G-Matrices of order 19

Xian-Mo Zhang

Department of Computer Science
University College
University of New South Wales
Australian Defence Force Academy
Canberra, ACT 2600, AUSTRALIA

Abstract

Let X_1, X_2, X_3, X_4 be four type 1 $(1,-1)$ matrices on the same group of order n(odd) with the properties:

(i) $(X_i - I)^T = -(X_i - I)$, $i = 1, 2$,

(ii) $X_i^T = X_i$, $i =, 3, 4$ and the diagonal elements are positive,

(iii) $X_1 X_1^T + X_2 X_2^T + X_3 X_3^T + X_4 X_4^T = 4nI_n$.

Call such matrices G-matrices. These were first introduced and applied to construct Hadamard matrices by Jennifer Seberry in "On Hadamard matrices", Combinatorial Th. Ser. A, 18 (1975), 149-164. G-matrices of orders $3, 5, 7, 9$ were known previously. This paper constructs G-matrices of order 19 for the first time by using cyclotomic classes and gives the new orders 13 and 15.

1 Introduction and Basic Definitions

Definition 1 Let G be an additive abelian group of order v with elements $g_1, g_2, ..., g_v$ and S a subset of G.
Define the *type 1 (1,-1) incidence matrix* M=(m_{ij}) of order v of S is

$$m_{ij} = \begin{cases} +1 & \text{if } g_j - g_i \in X, \\ -1 & \text{otherwise;} \end{cases}$$

and the *type 2 (1,-1) incidence matrix* $N = (n_{ij})$ of order v of S is

$$n_{ij} = \begin{cases} +1 & \text{if } g_j + g_i \in X, \\ -1 & \text{otherwise.} \end{cases}$$

In particular, if G is cyclic the matrices M and N are called *circulant* and *back circulant* respectively. In this case $m_{1,j+1} = m_{i,j+i}$ and $n_{1,j} = n_{1+i,J+i}$.

Seberry and Whiteman [?] give similar definitions for type 1 matrices , type 2 matrices on abelian groups.

Definition 2 Let X_1, X_2, X_3, X_4 be four type 1 $(1,-1)$ matrices on the same group of order n(odd) with the properties:

(i) $(X_i - I)^T = -(X_i - I)$, $i = 1,2$,

(ii) $X_i^T = X_i$, $i =, 3, 4$ and the diagonal elements are positive,

(iii) $X_1X_1^T + X_2X_2^T + X_3X_3^T + X_4X_4^T = 4nI_n$.

Call such matrices *G-matrices* of order n.

G-matrices were introduced and applied to construct Hadamard matrices by Jennifer Seberry [**?**]. If there exist G-matrices of order n then $4n-2$ is the sum of two square integers [**?**]. For this reason, there exist no G-matrices of order $11, 17, 29, 35, 39, 47$. Previously, G-matrices of order $3, 5, 7, 9$ were known. This paper construct G-matrices of order 19 by using cyclotomic classes and gives the new orders 13 and 15.

Definition 3 Let x be a primitive element of $GF(p^t)$, where p is a prime and $p^t = ef+1$. The *cyclotomic classes* C_i are $C_i = \{x^{es+i} : s = 0, 1, \ldots, f-1\}$, $i = 0, 1, \ldots, e-1$. For fixed i and j, the *cyclotomic number* (i,j) is defined to be the number of solutions of the equation $z_i + 1 = z_j$ $(z_i \in C_i,\ z_j \in C_j)$.

Let A be a subset of $GF(p^t)$. Define

$$\triangle A = \{a - b \mid a \neq b, a, b \in A\}.$$

From [**?**],

$$\triangle C_i = (0,0)C_i + (1,0)C_{i+1} + (2,0)C_{i+2} + \cdots.$$

Let

$$\triangle(C_i - C_j) = \{a - b \mid a \in C_i, b \in C_j\}.$$

See [**?**] or [**?**] for more details.

