12)
Eglin AFB, Florida 32542

Mr B.R. Locke
Technical Adviser, Requirements
USAF Security Service
Kelly Air Force Base, Texas 78241

Hq AMD (AMR)
Brooks AFB, Texas 78235

USAFSAM (SMKOR)
Brooks AFB, Texas 78235

Commanding General
Attn: STEWS-RE-L, Technical Library
White Sands Missile Range
New Mexico 88002 (2 copies)

Hq AEDC (AETS)
Attn: Library/Documents
Arnold AFS, Tennessee 37389

European Office of Aerospace Research
APO New York 09667

Phsical & Engineering Sciences Division
U.S. Army Research Office
3045 Columbia Pike
Arlington, Virginia 22204

Commanding General
U.S. Army Security Agency
Attn: IARD-T
Arlington Hall Station
Arlington, Virginia 22212

Commanding General
U.S. Army Materiel Command
Attn: AMCRD-TP
Washington, D.C. 20315

Technical Director (SMUFA-A2000-107-1)
Frankford Arsenal
Philadelphia, Pennsylvania 19137

Redstone Scientific Information Center
Attn: Chief, Document Section
U.S. Army Missile Command
Redstone Arsenal, Alabama 35809

Commanding General
U.S. Army Missile Command
Attn: AMSMI-REX
Redstone Arsenal, Alabama 35809

Commanding General
U.S. Army Strategic Communications Command
Attn: SCC-CG-SAE
Fort Huachuca, Arizona 85613

Commanding Officer
Army Materials and Mechanics Res. Center
Attn: Dr H. Priest
Watertown Arsenal
Watertown, Massachusetts 02172

Commandant
U.S. Army Air Defense School
Attn: Missile Science Division, C&S Dept
P.O. Box 9390
Fort Bliss, Texas 79916

Commandant
U.S. Army Command & General Staff College
Attn: Acquisitions, Library Division
Fort Leavenworth, Kansas 66027

Commanding Officer
U.S. Army Electronics R&D Activity
White Sands Missile Range, New Mexico 88002

Mr Norman J. Field, AMSEL-RD-S
Chief, Office of Science & Technology
Research and Development Directorate
U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Commanding Officer
Harry Diamond Laboratories
Attn: Dr Berthold Altman (AMXDO-TI)
Connecticut Avenue and Van Ness St N.W.
Washington, D.C. 20438

Director
Walter Reed Army Institute of Research
Walter Reed Army Medical Center
Washington, D.C. 20012

Commanding Officer (AMXRD-BAT)
U.S. Army Ballistics Research Laboratory
Aberdeen Proving Ground
Aberdeen, Maryland 21005

Technical Director
U.S. Army Limited War Laboratory
Aberdeen Proving Ground
Aberdeen, Maryland 21005

Commanding Officer
Human Engineering Laboratories
Aberdeen Proving Ground
Aberdeen, Maryland 21005

U.S. Army Munitions Command
Attn: Science & Technology Br. Bldg 59
Picatinny Arsenal, SMUPA-VA6
Dover, New Jersey 07801

U.S. Army Mobility Equipment Research
and Development Center
Attn: Technical Document Center, Bldg 315
Fort Belvoir, Virginia 22060

Director
U.S. Army Engineer Geodesy,
Intelligence & Mapping
Research and Development Agency
Fort Belvoir, Virginia 22060

Dr Herman Robl
Deputy Chief Scientist
U.S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

Richard O. Ulsh (CRDARD-IPO)
U.S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

Mr Robert O. Parker, AMSEL-RD-S
Executive Secretary, JSTAC
U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Attention:AMSEL-SC
RD-GF
RD-MT
XL-D
XL-E
XL-C
XL-S (Dr R. Buser)
HL-CT-DD
HL-CT-R
HL-CT-L (Dr W.S. McAfee)
HL-CT-O
HL-CT-I
HL-CT-A
NL-D
NL-A
NL-P
NL-P-2 (Mr D. Haratz)
NL-R (Mr R. Kulinyi)
NL-S
KL-D
KL-E
KL-S (Dr H. Jacobs)
KL-SM (Drs Schiel/Hieslmair)
KL-T
VL-D
VL-F (Mr R.J. Niemela)
WL-D

