An experimental search and new combinatorial designs via a generalisation of cyclotomy

Marc Gysin

Jennifer Seberry

University of Wollongong, jennie@uow.edu.au

Publication Details

An experimental search and new combinatorial designs via a generalisation of cyclotomy

Abstract
Cyclotomy can be used to construct a variety of combinatorial designs, for example, supplementary difference sets, weighing matrices and T-matrices. These designs may be obtained by using linear combinations of the incidence matrices of the cyclotomic cosets. However, cyclotomy only works in the prime and prime power cases. We present a generalisation of cyclotomy and introduce generalised cosets. Combinatorial designs can now be obtained by a search through all linear combinations of the incidence matrices of the generalised cosets. We believe that this search method is new. The generalisation works for all cases and is not restricted to prime powers. The paper presents some new combinatorial designs. We give a new construction for T-matrices of order 87 and hence an OD(4 x 87,87,87,87). We also give some D-optimal designs of order n = 2v = 2 x 145,2 x 157,2 x 181.

Disciplines
Physical Sciences and Mathematics

Publication Details
An Experimental Search and New Combinatorial Designs via a Generalisation of Cyclotomy

Marc Gysin and Jennifer Seberry
Centre for Computer Security Research
Department of Computer Science
The University of Wollongong
Wollongong, NSW 2522
Australia
email: marc@cs.uow.edu.au
j.seberry@cs.uow.edu.au

ABSTRACT. Cyclotomy can be used to construct a variety of combinatorial designs, for example, supplementary difference sets, weighing matrices and T-matrices. These designs may be obtained by using linear combinations of the incidence matrices of the cyclotomic cosets. However, cyclotomy only works in the prime and prime power cases. We present a generalisation of cyclotomy and introduce generalised cosets. Combinatorial designs can now be obtained by a search through all linear combinations of the incidence matrices of the generalised cosets. We believe that this search method is new. The generalisation works for all cases and is not restricted to prime powers. The paper presents some new combinatorial designs. We give a new construction for T-matrices of order 87 and hence an \(OD(4 \times 87; 87, 87, 87, 87)\). We also give some \(D\)-optimal designs of order \(n = 2v = 2 \times 145, 2 \times 157, 2 \times 181\).

1 Cyclotomy

The methods and techniques in this paper have been inspired by many authors including Dokovic [2], Furino [4] and Hunt and Wallis [9]. We use these methods and further generalisations to find many new combinatorial designs.

We now give a short introduction to cyclotomy. More details are given in [5] and [16]. We let \(I_n\) be the identity matrix of order \(n\) and \(J_n\) be the matrix of \(n \times n\) 1's.

JCMCC 27 (1998), pp. 143-160
Definition 1 Let \( x \) be a primitive element of \( F = GF(q) \), where \( q = p^e f + 1 \) is a prime power. Write \( G = \langle x \rangle \). The cyclotomic cosets \( C_i \) in \( F \) are:
\[
C_i = \{x^{es+i} : s = 0, 1, \ldots, f - 1\}, \quad i = 0, 1, \ldots, e - 1.
\]
We note that the \( C_i \)'s are pairwise disjoint and their union is \( G = F \setminus \{0\} \).

For fixed \( i \) and \( j \), the cyclotomic number \((i, j)\) is defined to be the number of solutions of the equation
\[
z_i + 1 = z_j \quad (z_i \in C_i, \quad z_j \in C_j),
\]
where \( 1 = x^0 \) is the multiplicative unit of \( F \). That is, \((i, j)\) is the number of ordered pairs \( s, t \) such that
\[
x^{es+i} + 1 = x^{et+j} \quad (0 \leq s, t \leq f - 1).
\]
Note that the number of times
\[
x^{es+i} - x^{et+k} \in C_j
\]
is the cyclotomic number \((k - j, i - j)\). It can be shown (see for example [16] or [19]) that
\[
(k - j, i - j) = (j - k, i - k).
\]

Notation 1 Let \( A = \{a_1, a_2, \ldots, a_k\} \) be a \( k \)-set; then we will use \( \Delta A \) for the collection of differences between distinct elements of \( A \), i.e,
\[
\Delta A = [a_i - a_j : i \neq j, 1 \leq i, j \leq k].
\]
Now
\[
\Delta C_i = (0, 0)C_i + (1, 0)C_{i+1} + (2, 0)C_{i+2} + \ldots
\]
and
\[
\Delta(C_i - C_j) = (0, 0)C_j + (1, 0)C_{j+1} + \ldots
\]
\[
\ldots + (0, 0)C_i + (1, 0)C_{i+1} + \ldots
\]
\[
\ldots + (0, i - j)C_j + (1, i - j)C_{j+1} + \ldots
\]
\[
\ldots + (0, j - i)C_i + (1, j - i)C_{i+1} + \ldots.
\]