2 Preliminaries

Lemma 1 $\triangle(C_i - C_j) = (j,i)C_0 + (j-1, i-1)C_1 + (i-2, j-2)C_2 + \cdots$.

Proof. For any $x^{es+i} \in C_i$ and $x^{et+j} \in C_j$, let $x^{es+i} - x^{et+j} = x^{er+k}$. Then $x^{er+k} \in C_k$ and $x^{e(s-r)+i-k} = x^{e(t-r)+j-k} + 1$. Since the number of solutions of the above equation is $(j-k, i-k)$, the x^{er+k} occurs $(j-k, i-k)$ times in $\triangle(C_i - C_j)$. Note for $r \neq q$, x^{er+k} and x^{eq+k} occur the same times then C_k occurs $(j-k, i-k)$ times in $\triangle(C_i - C_j)$. This proves the lemma. $\square$

Lemma 2 *Suppose P, Q, R, S are $4-\{2n+1;\ n, n, n-c, n-d;\ 2n-c-d-1\}$ supplementary difference sets on a cyclic group or abelian group of order $2n+1$, with P, Q skew-type i.e. $x \in P(\text{or } Q) \Rightarrow -x \notin P(\text{or } Q)$ and R, S symmetric i.e. $y \in R(\text{or } S) \Rightarrow -y \in R(\text{or } S)$. Then there exist circulant or type 1 G-matrices of order n.*

Proof. Let A, B, C, D be the type 1 (1 , -1) incidence matrices of P, Q, R, S respectively. By Lemma 1.20, [?], $AA^T + BB^T + CC^T + DD^T = 4nI_n$. By the construction of the type 1 incidence matrices, A, B, C, D are circulant if P, Q, R, S are sds on a cyclic group and satisfy

$$(A - I)^T = -(A - I),\ (B - I)^T = -(B - I),\ C^T = C,\ D^T = D.$$

□

3 Existence of G-Matrices of Order 19

To obtain G-matrices of order 19, by Lemma 1, we need $4 - \{19; 9, 9, 12, 6; 17\}$ supplementary difference sets. Clearly, 2 is a primitive element of $GF(19)$. Let $e = 6$, $f = 3$, then $19 = ef + 1$. By simple calculation,

$$C_0 = \{1, 7, 11\},\ C_1 = \{2, 3, 14\},\ C_2 = \{4, 6, 9\}, C_3 = \{8, 12, 18\},$$

$$C_4 = \{5, 16, 17\},\ C_5 = \{10, 13, 15\}.$$

Clearly $C_3 = -C_0$, $C_4 = -C_1$, $C_5 = -C_2$.
Set $P = C_1 \cup C_2 \cup C_3 = \{2, 3, 4, 6, 8, 9, 12, 14, 18\}$, $Q = C_3 \cup C_4 \cup C_5 = \{5, 8, 10, 12, 13, 15, 16, 17, 18\}$, $R = C_1 \cup C_2 \cup C_4 \cup C_5 = \{2, 3, 4, 5, 6, 9, 10, 13, 14, 15, 16, 17\}$, $S = C_2 \cup C_5 = \{4, 6, 9, 10, 13, 15\}$.

Lemma 3 *P, Q, R, S are $4 - \{19; 9, 9, 12, 6; 17\}$ supplementary difference sets.*

Proof.

$$\triangle(C_1 \cup C_2 \cup C_3) = 3C_0 + 4C_1 + 5C_2 + 3C_3 + 4C_4 + 5C_5.$$

Similarly,

$$\triangle(C_3 \cup C_4 \cup C_5) = 4C_0 + 5C_1 + 3C_2 + 4C_3 + 5C_4 + 3C_5,$$

$$\triangle(C_1 \cup C_2 \cup C_4 \cup C_5) = 9C_0 + 6C_1 + 7C_2 + 9C_3 + 6C_4 + 7C_5,$$

