New D–Optimal Designs via Cyclotomy and Generalised Cyclotomy

Marc Gysin

Centre for Computer Security Research,
Department of Computer Science,
The University of Wollongong,
Wollongong, NSW 2522, Australia

e–mail: marc@cs.uow.edu.au

Abstract

D–optimal designs are $n \times n$ ± 1–matrices where $n \equiv 2 \bmod 4$ with maximum determinant. D–optimal designs obtained via circulant matrices are equivalent to 2–$\{v; k_1; k_2; k_1 + k_2 - \frac{1}{2}(v-1)\}$ supplementary difference sets, where $v = \frac{n}{2}$.
We use cyclotomy to construct D–optimal designs, where v is a prime. We give a generalisation of cyclotomy and extend the cyclotomic techniques which enables use to find new D–optimal designs for composite numbers. In particular, we found, via computer–search, D–optimal designs for $v = \frac{n}{2} = 7, 13, 19, 21, 31, 33, 37, 41, 43, 61, 73, 85, 91, 93, 113$. The case $v = 85 = 5 \times 17$ is completely new. That is, D–optimal designs of order $n = 2v = 2 \times 85$ are given here for the first time.

1 Introduction

Definition 1 (Supplementary Difference Sets) Let $S_1, S_2, \ldots, S_e$ be subsets of Z_v (or any finite abelian group of order v) containing $k_1, k_2, \ldots, k_e$ elements respectively. Let T_i be the totality of all differences between elements of S_i (with repetitions), and let T be the totality of all the elements of T_i. If T contains each non–zero element of Z_v a fixed number of times, say λ, then the sets will be called e–$\{v; k_1, k_2, \ldots, k_e; \lambda\}$ *supplementary difference sets (SDS).*

The parameters of e–$\{v; k_1, k_2, \ldots, k_e; \lambda\}$ supplementary difference sets satisfy

$$\lambda(v-1) = \sum_{i=1}^{e} k_i(k_i - 1). \tag{1}$$

Australasian Journal of Combinatorics 15(1997), pp.247–255

If $k_1 = k_2 = \ldots = k_e = k$ we shall write e–$\{v; k; \lambda\}$ to denote the e SDS and (1) becomes

$$\lambda(v-1) = ek(k-1).$$

Definition 2 (D–optimal designs) Let $n \equiv 2 \bmod 4$, $v = \frac{1}{2}n$, I_v be the identity matrix and J_v be the all 1 matrix of order v. Let M, N be commuting $v \times v$ matrices, with elements ± 1, such that

$$MM^T + NN^T = (2v-2)I_v + 2J_v. \tag{2}$$

Now the $n \times n$ matrix

$$R = \begin{bmatrix} M & N \\ -N^T & M^T \end{bmatrix}$$

is called *a D–optimal design of order n.*

D–optimal designs have maximum determinant among all $n \times n$ ± 1–matrices, where $n \equiv 2 \bmod 4$ ([2], [4]). The following two theorems give rise to infinite families of D–optimal designs.

Theorem 1 (Whiteman [18]) There exist D–optimal designs of order $n \equiv 2 \bmod 4$ where

$$n = 2v = 2(2q^2 + 2q + 1)$$

and q is an odd prime power.

Theorem 2 (Koukouvinos, Kounias, Seberry [11]) There exist D–optimal designs of order $n \equiv 2 \bmod 4$ where

$$n = 2v = 2(q^2 + q + 1)$$

and q is a prime power.

Definition 3 (Periodic Autocorrelation Function)
Let $X = \{\{x_{10}, \ldots, x_{1,n-1}\}, \{x_{20}, \ldots, x_{2,n-1}\}, \ldots, \ldots, \{x_{m0}, \ldots, x_{m,n-1}\}\}$ be a family of m sequences of elements 1, 0 and -1 and length n. The *periodic autocorrelation function* of the family of sequences X, denoted by P_X, is a function defined by

$$P_X(s) = \sum_{i=0}^{n-1}(x_{1i}x_{1,i+s} + x_{2i}x_{2,i+s} + \ldots + x_{mi}x_{m,i+s}),$$

where s can range from 1 to $n-1$ and the indices are reduced mod n, if necessary.

