AN ALGORITHM FOR ORTHOGONAL DESIGNS

Peter Eades, Peter J. Robinson,

Jennifer Seberry Wallis, Ian S. Williams

Research School of Physical Sciences

Institute of Advanced Studies

Australian National University

Abstract

Let $A = (s_i)$ be an n-tuple of positive integers such that $\Sigma s_i = 2^k$. We give an algorithm which shows that there exists a $p = (R_A(n, k) - (k+1))$ such that there is an orthogonal design of type $(2^p s_1, 2^p s_2, \ldots, 2^p s_n)$ in order 2^{k+p}. We evaluate the maximum of p over n-tuples A which add to 2^k. Hence we deduce that for any n and k there is an integer $q = \max_A R_A(n, k) - (k+1)$ such that for any n-tuple A there is an orthogonal design of type $2^q A$ in order 2^{q+k}.

1. Introduction

An orthogonal design of order n and type $(s_1, s_2, \ldots, s_u)$ $(s_i > 0)$ on the commuting variables $x_1, x_2, \ldots, x_u$ is an $n \times n$

PROC. FIFTH MANITOBA CONFERENCE ON
NUMERICAL MATH., 1975, pp. 279-292.

matrix A with entries from $\{0, \pm x_1, \ldots, \pm x_u\}$ such that

$$AA^t = \left(\sum_{i=1}^{u} s_i x_i^2\right) I_n .$$

Alternatively, the rows of A are formally orthogonal and each row has precisely s_i entries of the type $\pm x_i$.

In [1], where this was first defined and many examples and properties of such designs were investigated, it is mentioned that

$$A^t A = \left(\sum_{i=1}^{u} s_i x_i^2\right) I_n$$

and so the alternative description of A applies equally well to the columns of A . It is also shown in [1] that $u \leq \rho(n)$, where $\rho(n)$ (Radon's function) is defined by

$$\rho(n) = 8c + 2^d$$

when

$$n = 2^a \cdot b \ , \quad b \ \text{odd}, \quad a = 4c + d \ , \quad 0 \leq d < 4 \ .$$

In a recent paper [4] one of us showed that a knowledge of orthogonal designs of type $(s_1, s_2, \ldots, s_n)$ where $\Sigma s_i = 2^k$ was the tool needed to gain deep insight into the existence question for Hadamard matrices. She also believes that the solution of the conjectures on the existence of weighing matrices and orthogonal designs is dependent on the knowledge of these designs.

Warren W. Wolfe developed the idea that "algebraic" existence questions about orthogonal designs can be answered by considering the properties of rational matrices. D. Shapiro has proved that these "algebraic" existence questions in orders $2^t n$, n odd, are completely answered by his results on "algebraic" existence in order 2^t.

This paper gives more knowledge about "combinatorial" existence in orders 2^t.

The following lemma which follows from results in [1] is needed in the algorithm of section 3:

LEMMA. *There exists an orthogonal design of type* $(1, 1, 2, 4, \ldots, 2^{t-1})$ *in order* 2^t.

2. n-tuples of the form $(2^p b_1, 2^p b_2, \ldots, 2^p b_n)$

We begin with a lemma about sequences of binary numbers. Use $\sum A$ to denote the sum of the entries of a sequence A.

LEMMA. *Let* $A = (b_1, b_2, \ldots, b_n)$ *be a sequence of ascending powers of* 2. *Suppose* $b_1 = b_2 = 1$ *and* $\Sigma A = 2^k$ *for some* $k > 0$. *Then we can decompose* A *into subsequences*

$$
\begin{aligned}
d_0 &= (1, 1) \\
d_1 &= (b_3, b_4, \ldots, b_{j_1}) \\
&\cdot \\
&\cdot \\
&\cdot \\
d_{k-1} &= (b_{j_{k-2}+1}, \ldots, b_{j_{k-1}})
\end{aligned}
$$

such that $\Sigma d_i = 2^i$, $i \le k$.

Proof. Use induction over k .

Let $A = (s_1, s_2, \ldots, s_n)$ be an n-tuple of positive integers adding to 2^k. Suppose the binary expansion of s_i is $(e_{ij})_{0 \le j \le k}$, let $e_j = \sum_{i=1}^{n} e_{ij}$. We define the *binary decomposition* of A to be

$$B = (1, 1, \ldots, 1, 2, 2, \ldots, 2, 4, \ldots, 2^{k-1}) = (b_1, b_2, \ldots, b_q)$$

where 2^j is repeated e_j times. We say the *binary length* of A is $q = R_A(n, k)$, the number of entries of B .

