Note

The construction of large sets of disjoint Mendelsohn triple systems of order $2^n + 2$

Qingde Kang

Department of Mathematics, Technische Universiteit Eindhoven, Eindhoven, Netherlands
Department of Mathematics, Hebei Normal College, Shijiazhuang, China

Received 22 February 1989

Abstract


We construct a LMTS(v) for $v = 2^n + 2$, $n \geq 3$.

1. Introduction

A Mendelsohn triple system on a set $X$ is a pair $(X, B)$, where $B$ is a collection of cyclically ordered triples of distinct elements from $X$ such that each ordered pair of distinct elements from $X$ is covered by a unique triple from $B$. (Here the cyclic triples $(x, y, z)$, $(y, z, x)$ and $(z, x, y)$ are considered equal, and cover the three pairs $(x, y)$, $(y, z)$ and $(z, x)$.) Let $X$ be a finite set of cardinality $v$. By simple counting one sees that $|B| = v(v-1)/3$. In particular, there is no Mendelsohn triple system of order $y$ (MTS($v$)) when $v = 2 \pmod{3}$. In fact, an MTS($v$) does exist if and only if $v = 0$ or $1 \pmod{3}$, $v \neq 6$ (Mendelsohn [1]).

Two Mendelsohn triple systems $(X, B)$ and $(X, B')$ on the same set $X$ are called disjoint when $B \cap B' = \emptyset$. By simple counting one sees that a collection of pairwise disjoint Mendelsohn triple systems can have size at most $v - 2$. Such a collection reaching this bound is called a Large set of Mendelsohn Triple Systems of order $v$, abbreviated LMTS($v$). Thus, a LMTS($v$) is a partition of all cyclic triples on a $v$-set into Mendelsohn triple systems. In this note we construct a
LMTS($2^n + 2$) for all $n \geq 3$. Some work on large sets of disjoint Mendelsohn triple systems can be found in Lindner [2], Teirlinck and Lindner [3], Wu [4] and Kang and Chang [5].

Let $F = GF(2^n)$ be the finite field with $2^n$ elements. Put $X = \{\infty_1, \infty_2\} \cup F$. The $2^n$ disjoint Mendelsohn triple systems of the LMTS($2^n + 2$) we shall construct are indexed with elements $x \in F$. The Mendelsohn triple system $(X, B_x)$ will contain the triples

- type I. $(\infty_1, \infty_2, x)$, $(\infty_2, \infty_1, x)$, this gives 2 cyclic triples,
- type II. $(\infty_1, v_1, w_1)$, $(\infty_2, v_2, w_2)$, $(x, v', w')$, this gives 3($2^n - 1$) cyclic triples,
- type III. $(u, v, w)$, this gives $\frac{1}{3}(2^n - 1)(2^n - 5)$ cyclic triples,

where $u \neq w_1$, $v \neq w_2$, $v' \neq w'$, $u \neq v \neq w \neq u$ and all belong to $F \setminus \{x\}$.

2. The pair class and the triple class

An arbitrary pair $(y, z)$ of distinct elements in $F \setminus \{x\}$ can be written uniquely as $(y, \alpha x + (1 - \alpha)z)$ with $\alpha \in F \setminus \{0, 1\}$. We shall call the class of such pairs with fixed $\alpha$ the pair class $\{\alpha\}$. When $y$ runs over $F \setminus \{x\}$, for fixed $x$, the elements $\alpha x + (1 - \alpha)y$ also runs over $F \setminus \{x\}$.

An arbitrary cyclic triple $(u, v, w)$ of distinct elements in $F$ can be written uniquely as $(u, \lambda u + (1 - \lambda)w, w)$ with $\alpha \in F \setminus \{0, 1\}$. We shall call the class of all such cyclic triples with fixed $\lambda$ the triple class $[\lambda]$. Note that since $(u, v, w) = (v, w, u) = (w, u, v)$, we have

$$[\lambda] = \left[ \frac{1}{1 - \lambda} \right] = \left[ \frac{1 - \lambda}{\lambda} \right].$$

For convenience, we shall call such three numbers $\lambda$, $1/(1 - \lambda)$ and $(1 - \lambda)/\lambda$ a trio $\{\lambda\}$.

About the pair class (brief PC) and the triple class (brief TC), we have the following lemma.

