Maximum Distance Q-Nary Codes

RICHARD C. SINGLETON, SENIOR MEMBER, IEEE

Summary—A q-nary error-correcting code with $N = q^k$ code words of length $n = k + r$ can have no greater minimum distance d than $r + 1$. The class of codes for which $d = r + 1$ is studied first in general, then with the restriction that the codes be linear. Examples and construction methods are given to show that these codes exist for a number of values of q, k, and r.

Introduction

A Q-NARY ERROR-correcting code is a code based on q symbols, rather than on two as in the case of binary codes. These codes have been studied by a number of authors and much of this work is summarized by Peterson.[1] A q-nary code with $N = q^k$ code words of length $n = k + r$ can have no greater (minimum) distance d than $r + 1$. In this paper, the class of codes with $d = r + 1$ and $N = q^k$ is considered. These codes will be called maximum-distance separable (M.D.S.) codes, since they have the maximum possible distance for given code size N and code word length n. The fact that they are necessarily separable will be shown, as will other theoretical results.

The Reed-Solomon[2] codes are a known class of M.D.S. code. Other M.D.S. codes that are new are given here.

The M.D.S. codes were investigated initially because of their usefulness in constructing constant-weight binary codes with large N and large binary distance for use as superimposed codes. This work will be reported on shortly.[3]

General Results

Theorem 1 establishes the distance bound stated in the opening paragraph.

Theorem 1. If $N = q^k$, then $d \leq r + 1$, where $r = n - k$.

Proof: Pick any k positions. There are q^k possible assignments of q-nary symbols to these positions. If any two among the q^k code words agree in these k positions, then $d \leq r$. If no two code words agree in all k positions, some pairs will agree in $k - 1$ positions; thus $d \leq r + 1$.

Theorem 2 shows an interesting symmetry property of M.D.S. codes.

Theorem 2. If $N = q^k$ and $d = r + 1$, any k code word positions can be regarded as information positions, and the remaining r as redundant (checking) positions.

Proof: Pick any k position. There are q^k possible assignments of q-nary symbols to these positions. Since $d = r + 1$, no two among the q^k code words can agree in all k of these positions. Thus each of the q^k possible assignments occurs in exactly one code word.

If $k = 1$, an M.D.S. code with $N = q$ code words and $d = r + 1$ can be constructed for any r by letting all positions in a code word have the same symbol. If $r = 1$, an M.D.S. code with $d = 2$ and any k can be formed by using the integers, 0, 1, $\cdots$ $q - 1$ as symbols and letting the code be those $(k + 1)$-tuples summing to zero mod q. There are $N = q^k$ such $(k + 1)$-tuples. Thus, the cases that require further study have $k \geq 2$ and $r \geq 2$.

An M.D.S. code with $k = 2$ is equivalent to a set of orthogonal Latin squares. This equivalence was pointed out recently by Golomb[4] and developed further in terms of projective planes by Posner.[5] A proof of this equivalence is shown in Theorem 3.

Theorem 3. A q-nary code with $N = q^2$ and $d = r + 1$ is equivalent to a set of r pair-wise orthogonal Latin squares of order q.

Proof: 1) Suppose we have a set of r orthogonal Latin squares of order q. We first number the rows and columns of the squares, using the same q symbols from which the squares are formed, then construct a code with q^2 words by using row number for the first position, column number for the second and the corresponding Latin square entries for the remaining r positions. Two different code words cannot agree in any pair of the last r positions, since each of the q^2 ordered pairs of q-nary symbols occurs exactly once in the corresponding pair of orthogonal Latin squares. Furthermore, if two code words agree in either of the first two positions, they can agree in none of the last r, since each of the q symbols appears exactly once in each row or column of a Latin square.

2) Suppose we have a q-nary code with $N = q^k$, $d = r + 1$ and $k = 2$. Using the first two positions to index row and column, we fill in a set of r squares with the remaining r positions as entries. Every square is a Latin square, since each of the q symbols occurs exactly once in a given row or column. Furthermore, every pair of squares is orthogonal, since each ordered pair of entires occurs exactly once.