Suppose there is an orthogonal design of type $2^r B$ in order $2^r m$, for some $r \ge 0$. Then equating variables there is an orthogonal design of type $2^r A$ in order $2^r m$. Also, suppose C is the sequence derived from B by replacing some entry 2^j by the two entries 2^{j-1} and 2^{j-1} , and then re-ordering. Then (also by equating variables) there is an orthogonal design of type $2^{r+1} C$ in order $2^{r+1} m$. Hence we state:

THEOREM 1. *Let* $A = \{s_i\}$ *be an* n*-tuple of positive integers such that at least two entries of* A *are odd, and* $\Sigma A = 2^k$. *Then there is an orthogonal design of type* $2^p A$ *in order* 2^{p+k} , *where* p *is the binary length of* A *minus* $k + 1$.

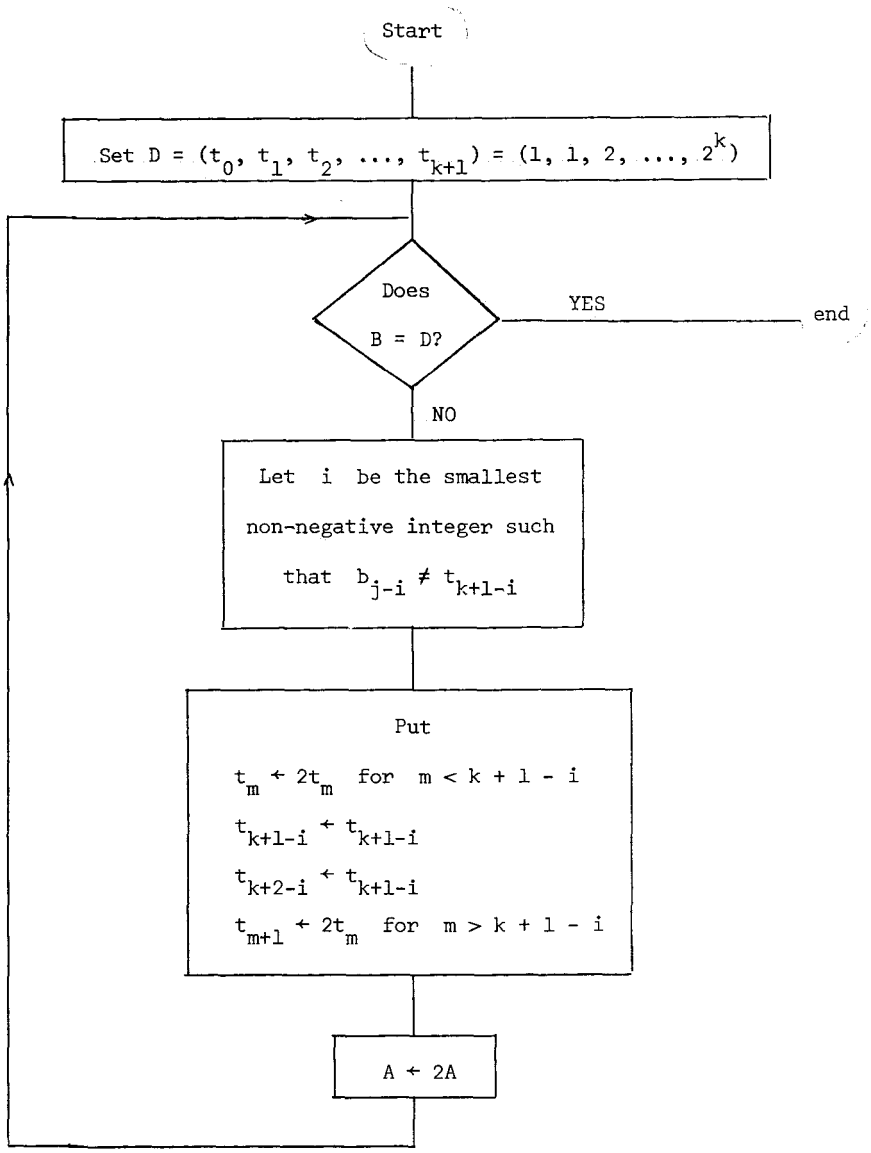
Proof. Let B be the binary decomposition of A and let $D = (1, 1, 2, 4, \ldots, 2^{k-1})$. Then there is an orthogonal design of type D in order 2^k; so, using the process of the lemma, we can transform D into 2^pB.

