A Note on Kerdock Codes

J. Mykkeltveit[1]
Communications Systems Research Section

The performance of an important class of low-rate nonlinear binary codes recently discovered by A. M. Kerdock is superior to linear codes with the same parameters. Before these codes can be put to practical use, several questions remain to be answered. This article considers one of the questions and shows that the nonlinear Kerdock codes are systematic; i.e., they have distinguishable information and check positions.

I. Introduction

Recently A. M. Kerdock (Ref. 1) discovered an important class of low-rate *nonlinear* binary codes whose performance is superior to linear codes with the same parameters. However, before these very powerful codes can be used practically, several questions remain to be answered. The question we shall be concerned with is whether or not the codes are *systematic*. A binary code with 2^k codewords is said to be systematic if there exists a fixed set of k positions in the code which can take on any of the 2^k binary k-tuples as values. If this is so, the code has distinguishable information and check positions, a very useful property. (Every linear code is systematic, so this question rarely arises in the literature, most of the well-known codes being linear.) In this article, we shall prove that Kerdock's codes are indeed systematic.

II. Definition of Kerdock Codes and Proof That They Are Systematic

Let $m = 2\ell - 1$, α be a primitive root of $GF(2^m)$ and $Tr(\cdot)$ the trace of $GF(2^m)$ over $GF(2)$. Define

$$Q(x) = Tr(x^3 + x^5 + x^9 + \cdots + x^{1+2^{\ell-1}})$$

For A, $B \in GF(2)$ and η, $\gamma \in GF(2^m)$ define two polynomials

$$f_L(x) = Tr(\eta x) + Q(\gamma x) + A$$
$$f_R(x) = Tr(\eta x + \gamma x) + Q(\gamma x) + B$$

Then the vector of length $2^{2\ell}$

$$(A, s_0, s_1, \cdots, s_{2^m-2}; B, t_0, t_1, \cdots, t_{2^m-2}) \qquad (1)$$

$$s_i = f_L(\alpha^i), \qquad t_i = f_R(\alpha^i), \qquad i = 0, 1, \cdots, 2^m - 2$$

[1] California Institute of Technology Research Fellow.

is a word in the Kerdock code of length $2^{2\ell}$. There are two choices for A, two for B, 2^m for η, and 2^m for γ for a total of $2^{4\ell}$ codewords. Kerdock (Ref. 1) proved that the minimum distance of this code is $2^{2\ell-1} - 2^{\ell-1}$. (The best known $(2^{2\ell},4\ell)$ *linear* code has only $d = 2^{2\ell-1} - 2^{\ell}$.) We shall prove that the code is systematic by showing that the 4ℓ components $A,s_0,\cdots,s_{m-1}$, $B,t_0,\cdots,t_{m-1}$ determine A,B,η, and γ uniquely. We begin with a lemma.

Lemma. *Let α be a primitive element of $GF(2^m)$. Then for $x \in GF(2^m)$ the m elements $Tr(x\alpha^i)$, $i = 0,1,\cdots$, $m-1$, of $GF(2)$ determine x uniquely.*

Proof. If the lemma is false, there are elements $x \neq y$ such that $Tr(x\alpha^i) = Tr(y\alpha^i)$ for $i = 0,1,\cdots,m-1$. Then if $z = x - y$, $z \neq 0$, and $Tr(z\alpha^i) = 0$ for $i = 0,1,\cdots,m-1$. Let β be chosen with $Tr(\beta) = 1$. Since $1,\alpha,\cdots,\alpha^{m-1}$ is by hypothesis a basis for $GF(2^m)$ over $GF(2)$, we may write $z^{-1}\beta = w_0 + w_1\alpha + \cdots + w_{m-1}\alpha^{m-1}$ for suitable $w_i \in GF(2)$. Then $Tr(\beta) = Tr(z \cdot z^{-1}\beta) = Tr(\sum z w_i \alpha^i) = \sum w_i Tr(z\alpha^i) = 0$, a contradiction.

We can now easily prove our main result.

Theorem. *The elements A,B,η and γ can be recovered uniquely from the 4ℓ components $A,s_0,\cdots,s_{m-1},B,t_0,\cdots,t_{m-1}$ of the codeword Eq. (1).*

Proof. Of course A and B can be read off directly. Now $s_i + t_i + A + B = Tr(\gamma\alpha^i)$ and so by the lemma γ can be recovered. Finally, knowing γ we can calculate $s_i + Q(\gamma\alpha^i) + A = Tr(\eta\alpha^i)$ and so again by the lemma η can be recovered.

Reference

1. Kerdock, A. M., "A Class of Low-Rate Nonlinear Codes," *Information and Control,* Vol. 20, pp. 182–187, 1972.