International Journal of Pure and Applied Mathematics

Volume 43 No. 4 2008, 709-716

CODES FROM ORTHOGONAL ARRAYS: APPLICATION TO THREE LEVEL ORTHOGONAL ARRAYS WITH 27 RUNS

C. Koukouvinos[1] [§], E. Lappas[2]

[1,2]Department of Mathematics
School of Applied Mathematics and Physical Sciences
National Technical University of Athens
Zografou Campus, Athens, 15780, GREECE
[1]e-mail: ckoukouv@math.ntua.gr
[2]e-mail: elappas@math.ntua.gr

Abstract: In this paper we present four methods to construct linear codes from orthogonal arrays. We apply these methods, to a large database of orthogonal arrays with parameters $(27, q, 3, t)$, for $q = 3, \dots, 13$, in order to construct a variety of ternary codes. For the codes that achieve the maximum minimum distance we search for inequivalent codes.

AMS Subject Classification: 94B05, 94B25, 05B15
Key Words: linear codes, generator matrix, minimum distance, inequivalent, orthogonal array

1. Introduction

A linear code C, of length n, dimension k, and minimum distance d denoted with $[n, k, d]$ (or $[n, k]$) is a $k-$ dimensional vector subspace of a Galois field $\mathbb{F}_p^n$, where p is prime or prime power. The elements of the code C are called codewords. The number of non-zero coordinates of a codeword is called (Hamming) weight of the codeword. In the case of a linear code the minimum distance is equivalent with the minimum weight of all the codewords. A matrix G is called generator matrix of the code C if its rows generate the code C. Hence, the codewords of C are all possible linear combinations of the rows of G.

Received: February 16, 2008

[§]Correspondence author

An orthogonal array $OA(n, q, s, t)$ is an $n \times q$ array with entries from a set of s distinct symbols arranged so that, for any collection of t columns of the array, each of the s^t row vectors appears equally often. Usually orthogonal arrays are used in statitics so some terminology from this area is used to name the parameters of an orthogonal array. We call n the number of runs, q the number of factors, s the number of levels for each factor and t the strength of the array.

Orthogonal arrays and codes are related in some cases, in the sence that it is possible to construct codes from an orthogonal array and also construct orthogonal arrays from a code [1, 2, 9, 10]. In this paper we will present four methods to construct linear codes from orthogonal arrays and produce results using three level orthogonal arrays with 27 runs, and $q = 3, \ \ldots, \ 13$ factors. We will use the OA's under some transformations as a generator matrix G.

Remark 1. We should emphasize that in some cases the rows of the matrix G are linearly dependent and so G is not the actual generator matrix in a tight mathematical sence.

2. Preliminaries and Basic Definitions

We will state some useful definitions and propositions that will be used throughout this paper.

2.1. Linear Codes

Two $[n, k]$ p-acid codes C, C' are said to be *equivalent* if there are n permutations $\pi_1, \ldots, \pi_n$ of the p elements and a permutation σ of the n coordinate positions for which, each codeword $(x_1, x_2, \ldots, x_n)$ of C implies that $\sigma(\pi_1(x_1), \pi_2(x_2), \ldots \pi_n(x_n))$ is a codeword of C', see [12].

For any $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{F}_p^n$, define their inner product:

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n.$$

Let C be a p-acid linear $[n, k]$ code. Define the *dual* code of C as:

$$C^{\perp} = \{x \in \mathbb{F}_p^n | \ \ x \cdot y = 0 \ \ \forall \ y \in C\}.$$

If $C \subseteq C^{\perp}$, then C is called *self-orthogonal.*

The following well known proposition that identifies self-orthogonal codes, except binaries, can be found in [13].

Proposition 2. *Let p be a power of an odd prime and C be a p-acid linear code. Then C is self-orthogonal if and only if $c \cdot c = 0$ for all codewords $c \in C$.*

2.2. Orthogonal Arrays

In this paper we will always assume that the strength t of an orthogonal array is 2 and the set denoted by s will be $\{0,\ 1,\ \ldots,\ s-1\}$.

Remark 3. By definition any column of an orthogonal array $(n, q, s, 2)$ contains $\frac{n}{s}$ elements equal to $i = 0,\ 1,\ \ldots,\ (s-1)$, and so, n is divisible by s.

Remark 4. By definition for any selection of two columns of an orthogonal array $(n, q, s, 2)$, the following pairs will appear exactly $\frac{n}{s^2}$ times, $\{0,0\}$, $\{0,1\}$, $\ldots$, $\{0, s-1\}$, $\{1,0\}$, $\{1,1\}$, $\ldots$, $\{1, s-1\}$, $\ldots$, $\{s-1, 0\}$, $\{s-1, 1\}$, $\ldots$, $\{s-1, s-1\}$.

Two orthogonal arrays based on s symbols are said to be *isomorphic* if one can be obtained from the other by a sequence of row permutations, column permutations and permutations of symbols in each column, see [9]. As a consequence, the orthogonal arrays that will be used throughout this paper will have its first row elements equal to 0.

