1998

Error Correcting Codes Associated with Complex Hadamard Matrices

I. Heng
Old Dominion University

C. H. Cooke
Old Dominion University

Original Publication Citation

Heng, I., & Cooke, C. H. (1998). Error correcting codes associated with complex Hadamard matrices. *Applied Mathematics Letters, 11*(4), 77-80. doi:10.1016/s0893-9659(98)00059-7

Pergamon

Appl. Math. Lett. Vol. 11, No. 4, pp. 77–80, 1998

Printed in Great Britain
0893-9659/98 $19.00 + 0.00

PII: S0893-9659(98)00059-7

Error Correcting Codes Associated with Complex Hadamard Matrices

I. HENG AND C. H. COOKE
Department of Mathematics
Old Dominion University
Norfolk, VA 23508, U.S.A.

(Received and accepted July 1997)

Abstract—For primes $p > 2$, the generalized Hadamard matrix $H(p, pt)$ can be expressed as $H = x^A$, where the notation means $h_{ij} = x^{a_{ij}}$. It is shown that the row vectors of A represent a p-ary error correcting code. Depending upon the value of t, either linear or nonlinear codes emerge. Code words are equidistant and have minimum Hamming distance $d = (p-1)t$. The code can be extended so as to possess $N = p^2t$ code words of length $pt - 1$. © 1998 Elsevier Science Ltd. All rights reserved.

Keywords—Error correcting codes, Complex Hadamard matrix, Hadamard exponent, Linear and nonlinear codes, Equidistant code words.

1. INTRODUCTION

The purpose of this paper is to introduce a class of error correcting codes which we call generalized Hadamard codes. Such codes are discovered by analyzing the Hadamard matrix of exponents E, which is associated with a complex Hadamard matrix H.

Hadamard matrices $H(p, q)$, of index p are matrices of dimension q whose elements are p^{th} roots of unity and whose rows are orthogonal. For the case $p = 2$, the elements are plus/minus one, and the matrix is referred to as a classical Hadamard matrix. References [1–6] provide a lengthy survey of theory and applications of classical Hadamard matrices, as well as their connections to designs, error correcting codes, and the Hadamard imbedding problem.

For $p > 2$, the elements are numbers on the unit circle, and the terminology used is that of a complex, or generalized Hadamard matrix. References [7–11] concern definition, structure, properties, and applications of generalized Hadamard matrices.

Butson [8] proves that for a fixed prime p, a necessary condition for existence of $H(p, q)$ is that p divides q. Thus, interest here is directed to complex Hadamard matrices $H(p, pt)$, where $p > 2$ is a fixed prime and t is a positive integer. When such matrices exist, a real matrix $E(p, pt)$, which is called a Hadamard exponent [9], can be associated with $H(p, pt)$. If x is a primitive p^{th} root of unity, the association is $H(p, pt) = x^{E(p,pt)}$. The notation means that matrix elements are related by $h_{ij} = x^{e_{ij}}$, where i, j are matrix indices.

The elements of the Hadamard exponent E lie in the Galois field $GF(p)$, and its row vectors can be viewed as the codewords of what shall be called a generalized Hadamard code. Depending upon the value of the integer t, either a linear group code or a nonlinear code may emerge.

2. TERNARY HADAMARD CODES

As a first example of a nonlinear Hadamard code, the array Q given below provides the Hadamard exponent for a standard form Hadamard matrix $H(3,6) = x^Q$:

$$\begin{bmatrix} * & * & Q & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 \end{bmatrix}.$$

Clearly, in forming code words by utilizing matrix row vectors, the first column is superfluous.

The next example exhibits a linear group code, obtained from the Hadamard exponent of $H(3,9)$, again written in standard form:

$$\begin{bmatrix} * & * & * & * & D & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \end{bmatrix}.$$

If the first all-zero column is omitted, one readily observes that the nine row vectors of $D = E(3,9)$ constitute a ternary linear error-correcting code characterized by parameters $(n,k,d) = (8,2,6)$. By augmentation, an (8,3,5) code having twenty-seven codewords can be obtained, which has the punctured $E(3,9)$ as a subcode.

