

# An Exponential Number of Generalized Kerdock Codes

WILLIAM M. KANTOR\*

Department of Mathematics, University of Oregon, Eugene, Oregon 97403

If  $n - 1$  is an odd composite integer then there are at least  $2^{(1/2)\sqrt{n}}$  pairwise inequivalent binary error-correcting codes of length  $2^n$ , size  $2^{2^n}$ , and minimum distance  $2^{n-1} - 2^{(1/2)n-1}$ .

## 1. INTRODUCTION

If a subcode of the second order Reed-Muller code of length  $2^n$  has minimum distance  $2^{n-1} - 2^{(1/2)n-1}$  then it has at most  $2^{2^n}$  words. A *generalized Kerdock code* is defined to be such a subcode in which this maximum is attained. Such codes were first constructed by Kerdock [7]. His codes are extended cyclic codes, in the sense that there is an automorphism of order  $2^n - 1$  fixing one coordinate and cyclically permuting the remaining ones. In this note we will construct a large number of cyclic generalized Kerdock codes:

**THEOREM 1.** *If  $n - 1$  is odd and composite, then there are more than  $2^{(1/2)\sqrt{n}}$  pairwise inequivalent extended cyclic generalized Kerdock codes of length  $2^n$ .*

For the same values of  $n$ , we will also construct more than  $2^{(1/2)\sqrt{n}}$  pairwise inequivalent generalized Kerdock codes of length  $2^n$  which are not extended cyclic.

There is a well-known formal duality between Kerdock codes and Preparata codes: their weight-enumerators are related in the same manner as are those of a linear code and its dual [5; 8, p. 468]. However, the weight enumerators of all generalized Kerdock codes of length  $2^n$  coincide [8, p. 668], which suggests that the aforementioned apparent relationship is merely a coincidence. It should be noted that fewer than  $n$  "generalized Preparata codes" of length  $2^n$  are presently known [1, 6].

\* This research was supported in part by NSF Grant MCS 79-03130.

All generalized Kerdock codes also have design-theoretic properties in common. The codewords of each weight in such a code form a 3-design [8, pp. 162, 461].

This article can be regarded as a continuation of [4, 5]: several results found near the beginning of those articles will be used. However, in order to prove Theorem 1 only rough estimates will be required, instead of the precise discussions of equivalence found in those articles.

## 2. KERDOCK SETS

A binary *Kerdock set*  $\mathcal{K}$  is a set of  $2^{n-1}$  binary skew symmetric  $n \times n$  matrices, each having zero diagonal, such that the sum of any two is nonsingular. Clearly,  $n$  must be even. We will always assume that  $0 \in \mathcal{K}$ .

Corresponding to each Kerdock set  $\mathcal{K}$  is a generalized Kerdock code  $C(\mathcal{K})$ , defined as follows. Each  $M = (\mu_{ij}) \in \mathcal{K}$  determines a quadratic form  $Q_M((x_i)) = \sum_{i < j} \mu_{ij} x_i x_j$ , where  $(x_i) \in \mathbb{Z}_2^n$ . Let  $L$  denote a linear functional on  $\mathbb{Z}_2^n$ . Then  $C(\mathcal{K})$  consists of all subsets of  $\mathbb{Z}_2^n$  which are the zero sets of functions of the form  $Q_M(v) + L(v) + c$ , where  $M$  ranges through  $\mathcal{K}$ ,  $L$  is an arbitrary linear functional, and  $c$  is constant (so  $c = 0$  or  $1$ ). A proof that this defines a generalized Kerdock code can be found in [2]. Letting  $M = 0$ , we see that  $C(\mathcal{K})$  contains the first order Reed-Muller code  $C_0$ .

**LEMMA 1.** (i) *Aut  $C(\mathcal{K})$  is contained in the group of all affine transformations of  $\mathbb{Z}_2^n$ .*

(ii) *Aut  $C(\mathcal{K})$  contains all translations  $v \rightarrow v + b$  of  $\mathbb{Z}_2^n$ .*

(iii) *Aut  $C(\mathcal{K})$  is transitive on coordinates.*

*Proof.* (i) Since  $C_0$  consists of all words in  $C(\mathcal{K})$  of weight 0,  $2^n$  or  $2^{n-1}$ ,  $\text{Aut } C(\mathcal{K}) \leq \text{Aut } C_0$ .