3. Construction Methods for Linear Codes

3.1. First Method

Let A be the matrix produced by an orthogonal array with parameters (n, q, s, t) after removing the first row of the OA, we emphasize that the elements of first row of the OA are always 0. Then define the generator matrix G as the transpose of the matrix A, that is $G = A^T$. It is obvious that the linear codes constructed with this method will have length, $n-1$.

Proposition 5. *The $[n-1, k, d]$ linear codes constructed with the method described previously are self-orthogonal.*

Proof. Let c be a codeword. Then c can be written as a linear combination of the rows of its generator matrix G,

$$c = \sum_{i=1}^{k} \lambda_i g_i \ ,$$

where with g_i we denote the i-th row of G. For $i, j,\ i \neq j$ from Remark 4 it holds that

$$\begin{aligned} g_i \cdot g_j &= (\frac{n}{s^2} - 1)(0 \cdot 0) + \frac{n}{s^2} \cdot \{(0 \cdot 1) + \cdots + (0 \cdot (s-1)) + \ldots \\ &\quad +((s-1) \cdot 0) + ((s-1) \cdot 1) + \cdots + ((s-1) \cdot (s-1))\} \\ \Rightarrow g_i \cdot g_j &= \frac{n}{s^2} \frac{(s-1)^2 s^2}{4} = n \frac{(s-1)^2}{4} \equiv 0 \pmod{s}\,. \end{aligned}$$

Similarly from Remark 3 it holds that

$$\begin{aligned} g_i \cdot g_i &= (\frac{n}{s} - 1)(0 \cdot 0) + \frac{n}{s}\{(1 \cdot 1) + \cdots + ((s-1) \cdot (s-1))\} \\ &= \frac{n}{s} \frac{(s-1)s(2s-1)}{6} = n \frac{(s-1)(2s-1)}{6} \equiv 0 \pmod{s}\,. \end{aligned}$$

So

$$c \cdot c = (\sum_{i=1}^{k} \lambda_i g_i)(\sum_{i=1}^{k} \lambda_i g_i) = 0$$

and by Proposition 2 the linear code is self-orthogonal. □

3.1.1. Codes Derived by the First Method Using Three Level Orthogonal Arrays with 27 Runs

We applied the previous method to a large number of three level orthogonal arrays with 27 runs and $q = 3, \ldots, 13$ factors. The derived codes are ternary self-orthogonal codes. All the different linear codes parameters are listed in http://www.math.ntua.gr/people/ckoukouv/. We notice that the dimension k of all codes is between 2 and 7, see Remark 1. From all these codes we focus on the code $[26, 3, 18]$ that has the maximum minimum distance $d = 18$, for length $n = 26$ and dimension $k = 3$. This code is equivalent to the code proposed by Grassl [7].

3.2. Second Method

Let A be the matrix produced by an orthogonal array with parameters (n, q, s, t) after removing the first row of the OA. Then define the generator matrix G as the matrix A, that is $G = A$. It is obvious that the linear codes constructed with this method will have length q. Although this method seems to have no theoretical background, at the moment, when applied to orthogonal arrays, the results were quite interesting.

3.2.1. Codes Derived by the Second Method Using Three Level Orthogonal Arrays with 27 Runs

We applied the previous method to a large number of three level orthogonal arrays with 27 runs and $q = 3, \ldots, 13$ factors. The derived codes are ternary and all the different linear codes parameters are listed in http://www.math.ntua.gr/people/ckoukouv/. We notice that the dimension k of all codes is between 2 and 7, see Remark 1. Below we present some interesting properties of codes that had maximum minimum distance.

1. We found one ternary code with parameters: $[13, 3, 9]$, $[12, 3, 8]$, $[11, 3, 7]$, $[9, 3, 6]$, $[8, 3, 5]$ and $[4, 3, 2]$, as it has been proved in [6] by M. van Eupen and M. Lisonek.

2. We found one ternary code with parameters $[7, 6, 2]$, $[6, 5, 2]$, $[5, 4, 2]$, $[4, 2, 3]$. These codes are equivalent to the one proposed by M. Grassl [5, 7].

3. We found one ternary code with parameters: $[13, 6, 6]$ and $[10, 7, 3]$. These codes are not equivalent to the one proposed by M. Grassl [5, 7].

4. We found one ternary code with parameters $[9, 6, 3]$. This code is not equivalent to the one proposed by M. Grassl [5, 7], while M. van Eupen and M. Lisonek in [6] proved that there are three such codes.

5. We found two ternary codes with parameters $[7, 3, 4]$. One of the codes is equivalent to the one proposed by M. Grassl [5, 7], while M. van Eupen and M. Lisonek in [6] proved that there are two such codes.

6. We found two ternary codes with parameters $[10, 3, 6]$. These codes are not equivalent to the one proposed by M. Grassl [5, 7], while M. van Eupen and M. Lisonek in [6] proved that there are six such codes.

7. We found three ternary codes with parameters $[6, 3, 3]$. One of the codes is equivalent to the one proposed by M. Grassl [5, 7], while M. van Eupen and M. Lisonek in [6] proved that there are four such codes.