The transformation of D into 2^pD is described in a flowchart below.

Example. A theorem of P. Robinson [2] shows that there is no orthogonal design of type $(1, 1, 1, 1, 1, 2^t-5)$ in any order $2^t > 40$. Now $2^t - 5$ has a binary expansion $1 + 2 + 2^3+2^4 + \ldots + 2^{t-1}$; so $B = (1, 1, 1, 1, 1, 1, 2, 8, 16, \ldots, 2^{t-1})$ and $p = t + 4 - (t+1) = 3$. Hence there is an orthogonal design of type $(2^3.1, 2^3.1, 2^3.1, 2^3.1, 2^3.1, 2^3(2^t-5))$ in every order 2^{t+3}.

3. Description of the Construction Algorithm

Let A be an n-tuple of positive integers and let B be the binary decomposition of A described in section 2. We write $B = (b_1, b_2, \ldots, b_j)$. Then the algorithm proceeds as follows:


Start
Set D = $(t_0, t_1, t_2, \ldots, t_{k+l}) = (1, 1, 2, \ldots, 2^k)$
Does
B = D?
YES
end
NO
Let i be the smallest non-negative integer such that $b_{j-i} \neq t_{k+l-i}$
Put
$t_m \leftarrow 2t_m$ for $m < k + l - i$
$t_{k+l-i} \leftarrow t_{k+l-i}$
$t_{k+2-i} \leftarrow t_{k+l-i}$
$t_{m+l} \leftarrow 2t_m$ for $m > k + l - i$
$A \leftarrow 2A$