Suppose now that we have two ± 1–sequences

$$\begin{aligned} A &= \{a_1, \ldots, a_n\} \\ B &= \{b_1, \ldots, b_n\}, \end{aligned}$$

with constant periodic autocorrelation function, that is

$$P_A(s) + P_B(s) = c, \ s = 1, \ldots, n-1; \tag{3}$$

with row sums $a = \sum_{i=1}^{n} a_i$ and $b = \sum_{i=1}^{n} b_i$. We let S_A, S_B be two sets with $k \in S_A \Leftrightarrow a_k = -1$, $j \in S_B \Leftrightarrow b_k = -1$. By examining the number of $(+1) \times (+1)$, $(+1) \times (-1)$, $(-1) \times (+1)$ and $(-1) \times (-1)$ terms from the periodic autocorrelation function, we can easily prove that S_A, S_B are $2-\{n; k_a, k_b; \lambda\}$ SDS, where

$$k_a = \frac{n-a}{2}, \ k_b = \frac{n-b}{2}, \ \lambda = k_a + k_b - \frac{1}{4}(2n - c).$$

The row sums of A and B can be written as

$$\begin{aligned} a^2 + b^2 &= (\sum_{i=1}^{n} a_i)^2 + (\sum_{i=1}^{n} b_i)^2 \\ &= 2n + \sum_{s=1}^{n-1}(P_A(s) + P_B(s)) \\ &= 2n + (n-1)c = 2n + cn - c. \end{aligned}$$

Therefore $2n + cn - c$ must be the sum of two squares.

If in (3) $c = 2$, then we can obtain two circulant matrices N and M where the first row in N is A and in M is B respectively. (The matrices are called *circulant* because all subsequent rows are obtained by shifting the row above by one position cyclically.) M and N now clearly satisfy (2). Hence we can obtain D–optimal designs from sequences of odd lengths with periodic autocorrelation function 2. If the length of these sequences is v and the numbers of minuses in the first and second sequence are k_a and k_b, respectively, then these sequences are equivalent to $2-\{v; k_a; k_b; \lambda\}$ SDS satisfying

$$\lambda = k_a + k_b - \frac{1}{2}(v-1), \tag{4}$$

$$(v - 2k_a)^2 + (v - 2k_b)^2 = 4v - 2. \tag{5}$$

SDS whose parameters satisfy (4) and (5) are also called *D–optimal SDS*.

2 Cyclotomy

In this section we give a short introduction to cyclotomy. More details are given in [15] and [5].

Definition 4 Let x be a primitive element of $F = GF(q)$, where $q = p^\alpha = ef + 1$ is a prime power. Write $G =< x >$. The *cyclotomic cosets* C_i *in* F are:

$$C_i = \{x^{es+i} : s = 0, 1, \ldots, f-1\}, \ i = 0, 1, \ldots, e-1.$$

We note that the C_i's are pairwise disjoint and their union is $G = F \setminus \{0\}$.

We define $[C_i]$ the incidence matrix of the cyclotomic coset C_i by

$$c_{jk} = \begin{cases} 1, & \text{if } z_k - z_j \in C_i \\ 0, & \text{otherwise.} \end{cases}$$

As $G = C_0 \cup C_1 \cup \ldots \cup C_{e-1} = GF(p^\alpha) \setminus \{0\}$, its incidence matrix is $J_{ef+1} - I_{ef+1}$ (i.e., $\sum_{s=0}^{e-1}[C_s] = J_{ef+1} - I_{ef+1}$), and the incidence matrix of $GF(p^\alpha)$ is J_{ef+1}. Therefore, the incidence matrix of $\{0\}$ will be I_{ef+1}.

The incidence matrices of $C_a \& C_b$ and $C_a \sim C_b$ will be given by

$$[C_a \& C_b] = [C_a] + [C_b] \text{ and } [C_a \sim C_b] = [C_a] - [C_b].$$

Following an idea of Hunt and Wallis [9], we use appropriate linear combinations of the incidence matrices of the cyclotomic cosets which give the matrices M and N for the D–optimal designs.

