JOURNAL OF COMBINATORIAL THEORY, Series A 37, 164–188 (1984)

On Large Sets of Disjoint Steiner Triple Systems, V

LU JIA-XI

Ninth Middle School of Baotou,
Inner Mongolia Autonomous Region, Baotou, China

Communicated by the Managing Editors

Received March 4, 1983

In a previous paper (*J. Combin. Theory Ser. A* **34** (1983), 156–182), to construct large sets of disjoint $STS(3n)$'s (i.e., $LTS(3n)$'s), a kind of combinatorial design, denoted by $LD(n)$, where n is the order of design, was introduced and it was shown that if there exist both an $LD(n)$ and an $LTS(n+2)$, then there exists an $LTS(3n)$ also. In this paper, after having established some recursive theorems of $LD(n)$, the following result was proved: If n is a positive integer such that $n \equiv 11 \pmod{12}$, then there exists an $LD(n)$, except possibly $n \in \{23, 47, 59, 83, 107, 167, 179, 227, 263, 299, 347, 383, 719, 767, 923, 1439\}$.

1. MAIN THEOREMS

As in our previous papers [2–5], we write $D(v)$ for the maximum number of pairwise disjoint STS(v)'s. The number $D(v)$ cannot exceed $v-2$; and if $D(v)=v-2$, we call any set of $v-2$ pairwise disjoint STS(v)'s a large set of disjoint STS(v)'s and denote it by LTS(v). To construct LTS($3n$)'s, where n is an odd number, in our previous paper [4] we introduced a kind of combinatorial design which is denoted by LD(n), where n is the order of design. We have shown the following:

THEOREM. *If there exist both an* LD(n) *and an* LTS($n+2$), *then there exists an* LTS($3n$) *also.*

In defining LD(n) in [4] we made use of the transversal design which occurs frequently in the literature on block designs. A transversal design $T(k, n)$ is a triad $(X, \mathcal{G}, \mathrm{cl})$, where X is a set of kn elements, $\mathcal{G} = \{G_i \mid i \in I\}$ (I is an indexing set of cardinality k) is a partition of X into k n-subsets G_i (called groups), and cl is a class of k-subsets of X (called blocks) such that $|A \cap G_i| = 1$ for each block A and group G_i, and for any pair of distinct elements which belong to different groups, there is a unique block A containing this pair.

Throughout this paper, F_q will denote the finite field of order q, $F_q^* =$

0097-3165/84 $3.00

$F_q \backslash \{0\}$. In particular, $F_4 = \{0, g^0, g^1, g^2\}$, where g is a fixed primitive root of F_4.

Let X be a set of n elements. We denote a set consisting of $n+2$ sets $\mathscr{L}_x$, (x runs over X), $\mathscr{L}^1$ and $\mathscr{L}^2$ of ordered triples or ordered quadruples of X by LD(n) or LD[X] (occasionally LD), if conditions (C_1)–(C_5) are satisfied:

(C_1) Each $\mathscr{L}_x$ consists of ordered triples of the set $X \backslash \{x\}$. Each of the $\mathscr{L}^1$ and $\mathscr{L}^2$ consists of ordered quadruples of the set X. Both the ordered triples in $\mathscr{L}_x$ ($x \in X$) and ordered quadruples in $\mathscr{L}^j$ ($j = 1, 2$) will be called blocks. Let $x \in X$, adjoining $\mathscr{L}_x$ we define a set of triples cl_x as $\mathrm{cl}_x = \{\{(g^0, x_0), (g^1, x_1), (g^2, x_2)\} | (x_0, x_1, x_2) \in \mathscr{L}_x\}$, and the second condition is

(C_2) For any $x \in X$, $(F_4^* \times (X \backslash \{x\}), \mathscr{G}_x, \mathrm{cl}_x)$ forms a transversal design $T(3, n-1)$, where $F_4^* \times (X \backslash \{x\})$ is a Cartesian product set and $\mathscr{G}_x = \{\{u\} \times (X \backslash \{x\}) | u \in F_4^*\}$.

Again, adjoining each $\mathscr{L}^j$ ($j = 1, 2$), we define a set of quadruples cl^j as: $\mathrm{cl}^j = \{\{(g^0, x_0), (g^1, x_1), (g^2, x_2), (0, x_3)\} | (x_0, x_1, x_2, x_3) \in \mathscr{L}^j\}$, and the third condition is

(C_3) For any $j \in \{1, 2\}$, $(F_4 \times X, \mathscr{G}, \mathrm{cl}^j)$ forms a transversal design $T(4, n)$, where $\mathscr{G} = \{\{u\} \times X | u \in F_4\}$.

The other conditions are

(C_4) There exists an element $c_0 \in X$ such that for arbitrary $x \in X$ and $j \in \{1, 2\}$, (x, x, x, c_0) belongs to $\mathscr{L}^j$.

(C_5) For any ordered triple (x_0, x_1, x_2) of the set X, either there exists x such that $(x_0, x_1, x_2) \in \mathscr{L}_x$, or there exist x_3 and j such that $(x_0, x_1, x_2, x_3) \in \mathscr{L}^j$.

Sometimes we may have to deal with a number of LDs at the same time. In such cases, in order to distinguish the LDs, we may mark the notations with circumflex, asterisk, or asterisks, and/or prime or primes such as $\mathscr{L}_{xz}$, $\mathscr{L}^*_{xz}$, $\mathscr{L}'^1$, $\mathscr{L}''^2$, $\mathscr{L}^{**1}$, and so on.

We shall denote by D the set of integers n for which LD(n)'s exist. For convenience, define $1 \in D$. It can easily be seen that none of 2, 3, and 6 belongs to D. The main purpose of this paper is to prove that all the positive integers $n \equiv 11 \pmod{12}$ belong to D, only with the possible exceptions of 16 values of n; namely we have

THEOREM 1. *If n is a positive integer, $n \equiv 11 \pmod{12}$, and $n \notin \{23, 47, 59, 83, 107, 167, 179, 227, 263, 299, 347, 383, 719, 767, 923, 1439\}$, then $n \in D$.*

This theorem together with the theorem mentioned before yields

THEOREM 2. *If $D(n+2) = n$, $n \equiv 11 \pmod{12}$, and $n \notin \{23, 47, 59, 83, 107, 167, 179, 227, 263, 299, 347, 383, 719, 767, 923, 1439\}$, then $D(3n) = 3n - 2$.*

Further, Theorem 2 combined with other known results enables us, in the next paper [6], to prove that $D(v) = v - 2$ holds for all $v \equiv 1, 3 \pmod 6$ ($v > 7$), only with the possible exceptions of six values of v. The proof of Theorem 1 is based on Theorems 3–6.

THEOREM 3. *If q is an odd prime power, $q \geqslant 7$, both r and t are nonnegative integers, $r > 2$, $t \leqslant 2^{r-1} - 3$, $1 + (q-1)t \in D$, and $1 + q \in D$, then $1 + (q-1)t + 2^r q \in D$.*

THEOREM 4. *If q and q' are two odd prime powers, $q \geqslant 7$, $q' \geqslant 7$, both r and t are nonnegative integers, $r > 2$, $t \leqslant (2^{r-1} - 3)(q' - 3)$, $1 + (q-1)t \in D$, and $1 + q'q \in D$, then $1 + (q-1)t + 2^r q'q \in D$.*

THEOREM 5. *If q is an odd prime power, $q \geqslant 5$, both r and t are nonnegative integers, $r > 2$, $t \leqslant 2^{r-2} - 1$, $1 + (q-1)t \in D$, and $1 + q \in D$, then $1 + (q-1)t + 2^r q \in D$.*

THEOREM 6. *If q and q' are two odd prime powers, $q \geqslant 5$, $q' \geqslant 5$, both r and t are nonnegative integers, $r > 2$, $t \leqslant (2^{r-2} - 1)(q' - 3)$, $1 + (q-1)t \in D$, and $1 + q'q \in D$, then $1 + (q-1)t + 2^r q'q \in D$.*

Theorems 3 and 4 will be proved in Sections 6 and 7, and Theorems 5 and 6 in Section 8. Then we shall be able to prove Theorem 1 in Section 9.

2. PRELIMINARIES

In our previous paper [4], we proved some existencing theorems of LD(n), all of which are useful in this paper. We now state them as lemmas.

LEMMA 1. *If t is a nonnegative integer, then $7 + 12t \in D$ and $5 + 8t \in D$.*

LEMMA 2. *If p^r is a prime power, $p > 2$ and $p^r \in D$, then $3p^r \in D$.*

EXAMPLES. By Lemma 1 we have 5, 13, 29 $\in D$, and by Lemma 2, 15, 39, 87 $\in D$ follows.

LEMMA 3. *If $m \in D$, and $q = 2^r$ (r is an integer greater than 1) or $q \in \{5, 7, 11, 19\}$, then $qm \in D$.*

LEMMA 4. *If q is a prime power greater than 4 and $1 + m \in D$, then $1 + qm \in D$.*

TABLE I

Some $LD(n)$'s Obtained by Lemma 3

n	q	m	n	q	m	n	q	m	n	q	m
7	7	1	203	7	29	695	5	139	1055	5	211
8	8	1	215	5	43	707	7	101	1067	11	97
11	11	1	275	5	55	755	5	151	1115	5	223
20	4	5	335	5	67	935	5	187	1211	7	173
35	5	7	371	7	53	1001	11	91	1235	5	247
95	19	5	395	5	79	1043	7	149	1415	5	283
155	5	31	671	11	61						

As examples, we give some LD(n)'s obtained by Lemma 3 in Table I. Except $m = 1$ is the trivial case and $m = 97 \in D$ is seen in Table II, for all remaining cases in Table I, the fact $m \in D$ can be derived from Lemma 1. We also give some LD(n)'s obtained by Lemma 4 in Table II. Except for cases of Nos. 16 and 28, where $m + 1 = 63$, we give the reason of $m + 1 \in D$ in the last column of this table. Thus, a symble A means that $m + 1 \in D$ is seen in Table I, and a symbol B means that $m + 1 \in D$ is an example of Lemma 2. Taking $r = 3$, $q = 7$ and $t = 1$ in Theorem 3, we can obtain

TABLE II

Some $LD(n)$'s Obtained by Lemma 4

No.	n	q	m		No.	n	q	m	
1	51	5	10	*A*	16	683	11	62	
2	57	8	7	*A*	17	731	73	10	*A*
3	71	7	10	*A*	18	743	53	14	*B*
4	78	11	7	*A*	19	911	13	70	[a]
5	96	5	19	*A*	20	947	11	86	*B*
6	97	16	6	*A*	21	1079	7	154	*A*
7	191	19	10	*A*	22	1091	109	10	*A*
8	239	7	34	*A*	23	1103	29	38	*B*
9	251	25	10	*A*	24	1223	13	94	*A*
10	311	31	10	*A*	25	1247	89	14	*B*
11	323	23	14	*B*	26	1259	37	34	*A*
12	407	29	14	*B*	27	1271	127	10	*A*
13	419	11	38	*B*	28	1427	23	62	
14	431	43	10	*A*	29	1451	29	50	[b]
15	443	13	34	*A*	30	1787	19	94	*A*

[a] See No.3.

[b] See No. 1.

$63 \in D$. Most examples given in Tables I and II are of the form $n \equiv 11 \pmod{12}$. Except for the case $n = 1001$ in Table I, all the examples given in these tables are useful later in this paper. And since $1001 \in D$, if $D(1003) = 1001$ then $D(3003) = 3001$ follows. This fact will be useful in the next paper.