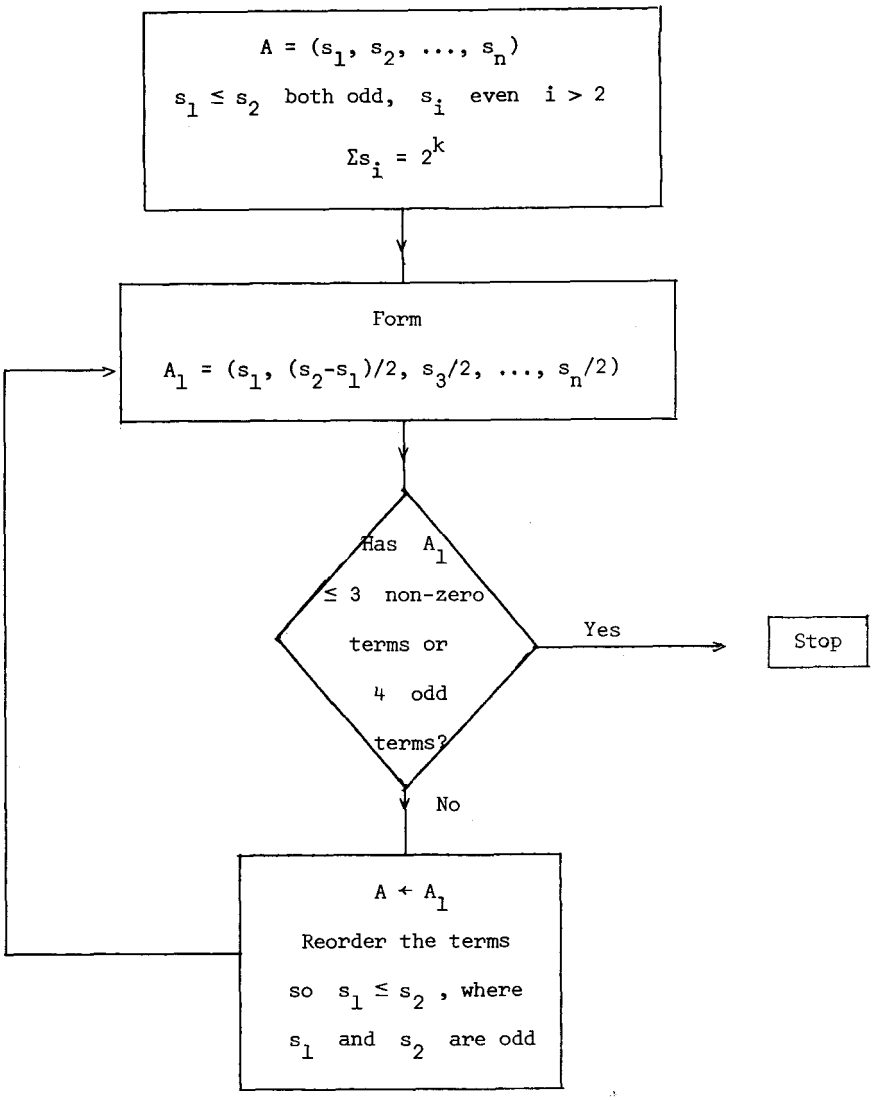
4. Implementing the algorithm

If all the entries of the n-tuple $A = (s_1, \ldots, s_n)$, $\Sigma s_i = 2^k$, in order 2^k are divisible by 2^i we consider the n-tuple $A/2^i$ in order 2^{k-i}. Theorem 1 allows us to calculate r when at least two s_i are odd showing the algorithm is finite.

Suppose $n \leq 3$. Then by a theorem of J. Wallis [4] A corresponds to the type of an orthogonal design.

Suppose $n > 3$ and 2^j is the highest power of two which divides each s_i. Then we can use Theorem 1 with the n-tuple $(s_1/2^j, \ldots, s_n/2^j) = (t_1, \ldots, t_n)$ in order 2^{k-j}.

In fact for $n > 3$ and only two odd entries in A we can usually use the following process to obtain a starting point for the algorithm in a lower power of 2.


A = (s1, s2, ..., sn)
s1 ≤ s2 both odd, si even i > 2
Σsi = 2^k
Form
A1 = (s1, (s2-s1)/2, s3/2, ..., sn/2)
Has A1 ≤ 3 non-zero terms or 4 odd terms?
Yes
Stop
No
A ← A1
Reorder the terms so s1 ≤ s2 , where s1 and s2 are odd

Example. Consider the 5-tuple $A = (3, 3, 6, 20, 96)$ in order 128. $R_A(5, 7) = 10$ so Theorem 1 guarantees the existence of a 5-tuple $(2^3\cdot 3, 2^3\cdot 3, 2^3\cdot 6, 2^3\cdot 20, 2^3\cdot 96)$ in order 2^{10}. But if we use the method of this section we form $(3, (3-3)/2, 6/2, 20/2, 96/2) = (3, 3, 10, 48)$ in order 64 and then $(3, (3-3)/2, 10/2, 48/2) = (3, 5, 24)$ in order 32. But all 3-tuples $(a, b, 32-a-b)$ exist in order 32 so $(3, 3, 6, 20, 96)$ *is* the type of an orthogonal design in order 128.

5. The power of 2 in Theorem 1

Let $A = (a_1, a_2, \ldots, a_n)$ be a sequence such that $\sum_{i=1}^{n} a_i = 2^t$. Let $a_i = b_{i0} + b_{i1}.2 + \ldots + b_{ik_i} 2^{k_i}$ be the binary expansion of a_i.

Define

$$R_A(n, t) = \sum_{i=1}^{n} \sum_{j=0}^{k} b_{ij} , \quad k = \max_i k_i ,$$

and

$$R(n, t) = \max_A R_A(n, t) .$$

Now assume there exists a j such that one of the b_{ij}'s is non zero, say b_{1j}, and two of the $b_{i,j-1}$'s are zero, say $b_{n-1,j-1}$ and $b_{n,j-1}$, then we consider the sequence

$$A_1 = (a_1 - 2^j, a_2, \ldots, a_{n-2}, a_{n-1} + 2^{j-1}, a_n + 2^{j-1}) .$$

Now

$$R_{A_1}(n, t) = R_A(n, t) + 1 ,$$

and hence any sequence A such that $R_A(n, t) = R(n, t)$ has the property that the sequences $(b_{1j}, b_{2j}, \ldots, b_{nj})$, $j = 0, \ldots, k - 1$, contain as many one's as possible. That is, $(b_{1j}, \ldots, b_{nj})$, $j = 0, \ldots, k -$ contains at most one zero.