8. We found two ternary codes with parameters $[5, 3, 2]$. These codes are not equivalent to the one proposed by M. Grassl [5, 7].

9. We found three ternary codes with parameters $[9, 7, 2]$. These codes are not equivalent to the one proposed by M. Grassl [5, 7].

10. We found five ternary codes with parameters: $[7, 5, 2]$ and $[6, 4, 2]$. These codes are not equivalent to the one proposed by M. Grassl [5, 7].

11. We found six ternary codes with parameters $[8, 6, 2]$. These codes are not equivalent to the one proposed by M. Grassl [5, 7].

3.3. Third Method

Let A be the matrix produced by an orthogonal array with parameters (n, q, s, t) after removing the first row of the OA. Then define the generator matrix $G = [I, A]$, where I is the identity matrix of order $n-1$. It is obvious that the linear codes constructed with this method will have length $n-1+q$ and dimension $k = n-1$, since we attached the identity matrix I and make the rows of G linear independent.

3.3.1. Codes Derived by the Third Method Using Three Level Orthogonal Arrays with 27 Runs

We applied the previous method to a large number of three level orthogonal arrays with 27 runs and $q = 3, \ldots, 13$ factors. The derived codes are ternary and all the different linear codes parameters are listed in http://www.math.ntua.gr/people/ckoukouv/. Below we present some interesting properties of codes, that had maximum minimum distance.

— We found four ternary codes with parameters $[33, 26, 4]$, $[29, 26, 2]$. These codes are not equivalent to the one proposed by M. Grassl [5, 7].

3.4. Fourth Method

Let A be the matrix produced by an orthogonal array with parameters (n, q, s, t) after removing the first row of the OA. Then define the generator matrix $G = [I, A^T]$, where I is the identity matrix of order q. It is obvious that the linear codes constructed with this method will have length $n+q$ and dimension $k = q$, since we attached the identity matrix I and make the rows of G linear independent.

3.4.1. Codes Derived by the Fourth Method Using Three Level Orthogonal Arrays with 27 Runs

We applied the previous method to a large number of three level orthogonal arrays with 27 runs and $q = 3, \ldots, 13$ factors. The derived codes will be ternary and all the different linear codes parameters are listed in http://www.math.ntua.gr/people/ckoukouv/. Below we present some interesting properties of codes, that had maximum minimum distance.

— We found two ternary codes with parameters $[29, 3, 19]$. One of these codes is equivalent to the one proposed by M. Grassl [5, 7].

Remark 6. The generator matrices of all referenced codes is uploaded in http://www.math.ntua.gr/people/ckoukouv/. All equivalency checks on codes have been performed with *MAGMA* software.

Acknowledgements

This research was financially supported from the General Secretariat of Research and Technology by a grant PENED 03ED740.

References

[1] M.L. Aggarwal, V. Budhraja, On construction of some new symmetric and asymmetric orthogonal arrays, *Discrete Math. Sci. Cryptography*, **5**, No. 3 (2002), 215-225.

[2] M.L. Aggarwal, V. Budhraja, Some new asymmetric orthogonal arrays, *J. Korean Statist. Soc.*, **32**, No. 3 (2003), 225-233.

[3] A.E. Brouwer, Bounds on linear codes, In: *Handbook of Coding Theory* (Ed-s: V.S. Pless, W.C. Huffman), Elsevier (1998), 295-461.

[4] A.E. Brouwer, Server for bounds on the minimum distance of q-ary linear codes, $q = 2, 3, 4, 5, 7, 8, 9$, http://www.win.tue.nl/∼aeb/voorlincod.html

[5] J.J. Cannon, W. Bosma, Eds., *Handbook of Magma Functions*, Edition 2.13 (2006).

[6] M. van Eupen, P. Lisonek, Classification of some optimal ternary codes of small length, *Designs, Codes and Cryptography*, **10** (1997), 63-84.

[7] M. Grassl, Bounds on the minimum distance of linear codes, http://www.codetables.de

[8] M. Grassl, Searching for linear codes with large minimum distance, In: *Discovering Mathematics with Magma* (Ed-s: Wieb Bosma, John Cannon), Springer (2006).

[9] A.S. Hedayat, N.J.A. Sloane, J. Stufken, *Orthogonal Arrays: Theory and Applications*, Springer-Verlag, New York (1999).

[10] C. Lam, V.D. Tonchev, Classification of affine resolvable 2-(27, 9, 4) designs, *Journal of Statistical Planning and Inference*, **56** (1996), 187-202.

[11] C. Lam, V.D. Tonchev, Corrigendum to classification of affine resolvable 2-(27,9,4) designs, *Journal of Statistical Planning and Inference*, **56** (1996), 187-202; *Journal of Statistical Planning and Inference*, **86** (2000), 277-278.

[12] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland Pub. Co., Amsterdam (1977).

[13] Z.X. Wan, A characteristic property of self-orthogonal codes and its application to lattices, *Bull. Belg. Math. Soc.*, **5** (1998), 477-482.