The existence of a large set of idempotent quasigroups of order 62

Chang Yanxun
Department of Mathematics
Northern Jiaotong University
Beijing, 100044
P.R. China

ABSTRACT. In this article we construct a large set of idempotent quasigroups of order 62. The spectrum for large sets of idempotent quasigroups of order n (briefly, $LIQ(n)$) is the set all integers $n \geq 3$ with the exception $n = 6$ and the possible exception $n = 14$.

1 Introduction

An $n^2 \times 3$ array (defined on a set of size n) A is *orthogonal* if we run our fingers down any two columns of A we get each ordered pair belonging to $Q \times Q$ exactly once. Let $(Q, \circ)$ be a quasigroup of order n and define an $n^2 \times 3$ array A by: (x, y, z) is a row of A if and only if $x \circ y = z$. Then A is an $n^2 \times 3$ orthogonal array. Conversely, if A is any $n^2 \times 3$ orthogonal array (defined on a set Q) and we define a binary operation '$\circ$' on Q by $x \circ y = z$ if and only if (x, y, z) is a row of A, then $(Q, \circ)$ is a quasigroup. Hence we can think of a quasigroup of order n as an $n^2 \times 3$ orthogonal array and conversely. The quasigroup $(Q, \circ)$ is said to be idempotent provided it satisfies the identity $a^2 = a$ for all $a \in Q$. The corresponding orthogonal array A is called *idempotent orthogonal array*, which has the property that $(a, a, a) \in A$ for every $a \in Q$. Hence the $n(n-1)$ non-idempotent rows of A each consist of 3 distinct elements.

Two $n^2 \times 3$ idempotent orthogonal arrays defined on the same set are called *disjoint* if they have only the idempotent rows in common. $n - 2$ pairwise disjoint $n^2 \times 3$ idempotent orthogonal arrays are called *a large set of idempotent orthogonal arrays.* The corresponding quasigroups are called *a large set of idempotent quasigroups*, denoted by $LIQ(n)$. Teirlinck and Lindner [2] proved that there exists an $LIQ(n)$ for any $n \geq 3$, $n \neq 6, 14, 62$, and no $LIQ(6)$ exists. In this article we will give a construction of an $LIQ(62)$.

2 Symmetric $LMTS(22)$

Let x, y, z be distinct elements of a set X. The cyclic triple $\langle x, y, z\rangle$ is defined to be the set of three ordered pairs (x, y), (y, z) and (z, x). The cyclic triples $\langle x, y, z\rangle$, $\langle y, z, x\rangle$ and $\langle z, x, y\rangle$ will be regarded as identical. A *Mendelsohn triple system* of order v ($MTS(v)$) is a pair $(X, \mathcal{B})$, where X is a set containing v elements and $\mathcal{B}$ is a collection of cyclic triples of X such that every ordered pair of distinct elements of X appears in exactly one cyclic triple of $\mathcal{B}$. Mendelsohn [1] proved that the spectrum for $MTS(v)$'s is the set of all positive integers $v \equiv 0, 1 \pmod 3$ and $v \neq 6$.

A *large set of disjoint Mendelsohn triple systems* of order v or $LMTS(v)$ is a collection of $v-2$ pairwise disjoint $MTS(v)$s. Let $LMTS(v) = \{(X, \mathcal{B}): i = 1, 2, \ldots, v-2\}$. An $LMTS(v)$ is called *symmetric* if there exist $a, b \in X$ $(a \neq b)$ such that

(1) $\langle a, b, x\rangle \in \mathcal{B} \iff \langle b, a, x\rangle \in \mathcal{B}$;

(2) $\langle a, x, y\rangle \in \mathcal{B} \iff \langle b, y, x\rangle \in \mathcal{B}$ where $x, y \in X \setminus \{a, b\}$.

Lemma 2.1. [3] *There exists a symmetric $LMTS(n+2)$ for any positive integer $n \equiv \pm 1$ (mod 6).*

Theorem 2.2. *There exists a symmetric $LMTS(4n+2)$ for any positive integer $n \equiv \pm 1$ (mod 6).*

Construction: Let $\{(Z_n \cup \{\infty_1, \infty_2\}, C_k): k \in Z_n\}$ be a symmetric $LMTS$ $(n+2)$ which exists by Lemma 2.1. Now, we construct symmetric $LMTS$ $(4n+2)$

$$\{(X, B_k^t): k \in Z_n, t \in Z_4\}$$

on the set $X = (Z_4 \times Z_n) \cup \{\infty_1, \infty_2\}$. Each B_k^t $(k \in Z_n, t \in Z_4)$ consists of the following cyclic triples (where x and y run over Z_n)

$\mathbf{B_k^0}$ $(\mathbf{k \in Z_n})$:

(I) $\langle (0, u), (0, v), (0, w)\rangle$ with $\langle u, v, w\rangle \in C_k$, except that ∞_1 or ∞_2 appears as u, v or w, omit the first coordinate 0;

(II) $\langle (1, x-y), (2, x+2y+k), (3, x+y+k)\rangle$ with $y \neq k,\ k+1$;

(III) $\langle (3, x+y+k), (2, x+2y+k), (1, x-y)\rangle$ with $y \neq k+1$;

(IV) $\langle (1, x), (1, y), (0, \frac{x+y}{2}+k)\rangle$, $\langle (2, x), (2, y), (0, \frac{x+y}{2}-3k)\rangle$, $\langle (3, x), (3, y), (0, \frac{x+y}{2}-2k)\rangle$ with $x \neq y$;

(V) $\langle(0,x),(1,x-k),(2,x+3k)\rangle$, $\langle(0,x),(2,x+3k),(3,x+2k)\rangle$, $\langle(0,x),(3,x+2k),(1,x-k)\rangle$;

(VI) $\langle\infty_1,(1,x-k-1),(2,x+3k+2)\rangle$, $\langle\infty_1,(2,x+3k+2),(3,x+2k+1)\rangle$, $\langle\infty_1,(3,x+2k+1),(1,x-k-1)\rangle$, $\langle\infty_2,(3,x+2k+1),(2,x+3k+2)\rangle$, $\langle\infty_2,(2,x+3k+2),(1,x-k-1)\rangle$, $\langle\infty_2,(1,x-k-1),(3,x+2k+1)\rangle$.

$\mathbf{B_k^1}$ $(\mathbf{k}\in\mathbf{Z_n})$:

(I) $\langle(1,u),(1,v),(1,w)\rangle$ with $\langle u,v,w\rangle\in C_k$, except that ∞_1 or ∞_2 appears as u, v or w, omit the first coordinate 1;

(II) $\langle(0,x),(3,x+y+k),(2,x+2y+k)\rangle$ with $y\neq k,\ k+1$;

(III) $\langle(2,x+2y+k),(3,x+y+k),(0,x)\rangle$ with $y\neq k$;

(IV) $\langle(2,x),(2,y),(1,\frac{x+y}{2}-4k-3)\rangle$, $\langle(3,x),(3,y),(1,\frac{x+y}{2}-4k-3)\rangle$, $\langle(0,x),(0,y),(1,\frac{x+y}{2}-k-1)\rangle$ with $x\neq y$;

(V) $\langle(1,x-k-1),(0,x),(3,x+2k+1)\rangle$, $\langle(1,x-k-1),(3,x+2k+1),(2,x+3k+2)\rangle$, $\langle(1,x-k-1),(2,x+3k+2),(0,x)\rangle$;

(VI) $\langle\infty_1,(0,x),(3,x+2k)\rangle$, $\langle\infty_1,(3,x+2k),(2,x+3k)\rangle$, $\langle\infty_1,(2,x+3k),(0,x)\rangle$, $\langle\infty_2,(2,x+3k),(3,x+2k)\rangle$, $\langle\infty_2,(3,x+2k),(0,x)\rangle$, $\langle\infty_2,(0,x),(2,x+3k)\rangle$.

$\mathbf{B_k^2}$ $(\mathbf{k}\in\mathbf{Z_n})$:

(I) $\langle(2,u),(2,v),(2,w)\rangle$ with $\langle u,v,w\rangle\in C_k$, except that ∞_1 or ∞_2 appears as u, v or w, omit the first coordinate 2;

(II) $\langle(1,x-y),(0,x),(3,x+y+k)\rangle$ with $y\neq k,\ k+1$;

(III) $\langle(3,x+y+k),(0,x),(1,x-y)\rangle$ with $y\neq k+1$;

(IV) $\langle(3,x),(3,y),(2,\frac{x+y}{2}+k)\rangle$, $\langle(0,x),(0,y),(2,\frac{x+y}{2}+3k)\rangle$, $\langle(1,x),(1,y),(2,\frac{x+y}{2}+4k)\rangle$ with $x\neq y$;

(V) $\langle(2,x+3k),(1,x-k),(0,x)\rangle$, $\langle(2,x+3k),(0,x),(3,x+2k)\rangle$, $\langle(2,x+3k),(3,x+2k),(1,x-k)\rangle$;

(VI) $\langle\infty_1,(3,x+2k+1),(0,x)\rangle$, $\langle\infty_1,(0,x),(1,x-k-1)\rangle$, $\langle\infty_1,(1,x-k-1),(3,x+2k+1)\rangle$, $\langle\infty_2,(1,x-k-1),(0,x)\rangle$, $\langle\infty_2,(0,x),(3,x+2k+1)\rangle$, $\langle\infty_2,(3,x+2k+1),(1,x-k-1)\rangle$.