Notation 2 We use \( C_a \sim C_b \) to denote the adjunction of two sets with repetitions remaining. If \( A = \{a, b, c, d\} \) and \( B = \{b, c, e\} \), then \( A \& B = \{a, b, b, c, c, d, e\} \). \( C_a \sim C_b \) is used to denote adjunction, but with the elements of the second set becoming signed. So \( A \sim B = \{a, b, -b, c, -c, d, -e\} \).
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 \(G = C_0 \cup C_1 \cup \ldots \cup C_{p-1} = GF(p^a) \setminus \{0\}\), its incidence matrix is \(J_{ef+1} - I_{ef+1}\) (i.e., \(\sum_{e=0}^{a-1}[C_e] = J_{ef+1} - I_{ef+1}\)), and the incidence matrix of \(GF(p^a)\) is \(J_{e+f}\). Therefore, the incidence matrix of \(\{0\}\) will be \(I_{e+f}\).

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

\([C_a \& C_b] = [C_a] + [C_b]\) and \([C_a \sim C_b] = [C_a] - [C_b]\).

**Example 1** We let \(q = p = 13\), \(e = 3\), \(f = 4\), \(x = 2\). The cyclotomic cosets are

\[
C_0 = \{1, 8, 12, 5\} \\
C_1 = \{2, 3, 11, 10\} \\
C_2 = \{4, 6, 9, 7\}
\]

The cyclotomic numbers are given in the following table. The number \((i, j)\) will be found in row \(i\) and column \(j\).

\[
\begin{array}{ccc}
0 & 1 & 2 \\
1 & 2 & 1 \\
2 & 1 & 1 \\
\end{array}
\]

Considering, for example, \(C_1\), we have

\[
\Delta C_1 = (0, 0)C_1 + (1, 0)C_2 + (2, 0)C_0 = C_2 + 2C_0,
\]

and

\[
[C_1] = \begin{bmatrix}
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
\end{bmatrix}.
\]
Observe that for prime $q$ the matrices $[G_i]$ are all circulant ("NW to SE strips") since we are working in $\mathbb{Z}_q$. However, this is not the case when $q$ is a prime power. In these cases the operations are done in $GF(q)$ and the elements may be represented by polynomials which does not lead to circulant $[G_i]$'s.

2 Combinatorial Designs

We first turn to ternary sequences, that is, sequences with entries 1, 0, -1 which have certain properties. From there we show how these sequences can be used to construct some combinatorial designs and how they correspond with the incidence matrices of the cyclotomic cosets.

Definition 2 (Periodic Autocorrelation Function)
Let $X = \{\{x_{10, \ldots, x_{1,n-1}}\}, \{x_{20, \ldots, x_{2,n-1}}\}, \ldots, \{x_{m0, \ldots, x_{m,n-1}}\}\}$ 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.

The weight $w$ of a family of $m$ sequences is defined as the total number of non-zero entries in these sequences.

Example 2 We write '+' for 1 and '-' for -1. Consider the four sequences of length $n = 4$ and weight $w = 10$

\begin{align*}
A &= ++-+ \\
B &= +++-
C &= 00+ \\
D &= -000.
\end{align*}

It is easy to see that these four sequences have zero periodic autocorrelation function. The weight $w$ of these four sequences is 10 and it is a well established fact (see, for example, [17]) that the sum of the squares of the row sums of the sequences must add to $w$ as a necessary (but not sufficient) condition for the periodic autocorrelation function to be zero. In this example we have $2^2 + 2^2 + 1^2 + 1^2 = 10$. 

146
Four sequences $A, B, C, D$ of length $n$ and weight $w$ with zero periodic autocorrelation function are equivalent to four circulant $n \times n$ matrices $M_A, M_B, M_C, M_D$ with first rows $A, B, C, D$ which satisfy

$$M_A M_A^T + M_B M_B^T + M_C M_C^T + M_D M_D^T = w I_n.$$ 

**Definition 3 (Orthogonal Design)** An orthogonal design $A$, of order $n$, and type $(s_1, s_2, \ldots, s_u)$, denoted $OD(n; s_1, s_2, \ldots, s_u)$ on the commuting variables $(\pm x_1, \pm x_2, \ldots, \pm x_u, 0)$ is a square matrix of order $n$ with entries $\pm x_k$ where each $x_k$ occurs $s_k$ times in each row and column such that the distinct rows are pairwise orthogonal.