(ii) Let  $v = (x_i)$  and  $M = (\mu_{ij}) \in \mathcal{K}$  with  $Q_M(v) = 0$ . Set  $b = (b_i)$  and  $(y_i) = v + b$ . Then

$$\begin{aligned} 0 &= \sum_{i < j} \mu_{ij} x_i x_j = \sum_{i < j} \mu_{ij} (y_i + b_i)(y_j + b_j) \\ &= \sum_{i < j} \mu_{ij} y_i y_j + \sum_{i < j} \mu_{ij} b_i y_j + \sum_{i < j} \mu_{ij} b_j y_i + \sum_{i < j} \mu_{ij} b_i b_j, \end{aligned}$$

so that  $(y_i) \in C(\mathcal{K})$ .

(iii) This is immediate in view of (ii).

**LEMMA 2.** *Let  $\mathcal{K}$  and  $\mathcal{K}'$  be Kerdock sets of  $n \times n$  matrices. Then*

$C(\mathcal{K})$  and  $C(\mathcal{K}')$  are equivalent if and only if there is a nonsingular  $n \times n$  matrix  $A$  such that the transformation  $M \rightarrow AMA^t$  sends  $\mathcal{K}$  to  $\mathcal{K}'$ .

*Proof.* Let  $g: C(\mathcal{K}) \rightarrow C(\mathcal{K}')$  be an equivalence. Since  $g$  sends  $C_0$  to itself,  $g$  is induced by an affine transformation of  $\mathbb{Z}_2^n$ . By Lemma 1(ii), we may assume that  $g$  has the form  $v \rightarrow vA^{-1}$  for some nonsingular matrix  $A^{-1}$ .

Let  $M = (\mu_{ij}) \in \mathcal{K}$ , and write  $A = (a_{ij})$ . If  $(x_i) \in C(\mathcal{K})$  and  $Q_M((x_i)) = 0$ , set  $(y_i) = (x_i)A^{-1}$  and compute as follows.

$$\begin{aligned} 0 &= \sum_{i < j} \mu_{ij} x_i x_j = \sum_{i < j} \mu_{ij} \left( \sum_k y_k a_{ki} \right) \left( \sum_l y_l a_{lj} \right) \\ &= \sum_{k, l} \left( \sum_{i < j} a_{ki} \mu_{ij} a_{lj} \right) y_k y_l. \end{aligned}$$

Let  $v_{kl} = \sum_{i < j} a_{ki} \mu_{ij} a_{lj}$  and  $c_k = \sum_{i < j} a_{ki} \mu_{ij} a_{kj}$ . Then

$$0 = \sum_{k < l} v_{kl} y_k y_l + \sum_k c_k y_k.$$

It follows that  $(v_{kl}) = AMA^t \in \mathcal{K}'$ , as required. The converse is obtained by reversing this argument.

Lemma 2 reduces the proof of Theorem 1 to the construction of sufficiently many Kerdock sets. The next reduction involves orthogonal geometry.

Define the quadratic form  $Q$  on  $\mathbb{Z}_2^{2n}$  by  $Q((x_i)) = \sum_{i=1}^n x_i x_{i+n}$ . A vector  $(x_i)$  is *singular* if  $Q((x_i)) = 0$ . Let  $E$  be the  $n$ -space in  $\mathbb{Z}_2^{2n}$  defined by  $x_i = 0$  for  $i > n$ ; similarly, let  $F$  be defined by  $x_i = 0$  for  $i \leq n$ . Then  $Q(E) = Q(F) = 0$ : these are *totally singular* (t.s.)  $n$ -spaces.

Let  $\mathcal{K}$  be any Kerdock set of  $n \times n$  matrices, and define  $\mathcal{S}(\mathcal{K})$  as follows:

$$\mathcal{S}(\mathcal{K}) = \{E\} \cup \left\{ F \begin{pmatrix} I & 0 \\ M & I \end{pmatrix} \mid M \in \mathcal{K} \right\}.$$

Then  $\mathcal{S}(\mathcal{K})$  is an *orthogonal spread*: a family of  $2^{n-1} + 1$  t.s.  $n$ -spaces such that every nonzero singular vector is in exactly one of them [4, Sect. 5]. Conversely, each orthogonal spread containing  $E$  and  $F$  produces a Kerdock set: just reverse this construction. Moreover, if  $\mathcal{S}(\mathcal{K})$  and  $\mathcal{S}(\mathcal{K}')$  are two orthogonal spreads which are inequivalent under the orthogonal group  $O^+(2n, 2)$ , then Lemma 2 and [4, (5.4)] imply that  $C(\mathcal{K})$  and  $C(\mathcal{K}')$  are inequivalent codes.