Example 1 Let $n = 19 = 6 \times 3 + 1$, $x = 2$, $e = 6$, $f = 3$. The cyclotomic classes are

$$\begin{array}{rclrcl} C_0 & = & \{1,7,11\} & C_3 & = & \{8,18,12\} \\ C_1 & = & \{2,14,3\} & C_4 & = & \{16,17,5\} \\ C_2 & = & \{4,9,6\} & C_5 & = & \{13,15,10\}. \end{array}$$

We note that $4 \times 19 - 2 = 7^2 + 5^2$ and we let

$$\begin{array}{rcl} M & = & [\{0\} \& C_0 \& C_1 \& C_2 \& C_3 \sim C_4 \sim C_5], \\ N & = & [\sim \{0\} \sim C_0 \& C_1 \& C_2 \& C_3 \& C_4 \sim C_5]. \end{array}$$

Now M and N satisfy (2) and hence we have a D–optimal design of order $38 = 2 \times 19$.

If we call the first rows of M and N A and B, respectively, and if we replace $+1$ by '$+$' and -1 by '$-$', we have

$$\begin{array}{rcl} A & = & + + + + + - + + + + - + + - + - - - +, \\ B & = & - - + + + + + + - + + - - + - + - + + +, \end{array}$$

where the periodic autocorrelation function of A and B is 2, for $s = 1, \ldots, 18$.

3 The Generalisation

We try to find similar partitions for *any number* n. We now work in Z_n and take the powers of any element y which is relatively prime to n to get an initial set which is a subgroup of the $\phi(n)$ elements which are relatively prime to n. The cosets are obtained by multiplying each element of the initial set by a fixed number. This fixed number does not need to be relatively prime to n. However, in this case the coset is not really a coset anymore in the group theoretical sense since we, clearly, are moving out of the group. We shall refer to such sets as *generalised cosets*.

Example 2 We let $n = 21 = 7 \times 3$, $y = 2$. (We are slightly inconsistent in enumerating the cosets: we now call the initial set C_1 while C_0 is the set containing only the element 0.)

$C_1 = \{1, 2, 4, 8, 16, 11\}$	initial set, powers of y
$C_2 = \{3, 6, 12\}$	multiply by 3, generalised coset
$C_3 = \{5, 10, 20, 19, 17, 13\}$	multiply by 5, coset
$C_4 = \{7, 14\}$	multiply by 7, generalised coset
$C_5 = \{9, 18, 15\}$	multiply by 9, generalised coset
$C_0 = \{0\}$	multiply by 0, generalised coset

Observe that the generalised cosets may or may not "collapse" into a smaller size, since $ma = mb$ is now possible even for $a \neq b$. It can be shown that the property that the differences of *any* coset whether proper or generalised can be expressed as the sum of other proper or generalised cosets, as in cyclotomy, remains. For example,

$$\Delta C_3 = C_1 + 2C_2 + C_3 + 3C_4 + 2C_5.$$

We can now again examine linear combinations of proper and generalised cosets to find the matrices M and N with the desired properties.

4 The Search and New Results

We can search for such linear combinations in cyclotomy or the general case on the computer. Similar ideas and/or searches have been used in [5], [6] and [7]. Note that the search is exponential only in the total number e of cyclotomic cosets and not in the length v of the initial sequences which form the circulant matrices M and N. The criterion of $4v - 2$ being the sum of two squares helps us to rule out certain cases immediately and to cut down the search drastically in other cases.

In the prime case we found D–optimal designs for

$$v = 7, 13, 19, 31, 37, 41, 43, 61, 73, 113.$$

In the general case D–optimal designs were found for

$$v = 21, 33, 85, 91, 93.$$

Table 1 and 2 show the generator y for the first coset, the linear combinations used and the first rows of the circulant matrices M and N for each v. (We use the general notation for enumerating the cosets for the prime case as well.) Table 3 shows the initial set C_1 for the composite cases.