In an analogous manner, an M.D.S. code with $k \geq 3$ can be used to form a set of r k-dimensional Latin hypercubes of order q. These Latin hypercubes will have an

Manuscript received May 10, 1963.

The author is with the Engineering Division of the Mathematical Sciences Department, Stanford Research Institute, Menlo Park, Calif.

[1] W. W. Peterson, "Error Correcting Codes," M.I.T. Press, Cambridge, Mass., and John Wiley and Sons, Inc., New York, N. Y.; 1961.

[2] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *J. Soc. Ind. Appl. Math.*, vol. 8, pp. 300–304; June, 1960.

[3] W. H. Kautz and R. C. Singleton, "Binary Superimposed Codes," to be published.

[4] S. W. Golomb, "The Sizes of Certain Code Dictionaries," Jet Propulsion Labs., Calif. Inst. Tech., Pasadena, Res. Summary No. 36-13, pp. 23–24; March, 1962.

[5] E. C. Posner, "Nonbinary Codes and Projective Planes," Jet Propulsion Labs., Calif. Inst. Tech., Pasadena, Space Programs Summary No. 37-16, vol. 4, pp. 42–45; August, 1962.

orthogonality relationship as a consequence of the fact that no two code words can agree in more than $k - 1$ positions. Correspondingly, a set of orthogonal Latin hypercubes can be used to form an M.D.S. code. This equivalence is independent of whether or not the code is linear.

It is easily shown that no set of more than $q - 1$ orthogonal Latin squares (or hypercubes) exists. Thus $r \leq q - 1$ or $d \leq q$ for an M.D.S. code with $k \geq 2$. On the other hand, the Hamming sphere-packing bound[1] for $r = 2$, $d = 3$ codes with $N = q^k$ gives $k \leq q - 1$. Combining results, if $k \geq 2$ and $r \geq 2$, then $k \leq q - 1$ and $r \leq q - 1$.

Linear Codes

For the remainder of this paper we consider a subclass of the M.D.S. codes, those for which q is a prime or a power of a prime and the code a linear code. In this case, the q-nary code words are vectors in an n-dimensional linear space over the finite field $GF(q)$.

Definition: A *linear q-nary code* is defined as the set of vectors contained in a k-dimensional linear subspace of all q^n n-dimensional vectors over $GF(q)$. A linear code can be described by an r-by-n *check matrix* H[1] of rank $r = n - k$, such that $Hx = 0$ if and only if x is a vector in the code; *i.e.*, the code is the null space of a check matrix H.

The number of code words in a linear q-nary code is always a power of q. If the rank of H is $r = n - k$, then $N = q^k$. A considerable body of theoretical results exists for linear codes.[1]

Theorem 4[1] relates distance to conditions on the columns of the check matrix H.

Theorem 4. A linear q-nary code with check matrix H has (minimum) q-nary distance d if and only if 1) every subset of $d - 1$ columns of H is linearly independent and 2) some subset of d columns of H is linearly dependent.

It is clear that distance is invariant under nonsingular row operations, column permutations and multiplication of columns of H by nonzero constants. We will consider codes that can be transformed into one another by these operations as equivalent. In particular, any linear code can be transformed into an equivalent code with a check matrix of the form $H = (A, I)$ or $H = (A, -I)$, where I is an r-by-r identity matrix.

Since every set of $r + 1$ columns of H is linearly dependent, $d \leq r + 1$ as was previously established under more general conditions. This observation leads to corollaries 1 and 2.

Corollary 1. For a linear q-nary code, $d = r + 1$ if and only if every set of r columns of its check matrix H is linearly independent.

Corollary 2. If the check matrix of a linear q-nary code is of the form $H = (A, I)$, then $d = r + 1$ if and only if every square submatrix of order j within A where $1 \leq j \leq \min(r, k)$ has a nonzero determinant.

Given an M.D.S. linear code with k information and r check positions, a dual code with $k' = r$, $r' = k$, and $d' = r' + 1$ can always be formed. The check matrix is first transformed to $H = (A, I)$ and then the matrix $H' = (A^t, I)$ is formed by adjoining a k-by-k identity matrix to the transpose of A. From corollary 2 it can be seen that the dual code has distance $d' = r' + 1$.

