SOME NEW MOLS OF ORDER $2^n p$ FOR p A PRIME POWER

R.J.R. Abel and Y.W. Cheng

School of Mathematics,
University of New South Wales,
Kensington, N.S.W. 2033, Australia

Abstract

This paper describes a method of obtaining MOLS of order $v = 2^n p$ for p a prime power. In particular, it gives 5,7 and 9 MOLS of orders 48,40 and 80 respectively. If $x = \mathrm{Min}(2p\text{-}1, 2^n\text{-}1, 4n\text{-}2)$, it is conjectured that x MOLS of order v are always obtainable by this method.

1. Introduction

A transversal design, TD(k,λ,v) consists of a set X of kv points divided into k groups of size v plus a collection of k-element subsets of X called blocks so that:

(i) Each block contains one point from each group

(ii) Any two points in different groups appear together in λ blocks

The parameter λ is usually omitted if it equals 1; the design is then just called a TD(k,v).

Such a design is called α-resolvable (or just resolvable if $\alpha = 1$) if its blocks can be partitioned into classes so that each point appears in α blocks from each class. If $\alpha = 1$, such a class is called a parallel class. The following result is well known:

Theorem 1.1:
A TD($k+1,\lambda,v$) exists if and only if a λ-resolvable TD(k,λ,v) exists.

2. Constructions Using Difference Families

There are many TD constructions using different families. The following theorem gives one such construction:

Theorem 2.1
Suppose G is an additive abelian group of size v and there exists a $\lambda v \times k$ array A with entries from G so that for any $j_1, j_2 \in \{1 \ldots k\}$, each element of G occurs λ times amongst the differences $A_{i,j_2} - A_{i,j_1}$ ($i=1 \ldots \lambda v$). Then a resolvable TD(k,λ,v) exists.

Proof (outline): Here, and throughout this paper, rows in any difference array denote blocks. The v points in each group of the TD are written as elements of G and points in different groups are distinguished by the convention that the i' th element in any block comes from the i' th group of the TD. Let $B_i = \{A_{i,1}, A_{i,2} \ldots A_{i,k}\}$ and let $B_i + g$

denote the block obtained by adding g to all elements of B_i. It is readily confirmed that the blocks $B_i + g$ (i=1...λv, $g \in G$) form a resolvable TD(k,λ,v) with parallel classes $R_i = \{B_i + g, g \in G\}$.

The array A in Theorem 2.1 is called a TD(k,λ,v) difference array. Since being resolvable is a stronger condition than being α-resolvable, the conditions of Theorem 2.1 guarantee existence of a TD(k+1,λ,v) (by Theorem 1.1).

3. GF(2^n) as a Vector Space

Throughout this paper the variable z represents a given primitive root of unity in GF(2^n). The elements of GF(2^n) form the vector space of polynomials of degree less than n over GF(2); thus certain vector space terms such as 'linearly independent' can be defined in the normal way on the elements of GF(2^n). Also, two elements of GF(2^n), $\sum_{i=0}^{n-1} a_i z^i$ and $\sum_{i=0}^{n-1} b_i z^i$ ($a_i, b_i \in Z(2)$) are called orthogonal if $\sum_{i=0}^{n-1} a_i b_i = 0 \pmod 2$.

4. TD(k,$2^n p$) Difference Arrays

For all the new TD(k,v)'s in this paper, v is of the form $2^n p$ for p an odd prime power and the group G is GF(p) x GF(2^n). In addition, calculation of the difference array A for these TDs is simplified due to existence of an automorphism group of order 2^{n-1} which permutes the rows of A; thus only $\lambda v/2^{n-1} = 2p$ rows of A need to be specified. From here on A* will denote the array consisting of these $2p$ generating rows. The following theorem is fundamental for determining the GF(p) components for the entries in A*:

Theorem 4.1

Suppose p is an odd prime power. Then:

(i) No TD(k,2,p) difference array exists for $k > 2p$.

(ii) A TD(k,2,p) difference array exists for $k = 2p$.