$\mathbf{B_k^3}$ $(\mathbf{k}\in\mathbf{Z_n})$:

(I) $\langle(3,u),(3,v),(3,w)\rangle$ with $\langle u,v,w\rangle\in C_k$, except that ∞_1 or ∞_2 appears as u, v or w, omit the first coordinate 3;

(II) $\langle(0,x),(1,x-y),(2,x+2y+k)\rangle$ with $y \neq k$, $k+1$;

(III) $\langle(2,x+2y+k),(1,x-y),(0,x)\rangle$ with $y \neq k$;

(IV) $\langle(0,x),(0,y),(3,\frac{x+y}{2}+2k+1)\rangle$, $\langle(1,x),(1,y),(3,\frac{x+y}{2}+3k+2)\rangle$, $\langle(2,x),(2,y),(3,\frac{x+y}{2}-k-1)\rangle$ with $x \neq y$;

(V) $\langle(3,x+2k+1),(0,x),(1,x-k-1)\rangle$, $\langle(3,x+2k+1),(1,x-k-1),(2,x+3k+2)\rangle$, $\langle(3,x+2k+1),(2,x+3k+2),(0,x)\rangle$;

(VI) $\langle\infty_1,(2,x+3k),(1,x-k)\rangle$, $\langle\infty_1,(1,x-k),(0,x)\rangle$, $\langle\infty_1,(0,x),(2,x+3k)\rangle$, $\langle\infty_2,(0,x),(1,x-k)\rangle$, $\langle\infty_2,(1,x-k),(2,x+3k)\rangle$, $\langle\infty_2,(2,x+3k),(0,x)\rangle$.

Proof: From Theorem 1 in [4], $\{\mathcal{B}_k^i\colon i \in Z_4, k \in Z_n\}$ form an $LMTS(4n+2)$. Note that $\{(Z_n \cup \{\infty_1,\infty_2\}, C_k)\colon k \in Z_n\}$ is a symmetric $LMTS(n+2)$. By the construction of (I) and (VI) , $\{\mathcal{B}_k^i\colon i \in Z_4, k \in Z_n\}$ is also symmetric. □

In Theorem 2.2, take $n=5$ we obtain

Corollary 2.3. *There exists a symmetric $LMTS(22)$.*

3 Construction

Theorem 3.1. *If there exists a symmetric $LMTS(n+2)$ and $LIQ(m+2)$, $m \geq 3$, then there exists an $LIQ(nm+2)$.*

Construction: Let $\{(Z_n \cup \{a,b\}, \mathcal{A}_i)\colon i \in Z_n\}$ with $\langle a,b,i\rangle \in \mathcal{A}_i$ be a symmetric $LMTS(n+2)$ and $\{(Q \cup \{a,b\}, \mathcal{B}_j)\colon j \in Q\}$ be an $LIQ(m+2)$, where $Q=\{0,1,\ldots,m-1\}$ is an idempotent quasigroup of order m (its binary operation is denoted by '$\circ$'), $Z_n=\{0,1,\ldots,n-1\}$, $a,b \notin Z_n \cup Q$. Let $\alpha=(0,1,\ldots,m-1)$ be a cycle of order m. Now we can construct nm idempotent orthogonal arrays $\mathcal{T}_{ij}$ $(i \in Z_n, j \in Q)$ on the set $X=(Z_n \times Q) \cup \{a,b\}$. Each $\mathcal{T}_{ij}$ consists of the following rows:

(1) $((x,u),(y,v),(z,(u\circ v)\alpha^j))$, $((y,u),(z,v),(x,(u\circ v)\alpha^j))$, $((z,u),(x,v),(y,(u\circ v)\alpha^j))$ with $\langle x,y,z\rangle \in \mathcal{A}_i$, $x,y,z \in Z_n$, $u,v \in Q$. This gives $m^2(n-1)(n-2)$ rows;

(2) $((x,u),(x,v),(y,(u\circ v)\alpha^j))$, $((x,v),(y,(u\circ v)\alpha^j),(x,u))$, $((y,(u\circ v)\alpha^j),(x,u),(x,v))$ with $\langle a,x,y\rangle \in \mathcal{A}_i$, $x,y \in Z_n$, $u \neq v \in Q$. This gives $3(m^2-m)(n-1)$ rows;

(3) $(a,(x,u),(y,u\alpha^j))$, $((x,u),a,(y,u\alpha^j))$, $((x,u),(y,u\alpha^j),a)$, $(b,(y,u\alpha^j),(x,u))$, $((y,u\alpha^j),b,(x,u))$, $((y,u\alpha^j),(x,u),b)$ with $\langle a,x,y\rangle \in \mathcal{A}_i$, $x,y \in Z_n$, $u \in Q$. This gives $6m(n-1)$ rows;

(4) $((i,u),(i,v),(i,w))$ with $(u,v,w) \in \mathcal{B}_j$, whenever a or b appears for u, v, w, omit the first coordinate i. This gives $(m+2)(m+1)$ rows;

(5) (s,s,s) for $s \in (Z_n \times Q) \cup \{a,b\}$. This gives $nm+2$ rows.