The question of the existence of M.D.S. linear codes will now be investigated. In the trivial case $k = 1$, r is unlimited for all q. Similarly, if $r = 1$, k is unlimited for all q.

For $k = 2$, M.D.S. linear codes exist for all $r \leq q - 1$, and thus the upper bound can be achieved. The following are examples of check matrices of M.D.S. codes with $k = 2$ and $r = q - 1$:

$$q = d = 3 \qquad H = \begin{bmatrix} 1 & 1 & -1 & 0 \\ 1 & 2 & 0 & -1 \end{bmatrix}$$

$$q = d = 4 \qquad H = \begin{bmatrix} 1 & 1 & -1 & 0 & 0 \\ 1 & t & 0 & -1 & 0 \\ 1 & t^2 & 0 & 0 & -1 \end{bmatrix}$$

$$t^2 + t + 1 = 0$$

$$q = d = 5 \qquad H = \begin{bmatrix} 1 & 1 & -1 & 0 & 0 & 0 \\ 1 & 2 & 0 & -1 & 0 & 0 \\ 1 & 3 & 0 & 0 & -1 & 0 \\ 1 & 4 & 0 & 0 & 0 & -1 \end{bmatrix}.$$

A general form for the $(q - 1)$-by-$(q + 1)$ check matrix of a $k = 2$, $r = q - 1$, $d = q$ code is an initial column of ones, a second column composed of the $q - 1$ nonzero marks of $GF(q)$, then a $(q - 1)$-by-$(q - 1)$ negative identity matrix. This form is based on Mann's construction of a "complete set" of orthogonal Latin squares.[6] Deletion of rows of this matrix and of the corresponding columns of the identity portion reduces both d and r by the number of rows deleted. Codes with $d = 3$, $r = 2$ and $2 \leq k \leq q - 1$ are obtained as duals of these codes.

For $k \geq 3$ and $r \geq 3$, the existence problem is only partially solved. If $k + r \leq q - 1$, an M.D.S. code exists and can be constructed from a Reed-Solomon code. The Reed-Solomon codes[2] are a family of linear q-nary codes with $d = r + 1$ and $k + r = q - 1$. They have a check matrix of the form $H = (\alpha^{ij})$, where α is a primitive root of $GF(q)$, $i = 0, 1, \cdots r - 1$ and $j = 0, 1, \cdots q - 2$. An M.D.S. code with $k + r \leq q - 1$ can be constructed from the r-by-$(q - 1)$ check matrix of a Reed-Solomon code by selecting any set of $k + r$ columns. The following check matrix is an example of a Reed-Solomon code based

[6] H. B. Mann, "Analysis and Design of Experiments," Dover Publications, Inc., New York, N. Y.; 1949. Mann also gives a method for constructing a number of orthogonal latin squares equal to one less than the smallest nonunity prime power factor of q for general q. This construction can be expressed in check matrix form, with each entry a j-tuple, where j is the number of nonunity prime power factors of q. The j-tuples are added and multiplied component by component. With this modification, the definition of linear q-nary codes can be extended to general q.

on the primitive root 3 of $GF(7)$, with $k = 3$, $r = 3$, and $d = 4$:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{bmatrix}.$$

For $k \geq 3$, $r \geq 3$ and $k + r > q - 1$, there are a few results known. The bounds $k \leq q - 1$ and $r \leq q - 1$ hold, of course. For $q = 5$ and 7, it can be shown by systematic consideration of possibilities that M.D.S. codes exist if and only if $k + r \leq q + 1$. An M.D.S. code of the form $H = (A, -I)$ can be formed by taking for A any rectangular submatrix from the following arrays:

$q = 5$

$$\begin{matrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & \\ 1 & 4 & & \end{matrix}$$

$q = 7$

$$\begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 6 & 4 & 2 & 5 \\ 1 & 6 & 4 & 2 & 5 & \\ 1 & 4 & 2 & 5 & & \\ 1 & 2 & 5 & & & \\ 1 & 5 & & & & \end{matrix}.$$

It is likely that similar arrays exist for larger prime numbers q, but a general form is not known.