Among the four lemmas mentioned above, the construction of $\mathrm{LD}(2^r m)$ of Lemma 3 is particular useful, especially in the case m is an odd prime power q or is a product of two odd prime powers q and q'. On this account, we will give here a construction of $\mathrm{LD}[F_{2^r} \times F_q]$ and a construction of $\mathrm{LD}[F_{2^r} \times F_{q'} \times F_q]$, respectively. Let θ be a fixed primitive root of F_{2^r}, and e and e' be the multiplicative identities of F_q and $F_{q'}$, respectively. Choose $\gamma \in F_{2^r}^* \backslash \{\theta^0\}$, $\alpha \in F_q^* \backslash \{e\}$, and $\alpha' \in F_{q'}^* \backslash \{e'\}$. Let $B^* = ((x_0, z_0), (x_1, z_1), (x_2, z_2))$ and $B^{**} = ((x_0, y_0, z_0), (x_1, y_1, z_1), (x_2, y_2, z_2))$, where $x_0, x_1, x_2 \in F_{2^r}$, $y_0, y_1, y_2 \in F_{q'}$, and $z_0, z_1, z_2 \in F_q$. *Note* that the two symbols B^* and B^{**} will be used not only in this section, but also in subsequent sections. Suppose B' is a block B^* or B^{**}, we define an element $x_{B'} \in F_{2^r}$ corresponding to B' by

$$x_0 + x_1 + \gamma x_2 = \gamma x_{B'}.$$

Take three linear equations on $F_{q'}$:

$$y_0 - y_1 + y_2 = y, \tag{1}$$

$$-\alpha' y_0 + y_1 + y_2 = (e' - \alpha') y, \tag{2}$$

$$y_0 - \alpha' y_1 + y_2 = (e' - \alpha') y; \tag{3}$$

and three linear equations on F_q:

$$z_0 - z_1 + z_2 = z, \tag{4}$$

$$-\alpha z_0 + z_1 + z_2 = (e - \alpha) z, \tag{5}$$

$$z_0 - \alpha z_1 + z_2 = (e - \alpha) z. \tag{6}$$

Further let there be given an $\mathrm{LD}[F_q] = \{\mathscr{L}'_z | z \in F_q\} \cup \{\hat{\mathscr{L}}'^1, \hat{\mathscr{L}}'^2\}$ and an $\mathrm{LD}[F_{q'} \times F_q] = \{\mathscr{L}'_{yz} | y \in F_{q'}, z \in F_q\} \cup \{\hat{\mathscr{L}}''^1, \hat{\mathscr{L}}''^2\}$. We are going to construct an $\mathrm{LD}[F_{2^r} \times F_q] = \{\mathscr{L}^*_{xz} | x \in F_{2^r}, z \in F_q\} \cup \{\mathscr{L}^{*1}, \mathscr{L}^{*2}\}$ and an $\mathrm{LD}[F_{2^r} \times F_{q'} \times F_q] = \{\mathscr{L}^{**}_{xyz} | x \in F_{2^r}, y \in F_{q'}, z \in F_q\} \cup \{\mathscr{L}^{**1}, \mathscr{L}^{**2}\}$. They are specified as follows.

(1) $\mathrm{LD}[F_{2^r} \times F_q]$. Each $\mathscr{L}^*_{xz}$ consists of five parts, and each of $\mathscr{L}^{*1}$ and $\mathscr{L}^{*2}$ consists of two parts. The blocks of the form B^* which are contained in each part of $\mathscr{L}^*_{xz}$, and the blocks of the form $((x_0, z_0), (x_1, z_1), (x_2, z_2), (x_3, z_3))$ which are contained in each part of $\mathscr{L}^{*1}$ and $\mathscr{L}^{*2}$, are specified by the corresponding conditions which are as follows.

$\mathscr{L}^*_{xz}$

Part 1. Inequalities $x_0 \neq x \neq x_1$ and $(x_2, z_2) \neq (x, z)$, and Eqs. $x_{B^*} = x$ and (4) are all fulfilled. This gives $(2^r - 1)^2 q^2 - (2^r - 1) q$ blocks.

Part 2. Inequalities $x_1 \neq x \neq x_2$ and $z_0 \neq z$, and Eqs. $x_0 = x = x_{B^*}$ and (5) are all fulfilled. This gives $(2^r - 1) q(q - 1)$ blocks.

Part 3. Inequalites $x_0 \neq x \neq x_2$ and $z_1 \neq z$, and Eqs. $x_1 = x = x_{B^*}$ and (6) are all fulfilled. This gives $(2^r - 1) q(q - 1)$ blocks.

Part 4. Inequality $x_0 \neq x$ and Eqs. $x_0 = x_1, x_0 + \gamma x_2 = (\gamma + \theta^0) x$, $z_0 = z_1$ and $z_2 = z - z_0$ are all fulfilled. This gives $(2^r - 1) q$ blocks.

Part 5. Eqs. $x_0 = x_1 = x_2 = x$ are all fulfilled, and (z_0, z_1, z_2) is contained in $\mathscr{L}'_z$. This gives $(q - 1)^2$ blocks.

$\mathscr{L}^{*1}$

Part 1. Equations $(\gamma + \theta^0)\, x_0 + x_1 + \gamma x_2 = 0$, $x_0 + x_1 + x_3 = 0$, $-z_0 + z_1 + z_2 = 0$, and $z_3 = z_0 + z_1$, and inequality $x_0 \neq x_1$ are all fulfilled. This gives $2^r(2^r - 1) q^2$ blocks.

Part 2. Equations $x_0 = x_1 = x_2$ and $x_3 = 0$ are all fulfilled, and (z_0, z_1, z_2, z_3) is contained in $\hat{\mathscr{L}}'^1$. This gives $2^r q^2$ blocks.

$\mathscr{L}^{*2}$

Part 1. Equations $x_0 + (\gamma + \theta^0) x_1 + \gamma x_2 = 0$, $x_0 + x_1 + x_3 = 0$, $z_0 - z_1 + z_2 = 0$ and $z_3 = z_0 + z_1$, and inequality $x_0 \neq x_1$ are all fulfulled. This gives $2^r(2^r - 1) q^2$ blocks.

Part 2. Equations $x_0 = x_1 = x_2$ and $x_3 = 0$ are all fulfilled, and (z_0, z_1, z_2, z_3) is contained in $\hat{\mathscr{L}}'^2$. This gives $2^r q^2$ blocks.

(2) $\mathrm{LD}[F_{2^r} \times F_{q'} \times F_q]$. Each $\mathscr{L}^{**}_{xyz}$ consists of five parts, and each of $\mathscr{L}^{**1}$ and $\mathscr{L}^{**2}$ consists of two parts. The blocks of the form B^{**} which are contained in each part of $\mathscr{L}^{**}_{xyz}$, and the blocks of the form $((x_0, y_0, z_0), (x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3))$ which are contained in each part of $\mathscr{L}^{**1}$ and $\mathscr{L}^{**2}$, are specified by the corresponding conditions which are as follows.

$\mathscr{L}^{**}_{xyz}$

Part 1. Inequalities $x_0 \neq x \neq x_1$ and $(x_2, y_2, z_2) \neq (x, y, z)$, and Eqs. $x_{B^{**}} = x$, (1) and (4) are all fulfilled. This gives $(2^r - 1)^2\, q'^2 q^2 - (2^r - 1)\, q' q$ blocks.

Part 2. Inequalities $x_1 \neq x \neq x_2$ and $(y_0, z_0) \neq (y, z)$, and Eqs. $x_{B^{**}} = x = x_0$, (2) and (5) are all fulfilled. This gives $(2^r - 1) q' q(q' q - 1)$ blocks.

Part 3. Inequalities $x_0 \neq x \neq x_2$ and $(y_1, z_1) \neq (y, z)$, and Eqs. $x_{B^{**}} = x = x_1$, (3) and (6) are all fulfilled. This gives $(2^r - 1)\, q' q(q' q - 1)$ blocks.

Part 4. Inequality $x_0 \neq x$ and Eqs. $x_0 = x_1$, $x_0 + \gamma x_2 = (\gamma + \theta^0) x$,

$y_0 = y_1$, $y_2 = y - y_0$, $z_0 = z_1$ and $z_2 = z - z_0$ are all fulfilled. This gives $(2^r - 1)\, q'q$ blocks.

Part 5. Equation $x_0 = x_1 = x_2 = x$ are all fulfilled, and $((y_0, z_0), (y_1, z_1), (y_2, z_2))$ is contained in $\mathscr{L}'_{yz}$. This gives $(q'q - 1)^2$ blocks.

$\mathscr{L}^{**1}$

Part 1. Equations $(\gamma + \theta^0)\, x_0 + x_1 + \gamma x_2 = 0$, $x_0 + x_1 + x_3 = 0$, $-y_0 + y_1 + y_2 = 0$, $y_3 = y_0 + y_1$, $-z_0 + z_1 + z_2 = 0$ and $z_3 = z_0 + z_1$, and inequality $x_0 \neq x_1$ are all fulfilled. This gives $2^r(2^r - 1)\, q'^2 q^2$ blocks.

Part 2. Equations $x_0 = x_1 = x_2$ and $x_3 = 0$ are all fulfilled, and $((y_0, z_0), (y_1, z_1), (y_2, z_2), (y_3, z_3))$ is contained in $\hat{\mathscr{L}}''^{1}$. This gives $2^r q'^2 q^2$ blocks.

$\mathscr{L}^{**2}$

Part 1. Equations $x_0 + (\gamma + \theta^0)\, x_1 + \gamma x_2 = 0$, $x_0 + x_1 + x_3 = 0$, $y_0 - y_1 + y_2 = 0$, $y_3 = y_0 + y_1$, $z_0 - z_1 + z_2 = 0$, and $z_3 = z_0 + z_1$, and inequality $x_0 \neq x_1$ are all fulfilled. This gives $2^r(2^r - 1)\, q'^2 q^2$ blocks.

Part 2. Equations $x_0 = x_1 = x_2$ and $x_3 = 0$ are all fulfilled and $((y_0, z_0), (y_1, z_1), (y_2, z_2), (y_3, z_3))$ is contained in $\hat{\mathscr{L}}''^{2}$. This gives $2^r q'^2 q^2$ blocks.

It is not hard to check $\mathrm{LD}[F_{2^r} \times F_q]$ or $\mathrm{LD}[F_{2^r} \times F_{q'} \times F_q]$ given above satisfying conditions (C_1)–(C_5), where $r > 1$ and where q and q' are two odd prime powers under the assumption q or $q'q \in D$, respectively. We will omit its details here. The use of the constructions we have just given lies in the fact that they can be partly changed, and some new elements and some new sets of blocks can be added to them, so that new LDs of higher orders are obtained. And this is the stating point of constructing LDs which are required to prove Theorems 3 and 4.