Similarly, there is associated with $H(3,27)$ the exponent $E(3,27)$ whose corresponding punctured linear Hadamard code has parameters $(26,3,18)$. This code augments to a code which possesses eighty-one codewords, and which has the punctured linear Hadamard code as a subcode.

2.1. Vectors Over C_p

In this section, the problem of establishing the value $d(K)$, which represents the minimum Hamming distance between the codewords of a generalized Hadamard code K is considered.

Let $C_p = \{1, x, x^2, \ldots, x^{p-1}\}$ be the cyclic group generated by x, where $x = \exp(2\pi j/p)$ is a complex primitive p^{th} root of unity, and $p > 2$ is a fixed prime. Further, let $A = (x^{a_i}), B = (x^{b_i})$ denote arbitrary vectors over C_p which are of length $N = pt$, where t is a positive integer. Define the collection of differences between exponents $Q = \{a_i - b_i, \bmod p : i = 1, 2, \ldots, N\}$, and let n_q be the multiplicity of element q of Z_p which appears in Q.

PROPERTY U. *Vectors A, B are said to satisfy* **Property U** *if each element q of Z_p appears in Q, exactly t times.*

The following lemma is of fundamental importance in constructing generalized Hadamard codes.

LEMMA 1. ORTHOGONALITY OF VECTORS OVER C_p. *For fixed primes p, arbitrary vectors A, B whose elements are from C_p are orthogonal iff for each element q in Z_p, q appears in Q with*

multiplicity t, where $N = pt$ is the length of A, B, and Q is the collection of mod p *differences between the Hadamard exponents associated with A, B.*

PROOF. SUFFICIENCY. If Q contains each element q of Z_p, t times, then the inner product of A, B,

$$(A, B) = t \sum_{j=0}^{p-1} x^j$$

vanishes, since x is a p^{th} root of unity. Hence, A, B are orthogonal.

NECESSITY. To the contrary, suppose n_q is not uniform as q varies over Q. If all n_q are nonzero, by using the fact that the sum of all p^{th} roots of unity vanishes, the circumstance is arrived at where the sum involved in (A, B) reduces to a integral linear combination which does not involve all p^{th} roots of unity. Moreover, if any $n_q = 0$, this circumstance is already present. Because the coefficients are positive integers, such a linear combination cannot vanish. (Indeed, if $p = 3$, for any arbitrary set of nonzero coefficients, the linear combination cannot vanish, as any two cube roots of unity represent noncolinear vectors in the plane.) Hence, A, B are not orthogonal.

COMMENT 1. Lemma 1 above can also be inferred from assertions of Butson [8], for which he provides no proof, but which he maintains are clearly valid.

COMMENT 2. For any p, Property U is sufficient for orthogonality. However, if p is not prime, cases are easily discovered of vectors over C_p which are orthogonal, but which do not satisfy Property U. Thus, Property U is not always necessary for orthogonality.

COROLLARY. *If p is a prime number and if the Hadamard matrix $H(p, pt)$ exists, the error correcting code $K(p, pt)$ associated with the corresponding row vectors of the Hadamard exponent $E(p, pt)$ is characterized by the error protection afforded by $d(K) = (p - 1)t$.*

PROOF. In the mod p difference of any two arbitrary row vectors of the Hadamard exponent matrix, the zero element of Z_p appears exactly t times; hence, two code words differ in $(p - 1)t$ symbols.

STANDARD FORM. Any Hadamard matrix can be transformed into a Hadamard matrix for which every element of the first row and first column is unity. In this case, the first row and column of the Hadamard exponent consists of elements which are all zero. Some equivalent of a standard form matrix which is obtained by row and/or column interchanges is necessary, but not sufficient in order to obtain from E a linear group code, as such codes require the presence of the zero vector.