1 copy to each symbol listed individually addressed

Dr A.D. Schnitzler, AMSEL-HL-NVII
Night Vision Laboratory, USAECOM
Fort Belvoir, Virginia 22060

Dr G.M. Janney, AMSEL-HL-NVOR
Night Vison Laboratory,USAECOM
Fort Belvoir, Virginia 22060

Atmospheric Sciences Office
Atmospheric Sciences Laboratory
White Sands Missile Range
New Mexico 88002

Missile Electronic Warfare,
Technical Area, AMSEL-WT-MT
White Sands Missile Range
New Mexico 88002

Project Manager
Common Positioning & Navigation Systems
Attn: Harold H. Bahr (AMCPM-NS-TM), Bldg 439
U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Director, Electronic Programs
Attn: Code 427
Department of the Navy
Washington, D.C. 20360

Commander
U.S. Naval Security Group Command
Attn: G43
3801 Nebraska Avenue
Washington, D.C. 20390

Director
Naval Research Laboratory
Washington, D.C. 20390
Attn: Code 2027 6 copies
Dr W.C. Hall, Code 7000 1 copy
Dr A. Brodizinsky, Sup.Elec Div. 1 copy

Dr G.M.R. Winkler
Director, Time Service Division
U.S. Naval Observatory
Washington, D.C. 20390

Naval Air Systems Command
AIR 03
Washington, D.C. 20360 2 copies

Naval Ship Systems Command
Ship 031
Washington, D.C. 20360

Naval ship Systems Command
Ship 035
Washington, D.C. 20360

U.S. Naval Weapons Laboratory
Dahlgren, Virginia 22448

Naval Electronic Systems Command
ELEX 03, Room 2046 Munitions Building
Department of the Navy
Washington, D.C. 20360 (2 copies)

Commander
Naval Electronics Laboratory Center
Attn: Library
San Diego, California 92152 (2 copies)

Deputy Director and Chief Scientist
Office of Naval Research Branch Office
1030 Est Gree Street
Pasadena, California 91101

Library (Code2124)
Technical Report Section
Naval Postgraduate School
Monterey, California 93940

Glen A. Myers (Code 52Mv)
Assoc Professor of Elec. Engineering
Naval Postgraduate School
Monterey, California 93940

Commanding Officer and Director
U.S. Naval Underwater Sound Laboratory
Fort Trumbull
New London, Connecticut 06840

Commanding Officer
Naval Avionics Facility
Indianapolis, Indiana 46241

Dr H. Harrison, Code RRE
Chief, Electrophysics Branch
National Aeronautics & Space Admin.
Washington, D.C. 20546

NASA Lewis Research Center
Attn: Library
21000 Brookpark Road
Cleveland, Ohio 44135

Los Alamos Scientific Laboratory
Attn: Report Library
P.O. Box 1663
Los Alamos, New Mexico 87544

Federal Aviation Administration
Attn: Admin Stds Div (MS-110)
800 Independence Ave S.W.
Washington, D.C. 20590

Head, Technical Services Division
Naval Investigative Service Headquarters
4420 North Fairfax Drive
Arlington, Virginia 22203

Commander
U.S. Naval Ordnance Laboratory
Attn: Librarian
White Oak, Maryland 21502 (2 copies)

Commanding Officer
Office of Naval Research Branch Office
Box 39 FPO
New York, New York 09510

Commanding Officer
Office of Naval Research Branch Office
219 South Dearborn Street
Chicago, Illinois 60604

Commanding Officer
Office of Naval Research Branch Office
495 Summer Street
Boston, Massachusetts 02210