Proof: See Corollary 8.3.7 in [1] for (i). Our proof of (ii) is a slight variation of their Theorem 8.3.14. Let m be any non-square in G = GF(p). We show the required difference array can be taken as $\begin{matrix} Q & R \\ S & T \end{matrix}$ where:

$$Q_{x,y} = xy \qquad R_{x,y} = (x-y)^2$$
$$S_{x,y} = xy + ((m-1)/4m)\, y^2 \qquad T_{x,y} = m(x-y)^2 \qquad (x,y \in GF(p))$$

It is easily confirmed that if U $\in$ { Q,R,S,T } and $y_1,y_2 \in$ GF(p) then $U_{x,y_1} - U_{x,y_2}$ is linear in x and hence U is a TD(k,p) difference array over GF(p). It remains to show that for any $y_1,y_2 \in$ GF(p) each element of GF(p) appears twice amongst the differences $R_{x,y_1} - Q_{x,y_2}$ and $T_{x,y_1} - S_{x,y_2}$ ($x \in$ GF(p)). A little calculation gives:

$$R_{x,y_1} - Q_{x,y_2} = (x - y_1 - y_2/2)^2 - y_2^2/4 - y_1 \cdot y_2$$
$$T_{x,y_1} - S_{x,y_2} = m(x - y_1 - y_2/2m)^2 - y_2^2/4 - y_1 \cdot y_2 \,;$$

since m is a non-square, this gives the required results.

5. An Example

Before going into the exact conditions required for our method to give a TD(k,$2^n p$), a small example is given - for $v = 48$, $p = 3$, $n = 4$, $k = 6$. Let z be a primitive element of GF(16) satisfying $z^4 = z + 1$. As mentioned in the previous section, A* will denote the array consisting of the $2p$ generating rows of A. Also, T(y) will represent the total of the GF(2^n) entries in column y of A*. For the current example, A* and T are:

A*:						
	(0,0)	(0,0)	(0,0)	(0,0)	(1,0)	(1,0)
	(0,0)	(1,0)	(2,1)	$(1,z^3+z)$	$(0,z^3+z)$	$(1,z^3)$
	(0,0)	(2,0)	$(1,z^2+z)$	$(1,z+1)$	$(1,z^2+z)$	$(0,z+1)$
	(0,0)	$(2,z^3)$	$(2,z^3+z^2)$	$(0,z^2)$	$(2,z^3+z)$	$(2,z^2+z)$
	(0,0)	$(0,z^3)$	$(1,z^2+z+1)$	$(2,z^3)$	$(0,z^2+z)$	$(2,z^2+1)$
	(0,0)	$(1,z^3)$	$(0,z^3+z)$	(2,0)	$(2,z^2)$	$(0,z)$
T:	0	z^3	z^2+z	z^2+1	z^2	z^3+z

Also relevant to this design is the following 3x6 array Y:

<u>y</u>	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>
$Y(1,y)$	0	1	z^2	z^2+z	z^3+1	z^3+z^2
$Y(2,y)$	0	z	z^3	z^3+z^2	1	z^3+z+1
$Y(3,y)$	0	z^2	$z+1$	z^3+z+1	z	z^2+1

The rows of the required TD(6,48) difference array are now obtained as follows:

If $A^*(x,y) = (a,b)$ then define three automorphisms τ_i $(i=1,2,3)$ by $\tau_i(\ A^*(x,y)\ ) = (\ a, b+Y(i,y)\ )$. Applying the automorphism group generated by τ_1, τ_2 and τ_3 to all 6 rows of A* gives 48 distinct rows; these form a suitable TD(6,48) difference array A.

6. Obtaining the Array A* in General

All TD($k,2^np$) difference arrays in this paper are obtained by a method similar to that used for the TD(6,48) in the previous section. First, a $2p$ x k array A* with entries from GF(p) x GF(2^n) and a (n-1) x k array Y with entries from GF(2^n) are given. For convenience two additional arrays B*, C* are defined as follows: if $A^*(x,y) = (a,b)$ then $B^*(x,y) = a$ and $C^*(x,y) = b$. Next, automorphisms τ_i $(i=1...n-1)$ are defined as follows: if $A^*(x,y) = (a,b)$ then $\tau_i(x,y) = (\ a,\ b+Y(i,y)\ )$. Finally, let A be the array consisting of the 2^np rows obtained by applying the automorphism group generated by τ_i (i = 1...n-1) to the rows of A*. A will be a TD(k,$2^n p$) over GF(p) x GF(2^n) if conditions 6.1 - 6.3 below hold for any y_1,y_2 and any $g \in$ GF(p).

6.1: Y(i,y_2) - Y(i,y_1) (i = 1...n-1) are linearly independent.

6.2: There are exactly two values of x in {1...2p} such that B*(x,y_2) - B*(x,y_1) = g.