**Definition 4 (Weighing Matrix)** A weighing matrix $W = W(n, k)$ is a square matrix with entries $0, \pm 1$ having $k$ non-zero entries per row and column and inner product of distinct rows zero. Hence, $W$ satisfies $WW^T = kI_n$. The number $k$ is called the weight of $W$. A $W(n, n)$, for $n \equiv 0 \pmod{4}$, 1 or 2, whose entries are $\pm 1$ only is called an Hadamard matrix.

If we have four sequences $A, B, C, D$ of length $n$ and weight $w$ with zero periodic autocorrelation function, $M_A, M_B, M_C, M_D$ may be “plugged into” a special array, called Goethals-Seidel array, which gives a weighing matrix $W(4n, w)$. Details of this standard construction, are again given in [17].

**Definition 5 (T-matrices)** A set of 4 $T$-matrices $T_i, i = 1, \ldots, 4$ of order $t$ are four circulant or type one matrices that have entries $0, +1$ or $-1$ and that satisfy

(i) $T_i \ast T_j = 0$, $i \neq j$, ($\ast$ denotes the Hadamard product);  
(ii) $\sum_{i=1}^4 T_i$ is a $(1, -1)$ matrix;  
(iii) $\sum_{i=1}^4 T_i T_i^T = t I_t$; and  
(iv) $t = t_1^2 + t_2^2 + t_3^2 + t_4^2$, where $t_i$ is the row (column) sum of $T_i$.

Four sequences $A, B, C, D$ of length $n$ and weight $w$ with zero periodic autocorrelation function and the additional property that they are disjoint, that is, $a_i \pm b_i \pm c_i \pm d_i = \pm 1$ (where $x_i$ is the $i$-th element of the sequence $X$) for all $i = 0, \ldots, n - 1$ are equivalent to four circulant $T$-matrices of order $n$. $T$-matrices can be used to construct orthogonal designs.
Definition 6 (D-optimal designs) Let $n \equiv 2 \mod 4$, $v = \frac{1}{2}n$, $I_v$ 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 $\pm 1$, such that

$$MM^T + NN^T = (2v - 2)I_v + 2J_v. \quad (1)$$

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 $n \times n \pm 1$-matrices, where $n \equiv 2 \mod 4$ ([1], [3]). The following two theorems give rise to infinite families of D-optimal designs.

Theorem 1 (Whiteman [21]) There exist D-optimal designs of order $n \equiv 2 \mod 4$ where

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

and $q$ is an odd prime power.

Theorem 2 (Koukouvinos, Kounias, Seberry [10]) There exist D-optimal designs of order $n \equiv 2 \mod 4$ where

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

and $q$ is a prime power.

D-optimal designs can be constructed from supplementary difference sets (see Definition 7) and sequences with constant periodic autocorrelation function. The details are, for example, given in [7].

We now consider supplementary difference sets. These are related to sequences as we now see.

Definition 7 (Supplementary Difference Sets) Let $S_1, S_2, \ldots, S_n$ be subsets of $Z_v$ (or any finite abelian group of order $v$) containing $k_1, k_2, \ldots, k_n$ 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 $\lambda$, then the sets will be called $n-\{v; k_1, k_2, \ldots, k_n; \lambda\}$ supplementary difference sets (SDS).
The parameters of \( n-\{v; k_1, k_2, \ldots, k_n; \lambda \} \) supplementary difference sets satisfy

\[
\lambda(v - 1) = \sum_{i=1}^{n} k_i(k_i - 1). \tag{2}
\]

If \( k_1 = k_2 = \ldots = k_n = k \) we shall write \( n-\{v; k; \lambda \} \) to denote the \( n \) supplementary difference sets and (2) becomes

\[
\lambda(v - 1) = nk(k - 1).
\]

**Example 3** The cyclotomic cosets of Example 1 form \( 3-\{13; 4; 3 \} \) supplementary difference sets. We have

\[
\begin{align*}
\Delta C_0 &= (0, 0)C_0 + (1, 0)C_1 + (2, 0)C_2 \\
\Delta C_1 &= (0, 0)C_1 + (1, 0)C_2 + (2, 0)C_0 \\
\Delta C_2 &= (0, 0)C_2 + (1, 0)C_0 + (2, 0)C_1.
\end{align*}
\]

Hence,

\[
\Delta C_0 + \Delta C_1 + \Delta C_2 = ((0, 0) + (1, 0) + (2, 0))(C_0 + C_1 + C_2)
\]

\[
= 3 \times G,
\]

which proves the claim made above.