3. C_{B^*} AND $C_{B^{**}}$

In this section, r is an integer greater than 2, q and q' are two odd prime powers greater than 5, θ is a fixed primitive root of F_{2^r}, and γ, α, and α' are three elements chosen as in the preceding section. Here we take $\gamma = \theta^4 + \theta^0$, and further, require α and α' to satisfy $-e \neq \alpha \neq 2e$ and $-e' \neq \alpha' \neq 2e'$ (obviously, which can be satisfied). In addition to these elements, choose β, $\delta \in F_q^*$ and $\beta' \in F_{q'}^*$ satisfying $\beta \notin \{e, -e, \alpha, -\alpha\}$, $0 \notin \{2\delta - e, 2\delta + e\}$, and $\beta' \notin \{e', -e', \alpha', -\alpha'\}$. Again, choose a set $Z \subset F_q^*$ satisfying: (i) $|Z| = (q-1)/2$, (ii) $z \in Z$ implies $-z \notin Z$, and (iii) $\delta - e, \delta, \delta + e \notin Z$. Set the integer $s = 2^{r-1}$. Choose a set K of integers satisfying (i) $K \subset \{-2^{r-1} + 1, -2^{r-1} + 2, \ldots, -1, 0, 1, \ldots, 2^{r-1} - 1\}$, (ii) $0, 2, -2, s, -s \notin K$, and (iii) $k \in K$ implies $-k \in K$. Then for each $k \in K$, choose a set $Y_k \subseteq F_{q'}^* \backslash \{e', -e'\}$ satisfying $Y_k = Y_{-k}$, and define $Y = \bigcup_{k \in K} (\{k\} \times Y_k)$.

For each $y \in F_{q'}$, let us define a linear form φ'_y on $F_{q'}$ by $\varphi'_y = y_0 - (e' + y) y_1 + y y_2$, where $y_0, y_1, y_2 \in F_{q'}$. We also define: $\psi'_0 = y_0 + (\alpha' - 2e') y_1 - \alpha' y_2$, $\psi'_1 = \alpha' y_0 - y_1 - \alpha' y_2$, $\psi'_2 = -(e' + \alpha') y_0 + y_1 + 2y_2$, and $\psi'_3 = y_0 - (e' + \alpha') y_1 + 2y_2$, where $y_0, y_1, y_2 \in F_{q'}$. Similarly, we define these linear forms on F_q: $\varphi_z = z_0 - (e + z) z_1 + z z_2$, $\psi_0 = z_0 + (\alpha - 2e) z_1 - \alpha z_2$, $\psi_1 = \alpha z_0 - z_1 - \alpha z_2$, $\psi_2 = -(e + \alpha) z_0 + z_1 + 2z_2$, and $\psi_3 = z_0 - (e + \alpha) z_1 + 2z_2$, where $z, z_0, z_1, z_2 \in F_q$.

Now we define a set $C_{B^*} \subseteq \{\infty\} \cup (K \times Z)$ for each B^* as follows (where ∞ is a new symbol).

(1) The element ∞ belongs to C_{B^*} if and only if conditions (C_6–C_8) are all satisfied:

(C_6) $x_{B^*} \notin \{x_0, x_1, x_2\}$.

(C_7) $\theta^s x_0 + \theta^{-s} x_1 = (\theta^s + \theta^{-s}) x_{B^*}$. (7)

(C_8) If (*) is satisfied, then $\varphi_\beta = 0$; and if (*) is not satisfied, then $\varphi_{-\alpha} = 0$.

(*) There exist two distinct k', $k'' \in K$ satisfying

$$\theta^{k'} x_0 + \theta^{-k'} x_1 = \theta^0 + (\theta^{k'} + \theta^{-k'}) x_{B^*}, \tag{8}$$

$$\theta^{k''} x_0 + \theta^{-k''} x_1 = \theta^0 + (\theta^{k''} + \theta^{-k''}) x_{B^*}. \tag{9}$$

(2) An element (k', z') ($k' \in K$, $z' \in Z$) belongs to C_{B^*} if and only if conditions (C_9)–(C_{12}) are all satisfied:

(C_9) Equation (8) holds.

(C_{10}) If $x_{B^*} \notin \{x_0, x_1, x_2\}$ and there exists $k'' \in K (k' \neq k'')$ satisfying (9), then $(\mathscr{L} + \varepsilon\beta)\, \varphi_{\varepsilon\alpha} = z'$ if (7) holds, and $\varphi_{\varepsilon\alpha} = z'$ if (7) does not hold, where ε is determined by the condition:

(**) $\varepsilon = e$ if $k' > k''$, and $\varepsilon = -e$ if $k' < k''$.

(C_{11}) If $x_{B^*} \notin \{x_0, x_1, x_2\}$, and there exists no $k'' \in K (k' \neq k'')$ satisfying (9), then $\varphi_{z' - \delta} = z'^2$ if

$$\theta^s x_0 + \theta^{-s} x_1 = \theta^0 + (\theta^s + \theta^{-s}) x_{B^*}, \tag{10}$$

and $\varphi_\alpha = z'$ if (10) does not hold.

(C_{12}) If $x_0 = x_{B^*}$ then $\psi_2 = z'$, if $x_1 = x_{B^*}$ then $\psi_3 = z'$, and if $x_2 = x_{B^*}$ then $\psi_0 = z'$ when $k' > 0$ and $\psi_1 = z'$ when $k' < 0$.

Let $<_{q'}$ be a fixed linear ordering on $F_{q'}$. We define a set $C_{B^{**}} \subseteq \{\infty\} \cup (Y \times Z)$ for each B^{**} as follows.

(1) The element ∞ belongs to $C_{B^{**}}$ if and only if conditions (C_{13})–(C_{15}) are all satisfied:

(C_{13}) $x_{B^{**}} \notin \{x_0, x_1, x_2\}$.

(C_{14}) $\theta^s x_0 + \theta^{-s} x_1 = (\theta^s + \theta^{-s}) x_{B^{**}}$. (11)

(C_{15}) If (*′) is satisfied, then $\varphi'_{\beta'} = 0$ and $\varphi_\beta = 0$, and if (*′) is not satisfied, then $\varphi'_{-\alpha'} = 0$ and $\varphi_{-\alpha} = 0$.

(*′) There exist two distinct $k', k'' \in K$ satisfying Eqs. (12) and (13).

$$\theta^{k'} x_0 + \theta^{-k'} x_1 = \theta^0 + (\theta^{k'} + \theta^{-k'}) x_{B^{**}}, \tag{12}$$

$$\theta^{k''} x_0 + \theta^{-k''} x_1 = \theta^0 + (\theta^{k''} + \theta^{-k''}) x_{B^{**}}. \tag{13}$$

(2) An element $(k', y', z')(k' \in K, y' \in Y_{k'}, z' \in Z)$ belongs to $C_{B^{**}}$ if and only if conditions (C_{16})–(C_{19}) are all satisfied:

(C_{16}) Equation (12) holds.

(C_{17}) If $x_{B^{**}} \notin \{x_0, x_1, x_2\}$ and there exists $k'' \in K (k' \neq k'')$ satisfying (13), then $\varphi'_{\varepsilon'\alpha'} = y'$ and $(\alpha + \varepsilon\beta)\varphi_{\varepsilon\alpha} = z'$ if (11) holds, and $\varphi'_{\varepsilon'\alpha'} = y'$ and $\varphi_{\varepsilon\alpha} = z'$ if (11) does not hold, where ε is determined by (**) and ε' is determined by (**′).

(**′) $\varepsilon' = e'$ if $k' > k''$, and $\varepsilon' = -e'$ if $k' < k''$.

(C_{18}) Consider the case where $x_{B^{**}} \notin \{x_0, x_1, x_2\}$, and where there exists no $k'' \in K (k'' \neq k')$ satisfying (13). If

$$\theta^s x_0 + \theta^{-s} x_1 = \theta^0 + (\theta^s + \theta^{-s}) x_{B^{**}}, \tag{14}$$

then $\varphi'_{y'} = y'^2$, moreover,

(i) $\varphi_{\varepsilon\alpha} = z'$ if there exists $y'' \in Y_{k'} (y'' \neq y')$ satisfying $\varphi'_{y''} = y''^2$, where $\varepsilon = e$ if $y' >_{q'} y''$ and $\varepsilon = -e$ if $y' <_{q'} y''$;

(ii) $\varphi_{z'-\delta} = z'^2$ if $y' = -y_1 + y_2$; and

(iii) $\varphi_\alpha = z'$ if $y' \neq -y_1 + y_2$ and there exists no $y'' \in Y_{k'}$ satisfying $y' \neq y''$ and $\varphi'_{y''} = y''^2$.

And if (14) does not hold, then $\varphi'_{\alpha'} = y'$ and $\varphi_\alpha = z'$.

(C_{19}) If $x_0 = x_{B^{**}}$ then $\psi'_2 = y'$ and $\psi_2 = z'$; if $x_1 = x_{B^{**}}$ then $\psi'_3 = y'$ and $\psi_3 = z'$; and if $x_2 = x_{B^{**}}$ then $\psi'_0 = y'$ and $\psi_0 = z'$ when $k' > 0$, and $\psi'_1 = y'$ and $\psi_1 = z'$ when $k' < 0$.

PROPOSITION. *For any B^* and B^{**}, each of $|C_{B^*}|$ and $|C_{B^{**}}|$ is less than* 3.

Proof. We only prove the case of $C_{B^{**}}$, the other case is similar to it. Suppose that $|C_{B^{**}}| > 2$. Consider the two cases separately: $\infty \in C_{B^{**}}$ and $\infty \notin C_{B^{**}}$.

Case 1. Suppose $\{\infty, (k', y', z'), (k'', y'', z'')\} \subseteq C_{B^{**}}$, where $k' \geqslant k''$ and $(k', y', z') \neq (k'', y'', z'')$. By ($C_{13}$), ($C_{14}$) and ($C_{16}$), this implies

$x_{B^{**}} \notin \{x_0, x_1, x_2\}$ and all the Eqs. (11), (12), and (13) hold. Then we distinguish the two subcases: (i) $k' > k''$ and (ii) $k' = k''$.

(i) $k' > k''$. By (C_{15}) and (C_{17}) we find $\varphi_\beta = 0$, $(\alpha+\beta)\,\varphi_\alpha = z'$ and $(\alpha-\beta)\,\varphi_{-\alpha} = z''$. Since $(\alpha+\beta)\,\varphi_\alpha + (\alpha-\beta)\,\varphi_{-\alpha} = 2\alpha\varphi_\beta$, we have $z' + z'' = 0$, but this contradicts the fact that z' and $z'' \in Z$. Hence we conclude that this subcase cannot happen.

(ii) $k' = k''$. If the presupposition of (C_{17}) were fulfilled, then we should have $\varphi'_{\varepsilon'\alpha'} = y' = y''$ and $(\alpha + \varepsilon\beta)\,\varphi_{\varepsilon\alpha} = z' = z''$, which contradicts the assumption $(k', y', z') \neq (k'', y'', z'')$. Also, if the presupposition of (C_{18}) were fulfilled, since Eq. (14) obviously cannot hold, we should have $\varphi'_{\alpha'} = y' = y''$ and $\varphi_\alpha = z' = z''$, which leads to the same contradiction. Hence this subcase cannot happen as well.

