New D-optimal designs of order 110

Roderick J. Fletcher

8460 Greystone Ln. Apt. 2F,
Columbia, Maryland 21045, USA

Jennifer Seberry*

Centre for Computer Security Research
School of Information Technology and Computer Science
The University of Wollongong
Wollongong NSW 2522, Australia

Abstract

We give two new D-optimal designs of order 110.

1 Introduction

A D–optimal design of order n is an $n \times n$ matrix with entries ± 1 having maximum determinant.

If $n \equiv 2 \pmod 4$, $n \neq 2$, Ehlich [6] showed that

$$d_n \leq (2n-2)(n-2)^{\frac{n}{2}-1}$$

and equality can hold only if $2n - 2 = x^2 + y^2$, where x and y are integers. Ehlich himself found matrices yielding equality for the seven values of $n \leq 38$, and Yang [14, 15, 16, 17, 18] for the next six values 42, 46, 50, 54, 62, and 66. Matrices yielding equality of the other values of n are constructed as follows: $n = 86$ [2], $n = 74, 82, 90, 98, 102$ [3, 4], $n = 114, 146, 182$ [12], $n = 122$ [13], $n = 126, 186$ [5], $n = 150$ [10]. Recently two infinite series of $n \times n$ ($n \equiv 2 \pmod 4$) matrices with elements ± 1 and maximum determinant were discovered. The first series (Koukouvinos-Kounias-Seberry-Singer-Spence $KKSSS$) [12], exists for $n = 2(q^2 + q + 1)$ where q is a prime power. The second series (Whiteman-Brouwer WB) [13], exists for $n = 2(2q^2+2q+1)$ where q is an odd prime power.

D-optimal designs of order $2v \equiv 2 \pmod 4$ can be constructed using two circulant ± 1 matrices A and B, of order v, satisfying

$$AA^T + BB^T = (2v-2)I_v + 2J_v.$$

Then D given by

*Research supported by ARC Large Grants A9803826 and A49703117.

$$D = \begin{bmatrix} A & B \\ B^T & -A^T \end{bmatrix}.$$

is a D-optimal design of order $2v \equiv 2 \pmod 4$.

The D-optimal design satisfies

$$DD^T = (2v-2)I_{2v} + 2I_2 \times J_v.$$

We conducted a search for a D-optimal design of order 110 using the power spectral density (PSD) test as described in Fletcher, Gysin and Seberry [8]. The PSD test makes use of a relationship between the discrete Fourier transforms and the periodic autocorrelation functions of the first rows of the matrices A and B, defined above. The PSD of a sequence is defined by taking the squared magnitude of each term in its discrete Fourier transform. It is shown in [8] that the sum of the PSDs of the first rows of A and B is a constant sequence. Moreover, the vast majority of ± 1-sequences that could form these rows (based on the number of ones and minus ones comprising them) have PSDs that exceed this constant in one or more of their terms. Since the PSDs are non-negative, it follows that such sequences can be eliminated from further consideration. Thus, only a small fraction of all possible sequences are left as viable candidates.

In this instance, we used the PSD test to find the first rows of circulant ± 1 matrices of order 55 satisfying

$$AA^T + BB^T = 108I_{55} + 2J_{55}.$$

Approximately four million sequences containing 34 ones and 21 minus ones passing the PSD test were found by random search, and one million candidate sequences with 31 ones and 24 minus ones were likewise found. The combined search time was about 94 hours on a personal computer using a 200 MHz Pentium ^{TM} microprocessor. As the search procedure eliminates shifts of the sequences and involves decimations, which correspond to multiplying all the elements of a set by an element x with $\gcd(x, 55) = 1$, solutions arising from different PSD are inequivalent.

Two solutions for the first rows of A and B were found as follows:

```
---11-1--111-11---11--1--1--1-1-1-1-1--1111111111--111
----1-111-11--1111-1111-1--1-111-111-1----11111-11-1111.

---1-----11-11-11--1111-1-111-1-1-11111111--111-1111-11
----1-1---1111-1-11-1111---1--1111-1--11--11-11-1-11111.
```

Alternatively these can be described as $2-(55; 21, 24; 18)$ supplementary difference sets.

This is the first time a D-optimal design has been found for order 110.

References

[1] A.E. Brouwer, An infinite series of symmetric designs, *Math. Centrum Amsterdam Report ZW* 202/83, 1983.

[2] T. Chadjipantelis, and S. Kounias, Supplementary difference sets and D-optimal designs for $n \equiv 2 \bmod 4$, *Discrete Math.*, 57 (1985),211-216.

[3] J.H.E. Cohn, On determinants with elements ± 1, II, *Bull. London Math. Soc.*, 21 (1989), 36-42.

[4] J.H.E. Cohn, A D-optimal design of order 102, *Discrete Math.*, 102 (1992), 61-65.

[5] D.Z. Dokovic, On maximal (1, -1)-matrices of order $2n$, n odd, *Radovi Matematicki*, 7 (1991), 371-378.

[6] H. Ehlich, Determinantenabschätzungen für binäre matrizen, *Math. Z.*, 83 (1964), 123-132.

[7] H. Ehlich, Determinantenabschätzungen für binäre matrizen mit $n \equiv 3 \bmod 4$, *Math. Z.*, 84 (1964), 438-447.

[8] Roderick J. Fletcher, Marc Gysin and Jennifer Seberry, Application of the Discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices, *Australas. J. Combin.*, 23 (2001), 75-86.

[9] M. Gysin, New D–optimal designs via Cyclotomy and generalised Cyclotomy, *Australas. J. Combinatorics,* 15 (1997), pp. 247-255.

[10] W.H. Holzmann, and H. Kharaghani, A D-optimal design of order 150, *Discrete Math.*, 190 (1998), 265-269.

[11] H. Kharaghani, A construction of D-optimal designs for $n \equiv 2 \bmod 4$, *J. Combin. Theory, Ser A*, 46 (1987), 156-158.

[12] C. Koukouvinos, S. Kounias, and J. Seberry, Supplementary difference sets and optimal designs, *Discrete Math.*, 88 (1991), 49-58.

[13] A.L. Whiteman, A family of D-optimal designs, *Ars Combinatoria*, 30 (1990), 23-26.

[14] C.H. Yang, Some designs for maximal (+1,-1)-determinant of order $n \equiv 2 \bmod 4$, *Math. Comp.*, 20 (1966), 147-148.

[15] C.H. Yang, A construction of maximal (+1,-1)-matrix of order 54, *Bull. Amer. Math. Soc.*, 72 (1966), 293.

[16] C.H. Yang, On designs of maximal (+1,-1)-matrices of order $n \equiv 2 \bmod 4$, *Math. Comp.*, 22 (1968), 174-180.

[17] C.H. Yang, On designs of maximal (+1,-1)-matrices of order $n \equiv 2 \bmod 4$, II, *Math. Comp.*, 23 (1969), 201-205.

[18] C.H. Yang, Maximal binary matrices and sum of two squares, *Math. Comp.*, 30 (1976), 148-153.

(Received 1/12/99)