In fact, it can be shown that the cyclotomic cosets \( C_i \) always form \( e-\{q; f; f - 1 \} \) difference sets ([18]). The challenge is to find other supplementary difference sets using only some of the cyclotomic cosets \( C_i \) ([16] and [20]).

Saying that the cyclotomic cosets \( C_i \) form \( e-\{q; f; f - 1 \} \) difference sets is equivalent to

\[
[C_0][C_0]^T + [C_1][C_1]^T + \ldots + [C_{e-1}][C_{e-1}]^T = (f - 1)J_q + (ef - (f - 1))I_q.
\]

We now see the correspondence between the above statement and ternary sequences. If the \( [C_i] \)'s are all circulant, that is, if \( q \) is prime, then the sequences which correspond to the first rows of the \( [C_i] \)'s have constant periodic autocorrelation function, \( \lambda = f - 1 \). If we take sequences which are formed in a similar way as the above set of sequences except that we change all zero entries into \(-1 \) entries we get again sequences with constant periodic autocorrelation function.

---

\(^{1}\text{We can of course take the } j\text{-th row of the } [C_i] \text{'s rather than the first row.}\)
Example 4 Referring to Example 1 we form the binary sequences \( X, Y, \) \( Z \) (entries \( \pm 1 \)) from the cosets \( C_0, C_1, C_2 \).

\[
\begin{align*}
X &= \quad + - - - + - - - - + - \\
Y &= \quad + + + - - - - - - + - \\
Z &= \quad - - - + - - + - + - - -
\end{align*}
\]

Observe that \( X, Y, Z \) have constant periodic autocorrelation function. The value of the periodic autocorrelation function can be calculated from \( \lambda \) and is \(-q + 4 + 4\lambda = -13 + 4 + 4 \times 3 = 3\).

3 The Experimental Search

In Example 4 we constructed some \( \pm 1 \)-sequences with constant periodic autocorrelation function from cyclotomic cosets. However, this constant usually will be different to zero. A more sophisticated (and indeed more successful) approach is to take linear combinations of the incidence matrices of the cyclotomic cosets. That is, we have

\[
\begin{align*}
M_A &= a_e[0] + a_0[C_0] + a_1[C_1] + \ldots + a_{e-1}[C_{e-1}] \\
M_B &= b_e[0] + b_0[C_0] + b_1[C_1] + \ldots + b_{e-1}[C_{e-1}] \\
M_C &= c_e[0] + c_0[C_0] + c_1[C_1] + \ldots + c_{e-1}[C_{e-1}] \\
M_D &= d_e[0] + d_0[C_0] + d_1[C_1] + \ldots + d_{e-1}[C_{e-1}],
\end{align*}
\]

where \( a_i, b_i, c_i, d_i \in \{1, 0, -1\} \). We hope that for some \( a_i, b_i, c_i, d_i \)

\[
M_A M_A^T + M_B M_B^T + M_C M_C^T + M_D M_D^T = wI_q,
\]

that is, \( M_A, M_B, M_C, M_D \) can be used to construct a weighing matrix of order \( 4q \) and weight \( w \).

If \( q \) is prime then the matrices involved are all circulant and we can express all the above “in the language of sequences”. That is, the cyclotomic cosets serve as “master switches” for four ternary sequences which we hope have zero periodic autocorrelation function and from these four sequences we can construct the desired combinatorial designs.

Example 5 We let \( q = p = 13, e = 4, f = 3, x = 2 \). The cyclotomic cosets are

\[
\begin{align*}
C_0 &= \{1, 3, 9\} \\
C_1 &= \{2, 6, 5\} \\
C_2 &= \{4, 12, 10\} \\
C_3 &= \{8, 11, 7\}.
\end{align*}
\]
Suppose we are looking for four sequences $A$, $B$, $C$, $D$ of length 13 and weight 10 with zero periodic autocorrelation function. Then the following sequences may be obtained by using appropriate “master switches”. It turns out that in this case there are many “master switches” which lead to the desired result.

$$
A = -0 + 00 + +00000 \\
B = -000 + 00000 + 0 + \\
C = + 00000000000 \\
D = + 00000000000.
$$

In matrix-form and using Notation 2 the same example may be written as

$$
M_A = [\sim \{0\} \& C_1] \\
M_B = [\sim \{0\} \& C_2] \\
M_C = \{\{0\}\} \\
M_D = \{\{0\}\}.
$$

$M_A$, $M_B$, $M_C$, $M_D$ can now be used in the Goethals-Seidel array to give a weighing matrix $W(52, 10)$.