**LEMMA 3.** *Let  $\mathcal{S}(\mathcal{K})$  be as above, and assume that there is an orthogonal transformation of order  $2^{n-1} - 1$  fixing  $E$  and  $F$  and cyclically*

permuting the remaining members of  $\mathcal{S}(\mathcal{K})$ . Then  $C(\mathcal{K})$  is an extended cyclic code.

*Proof.* The given transformation can be viewed as a matrix  $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ , where  $A, B$  and  $0$  are  $n \times n$  matrices. Since  $Q$  is preserved,  $B = (A^{-1})^t$ . The calculation used in Lemma 2 shows that the linear transformation  $M \rightarrow AMA^t$  acts on  $C(\mathcal{K})$  as desired (compare [4, (5.4)]).

In order to prove Theorem 1, we can now ignore codes and focus on spreads. Thus, Theorem 1 is an immediate consequence of the next result (for  $q = 2$ ).

**THEOREM 2.** *If  $q$  is even and  $n-1$  is odd and composite, then an  $\Omega^+(2n, q)$  space has more than  $q^{(1/2)\sqrt{n}}$  pairwise inequivalent spreads each of which admits an orthogonal automorphism fixing two members and cyclically permuting the remaining ones.*

Here, an  $\Omega^+(2n, q)$  space is (up to a change of coordinates) the vector space  $GF(q)^{2n}$  equipped with the quadratic form  $Q((x_i)) = \sum_{i=1}^n x_i x_{n+i}$ . A vector  $(x_i)$  or 1-space  $\langle(x_i)\rangle$  is called *singular* if  $Q((x_i)) = 0$  and *nonsingular otherwise*; and a subspace  $E$  is again called *t.s.* if  $Q(E) = 0$ . A spread of such a space is a family of  $q^{n-1} + 1$  t.s.  $n$ -spaces partitioning the nonzero singular vectors. Equivalence is defined in terms of the group  $\Gamma O^+(2n, q)$  of semilinear transformations preserving  $Q$  projectively (cf. [4, Sect. 2]); when  $q = 2$  this is just the orthogonal group determined by  $Q$ .

There is also a bilinear form  $(u, v) = Q(u+v) + Q(u) + Q(v)$  on  $GF(q)^{2n}$ , and hence a notion of perpendicularity. If  $S$  is any subset of  $GF(q)^{2n}$  then  $S^\perp = \{v \in V \mid (v, S) = 0\}$ . If  $y$  is any 1-space then  $y \subset y^\perp$  (since  $(v, v) = 0$  for any vector  $v$ ), and we can form the quotient space  $y^\perp/y$ . This inherits the form  $(u, v)$  via  $(u+y, v+y) = (u, v)$ , but it does not inherit  $Q$  if  $y$  is nonsingular. A subspace  $X$  of  $y^\perp/y$  is called *totally isotropic* if  $(X, X) = 0$ .

For further background, see [4, 5].

### 3. PROOF OF THEOREM 2

Set  $n-1 = me$ , where  $e \geq m > 1$ .

In [3; 4, Sect. 3], a spread  $\Sigma$  of an  $\Omega^+(2m+2, q^e)$  space was constructed (called a desarguesian orthogonal spread). Here,  $\Sigma$  admits an orthogonal automorphism  $g$  of order  $(q^e)^m - 1$  fixing two members of  $\Sigma$  and cyclically permuting the others. The proof of Theorem 2 will consist of suitably modifying  $\Sigma$  as described in [5, Sect. 2].

The transformation  $g$  fixes  $q^e - 1$  nonsingular 1-spaces  $y$  of the underlying

vector space. The  $2m$ -dimensional space  $y^\perp/y$  inherits a symplectic structure. The family

$$\Sigma(y) = \{\langle y, y^\perp \cap X \rangle / y \mid x \in \Sigma\}$$

consists of  $(q^e)^m + 1$  totally isotropic  $m - 1$ -spaces which partition the set of all nonzero vectors in  $y^\perp/y$ . Turn  $y^\perp/y$  into a  $2me$ -dimensional symplectic space over  $GF(q)$  (by following the bilinear form on  $y^\perp/y$  with the trace map  $GF(q^e) \rightarrow GF(q)$ ). Then  $\Sigma(y)$  becomes a family  $\Sigma(y)^e$  of  $q^{me} + 1$  totally isotropic  $me$ -spaces which still partitions the nonzero vectors in  $y^\perp/y$ . Note that  $g$  induces a symplectic transformation of  $y^\perp/y$  preserving both  $\Sigma(y)$  and  $\Sigma(y)^e$ , and permuting their members exactly as it permutes those of  $\Sigma$ .