The case $n = 2v = 2 \times 113$ is covered by Theorem 1 ($q = 7$). The case $n = 170 = 2v = 2 \times 85$ is believed to be completely new.

v	Squares	y	M, N
7	5^2+1^2	2	$[\sim C_0\&C_1\&C_2]$, $[C_0\&C_1\sim C_2]$
13	5^2+5^2	3	$[\sim C_0\&C_1\&C_2\&C_3\sim C_4]$, $[\sim C_0\&C_1\&C_2\&C_3\sim C_4]$
13	7^2+1^2	3	$[C_0\&C_1\&C_2\&C_3\sim C_4]$, $[C_0\sim C_1\&C_2\&C_3\sim C_4]$
19	7^2+5^2	7	$[C_0\&C_1\&C_2\&C_3\sim C_4\&C_5\sim C_6]$, $[\sim C_0\sim C_1\&C_2\&C_3\&C_4\&C_5\sim C_6]$
$21=3\times 7$	9^2+1^2	2	$[\sim C_0\&C_1\&C_2\&C_3\sim C_4\sim C_5]$, $[\sim C_0\&C_1\&C_2\sim C_3\&C_4\sim C_5]$
31	11^2+1^2	2	$[C_0\&C_1\&C_2\&C_3\sim C_4\&C_5\sim C_6]$, $[C_0\sim C_1\&C_2\&C_3\&C_4\sim C_5\sim C_6]$
$33=3\times 11$	11^2+3^2	5	$[\sim C_0\&C_1\sim C_2\&C_3\&C_4\&C_5]$, $[C_0\sim C_1\&C_2\&C_3\sim C_4\&C_5]$
37	11^2+5^2	10	$[\sim C_0\&C_1\&C_2\&C_3\&C_4\&C_5\&C_6 \sim C_7\&C_8\&C_9\sim C_{10}\sim C_{11}\sim C_{12}]$, $[\sim C_0\&C_1\sim C_2\&C_3\&C_4\sim C_5\sim C_6 \&C_7\&C_8\&C_9\sim C_{10}\&C_{11}\sim C_{12}]$
41	9^2+9^2	16	$[\sim C_0\&C_1\&C_2\&C_3\&C_4\&C_5\sim C_6\sim C_7\sim C_8]$, $[\sim C_0\&C_1\&C_2\sim C_3\sim C_4\&C_5\&C_6\&C_7\sim C_8]$
43	13^2+1^2	4	$[\sim C_0\&C_1\&C_2\&C_3\&C_4\sim C_5\sim C_6]$, $[C_0\sim C_1\sim C_2\&C_3\&C_4\&C_5\sim C_6]$
43	11^2+7^2	6	$[\sim C_0\&C_1\sim C_2\&C_3\&C_4\&C_5\&C_6\&C_7 \sim C_8\&C_9\&C_{10}\&C_{11}\sim C_{12}\sim C_{13}\sim C_{14}]$, $[C_0\sim C_1\&C_2\&C_3\&C_4\sim C_5\sim C_6\sim C_7 \&C_8\&C_9\&C_{10}\sim C_{11}\&C_{12}\&C_{13}\sim C_{14}]$
61	11^2+11^2	9	$[C_0\&C_1\&C_2\&C_3\&C_4\&C_5\&C_6 \sim C_7\&C_8\sim C_9\sim C_{10}\sim C_{11}\sim C_{12}]$, $[C_0\sim C_1\&C_2\&C_3\sim C_4\&C_5\&C_6 \&C_7\&C_8\sim C_9\&C_{10}\sim C_{11}\sim C_{12}]$
73	17^2+1^2	2	$[\sim C_0\&C_1\&C_2\&C_3\&C_4 \sim C_5\&C_6\sim C_7\sim C_8]$, $[C_0\&C_1\sim C_2\&C_3\sim C_4 \&C_5\&C_6\sim C_7\sim C_8]$
$85=5\times 17$	13^2+13^2	9	$[C_0\&C_1\&C_2\&C_3\&C_4\&C_5\sim C_6 \&C_7\sim C_8\sim C_9\sim C_{10}\sim C_{11}\sim C_{12}]$, $[C_0\sim C_1\&C_2\&C_3\&C_4\&C_5\&C_6 \sim C_7\sim C_8\sim C_9\sim C_{10}\&C_{11}\sim C_{12}]$
$91=7\times 13$	19^2+1^2	68	$[C_0\sim C_1\sim C_2\&C_3\&C_4\&C_5\&C_6\&C_7\&C_8 \&C_9\&C_{10}\sim C_{11}\&C_{12}\sim C_{13}\sim C_{14}\&C_{15}\sim C_{16}\&C_{17}]$, $[C_0\&C_1\sim C_2\sim C_3\&C_4\&C_5\sim C_6\&C_7\sim C_8 \sim C_9\sim C_{10}\&C_{11}\&C_{12}\&C_{13}\&C_{14}\sim C_{15}\sim C_{16}\sim C_{17}]$
$93=3\times 31$	17^2+9^2	4	$[\sim C_0\sim C_1\sim C_2\&C_3\&C_4\&C_5\sim C_6 \&C_7\&C_8\&C_9\&C_{10}\&C_{11}\sim C_{12}\&C_{13} \&C_{14}\sim C_{15}\&C_{16}\sim C_{17}\sim C_{18}\sim C_{19}\sim C_{20}]$, $[C_0\&C_1\&C_2\&C_3\sim C_4\&C_5\sim C_6 \sim C_7\&C_8\sim C_9\&C_{10}\sim C_{11}\sim C_{12}\&C_{13} \&C_{14}\sim C_{15}\sim C_{16}\&C_{17}\&C_{18}\sim C_{19}\sim C_{20}]$
113	15^2+15^2	16	$[C_0\&C_1\&C_2\&C_3\&C_4\&C_5\sim C_6\&C_7\sim C_8 \&C_9\&C_{10}\sim C_{11}\sim C_{12}\&C_{13}\sim C_{14}\sim C_{15}\sim C_{16}]$, $[C_0\&C_1\&C_2\&C_3\&C_4\sim C_5\&C_6\&C_7\sim C_8 \&C_9\sim C_{10}\sim C_{11}\&C_{12}\sim C_{13}\sim C_{14}\&C_{15}\sim C_{16}]$