The code words can now be shortened by removing the first column, obtaining what is called a punctured code, which possesses the same level of error protection. When the code is linear, it can be imbedded in a linear group code having p times as many code words, through augmentation accomplished by adding appropriate cosets (add, respectively, each element of Z_p to each symbol of each code word, to get a new codeword).

3. EXPONENT GENERATION BY DIRECT SUM

Whereas the matrix Q of Section 2 is tediously obtainable by trial and error, the matrix D easily follows by use of a direct sum, employing the matrix E now given,

$$\begin{bmatrix} * & E & * \\ 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix},$$

together with the direct sum below, plus row, and column interchanges.

LEMMA 1. *If $E = E(p, p)$ is a Hadamard exponent, then the direct sum $E(p, p^2) = (e_{ij} + E; i, j = 0, 1, \ldots, p - 1)$ is a block Hadamard exponent which is also a Hadamard exponent.*

Likewise, $E(3, 27)$ may be obtained as the direct sum of $E(3, 3)$ and $E(3, 9)$.

4. SUMMARY AND CONCLUSIONS

An initial exploration of the properties of the exponent matrix associated with a complex Hadamard matrix allows identification of a class of generalized Hadamard codes. For primes p, the sequence $K(p, p^n)$ appears to be a sequence of linear error correcting codes whose codewords are equidistant at Hamming distance $d(K) = p^n - p^{n-1}$. Butson's results [8] guarantee the existence of such codes; whereas, linearity has not been established for the general case. Establishment would require only a determination that the code space possesses n generating vectors, a pattern which has been verified for $n = 2, 3$.

For some values of q, it is not at all certain that $H(p, q)$ exists. In particular, the authors conjecture that $H(3, 15)$ does not exist, which is a case not covered by Butson's results on existence by construction or direct sums.

A particularly interesting question is whether the linear codes possess an equivalent cyclic version, as then the potential exists for burst error protection against bursts of increasingly long duration.

Finally, one questions whether there is a decoding technique which is unique to the Hadamard codes, and exactly what is the best use for the nonlinear codes. In all cases, nature seems to have formed a vast lode of interesting codes, waiting to be exploited.

REFERENCES

1. J. Adamek, *Foundations of Coding*, John Wiley, New York, (1991).
2. E.F. Assmus and J.D. Key, *Designs and Their Codes*, Cambridge University Press, New York, (1992).
3. J.H. Beder, Conjectures about Hadamard matrices, *Presented at the R. C. Bose Memorial Conference on Statistical Design and Related Combinatorics*, Colorado State University, June 7–11, (1995).
4. A. Hedayat and W.D. Wallis, Hadamard matrices and their applications, *Annals of Statistics* **6** (6), 1184–1238, (1978).
5. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes*, Ninth edition, North-Holland, Amsterdam, (1996).
6. K. Vijayan, Hadamard matrices and submatrices, *J. Australian Mathematical Society, Series A* **22**, 469–475, (1976).
7. J.A. Butson, Generalized Hadamard matrices, *Proc. Amer. Math. Soc.* **13**, 894–898, (1962).
8. J.A. Butson, Relations among generalized Hadamard matrices, *Can. J. Math.* **15**, 42–48, (1963).
9. C.H. Cooke, The Hadamard matroid and an anomaly in its single element extensions, *CMA* **38** (7), 115–120, (1997).
10. C.H. Cooke, The Hadamard matroid and generalized Hadamard codes, *Presented at the Tenth Cumberland Conference on Graph Theory, Combinatorics, and Computing*, Emory University, Atlanta, GA, May 16–18, 1997.
11. S.S. Shrikhande, Generalized Hadamard matrices and orthogonal arrays of strength, *Two. Can. J. Math.* **16**, 736–740, (1964).