Case 2. Suppose $\infty \notin C_{B^{**}}$, $\{(k, y, z), (k', y', z'), (k'', y'', z'')\} \subseteq C_{B^{**}}$ and $(k, y, z) \neq (k', y', z') \neq (k'', y'', z'') \neq (k, y, z)$. Both (12) and (13) hold by (C_{16}). Letting $x = \theta^{k'}$, we see that Eq. (12) is equivalent to the equation $(x_0 + x_{B^{**}})\,x^2 + x + (x_1 + x_{B^{**}}) = 0$, which is a quadratic equation or a linear equation in x. It follows that at least two of k, k', and k'' are equal (note (C_{16})). We assume $k = k'$. By the condition (C_{19}), we can see $x_{B^{**}} \notin \{x_0, x_1, x_2\}$. For instance, if $x_2 = x_{B^{**}}$, by (C_{19}) we should have $\psi'_i = y' = y$ and $\psi_i = z' = z$ ($i = 0$ or 1), but this contradicts the assumption $(k', y', z') \neq (k, y, z)$. Then we distinguish the two subcases: (i) $k' \neq k''$ and (ii) $k' = k''$.

(i) $k' \neq k''$. By (C_{17}) equations $\varphi'_{\varepsilon'\alpha'} = y' = y$, and $(\alpha + \varepsilon\beta)\,\varphi_{\varepsilon\alpha} = z' = z$ or $\varphi_{\varepsilon\alpha} = z = z'$ would be fulfilled ($\varepsilon = e$ or $-e$, $\varepsilon' = e'$ or $-e'$); but this leads to the same contradiction obtained above.

(ii) $k = k' = k''$. It deserves to be considered here only when the presupposition of (C_{18}) is fulfilled, which can easily be seen from the above discussion in (i). If Eq. (14) were not fulfilled, then by (C_{18}) equations $\varphi'_{\alpha'} = y = y' = y''$ and $\varphi_\alpha = z = z' = z''$ would hold, which leads to the same contradiction obtained above. Contrary, if the Eq. (14) were fulfilled, then by (C_{18}) all the Eqs. $\varphi'_{y'} = y'^2$, $\varphi'_{y''} = y''^2$, and $\varphi'_y = y^2$ would hold. Since $\varphi'_y = y^2$ is a quadratic equation in y, at least two of y, y', and y'' are equal. We may assume $y = y'$. If $y' \neq y''$, by (i) of (C_{18}) we should have $\varphi_{\varepsilon\alpha} = z' = z$ ($\varepsilon = e$ or $-e$), which yields the same contradiction. Then, what remains and deserves to be considered is only the subcase where $y = y' = y''$, and where the presupposition of (ii) or (iii) of (C_{18}) is fulfilled. If the presupposition of (ii) of (C_{18}) were fulfilled, all the equations $\varphi_{z-\delta} = z^2$, $\varphi_{z'-\delta} = z'^2$, and $\varphi_{z''-\delta} = z''^2$ would hold. Since $\varphi_{z-\delta} = z^2$ is a quadratic equation in z, at least two of z, z', and z'' are equal, and this yields a contradiction. Obviously, if the presupposition of (iii) of (C_{18}) were fulfilled, we should find a contradiction as well. We see that $|C_{B^{**}}| > 2$ cannot happen, and the proof is completed.

4. Construction of Theorem 3

In this section, we shall make some change in the construction of $\mathrm{LD}[F_{2^r} \times F_q]$ given in Section 2, adding $1+(q-1)t$ elements and $1+(q-1)t$ sets of blocks, so that a construction of $\mathrm{LD}(1+(q-1)t+2^r q)$ will be obtained, where q is an odd prime power greater than 5, and where both r and t are nonnegative integers with $r>2$ and $t \leqslant 2^{r-1}-3$. This is based on the work of the preceding section, but here we should take $|K|=2t$. Let there be given an $\mathrm{LD}[\{\infty\} \cup F_q] = \{\mathscr{L}_z \mid z \in F_q\} \cup \{\mathscr{L}'_\infty, \mathscr{L}'^1, \mathscr{L}'^2\}$ and an $\mathrm{LD}[\{\infty\} \cup (K \times Z)] = \{\mathscr{L}'_{k'z'} \mid k' \in K,\ z' \in Z\} \cup \{\mathscr{L}''_\infty, \mathscr{L}''^1, \mathscr{L}''^2\}$, and with the notation provision only, the condition (C_4) about $\mathscr{L}'^1$, $\mathscr{L}'^2$, $\mathscr{L}''^1$, and $\mathscr{L}''^2$ is fulfilled with $c_0=\infty$. Setting $X=\{\infty\} \cup (K \times Z) \cup (F_{2^r} \times F_q)$, $|X|=1+(q-1)t+2^r q$, we are going to construct an $\mathrm{LD}[X] = \{\mathscr{L}_{xz} \mid x \in F_{2^r},\ z \in F_q\} \cup \{\mathscr{L}_{k'z'} \mid k' \in K,\ z' \in Z\} \cup \{\mathscr{L}_\infty, \mathscr{L}^1, \mathscr{L}^2\}$.

Let C be a subset of $\{\infty\} \cup (K \times Z)$ with $|C| \leqslant 2$. For each block B^*, we define a set of blocks $\langle B^* - C \rangle$ as follows:

(i) if $C=\varnothing$, then $\langle B^* - C\rangle = \{B^*\}$;

(ii) if $|C|=1$ and $C=\{w\}$, then $\langle B^* - C \rangle = \{((X_0, z_0), (x_1, z_1), w), ((x_0, z_0), w, (x_2, z_2)), (w, (x_1, z_1), (x_2, z_2))\}$;

(iii) if $|C|=2$ and $C=\{w, w'\}$, then $\langle B^* - C\rangle = \{B^*, ((x_0, z_0), w, w'), ((x_0, z_0), w', w), (w, (x_1, z_1), w'), (w', (x_1, z_1), w), (w, w', (x_2, z_2)), (w', w, (x_2, z_2))\}$. So, if $C=\varnothing$ then $\langle B^* - C\rangle$ is B^* itself, if $|C|=1$ then $\langle B^* - C \rangle$ is a set of three ordered triples, and if $|C|=2$ then $\langle B^* - C\rangle$ is a set of seven ordered triples.

We now write the construction of $\mathrm{LD}[X]$. Each $\mathscr{L}_{xz}$ consists of four parts, each $\mathscr{L}_{k'z'}$ consists of two parts, $\mathscr{L}_\infty$ consists of three parts, and each of $\mathscr{L}^1$ and $\mathscr{L}^2$ consists of eight parts. These parts are specified as follows.

$\mathscr{L}_{xz}(x \in F_{2^r}, z \in F_q)$

Part 1. A block B is contained in this part if and only if there is a block B^* in Parts 1–3 of $\mathscr{L}^*_{xz}$ (see Section 2) such that $B \in \langle B^* - C_{B^*}\rangle$.

Part 2. This is the same part as Part 4 of $\mathscr{L}^*_{xz}$.

Part 3. A block B is contained in this part if and only if $B=((x, z_0), (x, z_1), (x, z_2))$, $z_0, z_1, z_2 \in \{\infty\} \cup F_q$ (whenever for z_0, z_1 or z_2 appears ∞, omit the first coordinate x), and $(z_0, z_1, z_2) \in \mathscr{L}_z$.

Part 4. This part consists of all the blocks of the following forms ($k \in K$, $z' \in F_q$): $((k, (a-e)z'-az), (x', z'), (-k, (a-e)z'-az))$ and $((x', z'), (k, (a-e)z'-az), (-k, (a-e)z'-az))$, where $x'=(\theta^k+\theta^{-k})^{-1}+x$ and $(a-e)z'-az \in Z$; $((k, -az+z'), (k, -az+z'), (x+\gamma^{-1}\theta^{\varepsilon k}, z'))$, $((k, -az+z'), (-k, -az+z'), (x+\gamma^{-1}\theta^{-\varepsilon k}, z'))$, $((k, -az+z'), (x+\theta^k,$

$z - z'), (k, -az + z'))$ and $((x + \theta^{-k}, z - z'), (k, -az + z'), (k, -az + z'))$, where $-az + z' \in Z$, $\varepsilon = 1$ if $k > 0$, and $\varepsilon = -1$ if $k < 0$.

$\mathscr{L}_\infty$

Part 1. A block B is contained in this part if and only if there is B^* such that $\infty \in C_{B^*}$ and $B \in \langle B^* - C_{B^*} \backslash \{\infty\} \rangle$.

Part 2. This is the same set of blocks as $\mathscr{L}''_\infty$.

Part 3. A block B is contained in this part if and only if $B = ((x, z_0), (x, z_1), (x, z_2))$, $x \in F_2r$ and $(z_0, z_1, z_2) \in \mathscr{L}'_\infty$.

$\mathscr{L}_{k'z'}(k' \in K, z' \in Z)$

Part 1. A block B is contained in this part if and only if there is B^* such that $(k', z') \in C_{B^*}$ and $B \in \langle B^* - C_{B^*} \backslash \{(k', z')\} \rangle$.

Part 2. This is the same set of blocks as $\mathscr{L}'_{k'z'}$.

Each form of the blocks which are contained in each corresponding part of $\mathscr{L}^1$ and $\mathscr{L}^2$, are specified as follows, where k' runs over $\{-2^{r-1} + 1, -2^{r-1} + 2, \ldots, -1, 0, 1, \ldots, 2^{r-1} - 1\} \backslash K$, and where k, x_0, x_1, z_0, z_1, and z run over $K, F_{2^r}, F_{2^r}, F_q, F_q$, and Z, respectively.

$\mathscr{L}^1$

Part 1. $((x_0, z_0), (x_0 + \theta^{k'}, z_1), (x_0 + \gamma^{-1}\theta^{k'}, z_0 - z_1), (x_0 + \gamma\theta^{k'}, z_0 + z_1))$ (this gives $2^r(2^r - 1 - 2t)q^2$ blocks).

Part 2. $((x_0, z_0), (x_0 + \theta^k, (e - \alpha)z_0), (x_0 + \gamma^{-1}\theta^k, az_0), (x_0 + \gamma\theta^k, \alpha(a - e)z_0))$ (this gives $2^{r+1}tq$ blocks).

Part 3. $((k, z), (x_0 + \theta^k, (e - \alpha)z_0 - z), (x_0 + \gamma^{-1}\theta^k, az_0 + z), (x_0 + \gamma\theta^k, \alpha(a - e)z + (2a - e)z))$ (this gives $2^r tq(q - 1)$ blocks).

Part 4. $((x_0, z_0), (k, z), (x_0 + \gamma^{-1}\theta^k, az_0 + z), (x_0 + \gamma\theta^k, \alpha(a - e)z_0 - z))$ (this gives $2^r tq(q - 1)$ blocks).

Part 5. $((x_0, z_0), (x_0 + \theta^k, (e - \alpha)z_0 - z), (k, z), (x_0 + \gamma\theta^k, \alpha(a - e)z_0 + z))$ (this gives $2^r tq(q - 1)$ blocks).

Part 6. $((x_0, z_0), (x_0 + \theta^k, (e - \alpha)z_0 + z), (x_0 + \gamma^{-1}\theta^k, az_0 - z), (k, z))$ (this gives $2^r tq(q - 1)$ blocks).

Part 7. This part contains every ordered quadruple $((x_0, z'_0), (x_0, z'_1), (x_0, z'_2), (x_0, z'_3))$ such that $x_0 \in F_{2^r}, z'_0, z'_1, z'_2, z'_3 \in \{\infty\} \cup F_q$ (whenever for z'_0, z'_1, z'_2 or z'_3 appears ∞, omit the first coordinate x_0), and $(z'_0, z'_1, z'_2, z'_3) \in \mathscr{L}'^1$; but the block $(\infty, \infty, \infty, \infty)$ is not included (cf. (C_4) and the beginning of this section). This gives $2^r q(q + 2)$ blocks.

