AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **33** (2005), Pages 237–246

Paley triple arrays

D. A. Preece

Queen Mary, University of London
U.K.
D.A.Preece@qmul.ac.uk
and
University of Kent, Canterbury, U.K.

W. D. Wallis   J. L. Yucas

Department of Mathematics
Southern Illinois University
U.S.A.
{wdwallis,jyucas}@math.siu.edu

Abstract

We provide a construction for a $q \times (q+1)$ Triple Array whenever q is an odd prime power.

1 Triple arrays

Agrawal [1] studied a class of designs for two-way elimination of heterogeneity. (One small example was discussed earlier by Potthoff [8] and another was published by Preece [9].) Such a design has three classes of constraints, called *rows*, *columns* and *symbols*. Suppose there are r rows, c columns and v symbols. If the design is interpreted as an $r \times c$ array in the natural way, it satisfies:

TA1 there are no repeated elements in any row or column;

and has positive integer parameters k, λ_{rr}, λ_{cc} and λ_{rc} such that:

TA2 each symbol occurs in k cells;
TA3 any two distinct rows contain λ_{rr} common symbols;
TA4 any two distinct columns contain λ_{cc} common symbols;
TA5 any row and column contain λ_{rc} common symbols.

An example (taken from [1, p1157]) is

$$\begin{array}{|cccccc|} 4 & 5 & 6 & 10 & 1 & 2 \\ 1 & 8 & 3 & 4 & 7 & 6 \\ 9 & 2 & 4 & 7 & 5 & 8 \\ 8 & 3 & 9 & 5 & 6 & 10 \\ 10 & 1 & 2 & 3 & 9 & 7 \end{array}. \qquad (1)$$

Such a design has a natural representation as a (binary) *row-column design*; if a, b and c are respectively a row, column and symbol, the block abc is represented by symbol c in cell (a, b). The properties mean that the row-column design is *equireplicate*, with every symbol appearing k times, it contains no empty cells, and if the rows and columns are treated as sets then the intersection of any two rows has size λ_{rr}, the intersection of any two columns has size λ_{cc}, and any row and column intersect in λ_{rc} elements. We shall call this array a *triple array* and denote it $TA(v, k, \lambda_{rr}, \lambda_{cc}, \lambda_{rc} : r \times c)$. The example above is a $TA(10, 3, 3, 2, 3 : 5 \times 6)$.

2 Triple arrays and other designs

Triple arrays were studied by Preece [10], although he did not use that name. He introduced them in the more general context of row-column designs. Triple arrays arise as fully proper O:YY(Q,Q,T) designs: that is, the row and column constraints are orthogonal, while the symbol constraints have overall total balance. In [10], there is a list of small triple arrays, some taken from [1] and some newly constructed.

Any triple array gives rise, in a natural way, to two balanced incomplete block designs. To construct them, suppose the rows of a $TA(v, k, \lambda_{rr}, \lambda_{cc}, \lambda_{rc} : r \times c)$ are labeled $R_1, R_2, \ldots, R_r$ and the columns are labeled $C_1, C_2, \ldots, C_c$. Then the *row design* or $BIBD_R$ has v blocks $B_1, B_2, \ldots, B_v$, corresponding to the v elements of V: if element x appears in rows $R_a, R_b, \ldots, R_z$ then $B_x = \{a, b, \ldots, z\}$. Similarly the *column design* or $BIBD_C$ is defined using the incidence of elements in columns. It follows from the definition that

(i) the row design is a balanced incomplete block design with parameters

$$(r, v, c, k, \lambda_{rr}).$$

(ii) the column design is a balanced incomplete block design with parameters

$$(c, v, r, k, \lambda_{cc}).$$

From these facts and the standard results about balanced incomplete block designs, it is easy to show that

$$vk = rc,$$

$$\begin{aligned}\lambda_{rr}(r-1) &= c(k-1),\\ \lambda_{cc}(c-1) &= r(k-1),\\ \lambda_{rr}r(r-1) &= \lambda_{cc}c(c-1).\end{aligned}$$

Moreover, as was shown in [4], any triple array satisfies

$$\lambda_{rc} = k.$$

An alternative approach is to construct from a triple array a block design for two sets of treatments, corresponding to rows and columns. The blocks of the new design correspond to the symbols in the triple array, and the entry in block x is the set of ordered pairs of row and column numbers of the cells containing entry x in the array. Such a design was called a graeco-latin design in [10], and the word *orthogonal* is used to describe the case where each possible ordered pair occurs exactly once in the design. So property **TA1** ensures that triple arrays are orthogonal graeco-latin designs. Another generalization of the triple array is a pair of orthogonal balanced incomplete block designs, as studied in [6].