There has been some analytical work about cyclotomic cosets and mainly supplementary difference sets in, for example, [5], [9], [16] and [19]. However, our search is, as the name suggests, completely experimental, and all we do is relying on the fact that the differences of the cyclotomic cosets have some “nice algebraic structure”, which may or may not be exploited to give us the sequences (or matrices) with the desired properties. We search for such sequences (or matrices) via computer by exhaustively going through all reasonable linear combinations.

Searching through linear combinations of cyclotomic cosets has been employed in a variety of papers and books ([5], [8], [9]) and has given rise to many new combinatorial designs. The lengths or sizes of these designs may be far beyond the limits if one searched for such designs exhaustively without the help of the cyclotomic cosets or such “master switches”. However, negative answers do of course not imply that such combinatorial designs do not exist. Note that cyclotomy is limited to primes and prime powers.

4 The Generalisation

So far we have introduced cyclotomy and we have stated that all the computer-searches were relying on was the “nice algebraic structure” of the cyclotomic cosets. The rest was experimental and good luck. This led us to find any partitions for any arbitrary number $n$, that is any composite $n$, which have some similar “nice algebraic structure”. We could then
carry out experimental searches again and hope again to find sequences or combinatorial designs with the desired properties.

Let us look again at Example 1. \( C_0 \) is merely the subgroup of order 2 of the subgroup containing all the powers of the generator \( y = 5 \mod 13 \) while \( C_1 \) and \( C_2 \) are its multiplicative cosets.

To find similar partitions for any number \( n \) we now work in \( \mathbb{Z}_n \) 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 6** 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.)

\[
\begin{align*}
C_1 &= \{1, 2, 4, 8, 16, 11\} & & \text{initial set, powers of } y \\
C_2 &= \{3, 6, 12\} & & \text{multiply by 3, generalised coset} \\
C_3 &= \{5, 10, 20, 19, 17, 13\} & & \text{multiply by 5, coset} \\
C_4 &= \{7, 14\} & & \text{multiply by 7, generalised coset} \\
C_5 &= \{9, 18, 15\} & & \text{multiply by 9, generalised coset} \\
C_6 &= \{0\} & & \text{multiply by 0, generalised coset}
\end{align*}
\]

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,

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

This fact entitles us to be confident when carrying out experimental computer-searches for combinatorial designs based on “master switches” which are obtained from such proper and generalised cosets.

We believe that this idea, that is, finding a partition of \( n \) as above and then searching through the corresponding linear combinations is new. However, we wish to refer to Golomb [6] who used proper and generalised cosets in a similar manner to find shift register sequences. This served definitely

---

2Note that for the prime case it makes sense to talk about the subgroup of a certain order, since there is only one such subgroup generated by a given generator \( g \). However, this is generally not true if \( n \) is composite.
as a seed (and we believe a very fruitful one) in our research. We would also like to cite Storer [19] who has made major contributions in the analysis of Galois domains \( GD(p^a q^b) = GF(p^a) \times GF(q^b) \) and difference sets.

We give an example (for a small \( n \)) of linear combinations of proper and generalised cosets which lead to the desired result.

**Example 7** We let \( n = 21, \ y = 2 \) as in Example 6. Consider the four sequences

\[
A = - + + + + + + + + + + + + + + -
\]
\[
B = - + + + + + + + + + + + + + + -
\]
\[
C = 0 + + + + + + + + + + + + + + -
\]
\[
D = 0 + + + + + + + + + + + + + + -
\]

and observe that \( A, B, C, D \) have zero periodic autocorrelation function.