**Lemma 1.** For the field $F = GF(2^n)$, $n \geq 3$ and a fixed $x \in F$.

(C1) Each ordered pair of distinct elements in $F \setminus \{x\}$ belongs to a uniquely determined PC. The total number of the PC is $2^n - 2$. Each PC contains $2^n - 1$ pairwise distinct ordered pairs.

(C2) Each cyclic triple of distinct elements in $F$ belongs to a uniquely determined TC. The total number of the TC is $(2^n - 2)/3$ if $n$ odd, or $(2^n - 4)/3 + 2$ if $n$ is even (Note: When $n$ is even, there are two trios $\{\lambda\}$, with $\lambda = \varepsilon$ or $\varepsilon^2$, where $\varepsilon^3 = 1$ and $\varepsilon \neq 1$, that contain only one number. We call such triple classes small triple classes. In all other cases, the three numbers $\lambda$, $1/(1 - \lambda)$ and $(1 - \lambda)/\lambda$ of the trio $\{\lambda\}$ are pairwise distinct.) Each small triple class contains
(2^n(2^n - 1))/3 different cyclic triples, and the each of other TC contains 2^n(2^n - 1) different cyclic triples.

(C3) If we take the following form of the cyclic triple of types II and III in Section 1, then we have

<table>
<thead>
<tr>
<th>name</th>
<th>cyclic triples</th>
<th>PC</th>
<th>TC</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\kappa_1)-triple</td>
<td>((x_1, y, \kappa_1x + (1 - \kappa_1)y))</td>
<td>(\kappa_1)</td>
<td>(\begin{bmatrix} \frac{\alpha}{1 - \alpha} \ 1 - \alpha \end{bmatrix}) or (1 - \alpha) or (\frac{1}{\alpha})</td>
</tr>
<tr>
<td>(\kappa_2)-triple</td>
<td>((x_2, y, \kappa_2x + (1 - \kappa_2)y))</td>
<td>(\kappa_2)</td>
<td>(\frac{\lambda + \mu}{\lambda + \mu}) or (\frac{\lambda - \mu}{\mu}) or (\frac{\mu}{\lambda})</td>
</tr>
<tr>
<td>x-triple</td>
<td>((x, y, \kappa x + (1 - \kappa)y))</td>
<td>(\kappa)</td>
<td>(\begin{bmatrix} \frac{\lambda + \mu}{\lambda - \mu} \ \frac{\mu}{\lambda - \mu} \end{bmatrix}) or (\begin{bmatrix} \lambda + \mu \ \mu \end{bmatrix}) or (\begin{bmatrix} \lambda - \mu \ \mu \end{bmatrix})</td>
</tr>
<tr>
<td>y-triple</td>
<td>((\mu x + (1 - \mu)y, y, \lambda x + (1 - \lambda)y))</td>
<td>(\lambda), (\begin{bmatrix} \frac{\lambda + \mu}{\lambda - \mu} \ \frac{\mu}{\lambda - \mu} \end{bmatrix}) or (\begin{bmatrix} \lambda + \mu \ \mu \end{bmatrix}) or (\begin{bmatrix} \lambda - \mu \ \mu \end{bmatrix})</td>
<td></td>
</tr>
</tbody>
</table>

where \(x\) is fixed, \(y \in \mathbb{F}\setminus\{x\}\), \(\kappa_1, \kappa_2, \kappa, \lambda, \mu \in \mathbb{F}\setminus\{0, 1\}\) and \(\lambda \neq \mu\).

The proof of the lemma is not difficult. We omit it.

Now, we want to choose the suitable parameters \(\kappa_1, \kappa_2, \kappa\) and those \(\lambda, \mu\) such that the PC and TC listed in (C3) exactly are all PC and TC. Note that all y-triples will occupy \((2^n - 5)/3\) TC if \(n\) odd, or \((2^n - 7)/3 + 2\) TC if \(n\) even (which contain two small triple classes). It seems the first problem is the choice of those \(\lambda\) and \(\mu\).

### 3. The choice of parameters

For a given TC, one can give \(3(2^n - 3)\) pairs \(\{\lambda, \mu\}\) the y-triples corresponding to which all belong to the given TC. But these PC given by them usually are rather chaotic which gave us much difficulties. However, luckily, we have found the following.

**Lemma 2.** The three PC of a y-triple \((\mu x + (1 - \mu)y, y, \lambda x + (1 - \lambda)y)\) can form a trio if and only if one of the following holds.