3 The extremal case

In [4] we prove

Theorem 1 *Any triple array with $k \neq r$ and $k \neq c$ satisfies*

$$v \geq r + c - 1.$$

The extremal case $v = r + c - 1$ (in which it is easy to show that $\lambda_{cc} = r - k$) is of special interest. Agrawal [1] gave a method that started from a symmetric $(v+1, r, \lambda_{cc})$-BIBD, where $v = r+c-1$, and constructed a $TA(v, k, \lambda_{rr}, \lambda_{cc}, \lambda_{rc} : r \times c)$. He could not prove his method, but had found it to work in every case that he tried, provided $r - \lambda_{cc} > 2$. (Not only does the method fail when $r - \lambda_{cc} = 2$, but no triple array exists in those cases.) It has not yet been shown that Agrawal's construction works for every symmetric BIBD, although no counterexample has yet been found. However, the converse is true:

Theorem 2 [4] *If there exists a triple array $TA(v, k, \lambda_{rr}, \lambda_{cc}, \lambda_{rc} : r \times c)$ with $k \neq r$, $k \neq c$ and $v = r + c - 1$, then there exists a symmetric $(v + 1, r, \lambda_{cc})$-BIBD.*

In the 1970's, Preece concocted, but did not prove or publish, some recipes for the infinite family of triple arrays $TA(2q, \frac{q+1}{2}, \frac{q+1}{2}, \frac{q-1}{2}, \frac{q+1}{2} : q \times (q+1))$ where q is an odd prime power. The underlying $(v + 1, r, \lambda_{cc})$-BIBDs of these arrays are the family of Hadamard designs constructed by Paley [7], so the arrays will be called *Paley triple arrays*. A construction subsequently appeared in [11], and some further partial results appear in [2, Method 4.9]. Some of the results of [11] were rediscovered in [3].

In this paper we generalize Preece's constructions and verify the generalizations.

4 Paley triple arrays

For $q = p^r$, an odd prime power, we let Q denote the set of non-zero squares of elements of $GF(q)$ and let N denote the set of non-squares of $GF(q)$. Further, set $Q_0 = Q \cup \{0\}$ and $N_0 = N \cup \{0\}$. Let $GF(q)^*$ denote the multiplicative group of non-zero elements of $GF(q)$. The *quadratic character* $\eta : GF(q)^* \to \{\pm 1\}$, defined by

$$\eta(a) = \begin{cases} 1 & \text{if } a \in Q \\ -1 & \text{if } a \in N, \end{cases}$$

is well known to be a surjective group homomorphism. In particular, $Q \cdot Q = N \cdot N = Q$ and $Q \cdot N = N$. Also well known is the fact that

$$\eta(-1) = \begin{cases} 1 & \text{if } q \equiv 1 (\mathrm{mod}\, 4) \\ -1 & \text{if } q \equiv 3 (\mathrm{mod}\, 4). \end{cases}$$

We first record some equalities, some of which have appeared sporadically in the literature.

Proposition 3 *If $q \equiv 1 (\mathrm{mod}\, 4)$ then for $a \neq 0$ in $GF(q)$:*
(1) $|(a+Q) \cap Q_0| = |(a+Q) \cap N| = |(a+Q_0) \cap Q| = |(a+N) \cap Q|$
$= |(a+N) \cap N_0| = |(a+N_0) \cap N| = (q-1)/4,$
(2) $|(a+Q_0) \cap N_0| = |(a+N_0) \cap Q_0| = (q+3)/4,$
(3) $|(a+Q_0) \cap N| = |(a+N) \cap Q_0| = |(a+N_0) \cap N_0| = (q-2\eta(a)+1)/4,$
(4) $|(a+Q) \cap N_0| = |(a+Q_0) \cap Q_0| = |(a+N_0) \cap Q| = (q+2\eta(a)+1)/4,$
(5) $|(a+Q) \cap Q| = (q-2\eta(a)-3)/4,$
(6) $|(a+N) \cap N| = (q+2\eta(a)-3)/4.$

Proof. The proposition contains sixteen equalities. We prove four of them and indicate how the remainder can be proven similarly.