In matrix-form

\[
M_A = \begin{bmatrix} \sim C_0 & C_1 & C_2 & \sim C_3 & C_4 & \sim C_5 \end{bmatrix}
\]
\[
M_B = \begin{bmatrix} \sim C_0 & C_1 & C_2 & \sim C_3 & C_4 & \sim C_5 \end{bmatrix}
\]
\[
M_C = \begin{bmatrix} C_1 & C_2 & \sim C_3 & C_4 & C_5 \end{bmatrix}
\]
\[
M_D = \begin{bmatrix} C_1 & C_2 & \sim C_3 & C_4 & C_5 \end{bmatrix}
\]

\( M_A, M_B, M_C, M_D \) can now be used in the Goethals–Seidel array to form a weighing matrix \( W(84, 82) \).

5 The Search and Some New Results

Again we used raw computer-power to find appropriate “master–switches” for the desired combinatorial designs. In particular, we were searching for weighing matrices, supplementary difference sets, \( T \)-matrices and \( D \)-optimal designs. The search is being and has been carried out on a variety of sun workstations running under the UNIX™ operating system in our centre. The computer yielded many results and one of us (Gysin) had indeed to ask the system–administrator to increase the disk–quota in order to be able to store all the results. Search–times (that is, going exhaustively through all the “master–switches”) varied between a few seconds to a couple of months depending on the total number of “master–switches” or cyclotomic cosets used (and not depending on the length or size \( n \) of the final combinatorial designs). Of course the algorithm is exponential in the total number of “master–switches”. At any time we have about 20 different processes running on the workstations all searching for new results.

We give some combinatorial designs found.
Example 8 (Weighing Matrices) We let \( n = 66 = 2 \times 3 \times 11 \), \( y = 5 \). We get the following partition.

\[
\begin{align*}
C_1 &= \{1, 5, 25, 31, 49, 53\} \\
C_2 &= \{2, 10, 50, 62, 46, 28, 8\} \\
C_3 &= \{3, 15, 9, 45, 27\} \\
C_4 &= \{4, 20, 34, 58, 26, 64, 16\} \\
C_5 &= \{6, 30, 18, 24, 54\} \\
C_6 &= \{7, 35, 43, 17, 19, 29, 13\} \\
C_7 &= \{11, 55\} \\
C_8 &= \{12, 60, 36, 48, 42\} \\
C_9 &= \{21, 39, 63, 51, 57\} \\
C_{10} &= \{22, 44\} \\
C_{11} &= \{33\} \\
C_0 &= \{0\}.
\end{align*}
\]

In this case we were looking for four sequences of length \( n \) and weight \( w = 4n - 2 \). One (of the more than 1000 possibilities) is

\[
\begin{align*}
A &= +++-++-+++--+++-----++++--+-+--+++-+-++-+++++-++-++--+++-----\[+\]---+++-++--+++++---++--\
B &= <<-++--++++-+-++----+++--+--++---++++-++-+-+-+-++----+++--\[+\]+++-----++++-+++-----++---+++--
C &= 0--++-++-+-+-++++++++-+-+-++-++-+-++--+--+-+++--------+++-+--+--++
D &= 0+++-+--+++++--+------++-+-++--++---++--+-+-+++++++-++-+---++-+---.
\end{align*}
\]

The matrices and corresponding linear combinations are

\[
\begin{align*}
M_A &= [C_0 \& C_1 \& C_2 \& C_3 \& C_4 \& C_5 \sim C_6 \& C_7 \sim C_8 \& C_9 \sim C_{10} \& C_{11}] \\
M_B &= [C_0 \sim C_1 \& C_2 \& C_3 \sim C_4 \& C_5 \& C_6 \& C_7 \& C_8 \sim C_9 \sim C_{10} \sim C_{11}] \\
M_C &= [\sim C_1 \sim C_2 \& C_3 \& C_4 \& C_5 \& C_6 \& C_7 \& C_8 \sim C_9 \sim C_{10} \sim C_{11}] \\
M_D &= [C_1 \& C_2 \& C_3 \sim C_4 \& C_5 \sim C_6 \& C_7 \& C_8 \sim C_9 \& C_{10} \sim C_{11}].
\end{align*}
\]

From these matrices we can obtain a weighing matrix of order \( 264 = 4 \times 66 \) and weight \( 262 = 4 \times 66 - 2 \) via the standard construction in the Goethals-Seidel array.