Now, we let the binary expansion of $n - 1$ be $c_0 + c_1.2 + \ldots + c_m 2^m$ and consider the following $n \times (m+2)$ matrix

$$X = \begin{bmatrix} 1 & 1 & \dots & 1 & 1 & c_0 \\ 2 & 2 & \dots & 2 & 2 & c_1.2 \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ 2^m & 2^m & \dots & 2^m & 2^m & c_m.2^m \\ 2^{m+1} & \dots & 2^{m+1} & 0 & \dots & 0 \end{bmatrix}$$

Let the number of 2^{m+1}'s in the last row be a.

The sum, S, of all the entries in this matrix is

$$\begin{aligned} S &= (n-1-a)(2^{m+1}-1) + a(2^{m+2}-1) + n - 1 \\ &= (n-1-a)2^{m+1} + a.2^{m+2} \\ &= 2^{m+1}(n-1+a) . \end{aligned}$$

Now $m = [\log_2(n-1)]$ and so, when $n \neq 2^j + 1$ for some j, $n - 1 \leq 2^{m+1} < 2(n-1)$. However, since $0 \leq a \leq n - 1$, we can find an a such that

$$n - 1 + a = 2^{m+1} \quad \text{that is} \quad a = 2^{m+1} - n + 1$$

and so

$$S = 2^{2m+2} .$$

We now consider the matrix Y, which is obtained from X by replacing all non zero terms by 1, and define a sequence $A = \{a_i\}$ by letting row j of Y be $(b_{1j}, b_{2j}, \dots, b_{nj})$ and choosing $a_i = \sum_{j=0}^{m+1} b_{ij}2^j$.

It is obvious that the sequences $(b_{1j}, \dots, b_{nj})$,

$j = 0, \ldots, m$, are as full as possible, and since

$$S = 2^{2m+2} ,$$

$$R_A(n, 2m+2) = R(n, 2m+2) . \qquad (1)$$

But

$$R_A(n, 2m+2) = a + (n-1)(m+1) + B(n-1) ,$$

where $B(n-1)$ is the number of non zero terms in the binary expansion of $n - 1$.

Therefore

$$R(n, 2m+2) = 2^{m+1} + (n-1)m + B(n-1) .$$

We now consider

$$R(n, 2m+3) .$$

From our choice of a , it can be seen that

$$(n-1-a)2^{m+2} + a.2^{m+3} = 2^{2m+3} .$$

Therefore, to obtain an A such that $R_A(n, 2m+3) = R(n, 2m+3)$ we use the A of (1) and put $b_{a+1,\,m} = b_{a+2,\,m} = \ldots = b_{n-1,\,m} = 1$, $b_{nm} = 0$ and $b_{1,m+1} = b_{2,m+1} = \ldots = b_{a,m+1} = 1$. This produces sequences as full as possible and therefore $R(n, 2m+3) = R(n, 2m+2) + (n-1)$. We continue in this way to obtain the following

$$R(n, 2m+i) = 2^{m+1} + B(n-1) + (n-1)(m+i-2) \quad \text{where} \quad i = 2, 3, \ldots .$$

We note that if $n = 2^m + 1$ then

$$2^{2m} = (n-1)(2^m-1) + n - 1 .$$

So

$$R(2^m+1, 2m) = 2^m m + 1 .$$

The maximum number of steps in the algorithm of section 3 is $R(n, t) - (t+1)$. The actual number of steps for an n-tuple A is $p = R_A(n, t) - (t+1) \leq R(n, t) - (t+1)$. We have shown that $R(n, t)$ is finite and may be evaluated easily; hence the algorithm is finite.

References

[1] A.V. Geramita, Joan Murphy Geramita, Jennifer Seberry Wallis, Orthogonal designs, *Linear and Multilinear Algebra.*

[2] Peter J. Robinson, A non-existence theorem for orthogonal designs,

[3] D. Shapiro, private communication (1975).

[4] Jennifer Seberry Wallis, On the existence of Hadamard matrices, *J. Combinatorial Th.* Ser. A.

[5] Warren W. Wolfe, *Orthogonal designs - amicable orthogonal designs - some algebraic and combinatorial techniques,* PhD Dissertation, Queen's University, Kingston, Ontario, 1975.