$$\triangle(C_2 \cup C_5) = C_0 + 2C_1 + 2C_2 + C_3 + 2C_4 + 2C_5.$$

Thus the totality is

$$17(C_0 + C_1 + C_2 + C_3 + C_4 + C_5).$$

This proves the lemma. □

Theorem 1 *There exist G-matrices of order 19.*

Proof. Use P, Q, R, S to form the circulant (1 , -1)-matrices A, B, C, D with first rows are

$$\begin{array}{ccccccccccccccccccc}
+ & + & - & - & - & + & - & + & - & - & + & + & - & + & - & + & + & + & - \\
+ & + & + & + & + & - & + & + & - & + & - & + & - & - & + & - & - & - & - \\
+ & + & - & - & - & - & - & + & + & - & - & + & + & - & - & - & - & - & + \\
+ & + & + & + & - & + & - & + & + & - & - & + & + & - & + & - & + & + & +
\end{array}$$

respectively. Note A , B are skew and C, D are symmetric. By Lemma 2, A, B, C, D are G-matrices of order 19. $\square$

We give a list of all G-matrices known.

G-matrices of order 3: $++-,\ +-+,\ +--,\ +++,$
G-matrices of order 5: $+++--,\ +-+-+,\ +----,\ +----,$
G-matrices of order 7: $++++---,\ ++-+-+-,\ +--++--,\ +------,$
G-matrices of order 9:

$$+-++-+--+,\quad +++-+-+--$$

$$++-++++-+,\quad ++------+$$

G-matrices of order 13:

$$+-+++++-----+,\quad +--+-++--+-++,$$

$$++-+++--+++-+,\quad +++-+-++-+-++$$

G-matrices of order 15:

$$+++-++++----+--,\quad +---++-+-+--+++,$$

$$+--++-++++-++--,\quad ++-+-++++++-+-+$$

The following lemma is given by professor Jennifer Seberry.

Lemma 4 *Suppose X_1, X_2, X_3, X_4 are four type 1 (1 , -1) G matrices of odd order n, then there exists an $OD(4n;1,1,2n-1,2n-1)$.*

Proof. Let $Y = \frac{1}{2}(X_1 + X_2 - 2I)$, $Z = \frac{1}{2}(X_1 - X_2)$, $W = \frac{1}{2}(X_1 + X_4)$, $U = \frac{1}{2}(X_1 - X_4)$. Then $Y^T = -Y$, $Z^T = -Z$, $W^T = W$, $U^T = U$, $UW^T = WU^T$, $YZ^T = ZY^T$ and

$$YY^T + ZZ^T + WW^T + UU^T = (2n-1)I_n.$$

Let x_1, x_2, x_3, x_4 be commuting variables then $x_1I + x_3Y + x_4Z$, $x_2I + x_4Y - x_3Z$, $x_3W + x_4U$, $x_4W - x_3U$ are four type 1 matrices which can be used in the Goethal- Seidel or Wallis-Whiteman array to obtain the required $OD(4n;1,1,2n-1,2n-1)$. $\square$

We note these orthogonal designs were previously unknown for $4n = 60, 76$.

References

[1] Seberry-Wallis, J. Some remarks on supplementary difference sets. *Colloquia Mathematica Societies Janos Bolyai 10* (1973), 1503–1526.

[2] Seberry-Wallis, J. On Hadamard matrices. *Journal of Combinatorial Theory Ser. A, 18* (1975), 149–164.

[3] Storer, T. *Cyclotomy and Difference Sets.* Markham Publishing Company, Chicago, 1967.

[4] Wallis, J., and Whiteman, A. L. Some classes of Hadamard matrices with constant diagonal. *Bull. Austral. Math. Soc. 7* (1972), 233–249.

[5] Wallis, W. D., Street, A. P., and Wallis, J. S. *Combinatorics: Room Squares, sum-free sets, Hadamard Matrices*, vol. 292 of Lecture Notes in Mathematics. Springer-Verlag, Berlin, Heidelberg, New York, 1972.