6.3: If x_1,x_2 are the two x values in 6.2 then exactly one of C*(x_i,y_2) - C*(x_i,y_1) (i = 1,2) lies in V(y_1,y_2) where V(y_1,y_2) is the n-1 dimensional vector space over GF(2) spanned by (Y_{i,y_2} - Y_{i,y_1}) (i = 1...n-1).

If conditions 6.1 - 6.3 hold for any given y_1,y_2 and all $g \in$ GF(p) then columns y_1,y_2 of A*,B*,C* and Y are said to be perpendicular.

Note that condition 6.2 holds for all y_1,y_2,g if and only if B* is a TD(k,2,p) difference array. Also each of the n-1 dimensional vector spaces V(y_1,y_2) in 6.3 is most easily specified by giving the element H(y_1,y_2) of GF(2^n) orthogonal to all its elements. For the TD(6,48) given earlier, the H(y_1,y_2) values for $y_1 < y_2$ are:

y_1 \ y_2	2	3	4	5	6
1	z^3	$z+1$	z^3+z^2+z	z^2	z^3+z^2+1
2		z^2+1	z^2+z	z^2+z+1	z
3			1	z	z^2+z+1
4				z^3+1	z^3+z+1
5					z^2+1

Four convenient assumptions that will be made are:

6.4 $\quad Y(i,1) = 0 \ (i = 1 \ldots n\text{-}1)$

6.5 $\quad Y(1,2) = 1$

6.6 $\quad C^*(x,1) = 0 \ (x = 1 \ldots 2p)$

6.7 $\quad C^*(1,y) = 0 \ (y = 1 \ldots k)$

From 6.3, exactly p of the values $C^*(x,y_2) - C^*(x,y_1)$ must be orthogonal to $H(y_1,y_2)$ for any y_1,y_2; since p is odd, this means that $T(y_2) - T(y_1) = \sum_{x=1}^{2p}(C^*(x,y_2) - C^*(x,y_1))$ is not orthogonal to $H(y_1,y_2)$. If 6.4, 6.6 hold, this condition will be met if T(2) is not orthogonal to H(1,2) and the entries in T,Y are obtained using the following formulae:

6.8 $$T(y) = \frac{T(2)}{Y(1,2)} \cdot Y(1,y)$$

6.9 $$Y(x,y) = \frac{Y(x,2)}{Y(1,2)} \cdot Y(1,y)$$

To use these formulae, the only entries in T,Y that need to be specified are T(2) plus the first row and second column of Y. Note that the entries in T,Y for the TD(6,48) in Section 5 satisfy 6.8 and 6.9.

If 6.8 and 6.9 hold, we can also assume:

6.10 $\quad C^*(x,2) \in \{0, T(2)\}$ for all x.

Proof: If 6.10 does not hold for any given x then there is an automorphism in the group generated by τ_i ($i = 1...n - 1$) which adds:

<u>$Y(1,y)$</u>. $C^*(x,2)$ to $C^*(x,y)$ ($y = 1...k$) if $C^*(x,2) \in V(1,2)$ or $Y(1,2)$

<u>$Y(1,y)$</u>. $[C^*(x,2) + T(2)]$ to $C^*(x,y)$ ($y = 1...k$) if $C^*(x,2) \notin V(1,2)$ $Y(1,2)$

After applying this automorphism to row x of C^* we obtain $C^*(x,1) = 0$ and $C^*(x,2) = 0$ (in the first case) or $C^*(x,2) = T(2)$ (in the second case).

<u>7. Obtaining C* and a Practical Upper Limit on *k*</u>

Section 3 gave a possible formula for B^*; thus the major part of the work in finding these designs is obtaining a solution for C^*. It is easy to show that if $\alpha < k$ and B^*, T and Y plus α columns of C^* are specified then finding the remaining columns of C^* comes down to solving a set of linear equations mod 2. For $0 \leq t \leq n - 1$, let:

$CC^*(x,y,t)$ = coefficient of z^t in $C^*(x,y)$
$TT^*(x,y,t)$ = coefficient of z^t in $T^*(x,y)$
$HH^*(y_1,y_2,t)$ = coefficient of z^t in $H^*(y_1,y_2)$

The equations required to determine the entries of C^* are as follows:

- To give the correct column totals $T(y)$:

<u>7.5</u> $$\sum_{x=1}^{2p} CC^*(x,y,t) = TT(y,t) \qquad (0 \leq t \leq n\text{-}1,\ \alpha+1 \leq y \leq k)$$

- To ensure perpendicularity of columns y_1, y_2 in B^*, C^*, Y:

7.6 Whenever x_1, x_2 satisfy $B^*(x_1,y_2) - B^*(x_1,y_1) = B^*(x_2,y_2) - B^*(x_2,y_1)$ then

$$\sum_{t \mid HH^*(y_1,y_2,t) = 1} [\, CC^*(x_2,y_2,t) - CC^*(x_2,y_1,t) + CC^*(x_1,y_2,t) - CC^*(x_1,y_1,t) \,] = 1$$

$$(\alpha+1 \le y_1 \le k,\ 1 \le y_2 \le y_1\text{-}1).$$

Two obvious upper limits on k are (i) $k \le 2p$ (since by Theorem 3.1, a TD(k,2,p) difference array cannot exist for $k > 2p$) and (ii) $k \le 2^n$ (since the values $Y_{1,y}$ ($y = 1...k$) must all be distinct). From here on, we assume the entries in C*, Y and T satisfy conditions 6.4 - 6.10. Given this, we now show that provided $\alpha \ge 2$, the number of non-redundant variables equals the number of non-redundant linear equations to be solved if $k = 4n - \alpha + 1$. When $\alpha = 2$ this gives $k = 4n - 1$; thus in most practical cases, the maximum possible value of k is likely to be approximately min($2p$,2^n,$4n$-1).

When $\alpha \ge 2$, 6.10 does not affect the number of non-redundant variables. In this case, the only redundant variables $CC^*(x,y,t)$ are for $x = 1$ (by 6.7). The non-redundant variables for which solutions have to be found are $CC^*(x,y,t)$ for $2 \le x \le 2p$, $\alpha+1 \le y \le k$ and $0 \le t \le n\text{-}1$. In other words, the number of non-redundant variables is $(2p\text{-}1)(k\text{-}\alpha)n$ ($= (4n\text{-}2\alpha\text{-}1)n(2p\text{-}1)$ if $k = 4n\text{-}\alpha\text{-}1$).

We now calculate the number of non-redundant linear equations.

As mentioned earlier when 6.4 - 6.10 hold, $T(y_2) - T(y_1)$ does not lie in $V(y_1,y_2)$. With this condition, any p - 1 of the p equations in 7.6 for given y_1,y_2 plus the equations in 7.5 for $y = y_1,y_2$ imply the p'th equation in 7.6 for y_1,y_2. Thus, for all y_1,y_2, the p'th equation in 7.6 can be considered redundant and there are:

$(p\text{-}1)(k\text{-}\alpha)(\ \alpha+(k\text{-}1)\ )/2$ non-redundant equations in 7.6 for all y_1,y_2
$n(k\text{-}\alpha)$ equations in 7.5 for all y.

Thus when $k = 4n - \alpha + 1$, the total number of non-redundant equations is $(4n\text{-}2\alpha+1)[(p\text{-}1)2n + n] = (4n\text{-}2\alpha+1)n(2p\text{-}1)$, the total number of non-redundant variables as required.

8. Concluding Remarks

A few computer runs showed that for some choices of α, B*, Y and T the linear equations in 7.5 and 7.6 may have no solution even if the first α columns of Y, B* and C* are perpendicular and satisfy conditions 6.4 - 6.10. However, the following two problems remain open:

(i) If p is an odd prime power and $k = \mathrm{Min}(2p, 2^n, 4n-1)$ then can a TD($k,2^np$) difference array always be obtained by the method described?

(ii) Are there any values of p,n,k with $k > 4n - 1$ for which the method described can give a TD($k,2^np$) difference array?

For p prime (not a prime power), either (i) $n \leq 5$ $p \leq 17$ or (ii) $n \leq 7$ $p \leq 7$, $p < \mathrm{Min}(2^n, 4n-2)$ and $k = \mathrm{Min}(2p, 2^n, 4n-1)$ we tried to obtain by computer a TD($k,2^np$) difference array by the method described. Solutions were found for all possible values of n,p,k. Two of these difference arrays, namely TD(8,40) and TD(10,80) are given in Appendix A. The larger ones will appear in the first author's thesis. The values of k and $v = 2^np$ for which we found a TD(k,v) difference array (and hence also k - 1 MOLS of order v) are given in Table 8.1.

Table 8.1

k	v	k	v
6	24,48	15	176,208
8	40,56	19	352,416,544
10	80,160,640		
14	112,224,896		

Alternative constructions for 7 MOLS of order 56 and 5 MOLS of order 24 are known (see [2],[3]). However, for the other values of v,k in Table 8.1, no set of k - 1 MOLS of order v appears to have been published, although C. Colbourn has informed us that C. Roberts has obtained 5 MOLS of order 48.