Part 8. This is the same set of blocks as $\mathscr{L}''^1$, which consists of $(1 + (q - 1)t)^2$ blocks.

$\mathscr{L}^2$

Part 1. $((x_1 + \theta^{-k'}, z_0), (x_1, z_1), (x_1 + \gamma^{-1}\theta^{-k'}, z_1 - z_0), (x_1 + \gamma\theta^{-k'}, z_0 + z_1))$ (this gives $2^r(2^r - 1 - 2t)q^2$ blocks).

Part 2. $((x_1+\theta^{-k},\ (e-\alpha)z_1),\ (x_1,z_1),\ (x_1+\gamma^{-1}\theta^{-k},\ \alpha z_1),\ (x_1+\gamma\theta^{-k},\ \alpha(\alpha-e)z_1))$ (this gives $2^{r+1}tq$ blocks).

Part 3. $((x_1+\theta^{-k},\ (e-\alpha)z_1-z),\ (k,z),\ (x_1+\gamma^{-1}\theta^{-k},\ \alpha z_1+z),\ (x_1+\gamma\theta^{-k},\ \alpha(\alpha-e)z_1+(2\alpha-e)z))$ (this gives $2^rtq(q-1)$ blocks).

Part 4. $((k,z),\ (x_1,z_1),\ (x_1+\gamma^{-1}\theta^{-k},\alpha z_1+z),\ (x_1+\gamma\theta^{-k},\ \alpha(\alpha-e)z_1-z))$ (this gives $2^rtq(q-1)$ blocks).

Part 5. $((x_1+\theta^{-k},\ (e-\alpha)z_1-z),\ (x_1,\ z_1),\ (k,z),\ (x_1+\gamma\theta^{-k},\ \alpha(\alpha-e)z_1+z))$ (this gives $2^rtq(q-1)$ blocks).

Part 6. $((x_1+\theta^{-k},\ (e-\alpha)z_1+z),(x_1,z_1),\ (x_1+\gamma^{-1}\theta^{-k},\ \alpha z_1-z),\ (k,z))$ (this gives $2^rtq(q-1)$ blocks).

Part 7. This part contains every ordered quadruple $((x_1,z_0'),\ (x_1,z_1'),\ (x_1,z_2'),\ (x_1,z_3'))$ such that $x_1\in F_{2^r},\ z_0',z_1',z_2',z_3'\in\{\infty\}\cup F_q$ (whenever for $z_0',\ z_1',\ z_2'$ or z_3' appears ∞, omit the first coordinate x_1), and $(z_0',\ z_1',\ z_2',\ z_3')\in\mathscr{L}'^2$; but the block $(\infty,\ \infty,\ \infty,\ \infty)$ is not included. This gives $2^rq(q+2)$ blocks.

Part 8. This is the same set of blocks as $\mathscr{L}''^2$, which consists of $(1+(q-1)t)^2$ blocks.

In contriving the constructions of $\mathscr{L}^1$ and $\mathscr{L}^2$, we were inspired by the method of sum composition of constructing pairwise orthogonal Latin squares, which is stated in [1].

5. Construction of Theorem 4

The construction of Theorem 4 is similar to that of Theorem 3. We need the $\mathrm{LD}[F_{2^r}\times F_{q'}\times F_q]=\{\mathscr{L}^{**}_{xyz}\,|\,x\in F_{2^r},y\in F_{q'},\ z\in F_q\}\cup\{\mathscr{L}^{**1},\ \mathscr{L}^{**2}\}$ given in Section 2 (where q and q' are two odd prime powers >5, and where r is a nonnegative integer >2), and the result given in Section 3, but here we take $|Y|=2t$ (where t is a nonnegative integer $\leqslant(2^{r-1}-3)(q'-3)$). Let there be given an $\mathrm{LD}[\{\infty\}\cup(F_{q'}\times F_q)]=\{\mathscr{L}_{yz}\,|\,y\in F_{q'},z\in F_q\}\cup\{\mathscr{L}'_\infty,\ \mathscr{L}'^1,\ \mathscr{L}'^2\}$ and an $\mathrm{LD}[\{\infty\}\cup(Y\times Z)]=\{\mathscr{L}'_{k'y'z'}\,|\,k'\in K,\ \ y'\in Y_{k'},\ z'\in Z\}\cup\{\mathscr{L}''_\infty,\ \mathscr{L}''^1,\ \mathscr{L}''^2\}$, and with the notation provision only, the condition (C_4) about $\mathscr{L}'^1,\ \mathscr{L}'^2,\ \mathscr{L}''^1$, and $\mathscr{L}''^2$ is fulfilled with $c_0=\infty$. Setting $X=\{\infty\}\cup(Y\times Z)\cup(F_{2^r}\times F_{q'}\times F_q)$, $|X|=1+(q-1)t+2^rq'q$, we are going to construct an $\mathrm{LD}[X]=\{\mathscr{L}_{xyz}\,|\,x\in F_{2^r},y\in F_{q'},\ z\in F_q\}\cup\{\mathscr{L}_{k'y'z'}\,|\,k'\in K,y'\in Y_{k'},\ z'\in Z\}\cup\{\mathscr{L}_\infty,\ \mathscr{L}^1,\ \mathscr{L}^2\}$.

Let C be a subset of $\{\infty\}\cup(Y\times Z)$ with $|C|\leqslant 2$. For each block B^{**}, we define a set of blocks $\langle B^{**}-C\rangle$ as follows:

(i) if $C=\varnothing$, then $\langle B^{**}-C\rangle=\{B^{**}\}$;

(ii) if $|C|=1$ and $C=\{w\}$, then $\langle B^{**}-C\rangle=\{((x_0,y_0,z_0),\ (x_1,y_1,z_1),w),\ ((x_0,y_0,z_0),\ w,\ (x_2,\ y_2,\ z_2)),\ (w,\ (x_1,y_1,z_1),\ (x_2,\ y_2,\ z_2))\}$;

(iii) if $|C|=2$ and $C=\{w,\ w'\}$, then $\langle B^{**}-C\rangle=\{B^{**},\ ((x_0,y_0,z_0),$

$w, w'), ((x_0, y_0, z_0), w', w), (w, (x_1, y_1, z_1), w'), (w', (x_1, y_1, z_1), w), (w, w', (x_2, y_2, z_2)), (w', w, (x_2, y_2, z_2))\}$.

We now write the construction of LD$[X]$. Each $\mathscr{L}_{xyz}$ consists of four parts, each $\mathscr{L}_{k'y'z'}$ consists of two parts, $\mathscr{L}_\infty$ consists of three parts, and each of $\mathscr{L}^1$ and $\mathscr{L}^2$ consists of eight parts. These parts are specified as follows.

$\mathscr{L}_{xyz}(x \in F_{2^r}, y \in F_{q'}, z \in F_q)$

Part 1. A block B is contained in this part if and only if there is a block B^{**} in Parts 1–3 of $\mathscr{L}^{**}_{xyz}$ such that $B \in \langle B^{**} - C_{B^{**}} \rangle$.

Part 2. This is the same part as Part 4 of $\mathscr{L}^{**}_{xyz}$.

Part 3. A block B is contained in this part if and only if $B = ((x, v_0), (x, v_1), (x, v_2))$, $v_0, v_1, v_2 \in \{\infty\} \cup (F_{q'} \times F_q)$(whenever for v_0, v_1 or v_2 appears ∞, omit the first coordinate x), and $(v_0, v_1, v_2) \in \mathscr{L}_{yz}$.

Part 4. This part consists of all the blocks of the following forms ($k \in K$, $y' \in F_{q'}$, $z' \in F_q$): $((k, (\alpha' - e')\, y' - \alpha' y, (\alpha - e)\, z' - \alpha z), (x', y', z'), (-k, (\alpha' - e')\, y' - \alpha' y, (\alpha - e)\, z' - \alpha z))$ and $((x', y', z'), (k, (\alpha' - e')\, y' - \alpha' y, (\alpha - e)\, z' - \alpha z), (-k, (\alpha' - e')\, y' - \alpha' y, (\alpha - e)\, z' - \alpha z))$, where $x' = (\theta^k + \theta^{-k})^{-1} + x$, $(\alpha' - e')\, y' - \alpha' y \in Y_k$, and $(\alpha - e)\, z' - \alpha z \in Z$; $((k, -\alpha' y + y', -\alpha z + z'), (k, -\alpha' y + y', -\alpha z + z'), (x + \gamma^{-1}\theta^{\varepsilon k}, y', z'))$, $((k, -\alpha' y + y', -\alpha z + z'), (-k, -\alpha' y + y', \alpha z + z'), (x + \gamma^{-1}\theta^{-\varepsilon k}, y', z'))$, $((k, -\alpha' y + y', -\alpha z + z'), (x + \theta^k, y - y', z - z'), (k, -\alpha' y + y', -\alpha z + z'))$, and $((x + \theta^{-k}, y - y', z - z'), (k, -\alpha' + y + y', -\alpha z + z'), (k, -\alpha' y + y', -\alpha z + z'))$, where $-\alpha' y + y' \in Y_k$, $-\alpha z + z' \in Z$, $\varepsilon = 1$ if $k > 0$, and $\varepsilon = -1$ if $k < 0$.

$\mathscr{L}_\infty$

Part 1. A block B is contained in this part if and only if there is B^{**} such that $\infty \in C_{B^{**}}$ and $B \in \langle B^{**} - C_{B^{**}} \backslash \{\infty\} \rangle$.

Part 2. This is the same set of blocks as $\mathscr{L}''_\infty$.

Part 3. A block B is contained in this part if and only if $B = ((x, y_0, z_0), (x, y_1, z_1), (x, y_2, z_2))$, $x \in F_{2^r}$, and $((y_0, z_0), (y_1, z_1), (y_2, z_2)) \in \mathscr{L}'_\infty$.

$\mathscr{L}_{k'y'z'}(k' \in K, y' \in Y_{k'}, z' \in Z)$

Part 1. A block B is contained in this part if and only if there is B^{**} such that $(k', y', z') \in C_{B^{**}}$ and $B \in \langle B^{**} - C_{B^{**}} \backslash \{(k', y', z')\} \rangle$.

Part 2. This is the same set of blocks as $\mathscr{L}'_{k'y'z'}$.

Each form of the blocks which are contained in each corresponding part of $\mathscr{L}^1$ and $\mathscr{L}^2$, are specified as follows, where $k, x_0, x_1, y_0, y_1, z_0, z_1, y$, and z run over $K, F_{2^r}, F_{2^r}, F_{q'}, F_{q'}, F_q, F_q, Y_k$, and Z, respectively.

$\mathscr{L}^1$

Part 1. $((x_0, y_0, z_0), (x_0 + \theta^{k'}, (e' - \alpha')\, y_0 - y', z_1), (x_0 + \gamma^{-1}\theta^{k'},$

$\alpha' y_0 + y'$, $z_0 - z_1$), $(x_0 + \gamma\theta^{k'}$, $(2e' - \alpha') y_0 - y'$, $z_0 + z_1$)) with $k' \in \{-2^{r-1} + 1, -2^{r-1} + 2, \ldots, -1, 0, 1, \ldots, 2^{r-1} - 1\} \backslash K$ and $y' \in F_{q'}$, or $k' \in K$ and $y' \notin Y_{k'}$ (this gives $2^r((2^r - 1) q' - 2t) q' q^2$ blocks).