1. \(\lambda + \mu = 1\); in this case, its TC and PC are the same, i.e., \(\lambda\), \(1/(1 - \lambda)\) and \((1 - \lambda)/\lambda\).
2. \(\lambda \mu = 1\); in this case, its PC are

\[
\begin{align*}
\langle \lambda \rangle, & \quad \langle \frac{1}{1 - \lambda} \rangle \text{ and } \langle \frac{1 - \lambda}{2} \rangle,
\end{align*}
\]

but its TC are

\[
[\lambda^{-2}] \text{ or } \left[\left(\frac{1}{1 - \lambda}\right)^{-2}\right] \text{ or } \left[\left(\frac{1 - \lambda}{\lambda}\right)^{-2}\right].
\]
**Proof.** Note that the three numbers in a trio are $\alpha$, $1/(1-\alpha)$ and $(1-\alpha)/\alpha$. By Lemma 1 (C3), we have only two possibilities:

1. \[
\frac{1}{1-\lambda} = \frac{\lambda + \mu}{1-\lambda} \quad \text{and} \quad \frac{1-\lambda}{\lambda} = \frac{\mu}{1-\mu}, \quad \text{This gives } \lambda + \mu = 1.
\]
2. \[
\frac{1}{1-\lambda} = \frac{\mu}{1-\mu} \quad \text{and} \quad \frac{1-\lambda}{\lambda} = \frac{\lambda + \mu}{1-\lambda}, \quad \text{This gives } \lambda \mu = 1. \quad \square
\]

Below, we will consider other triples. Note that for the $x$-triple its PC and TC are different (if PC belongs to the trio $\{\alpha\}$, then the TC belongs the trio $\{\alpha^{-1}\}$, but always $\{\alpha\} \neq \{\alpha^{-1}\}$), so we cannot use case (1) of Lemma 2 for all $y$-triples.

A feasible method is: If there exists a number $\alpha \in \mathbb{F} \setminus \{0,1\}$, such that $\{\alpha^{-2}\} = \{\alpha^{-1}\}$, and take for $t$ the minimal positive integer satisfying this equation, then we can use case (2) of Lemma 2 for the trios $\{\alpha\}$, $\{\alpha^{-2}\}$, $\{\alpha^{-3}\}$, . . . , $\{\alpha^{-2n}\}$ (to construct corresponding $y$-triples). And for the $x$-triple, $\infty_1$-triple and $\infty_2$-triple we can let $\alpha$, $\alpha_1$ and $\alpha_2$ be $1/\alpha$, $\alpha/(1-\alpha)$ and $1-\alpha$ (they form a trio $\{\alpha^{-1}\}$), respectively. For all other trios we still use (1) of Lemma 2. Hence, indeed we will complete all work to construct LMTS($2^n + 2$), for all $n \geq 3$. At present, our last task is finding such a number $\alpha$.

**Lemma 3.** For every $n \geq 3$, there exists an element $\alpha \in \mathbb{F} = GF(2^n)$ and a minimal positive $t$, such that $\{\alpha^{-2}\} = \{\alpha^{-1}\}$.

1. If these exists an odd $m > 1$ with $m \mid n$ then $\alpha = g^{(2^n-1)/(2m-1)}$ and $t = m$ when $3 \nmid m$, $t = 1$ when $m = 3$.
2. If $4 \mid n$, then $\alpha = g^{(2^n-1)/15}$ and $t = 2$, where $g$ is a primitive element of $\mathbb{F}$.

**Proof.** (1) Firstly we have, $\alpha^{(-2)m+1} = g^{1-2m} = 1$, so $\alpha^{(-2)m} = \alpha^{-1}$ (*). Thus $\alpha^{(-2)m} = \alpha$ (**), and $m$ is the minimal positive integer satisfying the equation.

When $3 \nmid m$, let $\{\alpha^{(-2)m}\} = \{\alpha^{-1}\}$ and $t$ is the minimal positive integer satisfying the equation. Then $\{\alpha^{(-2)m}\} = \{\alpha\}$ and $t \leq m$ (by (*)).

(i) If $\alpha^{(-2)^m} = \alpha$, then $2m \mid 2t$ by (**), so $m \mid t$. Thus $t = m$;

(ii) If $\alpha^{(-2)^m} = 1/(1-\alpha)$, then $\alpha^{(-2)^m} = (1-\alpha)/\alpha$, $\alpha^{(-2)^m} = \alpha$. So, by (**), $2m \mid 3t$. But $3 \nmid m$, thus $m \mid t$, so $t = m$.