Table 1: D–optimal designs for some primes and composite numbers.

v	First Rows of M and N
7	-++++++, +++-+--
13	-++++++--++-+, -++++++--++-+
13	+++++++--++-+, +-+-+++---+-+
19	+++++-++++-++-+---+, --+++++-++--+-+-+++
21	-++++++-+-++++--++-++, -++++-+++--++-+-+----
31	+++++++-++++++--+++-+++-+-+----, +--+-+++-++-+-+--++++---++--+--
33	-+-++++--+-++-+++-+-++++++++--++-, +-++---+++++++-+-+-+--+----+++--+
37	-++++++++-++-+++---++--+--++-+++-++-+, -+-+++---++++++-+-++----+-++-++++---+
41	-+++++-++++--+--+-+-++-+-+---+++++--++-++, -++--++-+++++-+-++++++----+-+---+++-++++-
43	-++++++-+-+++---+--++++++--+---+++-+-++++++, +--+-+++--+-+-----+++--++-+-++++-++--++-+--
43	-+-+++++++-+-+++--++--+++---+-++---+++++-++, +-+++-----+-+++++++-+++-++---+-++-++--+-++-
61	++++++++-++---+--+++++-----+-+- +--+++--+++-+-++-++--+-++--+++, +-++-++++-++-+-++++--++----+++- +---+-+++++-+-++-+---+-+++--++
73	-++++++++++-+++-+-+++--++-+-++-++---+ +++++-+--+-+--++--++++---+-++---+-++, +++-++-++-++-++++---+++---+-+++++---- +-++-+++--+---++--++-+-+-+-+--------
85	++++++-++++--+--+-++++----++----++--+-+-+-+ +-+-+++--++---+-+--++++++-+--++-+++--++-++, +-++++++--++-++---+-+---+-++-+-+++--+-+++++ -+++-+-----+-++---++++++--+-+-+++++-++---+
91	+--++++++++++-+--+--+++++---++----++-+--+-+++- ++++-+-+-++--+-+-++-++-+++---+-+-+++--+++-+++, ++--+++-+----+++++++---+-+++--++--++++++-++-+- +-----+-----++--+-++-++--+--++--+-+-+----+-++
93	---+-+++--++++++---++++++++++++--+----+++++-+-- -+++-+++-++-++--+--++---+-+-++++-+-+++---++--+, +++++-+++--++-+-+--+-+-++++-++--+-++-++---++++- ++-+--+-+++-+----+----++----+++-+-+-++--+-++-+
113	++++++-++-++--++++-+----+--++-+-+-+-++ +---++-+++++---++-+++-+--++----+---++- --+-++++++-+--+-++---+++-+--++++-+-++, +++++-+++-+--++++---+-+--+--+-+-++++-- +----+---+++-+-+++++--++--+--++--++++- +----+-++++--++-+-++++++-+---++-++-++