Part 2. $((x_0, y_0, z_0), (x_0 + \theta^k, (e' - \alpha') y_0 - y, (e - \alpha) z_0), (x_0 + \gamma^{-1}\theta^k, \alpha' y_0 + y, \alpha z_0), (x_0 + \gamma\theta^k, (2e' - \alpha') y_0 - y, \alpha(\alpha - e) z_0))$, (this gives $2^{r+1} t q' q$ blocks).

Part 3. $((k, y, z), (x_0 + \theta^k, (e' - \alpha') y_0 - y, (e - \alpha) z_0 - z), (x_0 + \gamma^{-1}\theta^k, \alpha' y_0 + y, \alpha z_0 + z), (x_0 + \gamma\theta^k, (2e' - \alpha') y_0 - y, \alpha(\alpha - e) z_0 + (2\alpha - e) z))$ (this gives $2^r t q' q(q - 1)$ blocks).

Part 4. $((x_0, y_0, z_0), (k, y, z), (x_0 + \gamma^{-1}\theta^k, \alpha' y_0 + y, \alpha z_0 + z), (x_0 + \gamma\theta^k, (2e' - \alpha') y_0 - y, \alpha(\alpha - e) z_0 - z))$ (this gives $2^r t q' q(q - 1)$ blocks).

Part 5. $((x_0, y_0, z_0), (x_0 + \theta^k, (e' - \alpha') y_0 - y, (e - \alpha) z_0 - z), (k, y, z), (x_0 + \gamma\theta^k, (2e' - \alpha') y_0 - y, \alpha(\alpha - e) z_0 + z))$ (this gives $2^r t q' q(q - 1)$ blocks).

Part 6. $((x_0, y_0, z_0), (x_0 + \theta^k, (e' - \alpha') y_0 - y, (e - \alpha) z_0 + z), (x_0 + \gamma^{-1}\theta^k, \alpha' y_0 + y, \alpha z_0 - z), (k, y, z))$ (this gives $2^r t q' q(q - 1)$ blocks).

Part 7. This part contains every ordered quadruple $((x_0, v_0), (x_0, v_1), (x_0, v_2), (x_0, v_3))$ such that $x_0 \in F_{2^r}$, $v_0, v_1, v_2, v_3 \in \{\infty\} \cup (F_{q'} \times F_q)$ (whenever for v_0, v_1, v_2 or v_3 appears ∞, omit the first coordinate x_0), and $(v_0, v_1, v_2, v_3) \in \mathscr{L}'^1$, but the block $(\infty, \infty, \infty, \infty)$ is not included. This gives $2^r q' q(q' q + 2)$ blocks.

Part 8. This is the same set of blocks as $\mathscr{L}''^1$, which consists of $(1 + (q - 1) t)^2$ blocks.

$\mathscr{L}^2$

Part 1. $((x_1 + \theta^{-k'}, (e' - \alpha') y_1 - y', z_0), (x_1, y_1, z_1), (x_1 + \gamma^{-1}\theta^{-k'}, \alpha' y_1 + y', z_1 - z_0), (x_1 + \gamma\theta^{-k'}, (2e' - \alpha') y_1 - y', z_0 + z_1))$ with $k' \in \{-2^{r-1} + 1, -2^{r-1} + 2, \ldots, -1, 0, 1, \ldots, 2^{r-1} - 1\} \backslash K$ and $y' \in F_{q'}$, or $k' \in K$ and $y' \notin Y_k'$ (this gives $2^r((2^r - 1) q' - 2t) q' q^2$ blocks).

Part 2. $((x_1 + \theta^{-k}, (e' - \alpha') y_1 - y, (e - \alpha) z_1), (x_1, y_1, z_1), (x_1 + \gamma^{-1}\theta^{-k}, \alpha' y_1 + y, \alpha z_1), (x_1 + \gamma\theta^{-k}, (2e' - \alpha') y_1 - y, \alpha(\alpha - e) z_1))$ (this gives $2^{r+1} t q' q$ blocks).

Part 3. $((x_1 + \theta^{-k}, (e' - \alpha') y_1 - y, (e - \alpha) z_1 - z), (k, y, z), (x_1 + \gamma^{-1}\theta^{-k}, \alpha' y_1 + y, \alpha z_1 + z), (x_1 + \gamma\theta^{-k}, (2e' - \alpha') y_1 - y, \alpha(\alpha - e) z_1 + (2\alpha - e) z))$ (this gives $2^r t q' q(q - 1)$ blocks).

Part 4. $((k, y, z), (x_1, y_1, z_1), (x_1 + \gamma^{-1}\theta^{-k}, \alpha' y_1 + y, \alpha z_1 + z), (x_1 + \gamma\theta^{-k}, (2e' - \alpha') y_1 - y, \alpha(\alpha - e) z_1 - z))$ (this gives $2^r t q' q(q - 1)$ blocks).

Part 5. $((x_1 + \theta^{-k}, (e' - \alpha') y_1 - y, (e - \alpha) z_1 - z), (x_1, y_1, z_1), (k, y, z), (x_1 + \gamma\theta^{-k}, (2e' - \alpha') y_1 - y, \alpha(\alpha - e) z_1 + z))$ (this gives $2^r t q' q(q - 1)$ blocks).

Part 6. $((x_1 + \theta^{-k}, (e' - \alpha') y_1 - y, (e - \alpha) z_1 + z), (x_1, y_1, z_1), (x_1 + \gamma^{-1}\theta^{-k}, \alpha' y_1 + y, \alpha z_1 - z), (k, y, z))$ (this gives $2^r t q' q(q - 1)$ blocks).

Part 7. This part contains every ordered quadruple $((x_1, v_0), (x_1, v_1), (x_1, v_2), (x_1, v_3))$ such that $x_1 \in F_{2^r}$, $v_0, v_1, v_2, v_3 \in \{\infty\} \cup (F_{q'} \times F_q)$ (whenever for v_0, v_1, v_2, or v_3 appears ∞, omit the first coordinate x_1), and $(v_0, v_1, v_2, v_3) \in \mathscr{L}'^2$, but the block $(\infty, \infty, \infty, \infty)$ is not included. This gives $2^r q'q(q'q+2)$ blocks.

Part 8. This is the same set of blocks as $\mathscr{L}''^2$, which consists of $(1+(q-1)t)^2$ blocks.

6. Proof of Theorems 3 and 4

Theorem 3. *If q is an odd prime power, $q \geqslant 7$, both r and t are nonnegative integers, $r > 2$, $t \leqslant 2^{r-1} - 3$, $1 + (q-1)t \in D$, and $1 + q \in D$, then $1 + (q-1)t + 2^r q \in D$.*

Theorem 4. *If q and q' are two odd prime powers, $q \geqslant 7$, $q' \geqslant 7$, both r and t are nonnegative integers, $r > 2$, $t \leqslant (2^{r-1} - 3)(q' - 3)$, $1 + (q-1)t \in D$, and $1 + q'q \in D$, then $1 + (q-1)t + 2^r q'q \in D$.*

At first we point out, though not necessary, that in the case $t = 0$ these theorems are two special cases of Lemma 4. What we want to prove is that the constructions given in Sections 4 and 5 satisfy conditions (C_1)–(C_5). We shall only write the one part of the proof of Theorem 4, for this can be repeated almost verbatim for the other part of the proof of Theorem 3. Obviously, (C_1) is satisfied, and so is (C_4) with $c_0 = \infty$. Here we are going to prove that (C_2) is satisfied, leaving the (C_3) and (C_5) to be discussed in the next section.

Let us consider the cl_w determined by $\mathscr{L}_w$ (see (C_2)), where $w \in X$ and $X = \{\infty\} \cup (Y \times Z) \cup (F_{2^r} \times F_{q'} \times F_q)$. Let $\{(g^i, v), (g^j, v')\}$ be an arbitrary pair, where $i, j \in \{0, 1, 2\}$, $i \neq j$, and $v, v' \in X \backslash \{w\}$, we want to show there is a block $\{(g^0, v_0), (g^1, v_1), (g^2, v_2)\}$ in cl_w containing this pair, where $B = (v_0, v_1, v_2) \in \mathscr{L}_w$. We shall point out the existence and uniqueness of B in various cases. All the possibilities are exhausted as follows.

(1) $\mathscr{L}_{xyz} (x \in F_{2^r}, y \in F_{q'}, z \in F_q)$. There are 9 cases.

Case i. $v. v' \in \{\infty\} \cup (\{x\} \times F_{q'} \times F_q)$ and $v \neq (x, y, z) \neq v'$. The block B can be contained neither in Part 2 nor in Part 4 nor in Part 1 (note (C_{13})). It uniquely appears in Part 3.

Case ii. $v = \infty$, $v' = (x', y', z') \in F_{2^r} \times F_{q'} \times F_q$, and $x' \neq x$. The block B can only be contained in Part 1, and the corresponding block B^{**} can only be contained in Part 1 of $\mathscr{L}^{**}_{xyz}$ (note (C_{13})) and is uniquely determined by the following conditions: (a) equations $x_{B^{**}} = x$, $x_j = x'$, (11), (1), (4), $y_j = y'$, and $z_j = z'$ are all fulfilled (thereby (C_{13}) holds); (b) equations

$\varphi'_{\beta'}=0$ and $\varphi_\beta=0$ are fulfilled if $(*)'$ is satisfied, and equations $\varphi'_{-\alpha'}=0$ and $\varphi_{-\alpha}=0$ are fulfilled if $(*)'$ is not satisfied.

Case iii. $v=\infty$ and $v'=(k', y', z')\in Y\times Z$. The block B can only be contained in Part 1, and the corresponding block B^{**} is uniquely determined by the following conditions: (a) equations $x_{B^{**}}=x$, (11), (12), (1), and (4) are all fulfilled (thereby (C_{13}) holds); (b) equations $\varphi'_{-\alpha'}=0$, $\varphi'_{\alpha'}=y'$, $\varphi_{-\alpha}=0$, and $\varphi_\alpha=z'$ are all fulfilled if $(*')$ is not satisfied, and equations $\varphi'_{\beta'}=0$, $\varphi'_{\varepsilon'\alpha'}=y'$, $\varphi_\beta=0$, and $(\alpha+\varepsilon\beta)$ $\varphi_{\varepsilon\alpha}=z'$ are all fulfilled if $(*')$ is satisfied, where ε and ε' are determined by $(**)$ and $(**')$.

Case iv. $v=(k', y', z')$, $v'=(k'', y'', z'')$, $v, v'\in Y\times Z$, $k'>k''$, and $(k', y', z')\neq(-k'', y'', z'')$. The block B can only be contained in Part 1, and the corresponding block B^{**} is uniquely determined by the following conditions:

(a) equations $x_{B^{**}}=x$, (12), (13), (1), and (4) are all fulfilled (thereby $x_0\neq x_1$);

(b) equations $\varphi'_{\alpha'}=y'$, $\varphi'_{-\alpha'}=y''$, $(\alpha+\beta)$ $\varphi_\alpha=z'$, and $(\alpha-\beta)\,\varphi_{-\alpha}=z''$ are all fulfilled if $x_2\neq x$ and Eq. (11) holds; (c) equations $\varphi'_{\alpha'}=y'$, $\varphi'_{-\alpha'}=y''$, $\varphi_\alpha=z'$ and $\varphi_{-\alpha}=z''$ are all fulfilled if $x_2\neq x$ and Eq. (11) does not hold; (d) equations $\psi'_0=y'$, $\psi'_1=y''$, $\psi_0=z'$, and $\psi_1=z''$ are all fulfilled if $x_2=x$ (thereby $(y_2, z_2)\neq(y, z)$). Note that if $x_2=x$, then certainly, $x_0=x_1$ and $k'=-k''$.