Appendix A

Here suitable arrays A* and Y are given for TD(8,40) and TD(10,80) difference arrays. For convenience, the elements of GF(2^n) (but not GF(p)) are given exponentially; i.e. if z is a root of the given irreducible polynomial for GF(2^n), the element z^i is specified as i. Also, the zero element of GF(2^n) is specified as Z.

A TD(8,40) array:

Irreducible polynomial for GF(2^3): $z^3 + z + 1$.

Y:	Z	0	1	6	5	4	3	2
	Z	1	2	0	6	5	4	3

A*:	(0,Z)	(0,Z)	(0,Z)	(0,Z)	(0,Z)	(0,Z)	(1,Z)	(4,Z)
	(0,Z)	(1,Z)	(2,5)	(3,4)	(4,6)	(1,2)	(0,3)	(1,3)
	(0,Z)	(2,2)	(4,5)	(1,4)	(3,Z)	(4,6)	(1,2)	(0,0)
	(0,Z)	(3,2)	(1,2)	(4,0)	(2,3)	(4,4)	(4,5)	(1,1)
	(0,Z)	(4,2)	(3,6)	(2,5)	(1,4)	(1,0)	(4,Z)	(4,0)
	(0,Z)	(2,Z)	(3,4)	(3,Z)	(2,1)	(0,6)	(2,3)	(3,1)
	(0,Z)	(3,Z)	(0,0)	(1,0)	(1,Z)	(2,3)	(0,0)	(2,5)
	(0,Z)	(4,Z)	(2,1)	(4,1)	(0,4)	(3,6)	(2,2)	(0,Z)
	(0,Z)	(0,2)	(4,1)	(2,2)	(4,0)	(3,5)	(3,0)	(2,1)
	(0,Z)	(1,2)	(1,6)	(0,3)	(3,2)	(2,5)	(3,Z)	(3,Z)

A TD(10,80) array:

Irreducible polynomial for GF(2^4): $z^4 + z + 1$.

Y:	Z	0	1	14	12	7	2	11	3	6
	Z	1	2	0	13	8	3	12	4	7
	Z	2	3	1	14	9	4	13	5	8

A*:	(0,Z)	(0,Z)	(0,Z)	(0,Z)	(0,Z)	(0,Z)	(1,Z)	(4,Z)	(4,Z)	(1,Z)
	(0,Z)	(1,Z)	(2,8)	(3,11)	(4,8)	(1,8)	(0,6)	(1,9)	(4,6)	(4,9)
	(0,Z)	(2,3)	(4,6)	(1,0)	(3,14)	(4,14)	(1,1)	(0,7)	(1,2)	(4,1)
	(0,Z)	(3,Z)	(1,3)	(4,9)	(2,14)	(4,12)	(4,4)	(1,1)	(0,Z)	(1,0)
	(0,Z)	(4,3)	(3,3)	(2,0)	(1,12)	(1,1)	(4,13)	(4,8)	(1,13)	(0,4)
	(0,Z)	(2,Z)	(3,13)	(3,7)	(2,10)	(0,1)	(2,6)	(3,5)	(3,8)	(2,5)
	(0,Z)	(3,3)	(0,13)	(1,8)	(1,10)	(2,8)	(0,14)	(2,14)	(3,2)	(3,Z)
	(0,Z)	(4,Z)	(2,6)	(4,10)	(0,3)	(3,12)	(2,9)	(0,0)	(2,0)	(3,5)
	(0,Z)	(0,3)	(4,14)	(2,10)	(4,5)	(3,6)	(3,0)	(2,Z)	(0,14)	(2,Z)
	(0,Z)	(1,3)	(1,12)	(0,11)	(3,8)	(2,1)	(3,3)	(3,0)	(2,Z)	(0,Z)

References

[1]. T. Beth, D. Jungnickel and H. Lenz, "Design Theory", Cambridge Univ. Press, Cambridge, England, 1986.

[2]. W.H. Mills, "Some Mutually Orthogonal Latin Squares", *Proc. 8th S-E Conf. on Combinatorics, Graph Theory and Computing* (1977), 473-487.

[3]. C. Roberts, "Sets of Mutually Orthogonal Latin Squares with 'like subsquares' ", *J. Combin. Theory Ser. A* 61, (1992), 50-63.

(Received 17/1/94)