Commander (ADL)
Naval Air Development Center
Johnsville, Warminster, Pa 18974

Commanding Officer
Naval Training Device Center
Orlando, Florida 32813

Commander (Code 753)
Naval Weapons Center
Attn: Technical Library
China Lake, California 93555

Commanding Officer
Naval Weapons Center
Corona Laboratories
Attn: Library
Corona, California 91720

Commander, U.S. Naval Missile Center
Point Mugu, California 93041

W.A. Eberspacher, Associate Head
Systems Integration Division
Code 5340A, Box 15
U.S. Naval Missile Center
Point Mugu, California 93041

Mr M. Zane Thornton, Chief
Network Engineering, Communications
and Operations Branch
Lister Hill National Center for
Biomedical Communications
8600 Rockville Pike
Bethesda, Maryland 20014

U.S. Post Office Department
Library - Room 1012
12th & Pennsylvania Ave, N.W.
Washington, D.C. 20260

Director
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

Mr Jerome Fox, Research Coordinator
Polytechnic Institute of Brooklyn
55 Johnson Street
Brooklyn, New York 11201

Director
Columbia Radiation Laboratory
Columbia University
538 West 120th Street
New York, New York 10027

Director
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois 61801

Director
Stanford Electronics Laboratories
Stanford University
Stanford, California 94305

Director
Microwave Physics Laboratory
Stanford University
Stanford, California 94305

Director, Electronics Research Laboratory
University of California
Berkeley, California 94720

Director
Electronic Sciences Laboratory
University of Southern California
Los Angeles, California 90007

Director
Electronics Research Center
The University of Texas at Austin
Austin Texas 78712

Division of Engineering and Applied Physics
210 Pierce Hall
Harvard University
Cambridge, Massachusetts 02138

Dr G.J. Murphy
The Technological Institute
Northwestern University
Evanston, Illinois 60201

Dr John C. Hancock, Head
School of Electrical Engineering
Purdue University
Lafayette, Indiana 47907

Dept of Electrical Engineering
Texas Technological College
Lubbock, Texas 79409

Aerospace Corporation
P.O. Box 95085
Los Angeles, California 90045
Attn: Library Acquisitions Group

Proffessor Nicholas George
California Inst of Technology
Pasadena, California 91109

Aeronautics Library
Graduat Aeronautical Laboratories
California Institute of Technology
1201 E. California Blvd
Pasadena, California 91109

The John Hoplins University
Applied Physics Laboratory
Attn: Document Librarian
8621 Georgia Avenue
Silver Spring, Maryland 20910

Raytheon Company
Attn: Librarian
Bedford, Massachusetts 01730

Raytheon Company
Research Division Library
28 Seyon Street
Waltham, Massachusetts 02154

Dr Sheldon J. Wells
Electronic Properties Information Center
Mail Station E-175
Hughes Aircraft Company
Culver City, California 90230

Dr Robert E. Fontana
Systems Research Laboratories Inc.
7001 Indian Ripple Road
Dayton, Ohio 45440

Nuclear Instrumentation Group
Bldg 29, Room 101
Lawrence Radiation Laboratory
University of California
Berkeley, California 94720

Sylvania Electronic Systems
Applied Research Laboratory
Attn: Documents Librarian
40 Sylvan Road
Waltham, Massachusetts 02154

Hollander Associates
P.O. Box 2276
Fullerton, California 92633

Illinois Institute of Technology
Dept of Electrical Engineering
Chicago, Illinois 60616

The University of Arizona
Dept of Electrical Engineering
Tucson, Arizona 85721

Utah State University
Dept Of Electrical Engineering
Logan, Utah 84321

Case Institute of Technology
Engineering Division
University Circle
Cleveland, Ohio 44106

Hunt Library
Carnegie-Mellon University
Schenley Park
Pittsburgh, Pennsylvania 15213

Dr Leo Youns
Stanford Research Institute
Menlo Park, California 94025

School of Engineering Sciences
Arizona State University
Tempe, Arizona 85281

Engineering & Mathmatical Sciences Library
University of California at Los Angeles
405 Hilgred Avenue
Los Angeles, California 90024