Case v. $v=(k', y', z')$, $v'=(k', y'', z'')$, $v, v'\in Y\times Z$, $v\neq v'$ and $y'\geqslant_{q'}y''$. The block B can only be contained in Part 1. The corresponding block B^{**} must not satisfy the presupposition of (C_{17}), otherwise we should have $\varphi'_{\varepsilon'\alpha'}=y'=y''$, and $(\alpha+\varepsilon\beta)$ $\varphi_{\varepsilon\alpha}=z'=z''$ or $\varphi_{\varepsilon\alpha}=z'=z''$ for some ε and ε', which contradicts the assumption $v\neq v'$. In the same way, we can show that B^{**} does not satisfy the presupposition of (C_{19}), Eq. (14) must hold, and we have $y'=-y_1+y_2$ whenever $y'=y''$. Note that if $y'\neq y''$, $\varphi'_{y'}=y'^2$ and $\varphi'_{y''}=y''^2$, then we can infer $-y_1+y_2=y'+y''$; and since y', $y''\in Y_{k'}$ and $y'\neq 0\neq y''$, we arrive at $y'\neq -y_1+y_2\neq y''$. In view of the above facts, we see the block B^{**} is uniquely determined by the following conditions: (a) equations $x_{B^{**}}=x$, (12), (14), (1), (4), $\varphi'_{y'}=y'^2$, and $\varphi'_{y''}=y''^2$ are all fulfilled—thereby (C_{13}) holds (e.g., if $x_{B^{**}}=x_2$ then $(\theta^s+\theta^{k'})(\theta^s+\theta^{-k'})=0$, which is impossible), and since a quadratic equation has at most two roots, we infer that $(*')$ must not hold from the fact that Eqs. (12) and (14) hold (cf. Case 2 of the proof of the proposition in Section 3); (b) equations $\varphi_\alpha=z'$ and $\varphi_{-\alpha}=z''$ are all fulfilled if $y'\neq y''$; (c) equations $y'=-y_1+y_2$, $\varphi_{z'-\delta}=z'^2$, and $\varphi_{z''-\delta}=z''^2$ are all fulfilled if $y'=y''$.

Case vi. $v = (k', y', z')$, $v' = (k'', y', z')$, $v, v' \in Y \times Z$, and $k' = \pm k''$. The block B cannot be contained in Parts 1–3. This is clear for the case $k' = k''$. If $k' = -k''$, by the fact that (C_{16}) holds and equations $x_{B^{**}} = x$, (12), and (13), the corresponding block B^{**} satisfies $x_0 = x_1 \neq x$ and $x_2 = x_{B^{**}} = x$; further, by the fact that (C_{19}) holds, and Eqs. (1), (4), $\psi'_0 = \psi'_1 = y'$, and $\psi_0 = \psi_1 = z'$, we have $y_0 = y_1$, $z_0 = z_1$, $y_2 = y$, and $z_2 = z$; but this is impossible for the blocks in Parts 1–3 of $\mathscr{L}^{**}_{xyz}$. The block B is uniquely contained in Part 4, however.

Case vii. $v = (k', y', z') \in Y \times Z$, $v' = (x', y'', z'') \in F_{2^r} \times F_{q'} \times F_q$, $(x', y'', z'') \neq (x, y, z)$,

$$(j, x', y' - (\alpha' - e')\, y'', z' - (\alpha - e)\, z'') \neq (0 \text{ or } 1, x + (\theta^k + \theta^{-k})^{-1}, -\alpha' y, -\alpha z), \tag{15}$$

$$(j, x', y' - y'', z' - z'') \neq (2, x + y^{-1}\theta^{\pm k}, -\alpha' y, -\alpha z), \tag{16}$$

$$(j, x'y' + y'', z' + z'') \neq (0, x + \theta^{-k}, (e' - \alpha')\, y, (e - \alpha)\, z), \tag{17}$$

and

$$(j, x', y' + y'', z' + z'') \neq (1, x + \theta^k, (e' - \alpha')\, y, (e - \alpha)\, z). \tag{18}$$

It can easily be seen that the block B can only be contained in Part 1, and the corresponding block B^{**} is uniquely determined by the following conditions: (a) equations $x_{B^{**}} = x$, $x_j = x'$, (12), $y_j = y''$, and $z_j = z''$ are all fulfilled; (b) equations (1) and (4) are fulfilled if $x_0 \neq x \neq x_1$, Eqs. (2) and (5) are fulfilled if $x_0 = x$, and Eqs. (3) and (6) are fulfilled if $x_1 = x$ (it is impossible that $x_0 = x_1 = x$); (c) the conditions (C_{17}), (C_{18}), and (C_{19}) are all satisfied. The inequalities (15)–(18) guarantee that the block B^{**} satisfying the above conditions is contained in $\mathscr{L}^{**}_{xyz}$.

Case viii. $v = (k', y', z') \in Y \times Z$, $v' = (x', y'', z'') \in F_{2^r} \times F_{q'} \times F_q$, $(x', y'', z'') \neq (x, y, z)$ and not all the inequalities (15)–(18) hold. The block B is in Part 4, and it is unique (cf. the above case).

Case ix. $v = (x', y', z')$, $v' = (x'', y'', z'')$, $v, v' \in F_{2^r} \times F_{q'} \times F_q$, and $(x', x'') \neq (x, x)$. The block B can only be contained in Part 1 or 2. There is a unique B^{**} in $\mathscr{L}^{**}_{xyz}$ meeting the case. If B^{**} is contained in Part 4 of $\mathscr{L}^{**}_{xyz}$, then $B = B^{**}$ is contained in Part 2 of $\mathscr{L}_{xyz}$; and if B^{**} is contained in Parts 1–3 of $\mathscr{L}^{**}_{xyz}$, then $B \in \langle B^{**} - C_{B^{**}} \rangle \subset$ Part 1 of $\mathscr{L}_{xyz}$. Clearly, B is unique.

(2) $\mathscr{L}_\infty$. There are 4 cases.

Case i. $v, v' \in Y \times Z$. The unique block B is contained in Part 2.

Case ii. $v = (k', y', z') \in Y \times Z$ and $v' = (x, y, z) \in F_{2^r} \times F_{q'} \times F_q$. The block B can only be contained in Part 1, and the corresponding block B^{**} is uniquely determined by the following conditions: (a) Eqs. (11), (12), $x_j = x$, $y_j = y$, and $z_j = z$ are all fulfilled (thereby (C_{13}) holds and (14) does not); (b) conditions (C_{15}), (C_{17}), and (C_{18}) are all satisfied.

Case iii. $v = (x, y, z)$, $v' = (x, y', z')$ and $v, v' \in F_{2^r} \times F_{q'} \times F_q$. The block B cannot be in Part 1, since the corresponding B^{**} must satisfy $x_0 = x_1 = x_2 = x_{B^{**}}$ by Eq. (11), which does not coincide with condition (C_{13}). But B is uniquely in Part 3.

Case iv. $v = (x, y, z)$, $v' = (x', y', z')$, $v, v' \in F_{2^r} \times F_{q'} \times F_q$ and $x \neq x'$. The block B can only be contained in Part 1, and the corresponding block B^{**} is uniquely determined by the following conditions: (a) Eqs. (11), $x_i = x$, $x_j = x'$, $y_i = y$, $y_j = y'$, $z_i = z$, and $z_j = z'$ are all fulfilled (thereby (C_{13}) holds); (b) condition (C_{15}) holds.

(3) $\mathscr{L}_{k'y'z'}(k' \in K, y' \in Y_{k'}, z' \in Z)$. There are 5 cases.

Case i. $v, v' \in \{\infty\} \cup (Y \times Z)$ and $v \neq (k', y', z') \neq v'$. The block B is uniquely in Part 2.

Case ii. $v = \infty$ and $v' = (x, y, z) \in F_{2^r} \times F_{q'} \times F_q$. The block B can only be contained in Part 1, and the corresponding block B^{**} is uniquely determined by the same condition as in the case (ii) of $\mathscr{L}_\infty$.

Case iii. $v = (k'', y'', z'') \in Y \times Z$, $v' = (x, y, z) \in F_{2^r} \times F_{q'} \times F_q$, and $k' \neq k''$. The block B can only be contained in Part 1, and the corresponding block B^{**} is uniquely determined by the following conditions: (a) Eqs. (12), (13), $x_j = x$, $y_j = y$, and $z_j = z$ are all fulfilled (thereby $x_0 \neq x_{B^{**}} \neq x_1$); (b) if $x_2 \neq x_{B^{**}}$, then $\varphi'_{\varepsilon'\alpha'} = y'$ and $\varphi'_{-\varepsilon'\alpha'} = y''$ (where ε' is determined by $(**')$), $(\alpha + \varepsilon\beta)\, \varphi_{\varepsilon\alpha} = z'$ and $(\alpha - \varepsilon\beta)\, \varphi_{-\varepsilon\alpha} = z''$ if Eq. (11) holds, and $\varphi_{\varepsilon\alpha} = z'$ and $\varphi_{-\varepsilon\alpha} = z''$ if Eq. (11) does not hold (where ε is determined by $(**)$); (c) if $x_2 = x_{B^{**}}$ (thereby $k' = -k''$), then $\psi'_0 = y'$, $\psi'_1 = y''$, $\psi_0 = z'$, and $\psi_1 = z''$ when $k' > 0$, and $\psi'_1 = y'$, $\psi'_0 = y''$, $\psi_1 = z'$, and $\psi_0 = z''$ when $k' < 0$.

Case iv. $v = (k', y'', z'') \in Y \times Z$, $v' = (x, y, z) \in F_{2^r} \times F_{q'} \times F_q$, and $(y', z') \neq (y'', z'')$. The block B can only be contained in Part 1, and the corresponding block B^{**} is uniquely determined by the following conditions (cf. Case v of $\mathscr{L}_{xyz}$): (a) Eqs. (12), (14), $x_j = x$, $y_j = y$, $\varphi'_{y'} = y'^2$, $\varphi'_{y''} = y''^2$, and $z_j = z$ are all fulfilled; (b) equations $\varphi_{\varepsilon\alpha} = z'$ and $\varphi_{-\varepsilon\alpha} = z''$ are all fulfilled if $y' \neq y''$, where $\varepsilon = e$ if $y' >_{q'} y''$ and $\varepsilon = -e$ if $y' <_{q'} y''$; (c) equations $y' = -y_1 + y_2$, $\varphi_{z'-\delta} = z'^2$ and $\varphi_{z''-\delta} = z''^2$ are all fulfilled if $y' = y''$.

Case v. $v = (x, y, z)$, $v' = (x', y', z')$, and v, $v' \in F_{2^r} \times F_{q'} \times F_q$. The block B can only be contained in Part 1, and the corresponding block B^{**} is uniquely determined by the following: Eqs. (12), $x_i = x$, $x_j = x'$, $y_i = y$, $y_j = y'$, $z_i = z$, and $z_j = z'$, and conditions (C_{17}), (C_{18}), and (C_{19}), are all fulfilled.

We thus have proved that condition (C_2) is satisfied by $\mathscr{L}_\infty$, every $\mathscr{L}_{xyz}$, and every $\mathscr{L}_{k'y'z'}$.