Example 9 (T-matrices) We let \( n = 87 = 3 \times 29 \), \( y = 7 \). We get the
The first rows of the circulant $T$-matrices of order 87 are
\[
A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}
\]
\[
B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}
\]
\[
C = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}
\]
\[
D = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}
\]

The matrices and linear combinations are
\[
T_1 = [C_0 & C_2 & C_6 \sim C_{11} \sim C_{12}]
\]
\[
T_2 = [\sim C_3 \sim C_4 & C_8 & C_{10} & C_{13}]
\]
\[
T_3 = [C_1 & C_5 \sim C_7]
\]
\[
T_4 = [C_8 \sim C_{14}]
\]

These $T$-matrices give new orthogonal designs.
Lemma 1 Let $x, y, z, w$ be commuting variables and let

\[
X = xT_1 + yT_2 + zT_3 + wT_4 \\
Y = -yT_1 + zT_2 + wT_3 - zT_4 \\
Z = -zT_1 - wT_2 + xT_3 + yT_4 \\
W = -wT_1 + zT_2 - yT_3 + xT_4.
\]

Now $X, Y, Z, W$ can be used in the Goethals-Seidel array to construct new $OD(4 \times 87; 87, 87, 87, 87)$.

Example 10 (D-optimal designs) In this case we are looking for two circulant matrices $M$ and $N$ which satisfy (1). Many examples are given in [7]. We give $D$-optimal designs of order $n = 2v = 2 \times 145, 2 \times 157, 2 \times 181$.

The case $n = 2v = 2 \times 145$: We let $y = 24$. Now

\[
C_1 = \{1, 24, 141, 49, 16, 94, 81, 59, 111, 54, 126, 74, 36, 139\} \\
C_2 = \{2, 48, 137, 98, 32, 43, 17, 118, 77, 108, 127, 3, 72, 133\} \\
C_3 = \{4, 96, 129, 51, 64, 86, 34, 91, 9, 71, 109, 6, 144, 121\} \\
C_4 = \{5, 120, 125, 100, 80, 35, 115\} \\
C_5 = \{7, 23, 117, 53, 112, 78, 132, 123, 52, 88, 82, 83, 107, 103\} \\
C_6 = \{8, 47, 113, 102, 128, 27, 68, 37, 18, 142, 73, 12, 143, 97\} \\
C_7 = \{10, 95, 105, 55, 15, 70, 85\} \\
C_8 = \{11, 119, 101, 104, 31, 19, 21, 69, 61, 14, 46, 89, 106, 79\} \\
C_9 = \{13, 22, 93, 57, 63, 62, 38, 42, 138, 122, 28, 92, 33, 67\} \\
C_{10} = \{20, 45, 65, 110, 30, 140, 25\} \\
C_{11} = \{26, 44, 41, 114, 126, 124, 76, 84, 131, 99, 56, 39, 66, 134\} \\
C_{12} = \{29, 116\} \\
C_{13} = \{40, 90, 130, 75, 60, 135, 50\} \\
C_{14} = \{58, 87\}.
\]

The matrices $M$ and $N$ are now given by

\[
M = [\sim C_5 \sim C_1 & C_2 & C_3 & C_4 & C_5 \sim C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14}] \\
N = [\sim C_6 & C_1 \sim C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14}].
\]

[2] gives a $D$-optimal design for the same case. However, the design given there is inequivalent to the above one.
The case $n = 2v = 2 \times 157$: Note that 157 is prime. We let $y = 130$, that is, we take the subgroup of order 13 and its cosets. The matrices $M$ and $N$ are now given by

$$M = [\sim (0) & C_0 \& C_3 \sim C_4 \sim C_5 \& C_6 \sim C_7 \& C_8 \& C_9 \& C_{10} \sim C_{11}]$$

$$N = [(0) \& C_0 \sim C_1 \& C_2 \sim C_3 \sim C_4 \sim C_5 \& C_6 \& C_7 \& C_8 \& C_9 \& C_{10} \sim C_{11}].$$

This case is believed to be completely new.

The case $n = 2v = 2 \times 181$: This case is covered by [14]. We independently found $D$-optimal designs for the same case using the generator $y = 39$. The generator used in [14] is the same.

**Example 11 (First Construction for SDS)**

From the four sequences $A$, $B$, $C$, $D$ in Example 8 we can construct the eight sequences $A$, $A$, $B$, $B$, $C \cup 1 \circ 0$, $C \cup -1 \circ 0$, $D \cup 1 \circ 0$, $D \cup -1 \circ 0$, where $X \cup e \circ k$ means replace the element at position $k$ in $X$ by $e$. It can be easily shown that

(i) these eight new sequences have zero periodic autocorrelation function if $A$, $B$, $C$, $D$ have zero periodic autocorrelation function and the element at position 0 of $C$ and $D$ is zero;

(ii) the position of the minuses ('-') in these eight sequences form supplementary difference sets.