(iii) If $\alpha^{(-2)^m} = (1-\alpha)/\alpha$, then $\alpha^{(-2)^m} = 1/(1-\alpha)$, $\alpha^{(-2)^m} = \alpha$. So $t = m$, also.

When $m = 3$, we have

$$\alpha^8 - \alpha = \alpha(\alpha - 1)(\alpha^3 + \alpha + 1)(\alpha^3 + \alpha^2 + 1) = 0,$$

but $\alpha \neq 0, 1$, either $\alpha^3 + \alpha + 1 = 0$ or $\alpha^3 + \alpha^2 + 1 = 0$. These imply $\alpha^{-2} = \alpha/(1-\alpha)$ or $\alpha^{-2} = 1 - \alpha$. In both cases $\{\alpha^{-2}\} = \{\alpha^{-1}\}$, so $t = 1$.

(2). If $\alpha = g^{(2^n-1)/15}$, we have

$$\alpha^{16} - \alpha = \alpha(\alpha^5 - 1)(\alpha^2 + \alpha + 1)(\alpha^4 + \alpha + 1)(\alpha^4 + \alpha^3 + 1) = 0,$$
but \(\alpha \neq 0\), \(\alpha^2 \neq 1\) and \(\alpha^3 \neq 1\), so either \(\alpha + 1 = 0\) or \(\alpha^4 + \alpha^3 + 1 = 0\). These imply \(\alpha^{(-2)^2} = 1 - \alpha\) or \(\alpha^{(-2)^2} = \alpha/(1 - \alpha)\). In both cases \(\{\alpha^{(-2)^2}\} = \{\alpha^{-1}\}\). Obviously, \(t = 2\) is the minimal. \(\square\)

By the lemma, we can quickly get such number \(\alpha = g^{(2^n-1)/(2^n-1)}\) that \(\{\alpha^{(-2)^t}\} = \{\alpha^{-1}\}\), where \(t\) is the minimal. For \(3 \leq n \leq 17\), we have:

<table>
<thead>
<tr>
<th>(n)</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td>(m)</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>7</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>11</td>
<td>3</td>
<td>4</td>
<td>13</td>
<td>7</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>(\text{ind}(\alpha))</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>9</td>
<td>1</td>
<td>17</td>
<td>73</td>
<td>33</td>
<td>585</td>
<td>273</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4681</td>
<td>1057</td>
</tr>
<tr>
<td>(t)</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>11</td>
<td>1</td>
<td>2</td>
<td>13</td>
<td>7</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

If \(\alpha = g^\lambda\), we denote \(\lambda = \text{ind}(\alpha)\).

4. The construction and examples

Let \(\alpha\) and \(t\) be given by Lemma 3 such that \(\{\alpha^{(-2)^t}\} = \{\alpha^{-1}\}\). Denote \(\alpha_i = \alpha^{(-2)^i}, 0 \leq i \leq t - 1\). And denote all other trios (besides \(\{\alpha_0\}, \{\alpha_1\}, \ldots, \{\alpha_{t-1}\}\) and \(\{\alpha^{-1}\}\)) by \(\{\lambda_j\}, 1 \leq j \leq s\), where \(s = (2^n - 5)/3 - t\) if \(n\) odd, or \(s = (2^n - 1)/3 - t\) if \(n\) even. As announced in Section 1, \(B_s\) will contain the triples:

1. \((\infty_1, \infty_2, x), (\infty_2, \infty_1, x)\),

2. \(\left(\infty_1, y, \frac{x}{1 - \alpha} + \frac{1}{1 - \alpha} y\right), (\infty_2, y, (1 - \alpha)x + \alpha y), (x, y, \frac{1}{\alpha} x + \frac{1 - \alpha}{\alpha} y)\),

3. \(\left(\frac{1}{\alpha_i} x + \frac{1 - \alpha_i}{\alpha_i} y, y, \alpha_i x + (1 - \alpha_i)y\right) 0 \leq i \leq t - 1,\)

4. \((1 - \lambda_j)x + \lambda_j y, y, \lambda_j x + (1 - \lambda_j)y) 1 \leq j \leq s,\)

where \(y\) runs over \(\mathbb{F} \setminus \{x\}\).

Note that, when \(n\) is even, there are two small triple classes. For these classes, letting \(y\) run over \(\mathbb{F} \setminus \{x\}\) produces each element three times but we only retain one copy of each triple!

Now, we can give our main result.