By [5, Lemma 6.24], the quadratic equation $x^2 - y^2 = -a$ has $q-1$ solutions. If $(x_0, y_0) \neq (0,0)$ is a solution of this equation then so are $(\pm x_0, \pm y_0)$. This set of four solutions gives one element in $(a+Q) \cap Q$ since $(x_0)^2 = (-x_0)^2$ and $(y_0)^2 = (-y_0)^2$. Consequently, if all solutions satisfy $(x,y) \neq (0,0)$, which is the case when $a \in N$, then $|(a+Q) \cap Q)| = |(a+Q) \cap Q_0| = |(a+Q_0) \cap Q| = |(a+Q_0) \cap Q_0)| = \frac{q-1}{4}$. If $a \in Q$ then all solutions satisfy $(x,y) \neq (0,0)$ except for $(0, \pm\sqrt{-a})$ and $(\pm\sqrt{-a}, 0)$. Hence, $|(a+Q) \cap Q| = \frac{q-5}{4}$, $|(a+Q) \cap Q_0| = \frac{q-5}{4} + 1$, $|(a+Q_0) \cap Q| = \frac{q-5}{4} + 1$ and $|(a+Q_0) \cap Q_0| = \frac{q-5}{4} + 2$. This proves four of the equalities (two from (1), one from (4), and (5)).

To evaluate $|(a+Q) \cap N|, |(a+Q) \cap N_0|, |(a+Q_0) \cap N|$ and $|(a+Q_0) \cap N_0)|$, first select any element $n \in N$. Then $N = nQ$. Now consider the quadratic form $x^2 - ny^2 = -a$ and proceed as above. The remaining eight equalities are proven by considering the quadratic forms $nx^2 - y^2 = -a$ and $nx^2 - ny^2 = -a$. $\square$

Proposition 4 *If* $q \equiv 3 (\mathrm{mod}\, 4)$ *then for* $a \neq 0$ *in* $GF(q)$*:*
(1) $|(a+Q) \cap N_0| = |(a+Q_0) \cap Q_0| = |(a+Q_0) \cap N|$
$= |(a+N) \cap Q_0| = |(a+N_0) \cap Q| = |(a+N_0) \cap N_0| = (q+1)/4,$
(2) $|(a+Q) \cap Q| = |(a+N) \cap N| = (q-3)/4,$
(3) $|(a+Q) \cap Q_0| = |(a+N) \cap Q| = |(a+N_0) \cap N| = (q-2\eta(a)-1)/4,$
(4) $|(a+Q) \cap N| = |(a+Q_0) \cap Q| = |(a+N) \cap N_0| = (q+2\eta(a)-1)/4,$
(5) $|(a+Q_0) \cap N_0| = (q-2\eta(a)+3)/4,$
(6) $|(a+N_0) \cap Q_0| = (q+2\eta(a)+3)/4.$

The proof is similar to the proof of Proposition 3. □

Order the elements of $GF(q)$, say by $\{0 = w_0, w_1, w_2, \ldots, w_{q-1}\}$, and write $GF(q)' = \{0' = w_0', w_1', w_2', \ldots, w_{q-1}'\}$, a duplicate copy. For non-zero elements a and b in $GF(q)$, define the $q \times q$ matrix C_0 by:

$$C_0(i,j) = \begin{cases} w_i - \frac{w_i - w_j}{a} & \text{if } w_i - w_j \in Q, \\ (w_i + \frac{w_i - w_j}{b})' & \text{if } w_i - w_j \in N_0. \end{cases}$$

Let C be the $q \times (q+1)$ matrix obtained by appending $(w_0, w_1, \ldots, w_{q-1})$ to C_0 as column q, i.e. $C(i,q) = w_i$, for $i = 0, 1, \ldots, q-1$. Notice that row i of C consists of

$$\{w_i - \frac{w_i - w_j}{a} : w_i - w_j \in Q\} \cup \{(w_i + \frac{w_i - w_j}{b})' : w_i - w_j \in N_0\} \cup \{w_i\}.$$