Let  $V$  be an  $\Omega^+(2me + 2, q)$  space. Fix a nonsingular 1-space  $z$  of  $V$ , and identify  $z^\perp/z$  with  $y^\perp/y$ . Then the family  $\Sigma(y)^e$  determines an essentially unique orthogonal spread  $\Sigma^y$  (called  $S(\Sigma(y)^e)$  in [5, Sect. 2]) such that  $\Sigma^y(z) = \Sigma(y)^e$ . Moreover,  $g$  extends to an orthogonal transformation  $g^*$  of  $V$  fixing  $z$ , preserving  $\Sigma^y$  and permuting  $\Sigma^y$  as required in Theorem 2.

We will show that, as  $y$  ranges over the original set of  $q^e - 1$  nonsingular 1-spaces in the  $\Omega^+(2m + 2, q^e)$  space we started with,  $\Sigma^y$  ranges over sufficiently many pairwise inequivalent  $\Omega^+(2me + 2, q)$  spreads.

Consider the symplectic spreads  $\Sigma(y)^e$ . If  $N$  is the number of pairwise inequivalent symplectic spreads of this sort, then  $N \geq (q^e - 2)/(2 \log_2 q^e)$  (by [4, (4.2) or (3.5)]). These produce  $N$  orthogonal spreads  $\Sigma^y$ . Since  $N/(q + 1) > q^{(1/2)\sqrt{n}}$ , Theorem 2 is a consequence of the following lemma.

**LEMMA 4.** *There do not exist  $q + 2$  choices  $y(1), \dots, y(q + 2)$  for  $y$  such that the symplectic spreads  $\Sigma(y(i))$  are pairwise inequivalent while the orthogonal spreads  $\Sigma^{y(i)}$  are pairwise equivalent.*

*Proof.* Fix  $y$ , and let  $V$ ,  $z$  and  $g^*$  be as above. There is a prime  $r \mid q^{me} - 1$  such that  $r \nmid 2^i - 1$  whenever  $1 < 2^i < q^{em}$  [9]. Let  $\langle h \rangle$  be a Sylow  $r$ -subgroup of  $\langle g^* \rangle$ . Then  $\langle h \rangle$  is also a Sylow  $r$ -subgroup of  $\Gamma O^+(2me + 2, q)$ . Since  $h$  induces the identity on both  $z$  and  $V/z^\perp$ , there is a 2-space  $Z$  in  $V$  on which  $h$  induces the identity. Then  $h$  acts on  $Z^\perp/(Z \cap Z^\perp)$ ; using the order of  $h$ , we find that  $Z \cap Z^\perp = 0$  and  $Z$  consists of all vectors fixed by  $h$ . Let  $G$  consist of all elements of  $\Gamma O^+(2me + 2, q)$  preserving  $\Sigma^y$ .

Now consider two further choices  $y'$  and  $y''$  such that  $\Sigma(y)^e$ ,  $\Sigma(y')^e$  and  $\Sigma(y'')^e$  are pairwise inequivalent but such that  $\Sigma^y$  is equivalent to both  $\Sigma^{y'}$  and  $\Sigma^{y''}$ . Define  $V'$ ,  $z'$ ,  $h'$ ,  $Z'$ ,  $G'$  and  $V''$ ,  $z''$ ,  $Z''$  in the obvious manner. We may assume that  $V = V' = V''$ .

Let  $\phi, \psi \in \Gamma O^+(2me + 2, q)$ , where  $(\Sigma^{y'})^\phi = \Sigma^y$  and  $(\Sigma^{y''})^\psi = \Sigma^y$ .

Clearly,  $G'^\phi = G$  and  $\langle h' \rangle$  is a Sylow  $r$ -subgroup of  $G$ . Thus, we may

assume that  $h'^\phi = h$ . Then  $Z'^\phi = Z$ . Similarly, we may assume that  $Z''^\psi = Z$ .

The points  $z$ ,  $z'^\phi$  and  $z''^\psi$  are all different. For example, if  $z'^\phi = z''^\psi$  then  $\phi\psi^{-1}$  sends  $\Sigma^{y'}(z')$  to  $\Sigma^{y''}(z'')$ , whereas  $\Sigma(y')^e$  and  $\Sigma(y'')^e$  are inequivalent.