For $k = 3$, M.D.S. codes with $r = q - 1$ exist if and only if q is a power of 2. If q is a power of 2, a general form for the A portion of the check matrix is an initial column of ones, a second column 1, t, t^2, $\cdots$ t^{q-2}, where t is a primitive root of $GF(q)$ and a third column 1, t^2, t^4, $\cdots$ $t^{2(q-2)}$. All 1-by-1 determinants are nonzero since the first three columns contain no zeros. All 2-by-2 determinants of the first and second columns and of the first and third columns are nonzero since $t^i \neq t^j$ and $t^{2i} \neq t^{2j}$ for $i \neq j$; those of the second and third columns are nonzero since

$$t^{i+2i} - t^{j+2i} = t^{i+j}(t^i - t^j) \neq 0$$

for $i \neq j$. The 3-by-3 determinants are nonzero since

$$(t^{i+2k} - t^{2j+k}) - (t^{i+2k} - t^{2i+k}) + (t^{i+2j} - t^{2i+j})$$
$$= (t^i - t^j)(t^j - t^k)(t^k - t^i) \neq 0$$

for $i \neq j \neq k \neq i$. It may be noted that these determinants all reduce to van der Monde form.[1] An example of a $q = 4$ code of this type follows:

$$q = d = 4 \qquad H = \begin{bmatrix} 1 & 1 & 1 & -1 & 0 & 0 \\ 1 & t & t^2 & 0 & -1 & 0 \\ 1 & t^2 & t & 0 & 0 & -1 \end{bmatrix}$$

$$t^2 + t + 1 = 0.$$

For $k = 3$ and q not a power of 2, an M.D.S. code with $r = q - 1$, if it existed, could be constructed having a check matrix $H = (A, -I)$ with an initial column of ones and a second column 1, α, α^2, $\cdots$ α^{q-2}, where α is a primitive root of $GF(q)$. The third column then can have no zeros and must have no pair of elements in common with a multiple of either the first or second columns. To form a third column, it must be possible, then, to select the $q - 1$ nonzero elements of $GF(q)$ from the nonzero portion of the $GF(q)$ multiplication matrix, taking only one element from each row and column. The following lemma shows this cannot be done. Thus a linear M.D.S. code with $k \geq 3$ and $r = q - 1$ cannot exist if q is not a power of 2.

Lemma: If q is a prime or a power of a prime and is odd, it is impossible to select the $q - 1$ nonzero elements of $GF(q)$ from the nonzero portion of the $GF(q)$ multiplication matrix, taking only one element from each row and column.

Proof:[7] Form the multiplication matrix in terms of the powers of a primitive root α. The entries are then α^{i+j}, and if one element is taken from each row and column, the product of these elements is $\alpha^{q(q-1)} = 1$, since $\alpha^{q-1} = 1$. But the product of the $q - 1$ nonzero elements of $GF(q)$ is $\alpha^{q(q-1)/2} \neq 1$, since q is odd.

Conclusion

It has been shown that M.D.S. codes, *i.e.*, q-nary codes with $N = q^k$ code words and distance $d = r + 1$, exist for a number of combinations of q, k and r, subject to an upper bound of $k \leq q - 1$ and $r \leq q - 1$ when $k \geq 2$ and $r \geq 2$. There is an equivalence between these codes and sets of orthogonal Latin hypercubes.

Although M.D.S. codes need not be linear codes, most of those for which constructions are known are of this form. When q is a prime or a power of a prime, the existence question is largely solved, except for some cases in the region of $k \geq 3$ and $q - k \leq r \leq q - 1$. This uncertainty probably will be resolved by further work.[8]

Acknowledgment

The author is indebted to W. H. Kautz and B. Elspas for their frequent suggestions and advice at all stages of this work.

[7] This proof is due to Dr. Bernard Elspas.

[8] *Added in proof*: K. A. Bush, "Orthogonal arrays of index unity," *Ann. Math. Statist.*, vol. 23, pp. 426–434; September, 1952, partially resolves this uncertainty by giving a construction on which $k + r = q + 1$ codes can be based for any $k \geq 3$, any $r \geq 3$ and q a prime power. This paper also gives upper bounds on r similar to those shown here and gives a construction for a $k = 3$, $r = q - 1$ array when $q = 2^i$.