Proof: It is not difficult to see that each $\mathcal{T}_{ij}$ is an idempotent orthogonal array of order $nm+2$. We only need to show that every ordered triple T of distinct elements of X is contained in some $\mathcal{T}_{ij}$. All the possibilities are exhausted as follows:

(i) $T = (a,b,(i,w))$, $i \in Z_n$, $w \in Q$. There exists $j \in Q$ such that $\langle a,b,w\rangle \in \mathcal{B}_j$, then T appears in (4) of $\mathcal{T}_{ij}$ (and similarly for $T = (b,a,(i,w))$, $(a,(i,w),b)$, $(b,(i,w),a)$, $((i,w),a,b)$ and $((i,w),b,a)$).

(ii) $T = (a,(i,v),(i,w))$, $i \in Z_n$, $v \neq w \in Q$. There exists $j \in Q$ such that $\langle a,v,w\rangle \in \mathcal{B}_j$, then T appears in (4) of $\mathcal{T}_{ij}$ (and similarly for $T = (b,(i,v),(i,w))$, $((i,v),a,(i,w))$, $((i,v),a,(i,w))$, $((i,v),(i,w),a)$ and $((i,v),(i,w),b)$).

(iii) $T = (a,(x,u),(y,v))$, $x \neq y \in Z_n$, $u,v \in Q$. There exists $i \in Z_n$, $j \in Q$ such that $\langle a,x,y\rangle \in \mathcal{A}$, $v = u\alpha^j$, then T appears in (3) of $\mathcal{T}_{ij}$ (and similarly for $T = (b,(x,u),(y,v))$, $((x,u),a,(y,v))$, $((x,u),b,(y,v))$, $((x,u),(y,v),a)$ and $((x,u),(y,v),b)$).

(iv) $T = ((i,u),(i,v),(i,w))$, $i \in Z_n$, $u,v,w \in Q$ are pairwise distinct. There exists $j \in Q$ such that $\langle u,v,w\rangle \in \mathcal{B}_j$, then T appears in (4) of $\mathcal{T}_{ij}$.

(v) $T = ((x,u),(x,v),(y,w))$, $x \neq y \in Z_n$, $u,v,w \in Q$, $u \neq v$. There exists $i \in Z_n$ and $j \in Q$ such that $\langle a,x,y\rangle \in \mathcal{A}_i$, $(u \circ v)\alpha^j = w$, then T appears in (2) of $\mathcal{T}_{ij}$ (and similarly for $T = ((x,v),(y,w),(x,u))$, $((y,w),(x,u),(x,v))$).

(vi) $T = ((x,u),(y,v),(z,w))$, $x,y,z \in Z_n$ are pairwise distinct. There exists $i \in Z_n$ and $j \in Q$ such that $\langle x,y,z\rangle \in \mathcal{A}_i$, $(u \circ v)\alpha^j = w$, then T is appears in (1) of $\mathcal{T}_{ij}$.

This completes the proof. □

Corollary 3.2. *There exists an $LIQ(62)$.*

Proof: By Corollary 2.3 there exists a symmetric $LMTS(22)$. Take $n = 20$ and $m = 3$ in Theorem 3.1, an $LIQ(62)$ exists. □

Theorem 3.3. *There exists an $LIQ(n)$ for any $n \geq 3$ with the exception $n = 6$ and the possible exception $n = 14$.*

Proof: Teirlinck and Lindner [2] proved that there exists an $LIQ(n)$ for any $n \geq 3$, $n \neq 6, 14, 62$, and no $LIQ(6)$ exists. By Corollary 3.2 an $LIQ(62)$ exists. The conclusion follows. □

References

[1] N.S. Mendelsohn, A natural generalization of Steiner triple systems, in *Computers in Number Theory*, Academic Press, New York (1971), 323–338.

[2] L. Teirlinck and C.C. Lindner, The construction of large sets of idempotent quasigroups, *Eur. J. Combin.* **9** (1988), 83–89.

[3] Kang Qingde and Chang Yanxun, Symmetric Mendelsohn triple systems and large sets of disjoint Mendelsohn triple systems, Combinatorial designs and applications (*Lecture Notes in Pure and Applied Mathematics* **126**, Marcel Dekker Inc.) (1990), 69–78.

[4] Kang Qingde & Lei Jianguo, A completion of the spectrum for large sets of disjoint Mendelsohn triple systems, *Bulletin of the ICA* **9** (1993), 14–26.