Thus, if we leave  $y$  fixed and vary  $y'$ , there are at most  $q$  possibilities for  $z'^\phi$ . This proves the lemma, and completes the proof of Theorems 1 and 2.

#### 4. CONCLUDING REMARKS

1. Replacing  $(q^e)^m - 1$  by  $(q^e)^m + 1$  throughout Section 3, we obtain the following result.

**THEOREM 3.** *If  $q$  is even and  $n - 1$  is odd and composite, then an  $\Omega^+(2n, q)$  space has more than  $q^{(1/2)\sqrt{n}}$  pairwise inequivalent spreads, each of which admits an orthogonal automorphism cyclically permuting its  $q^{n-1} + 1$  members.*

Moreover, no orthogonal spread arising in Theorem 3 can be equivalent to any appearing in Theorem 2 (by [5, (3.3)]). Similarly, no generalized Kerdock code arising from Theorem 3 (with  $q = 2$ ) can be extended cyclic.

2. In Section 3,  $Z$  has only  $q - 1$  nonsingular 1-spaces. The estimates leading to  $q^{(1/2)\sqrt{n}}$  are very crude.

3. The Kerdock sets implicitly constructed in Section 3 are given explicitly in [5, (9.2)]. However, it is not clear how to choose more than  $2^{(1/2)\sqrt{n}}$  of them which produce pairwise inequivalent codes.

It seems likely that  $\Sigma^y$  and  $\Sigma^{y'}$  are inequivalent whenever  $\Sigma(y)$  and  $\Sigma(y')$  are.

#### REFERENCES

1. BAKER, R. D., AND WILSON, R. M., unpublished.
2. CAMERON, P. J., AND SEIDEL, J. J., Quadratic forms over  $GF(2)$ , *Nederl. Akad. Wetensch. Proc. Ser. A* **76** (1973), 1-8.
3. DYE, R. H., Partitions and their stabilizers for line complexes and quadrics, *Ann. Mat. Pura Appl.* (4) **114** (1977), 173-194.
4. KANTOR, W. M., Spreads, translation planes and Kerdock sets, I, *SIAM J. Disc. Alg. Methods* **3** (1982), 151-165.
5. KANTOR, W. M., Spreads, translation planes and Kerdock sets, II, *SIAM J. Disc. Alg. Methods* **3** (1982), 308-318.

6. KANTOR, W. M., On the inequivalence of generalized Preparata codes, *IEEE Trans. Inform. Theory*, in press.
7. KERDOCK, A. M., A class of low-rate non-linear binary codes, *Inform. and Control* **20** (1972), 182-187.
8. MACWILLIAMS, F. J., AND SLOANE, N. J. A., "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.
9. ZSIGMONDY, K., Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265-284.

## An Extension of the Entropy Theorem for Parameter Estimation

NARIYASU MINAMIDE

*Department of Electrical Engineering, Faculty of Engineering,  
Mie University, Tsu-city, Mie-prefecture, Japan*

A problem of parameter estimation for continuous-time systems is studied by employing the error entropy as a criterion functional. By examining the absolute continuity of the relevant induced measures in the function space, the entropy theorem for parameter estimation is extended to continuous-time systems. This theorem shows that the reduction in processed parameter entropy has an upper bound determined by the mutual information between the parameter and the sensor output. As an example, a linear Gaussian state estimation problem is studied using this entropy analysis.

### 1. INTRODUCTION

The general parameter estimation model of identifying the unknown parameter through observation is closely related with the Shannon's channel model. The set of unknown parameters corresponds to the information source, the observed data to output through the noisy channel, and the data processor to the decoder. Thus, in studying the parameter estimation problems, entropy and mutual information will be useful tools for estimating the system performance bound.

Recently, a problem of parameter estimation for non-linear and non-Gaussian discrete-time systems has been studied using the error entropy as a criterion functional (Weidemann and Stear, 1969). It is shown that the reduced error entropy is upper bounded by the amount of information obtained by observation. This theorem, called the entropy theorem, thus enables the system performance bounds to be estimated without explicitly determining the optimum data processor.

The present article aims to establish the entropy theorem under the description of the continuous-time estimation model. This extension is non-trivial because the entropy of continuous-time stochastic processes is no longer defined adequately and therefore, quite a different approach is to be employed.

In Section 3, a general parameter estimation problem for continuous-time