Since

$$w_i - \frac{w_i - w_j}{a} = w_j + \frac{a-1}{a}(w_i - w_j)$$

and

$$w_i + \frac{w_i - w_j}{b} = w_j + \frac{b+1}{b}(w_i - w_j)$$

we see that for $0 \leq j < q$, column j of C consists of

$$\{w_j + \frac{a-1}{a}(w_i - w_j) : w_i - w_j \in Q\} \cup \{(w_j + \frac{(b+1)}{b}(w_i - w_j))' : w_i - w_j \in N_0\}.$$

Proposition 5 *C satisfies TA1 and TA2.*

Proof. To see that there are no repetitions in a row notice that $w_i - (w_i - w_j)/a = w_i - (w_i - w_j')/a$ clearly implies that $w_j = w_j'$, and $w_i + (w_i - w_j)/b = w_i + (w_i - w_j')/b$ implies that $w_j = w_j'$. Also, if $w_i - (w_i - w_j)/a = w_i$ then $w_i - w_j = 0 \notin Q$. Similarly, there are no repetitions in a column. So TA1 is true.

For TA2, select $c \in GF(q)$. For each $w_i \in GF(q)$ there exists a unique $w_{j_i} \in GF(q)$ such that $w_i - (w_i - w_{j_i})/a = c$. It is $w_{j_i} = ac - aw_i + w_i$. Here $w_i - w_{j_i} = a(w_i - c)$ so as w_i ranges over $GF(q)$, so does $w_i - w_{j_i}$. Hence $|\{(i,j) : C_0(i,j) = c\}| = |Q| = (q-1)/2$. Notice that c also appears in the last column of C, so c appears $(q-1)/2 + 1 = (q+1)/2$ times in C. The case when $c \in GF(q)'$ is similar. One arrives at $|\{(i,j) : C(i,j) = c\}| = |N_0| = (q+1)/2$. □

Theorem 6 *Suppose $q \equiv 1 (\bmod 4)$. Choose a and b such that $ab \in Q$, $(a-1) \in Q$ and $(b+1) \in N$. Then C is a Paley triple array.*

Proof. Here there are two types of triple arrays. From the above remarks we see that if $a \in Q$ then row i and column j of C consists of

$$\left\{\begin{array}{ll} \text{row } i & (w_i + Q_0) \cup (w_i + N_0)' \\ \\ \text{column } j & (w_j + Q) \cup (w_j + Q_0)' \end{array}\right. \qquad \text{type 1}$$

for $0 \le j < q$. If $a \in N$ then row i and column j of C consists of

$$\left\{\begin{array}{ll} \text{row } i & (w_i + N_0) \cup (w_i + Q_0)' \\ \\ \text{column } j & (w_j + N) \cup (w_j + N_0)' \end{array}\right. \qquad \text{type 2}$$

for $0 \le j < q$.

The last column of C consists of $Q \cup N \cup \{0\}$ in either case. If $a \in Q$ then two different rows, say i_1 and i_2, intersect in $|(w_{i_1}+Q_0) \cap (w_{i_2}+Q_0)| + |(w_{i_1}+N_0) \cap (w_{i_2} + N_0)| = |[(w_{i_1} - w_{i_2}) + Q_0] \cap Q_0| + |[(w_{i_1} - w_{i_2}) + N_0] \cap N_0)|$ places. By Proposition 3(4) and Proposition 3(3), this is $(q+2\eta(w_{i_1} - w_{i_2})+1)/4 + (q-2\eta(w_{i_1} - w_{i_2})+1)/4 = (q+1)/2$ places. If $a \in N$, the result also follows from Proposition 3(3) and Proposition 3(4) in a similar manner. For columns, if $a \in Q$ then two different columns, say j_1 and j_2 with $j_1, j_2 < q$, intersect in $|(w_{j_1}+Q) \cap (w_{j_2}+Q)| + |(w_{j_1}+Q_0) \cap (w_{j_2}+Q_0)| = |[(w_{j_1} - w_{j_2}) + Q] \cap Q| + |[(w_{j_1} - w_{j_2}) + Q_0] \cap Q_0)|$ places. By Proposition 3(5) and Proposition 3(4), this is $(q-2\eta(w_{j_1} - w_{j_2})-3)/4 + (q+2\eta(w_{j_1} - w_{j_2})+1)/4 = (q-1)/2$ places. If $a \in N$, the result follows from Proposition 3(6) and Proposition 3(3) in a similar way. The last column of C intersects column j, with $j < q$, at either $w_j + Q$ or $w_j + N$. That is, in $(q-1)/2$ places also. For $i \ne j$ with $j < q$, we see that row i intersects column j in $(q-1)/4 + (q+3)/4 = (q+1)/4$ places by Proposition 3(1) and Proposition 3(2). If $i = j$, row i intersects column j in either $|Q|+1$ or $|N|+1$ places, that is, in $(q+1)/2$ places also. The last column of C intersects row i of C at $w_i + Q_0$ or at $w_i + N_0$. Again, in $(q+1)/2$ places. □