**Theorem.** For \(n \geq 3\), the above construction \(\{(\infty_1, \infty_2) \cup \mathbb{F}, B_s\); \(x \in \mathbb{F}\}\) gives a LMTS(\(2^n + 2\)), where \(\mathbb{F} = GF(2^n)\).
Example 1. \(n = 3, g^3 + g + 1 = 0, \alpha = \alpha_0 = g, t = 1, \alpha^{-1} = g^6\).

\(\text{trios: } \{g, g^2, g^4\}, \{g^3, g^5, g^6\}\).

\(\text{LMTS}(10) = \{(\infty_1, \infty_2) \cup \mathbb{F}_8, B_x); x \in \mathbb{F}_8\}.

\[ \begin{align*}
\mathbf{B}_x: \quad & (1) (\infty_1, \infty_2, x), (\infty_2, \infty_1, x) \\
& (2) (\infty_1, y, g^5x + g^4y) \quad (5) \\
& (\infty_2, y, g^3x + gy) \quad (3) \\
& (x, y, g^x + g^y) \quad (6) \quad [3, 5, 6] \\
& (3) (g^6x + g^3y, y, gx + g^3y) \quad (1) (2) (4) \quad [1, 2, 4]
\end{align*} \]

There are not any triples of the form (4).

Example 2. \(n = 4, g^4 + g + 1 = 0, \alpha = \alpha_0 - g, t = 2, \alpha_1 = g^{13}, \alpha^{-1} = g^{14}\).

\(\text{trios: } \{g, g^3, g^{11}\}, \{g^2, g^6, g^7\}, \{g^4, g^{12}, g^{14}\}, \{g^5, g^9, g^{13}\}, \{g^3\}, \{g^{10}\}\).

\(\text{LMTS}(18) = \{(\infty_1, \infty_2) \cup \mathbb{F}_{16}, B_x); x \in \mathbb{F}_{16}\}.

\[ \begin{align*}
\mathbf{B}_x: \quad & (1) (\infty_1, \infty_2, x), (\infty_2, \infty_1, x) \\
& (2) (\infty_1, y, g^{12}x + g^{11}y) \quad (14) \\
& (\infty_2, y, g^4x + gy) \quad (12) \\
& (x, y, g^4x + g^3y) \quad (4) \quad [3, 1, 11] \\
& (3) (g^{14}x + g^3y, y, gx + g^4y) \quad (1) (3) (11) \quad [9, 8, 13] \\
& (g^{2}x + g^5y, y, g^3x + g^6y) \quad (13) (8) (9) \quad [14, 12, 4] \\
& (4) (g^8x + g^2y, y, g^2x + g^3y) \quad (2) (7) (6) \quad [2, 7, 6] \\
& (g^{10}x + g^9y, y, g^2x + g^{10}y) \quad (5) (5) (5) \quad [5, 5, 5] \\
& (g^5x + g^{10}y, y, g^{10}x + g^3y) \quad (10) (10) (10) \quad [10, 10, 10]
\end{align*} \]

The last two triples are small triple classes. [Note: For brevity, the mark of the PC \(g^8\) is denoted as \(\lambda\). And for the TC we write all of the three numbers.]

5. Remarks

The result in this paper enlarges the known spectrum of large sets of disjoint MTSs. Firstly \(\text{LMTS}(v)\) is constructed for many unknown orders \(2^n + 2\), such as those with \(n = 4, 6, 7, 8, 10, 13, \ldots\). Furthermore, together with Theorem 6 in [5], we completely settle the case \(v = 42, 58 \mod 72\). Now all that remains for a complete solution of the existence problem for \(\text{LMTS}(v)\) is a construction of \(\text{LMTS}(v)\) for every order \(v, v = 6, 22 \mod 72\).

In cases where an \(\text{LMTS}(v)\) was known already our system may be non-isomorphic to the known systems. For example, the only known \(\text{LMTS}(10)\) is the one constructed in Lindner [1]. It is easy to see that since this system is constructed by a recursive construction \(v + 1 \rightarrow 3v + 1\), every \(\text{MTS}(10)\) in this system contains three sub-MTS(4). But one may check that the \(\text{MTS}(10)\) in the \(\text{LMTS}(10)\) constructed here do not have sub-MTS(4). By the way, our method
also gives the possibility to construct mutually nonisomorphic LMTS\(2^n + 2\), through different choices for the parameters.

The author wishes to thank Prof. A.E. Brouwer for reading the manuscript, improving the English and giving some good suggestions.

References