Table 2: First rows of M and N.

v	y	C_1
$21 = 3 \times 7$	2	$\{1, 2, 4, 8, 16, 11\}$
$33 = 3 \times 11$	5	$\{1, 5, 25, 26, 31, 23, 16, 14, 4, 20\}$
$85 = 5 \times 17$	9	$\{1, 9, 81, 49, 16, 59, 21, 19\}$
$91 = 7 \times 13$	68	$\{1, 68, 74, 27, 16, 87\}$
$93 = 3 \times 31$	4	$\{1, 4, 16, 64, 70\}$

Table 3: Initial sets for the composite cases.

Acknowledgment

Supported by an UPA (University of Wollongong Postgraduate Scholarship), The University of Wollongong and the Centre for Computer Security Research.

References

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

[2] J.H.E. Cohn, On determinants with elements ± 1 II, *Bulletin of the London Mathematical Society*, 21, 36–42, 1989.

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

[4] H. Ehlich, Determinantenabschätzungen für binäre Matrizen, *Mathematische Zeitschrift*, 83, 123–132, 1964.

[5] A.V. Geramita and J. Seberry, Orthogonal Designs, Quadratic Forms and Hadamard Matrices, Marcel Dekker, New York–Basel, 1979.

[6] S.W. Golomb, Shift Register Sequences, Aegean Park Press, Laguna Hills, California, 1982.

[7] M. Gysin and J. Seberry, On the weighing matrices of order $4n$ and weight $4n-2$ and $2n-1$, *Australasian Journal of Combinatorics*, 12, 157–174, 1995.

[8] M. Gysin and J. Seberry, An experimental search and new combinatorial designs via a generalisation of cyclotomy, to be published.

[9] D. Hunt and J.S. Wallis, Cyclotomy, Hadamard arrays and supplementary difference sets, *Proceedings of the Second Manitoba Conference on Numerical Mathematics*, Congressus Numerantium VII, Manitoba, 1972.

[10] H. Kharaghani, A construction of D–optimal designs for $n \equiv 2 \bmod 4$, *Journal of Combinatorial Theory*, Ser. A 46, 156–158, 1987.

[11] C. Koukouvinos, S. Kounias, J. Seberry, Supplementary difference sets and optimal designs, *Discrete Math.*, 88, 49–58, 1991.

[12] C. Koukouvinos, S. Kounias, J. Seberry, C.H. Yang and J. Yang, On sequences with zero autocorrelation, *Designs, Codes and Cryptography*, 4, 327–340, 1994.

[13] C. Koukouvinos, J. Seberry, A.L. Whiteman, M. Xia, Optimal designs, supplementary difference sets and multipliers, *Journal of Statistical Planning and Inference*, to be published.

[14] R. Lidl and G. Pilz, Applied Abstract Algebra, Undergraduate Texts in Mathematics, Springer Verlag, New York, 1984.

[15] J. Seberry Wallis, Some remarks on supplementary difference sets, *Colloquia Mathematica Societatis Janos Bolyai*, 10, 1503–1526, Hungary, 1973.

[16] J. Seberry and M. Yamada, Hadamard matrices, sequences and block designs, *Contemporary Design Theory – a Collection of Surveys*, eds. J.Dinitz and D.R. Stinson, John Wiley and Sons, New York, 431–560, 1992.

[17] T. Storer, Cyclotomy and Difference Sets, *Lectures in Advanced Mathematics*, 2, Markham Publishing Company, Chicago, 1967.

[18] A.L. Whiteman, A family of D–optimal designs, *Ars Combinatoria*, 30, 23–26, 1990.

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

[20] C.H. Yang, On designs of maximal $(+1,-1)$–matrices of order $n \equiv 2 \bmod 4$, *Mathematical Computation*, 23, 201–205, 1969.

(Received 12/8/96; revised 9/12/96)