Example 7 Order $GF(5)$ as $GF(5) = \{0, 1, 2, 3, 4\}$. Take $a = b = 2$. The type 2 $TA(10, 3, 3, 2, 3 : 5 \times 6)$ obtained from Theorem 6 is

$$\begin{bmatrix} 0' & 3 & 4' & 1' & 2' & 0 \\ 3 & 1' & 4 & 0' & 2' & 1 \\ 3' & 4 & 2' & 0 & 1' & 2 \\ 2' & 4' & 0 & 3' & 1 & 3 \\ 2 & 3' & 0' & 1 & 4' & 4 \end{bmatrix}.$$

Example 8 Let α be a root of the primitive polynomial x^2+x+2 over $GF(3)$. Order $GF(9)$ by $GF(9)=\{0,\alpha,\alpha^2,\ldots,\alpha^8\}$. Take $a=\alpha^4$ and $b=\alpha^6$. The type 1 $TA(18,5,5,4,5:9\times 10)$ obtained from Theorem 6 is

$$\begin{bmatrix}
0' & {\alpha^7}' & \alpha^6 & \alpha' & 1 & {\alpha^3}' & \alpha^2 & {\alpha^5}' & \alpha^4 & 0 \\
{\alpha^4}' & \alpha' & 0' & 1 & {\alpha^5}' & {\alpha^2}' & \alpha^7 & \alpha^6 & \alpha^3 & \alpha \\
\alpha^6 & 1' & {\alpha^2}' & \alpha^5 & {\alpha^7}' & \alpha^3 & 0 & \alpha' & {\alpha^4}' & \alpha^2 \\
{\alpha^6}' & 1 & \alpha^5 & {\alpha^3}' & 0' & \alpha^2 & {\alpha^7}' & {\alpha^4}' & \alpha & \alpha^3 \\
1 & {\alpha^3}' & {\alpha^6}' & {\alpha^2}' & {\alpha^4}' & \alpha^7 & \alpha' & \alpha^5 & 0 & \alpha^4 \\
1' & {\alpha^6}' & \alpha^3 & \alpha^2 & \alpha^7 & {\alpha^5}' & 0' & \alpha^4 & \alpha' & \alpha^5 \\
\alpha^2 & \alpha^7 & 0 & {\alpha^5}' & 1' & {\alpha^4}' & {\alpha^6}' & \alpha & {\alpha^3}' & \alpha^6 \\
{\alpha^2}' & \alpha^6 & {\alpha^3}' & 1' & \alpha^5 & \alpha^4 & \alpha & {\alpha^7}' & 0' & \alpha^7 \\
\alpha^4 & \alpha^3 & {\alpha^5}' & \alpha & 0 & {\alpha^7}' & {\alpha^2}' & {\alpha^6}' & 1' & 1
\end{bmatrix}.$$

Corollary 9 *Suppose $q\equiv 1 \pmod 4$. There are $(q-5)(q-1)/16$ pairs (a,b) with $a\in Q$ that satisfy the conditions of Theorem 6 and there are $(q-1)^2/16$ pairs (a,b) with $a\in N$ that satisfy the conditions of Theorem 6. In particular, Paley triple arrays of type 1 exist for every $q>5$ and Paley triple arrays of type 2 exist for every $q\geq 5$.*