Hence, we get the following $8$--{$66; 27, 27, 28, 28, 31, 32, 31; 104$} supplementary difference sets

$$S_1 = \{2, 7, 8, 10, 12, 13, 17, 19, 22, 28, 29, 32, 35, 36, 40, 41, 42, 43, 44, 46, 48, 50, 52, 60, 61, 62, 65\}$$

$$S_2 = S_1$$

$$S_3 = \{1, 4, 5, 14, 16, 20, 21, 22, 23, 25, 26, 31, 33, 34, 37, 38, 39, 44, 47, 49, 51, 53, 56, 57, 58, 59, 63, 64\}$$

$$S_4 = S_3$$

$$S_5 = \{1, 2, 5, 8, 10, 12, 21, 23, 25, 28, 31, 32, 33, 36, 37, 39, 40, 42, 46, 47, 48, 49, 50, 51, 52, 53, 57, 59, 60, 62, 63\}$$

$$S_6 = S_5 \cup \{0\}$$

$$S_7 = \{4, 6, 7, 13, 14, 16, 17, 18, 19, 20, 21, 24, 26, 29, 30, 33, 34, 35, 38, 39, 41, 43, 51, 54, 56, 57, 58, 61, 63, 64, 65\}$$

$$S_8 = S_7 \cup \{0\}.$$

---

3 Of course we could also take the positions of the plusses ('+') to get the complementary supplementary difference sets.
A similar construction for getting 4-supplementary difference sets out of circulant $T$-matrices (Example 9) uses the positions of the minuses (or plusses) in the four $\pm 1$-sequences $A+B+C+D$, $A+B-C-D$, $A-B+C-D$, $A-B-C+D$, where the sequences $A$, $B$, $C$, $D$ are the first rows of the $T$-matrices.

**Example 12 (Second Construction for SDS)** We can also test which of the proper and generalised cosets form supplementary difference sets. Again we may carry out an experimental search where we check $2^n$ possible configurations if there is a total of $n$ cosets. For example for $n = 121 = 11 \times 11$ we found the following $12-\{121; 5; 2\}$ supplementary difference sets.

\[
\begin{align*}
S_1 &= \{2, 6, 18, 54, 41\} & S_7 &= \{11, 33, 99, 55, 44\} \\
S_2 &= \{4, 12, 36, 108, 82\} & S_8 &= \{16, 48, 23, 69, 86\} \\
S_3 &= \{5, 15, 45, 14, 42\} & S_9 &= \{17, 51, 32, 96, 46\} \\
S_4 &= \{7, 21, 63, 68, 83\} & S_{10} &= \{19, 57, 50, 29, 87\} \\
S_5 &= \{8, 24, 72, 95, 43\} & S_{11} &= \{20, 60, 59, 56, 47\} \\
S_6 &= \{10, 30, 90, 28, 84\} & S_{12} &= \{40, 120, 118, 112, 94\}
\end{align*}
\]

Note that $S_7$ is the only generalised coset.

**6 Conclusions**

We gave a brief introduction into cyclotomy, cyclotomic cosets and their correspondence to some combinatorial designs. We presented an experimental search through linear combinations of the incidence matrices of cyclotomic cosets. By introducing generalised cosets we were able to extend the idea to any length or size $n$. We believe that this generalisation is new. Again we relied on the property that the proper and generalised cosets had some "nice algebraic structure" and performed an experimental search. The search led to many new results.

In the generalisation all the operations have been done in the ring $\mathbb{Z}_n$. The structure of the ring (which was neither a field nor an integral domain since $ab = 0$ did not imply $a = 0$ or $b = 0$) was obviously good enough to give us some nice results, that is, sequences with zero or constant periodic autocorrelation function. However, at this stage we have not yet obtained a theoretical model for our computational results. A more analytical approach would definitely be interesting and is subject to further research. We would also like to stress that one is of course not confined to work in $\mathbb{Z}_n$. Any algebraic structure may be exploited to get the desired results. This is again subject to further investigation. As already mentioned the search for combinatorial designs has been experimental and in $\mathbb{Z}_n$. It is by no means finished yet. Since this search is only limited by the number of proper and generalised cosets, we anticipate many new sizes and length $n$ will prove fruitful.
Acknowledgment

Supported by the ARC grants A49131885 and A9130102, The University of Wollongong and the Centre for Computer Security Research.

References