The Library
Government Publications Section
University of California
Santa Barbara, California 93106

Carnegie Institute of Technology
Electrical Engineering Department
Pittsburgh, Pennsylvania 15213

Professor Joseph E. Rowe
Chairman, Dept of Electrical Engineering
The University of Michigan
Ann Arbor, Michigan 48104

New York University
College of Engineering
New York, New York 10019

Syracuse University
Dept of Electrical Engineering
Syracuse, New York 13210

ERRATUM

Mr Jerome Fox, Research Coordinator
Polytechnic Institute of Brooklyn
55 Johnson St (should be 333 Jay St)
Brooklyn, N.Y. 11201

DELETE

Mr Morton M. Pavane, Chief
AFSC Scientific & Tech. Liaison Office
26 Federal Plaza, Suite 1313
New York, New York 10007

Commanding Officer
Office of Naval Research Branch Office
Box 39 FPO
New York, N.Y. 09510

Yale University
Engineering Department
New Haven, Connecticut 06520

Airborne Instruments Laboratory
Deerpark, New York 11729

Raytheon Company
Attn: Librarian
Bedford, Massachusetts 01730

Lincoln Laboratory
Massachusetts Institute of Technology
Lexington, Massachusetts 02173

The University of Iowa
The University Libraries
Iowa City, Iowa 52240

Lenkurt Electric Co,Inc
1105 County Road
San Carlos, California 94070
Attn: Mr E.K. Peterson

Philco Ford Corporation
Communications & Electronics Div.
Union Meeting and Jolly Rods
Blue Bell, Pennsylvania 19422

Union Carbide Corporation
Electronic Division
P.O. Box 1209
Mountain View, California 94041

Electromagnetic Compatibility Analysis Center
(ECAC), Attn: ACLP
North Severn
Annapolis, Maryland 21402

Director
U. S. Army Advanced Materiel Concepts Agency
Washington, D.C. 20315

Dept of Electrical Engineering
Rice University
Houston, Texas 77001

Research Laboratories for the Eng. Sc.
School of Engineering & Applied Science
University of Virginia
Charlottesville, Virginia 22903

Dept of Electrical Engineering
College of Engineering & Technology
Ohio University
Athens, Ohio 45701

Project Mac
Document Room
Massachusetts Institute of Technology
545 Technology Square
Cambridge, Massachusetts 02139

Lehigh University
Dept of Electrical Engineering
Bethelem, Pennsylvania 18015

Commander Test Command (TCD-)
Defense Atomic Support Agency
Sandia Base
Albuquerque, New Mexico 87115

Materials Center Reading Room 13-2137
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

Professor James A. Cadzow
Department of Electrical Engineering
State University of New York at Buffalo
Buffalo, New York 14214

Director, Naval Research Laboratory
Attn: Library, Code 2029 (ONRL)
Washington, D.C. 20390

Commanding Officer (Code 2064)
Navy Underwater Sound Laboratory
Fort Trumbull
New London, Connecticut 06320

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)* University of Illinois Coordinated Science Laboratory Urbana, Illinois 61801	2a. REPORT SECURITY CLASSIFICATION 2b. GROUP

3. REPORT TITLE

ON A ROOT-DISTANCE RELATION FOR ARITHMETIC CODES

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

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

CHIEN, R. T. & HONG, S. J.

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
October, 1969	11	13

8a. CONTRACT OR GRANT NO. DAAB-07-67-C-0199; also NSF Grant GK-2339. b. PROJECT NO. c. d.	9a. ORIGINATOR'S REPORT NUMBER(S) R-440 9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*

10. DISTRIBUTION STATEMENT

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

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	Joint Services Electronics Program thru U.S. Army Electronics Command Fort Monmouth, New Jersey 07703

13. ABSTRACT

NONE

DD FORM 1 NOV 65 1473

Security Classification

Security Classification

14 KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Error Correction						
Computer Arithmetic						
Computer Reliability						

Security Classification