Proof. By Proposition 3(5), $|(1+Q)\cap Q|=(q-2\eta(1)-3)/4=(q-5)/4$ and by Proposition 3(1), $|(-1+N)\cap Q|=(q-1)/4$. Also, by Proposition 3(1), $|(1+Q)\cap N|=(q-1)/4$ and by Proposition 3(6), $|(-1+N)\cap N|=(q+2\eta(-1)-3)/4=(q-1)/4$. The result now follows. □

Theorem 10 *Suppose $q\equiv 3 \pmod 4$. Choose a and b such that $(a-1)(b+1)\in Q$ and if $a-1\in N$ then $ab\in Q$. Then C is a Paley triple array.*

Proof. Here we arrive at six different types of triple arrays. (i) Assume $a\in Q$ and $b\in Q$. If $a-1\in Q$ then row i and column j of C consists of

$$\begin{cases} \text{row } i & (w_i+N_0)\cup(w_i+N_0)' \\ \text{column } j & (w_j+Q)\cup(w_j+N_0)' \end{cases} \qquad \text{type 1}$$

for $0\leq j<q$. If $a-1\in N$ then row i and column j of C consists of

$$\begin{cases} \text{row } i & (w_i+N_0)\cup(w_i+N_0)' \\ \text{column } j & (w_j+N)\cup(w_j+Q_0)' \end{cases} \qquad \text{type 2}$$

for $0\leq j<q$. The last column of C consists of $Q\cup N\cup\{0\}$. Two different rows, say i_1 and i_2, intersect in $|(w_{i_1}+N_0)\cap(w_{i_2}+N_0)|+|(w_{i_1}+N_0)\cap(w_{i_2}+N_0)|=2|[(w_{i_1}-w_{i_2})+N_0]\cap N_0|$ places. By Proposition 4(1), this is $(q+1)/2$ places. If $a-1\in Q$ then two different columns, say j_1 and j_2 with $j_1,j_2<q$, intersect in

$|(w_{j_1}+Q)\cap(w_{j_2}+Q)|+|(w_{j_1}+N_0)\cap(w_{j_2}+N_0)| = |[(w_{j_1}-w_{j_2})+Q]\cap Q|+|[(w_{j_1}-w_{j_2})+N_0]\cap N_0)|$ places. By Proposition 4(2) and Proposition 4(1), this is $(q-3)/4+(q+1)/4=(q-1)/2$ places. The last column of C intersects column j, with $j<q$, at w_j+Q. That is, in $(q-1)/2$ places also. If $a-1\in N$ the result also follows from Proposition 4(2) and Proposition 4(1). For $i\neq j$ with $j<q$, if $a-1\in Q$ we see that row i intersects column j in $(q+1)/4+(q+1)/4=(q+1)/2$ places by Proposition 4(1). If $a-1\in N$ the result follows from Proposition 4(3) and Proposition 4(6). If $i=j$, row i intersects column j in either $|N_0|$ or $|N|+1$ places, that is, in $(q+1)/2$ places also. The last column of C intersects row i of C at w_i+N_0. Again, in $(q+1)/2$ places.

The proofs of the other cases are similar. Here are their descriptions: (ii) Assume $a\in N$ and $b\in N$. If $a-1\in Q$ then row i and column j of C consists of

$$\left\{\begin{array}{ll}\text{row } i & (w_i+Q_0)\cup(w_i+Q_0)' \\ \text{column } j & (w_j+N)\cup(w_j+Q_0)'\end{array}\right. \qquad \text{type 3}$$

for $0\le j<q$. If $a-1\in N$ then row i and column j of C consists of

$$\left\{\begin{array}{ll}\text{row } i & (w_i+Q_0)\cup(w_i+Q_0)' \\ \text{column } j & (w_j+Q)\cup(w_j+N_0)'\end{array}\right. \qquad \text{type 4}$$

As before, the last column of C consists of $Q\cup N\cup\{0\}$. (iii) Assume $a\in Q$ and $b\in N$. Here, row i and column j are

$$\left\{\begin{array}{ll}\text{row } i & (w_i+N_0)\cup(w_i+Q_0)' \\ \text{column } j & (w_j+Q)\cup(w_j+Q_0)'\end{array}\right. \qquad \text{type 5}$$

for $0\le j<q$. As before, the last column of C consists of $Q\cup N\cup\{0\}$. (iv) Assume $a\in N$ and $b\in Q$. Here, row i and column j are

$$\left\{\begin{array}{ll}\text{row } i & (w_i+Q_0)\cup(w_i+N_0)' \\ \text{column } j & (w_j+N)\cup(w_j+N_0)'\end{array}\right. \qquad \text{type 6}$$

for $0\le j<q$. As before, the last column of C consists of $Q\cup N\cup\{0\}$. □

Example 11 Order $GF(7)$ as $GF(7)=\{0,1,2,3,4,5,6\}$ and take $a=4$ and $b=2$. The type 2 $TA(14,4,4,3,4:7\times 8)$ obtained from Theorem 10 is

$$\begin{bmatrix} 0' & 3' & 6' & 6 & 5' & 3 & 5 & 0 \\ 6 & 1' & 4' & 0' & 0 & 6' & 4 & 1 \\ 5 & 0 & 2' & 5' & 1' & 1 & 0' & 2 \\ 1' & 6 & 1 & 3' & 6' & 2' & 2 & 3 \\ 3 & 2' & 0 & 2 & 4' & 7 & 3' & 4 \\ 4' & 4 & 3' & 1 & 3 & 5' & 1' & 5 \\ 2' & 5' & 5 & 4' & 2 & 4 & 6' & 6 \end{bmatrix}.$$

Corollary 12 *Suppose* $q \equiv 3 (\mathrm{mod}\, 4)$. *The construction in Theorem 10 yields* $(q-3)^2/16$ *Paley triple arrays of type 1, type 4 and type 5 and* $(q-3)(q+1)/16$ *Paley triple arrays of type 2, type 3 and type 6. In particular, there exist Paley triple arrays of each type for every* $q > 3$.

Proof. This is similar to Corollary 9 with Proposition 4 replacing Proposition 3. □

Proposition 13 *If q is prime and $GF(q)$ is ordered by* $\{0, 1, 2, \ldots, q-1\}$ *then* C_0 *has cyclic transversals. That is,*

$$C_0(i+k, j+k) = C_0(i, j) + k$$

(where row and column numbers are interpreted as integers modulo q, when additions are involved).

Proof. First notice that $(i+k)-(j+k) = i-j$. Thus all elements on a transversal of C_0 are either in $GF(q)$ or all are in $GF(q)'$. When $i-j \in Q$, $C(i+k, j+k) = (i+k)-(i-j)/a = C(i,j)+k$. It is similar when $i-j \in N_0$. □

See Example 7 and Example 11 for examples of Proposition 13.

References

[1] H. Agrawal, Some methods of construction of designs for two-way elimination of heterogeneity. *J. Amer. Statist. Assoc.* **61** (1966), 1153–1171.

[2] H. L. Agrawal and K. L.Sharma, On construction of two-way designs. *J. Indian Statist. Assoc.* **13** (1975), 1–31.

[3] R. A. Bailey and P. Heidtmann, Extremal row-column designs with maximal balance and adjusted orthogonality. Working paper, 2001.

[4] J. P. McSorley, N. C. Phillips, W. D. Wallis and J. L. Yucas, Double arrays, triple arrays, and balanced grids. *Designs, Codes, Crypt.* **35** (2005), 21–45.

[5] R. Lidl and H. Niederreiter, *Finite Fields (second edition), Encyclopedia of Mathematics* **20** (Cambridge University Press, Cambridge, 1997).

[6] J.P. Morgan and N. Uddin, Optimal blocked main effects plans with nested rows and columns and related designs. *Ann. Statist.* **24** (1996), 1185–1208.

[7] R. E. A. C. Paley, On orthogonal matrices. *J. Math. and Phys.* **12** (1933), 311–320.

[8] R. F. Potthoff, Three-factor additive designs more general than the Latin square. *Technometrics* **4** (1962), 187–208.

[9] D. A. Preece, Some row and column designs for two sets of treatments. *Biometrics* **22** (1966), 1–25.

[10] D. A. Preece, Non-orthogonal graeco-latin designs. *Combinatorial Mathematics IV, Proceedings of the Fourth Australian Conference* (Springer-Verlag, 1976), 7–26.

[11] J. Seberry, A note on orthogonal Graeco-Latin designs. *Ars Combin.* **8** (1979), 85–94.

(Received 20 Jan 2004)