7. Proof of Theorems 3 and 4 (continued)

(1) We now proceed to show that both $\mathscr{S}^1$ and $\mathscr{S}^2$ given in Section 5 satisfy condition (C_3). We only discuss the case of $\mathscr{S}^1$, for this can be repeated verbatim for the case of $\mathscr{S}^2$. Direct calculation shows that the number of the blocks in $\mathscr{S}^1$ does not exceed $(1 + (q-1)t + 2^r q' q)^2$. Therefore, we only have to show that for any pair $P = \{(u, v), (u', v')\}$, there exists a block $\{(g^0, v_0), (g^1, v_1), (g^2, v_2), (0, v_3)\}$ in cl^1 cotaining P, where u, $u' \in F_4$, $u \neq u'$, v, $v' \in X$, and $B = (v_0, v_1, v_2, v_3) \in \mathscr{S}^1$ (cf. Sect. 1). Here we only discuss the case $u = g^1$ and $u' = g^2$, the other cases are similar to it. We shall point out the existence of B for various types of P. Consider 5 cases below which exhaust all the possibilities.

Case i. v, $v' \in \{\infty\} \cup (Y \times Z)$. The block B is contained in Part 8.

Case ii. $\{v, v'\} = \{\infty, (x, y, z)\}$ or $\{(x, y, z), (x, y', z')\}$, $x \in F_{2^r}$, y, $y' \in F_{q'}$, and z, $z' \in F_q$. The block B is contained in Part 7.

Case iii. $v = (k, y, z) \in Y \times Z$, $v' = (x', y', z') \in F_{2^r} \times F_{q'} \times F_q$. The block B is contained in Part 4.

Case iv. $v = (x', y', z') \in F_{2^r} \times F_{q'} \times F_q$, $v' = (k, y, z) \in Y \times Z$. The block B is contained in Part 5.

Case v. $v = (x, y, z)$, $v' = (x', y', z')$, v, $v' \in F_{2^r} \times F_{q'} \times F_q$, $x + x' = (\theta^0 + \gamma^{-1})\, \theta^k \neq 0$, and $k \in \{-2^{r-1} + 1, -2^{r-1} + 2, ..., -1, 0, 1, ..., 2^{r-1} - 1\}$. If $k \notin K$ or $(e' - \alpha')\, y' - \alpha' y \notin Y_k$, then the block B is contained in Part 1. Let $k \in K$ and $(e' - \alpha')\, y' - \alpha' y \in Y_k$, then B is contained in Part 2 if $\alpha z - (e - \alpha)\, z' = 0$, in Part 6 if $\alpha z - (e - \alpha)\, z' \in Z$, in Part 3 if $(e - \alpha)\, z' - \alpha z \in Z$.

(2) It remains only to show that condition (C_5) is also satisfied by the construction given in Section 5. Let $B = (v_0, v_1, v_2)$, v_0, v_1, $v_2 \in X$, and $\{h, i, j\} = \{0, 1, 2\}$. Consider 9 cases below which exhaust all the possibilities.

Case i. $v_0, v_1, v_2 \in \{\infty\} \cup (Y \times Z)$. Either the block B is contained in $\mathscr{L}_w$ (Part 2) for some $w \in \{\infty\} \cup (Y \times Z)$, or there is v_3 such that $(v_0, v_1, v_2, v_3) \in \mathscr{L}^1 \cup \mathscr{L}^2$ (Part 8), since $\mathrm{LD}[\{\infty\} \cup (Y \times Z)]$ satisfies condition (C_5).

Case ii. $v_0 = (x, v_0'), v_1 = (x, v_1'), v_2 = (x, v_2'), x \in F_{2^r}, v_0', v_1', v_2' \in \{\infty\} \cup (F_{q'} \times F_q)$ (whenever ∞ appears for v_0', v_1', or v_2', omit the first coordinate x), and $\{v_0, v_1, v_2\} \neq \{\infty\}$. Either the block B is contained in $\mathscr{L}_w$ (Part 3) for some $w \in \{\infty\} \cup (\{x\} \times F_{q'} \times F_q)$, or there is v_3 such that $(v_0, v_1, v_2, v_3) \in \mathscr{L}^1 \cup \mathscr{L}^2$ (Part 7), since $\mathrm{LD}[\{\infty\} \cup (F_{q'} \times F_q)]$ satisfies condition (C_5).

Case iii. $v_h = \infty$, $v_i = (k', y', z') \in Y \times Z$, and $v_j = (x', y'', z'') \in F_{2^r} \times F_{q'} \times F_q$. In this case, we have $B \in \langle B^{**} - C_{B^{**}}\rangle \subset \mathscr{L}_{xyz}$ (Part 1), where x, y, z, and B^{**} are determined by: (a) Eqs. (11), (12), $x_{B^{**}} = x$, $x_j = x'$, (1), (4), $y_j = y''$, and $z_j = z''$ are all fulfilled (thereby (C_{13}) holds); (b) equations $\varphi'_{\beta'} = 0$, $\varphi'_{\varepsilon'\alpha'} = y'$, $\varphi_\beta = 0$, and $(\alpha + \varepsilon\beta)\,\varphi_{\varepsilon\alpha} = z'$ are all fulfilled if $(*')$ is satisfied, where ε and ε' are determined by $(**)$ and $(**')$; (c) equations $\varphi'_{-\alpha'} = 0$, $\varphi'_{\alpha'} = y'$, $\varphi_{-\alpha} = 0$, and $\varphi_\alpha = z'$ are all fulfilled if $(*')$ is not satisfied.

Case iv. $v_h = \infty$, $v_i = (x', y', z')$, and $v_j = (x'', y'', z'')(v_i, v_j \in F_{2^r} \times F_{q'} \times F_q, x' \neq x'')$. Let (x, y, z) and B^{**} be the two blocks which are determined by: (a) equations $x_{B^{**}} = x$, (11), $x_i \times x'$, $x_j = x''$, (1), $y_i = y'$, $y_j = y''$, (4), $z_i = z'$, and $z_j = z''$ are all fulfilled; (b) equations $\varphi'_{\beta'} = 0$ and $\varphi_\beta = 0$ are fulfilled if $(*')$ holds, and equations $\varphi'_{-\alpha'} = 0$ and $\varphi_{-\alpha} = 0$ are fulfilled if $(*')$ does not hold. It is easily seen from the above conditions that (C_{13}) is satisfied and $\infty \in C_{B^{**}}$. If $|C_{B^{**}}| = 1$, then $B \in \langle B^{**} - C_{B^{**}}\rangle \subset \mathscr{L}_{xyz}$ (Part 1); and if $|C_{B^{**}}| = 2$, then $B \in \langle B^{**} - C_{B^{**}} \backslash \{w\}\rangle \subset \mathscr{L}_w$ (Part 1), where $\infty \neq w \in C_{B^{**}}$.

Case v. $v_h = (k', y', z')$, $v_i = (k'', y'', z'')$, $v_j = (x', y''', z''') \in F_{2^r} \times F_{q'} \times F_q$, $v_h, v_i \in Y \times Z$, $k' > k''$, and $(k', y', z') \neq (-k'', y'', z'')$. We have $B \in \langle B^{**} - C_{B^{**}}\rangle \subset \mathscr{L}_{xyz}$ (Part 1), where x, y, z, and B^{**} are determined by: (a) equations $x_{B^{**}} = x$, (12), (13), $x_j = x'$, (1), $y_j = y'''$, (4), and $z_j = z'''$ are all fulfilled (thereby $x_0 \neq x \neq x_1$); (b) equations $\varphi'_{\alpha'} = y'$, $\varphi'_{-\alpha'} = y''$, $(\alpha + \beta)\,\varphi_\alpha = z'$, and $(\alpha - \beta)\,\varphi_{-\alpha} = z''$ are all fulfilled if $x_2 \neq x$ and Eq. (11) holds; (c) equations $\varphi'_{\alpha'} = y'$, $\varphi'_{-\alpha'} = y''$, $\varphi_\alpha = z'$, and $\varphi_{-\alpha} = z''$ are all fulfilled if $x_2 \neq x$ and Eq. (11) does not hold; (d) equations $\psi_0' = y'$, $\psi_1' = y''$, $\psi_0 = z'$, and $\psi_1 = z''$ are all fulfilled if $x_2 = x$.

Case vi. $v_h = (k', y', z')$, $v_i = (\pm k', y', z')$ and $v_j = (x', y'', z'') \in F_{2^r} \times F_{q'} \times F_q$ $(v_h, v_i \in Y \times Z)$. In this case there exist x, y, and z such that $B \in \mathscr{L}_{xyz}$ (Part 4).

Case vii. $v_h = (k', y', z')$, $v_i = (k', y'', z'')$, $v_j = (x', y''', z''') \in F_{2^r} \times$

$F_{q'} \times F_q$, v_h, $v_i \in Y \times Z$, $y' \geqslant_{q'} y''$, and $(y', z') \neq (y'', z'')$. We have $B \in \langle B^{**} - C_{B^{**}} \rangle \subset \mathscr{L}_{xyz}$ (Part 1), and the two blocks (x, y, z) and B^{**} are determined by: (a) equations $x_{B^{**}} = x$, (12), (14), $x_j = x'$, (1), $y_j = y'''$, $\varphi'_{y'} = y'^2$, $\varphi'_{y''} = y''^2$, (4), and $z_j = z'''$ are all fulfilled (thereby (C_{13}) holds and $(*')$ does not, as is similar to Case v of $\mathscr{L}_{xyz}$ in the preceding section); (b) equations $\varphi_\alpha = z'$ and $\varphi_{-\alpha} = z''$ are fulfilled if $y' \neq y''$; (c) equations $y' = -y_1 + y_2$, $\varphi_{z'-\delta} = z'^2$, and $\varphi_{z''-\delta} = z''^2$ are all fulfilled if $y' = y''$.

Case viii. $v_h = (k', y', z') \in Y \times Z$, $v_i = (x', y'', z'')$, and $v_j = (x'', y''', z''')(v_i, v_j \in F_{2^r} \times F_{q'} \times F_q)$. Let (x, y, z) and B^{**} be the two blocks which are determined by: (a) equations $x_{B^{**}} = x$, (12), $x_i = x'$, $x_j = x''$, $y_i = y''$, $y_j = y'''$, $z_i = z''$, and $z_j = z'''$ are all fulfilled; (b) Eqs. (1) and (4), and conditions (C_{17}), (C_{18}), and (C_{19}), are all fulfilled if $x_0 \neq x \neq x_1$ (note that if $y' = -y_1 + y_2$ and $\varphi'_{y'} = y'^2$, then there must be no y'' satisfying $y'' \in Y_{k'}$, $y'' \neq y'$ and $\varphi'_{y''} = y''^2$); (c) Eqs. (2), (5), $\psi'_2 = y'$, and $\psi_2 = z'$ are all fulfilled if $x_0 = x$ (then certainly, $x_1 \neq x$); (d) Eqs. (3), (6), $\psi'_3 = y'$, and $\psi_3 = z'$ are all fulfilled if $x_1 = x$. It is easily seen from the above conditions that $(k', y', z') \in C_{B^{**}}$. If $|C_{B^{**}}| = 2$, then $B \in \langle B^{**} - C_{B^{**}} \backslash \{w\} \rangle \subset \mathscr{L}_w$ (Part 1), where $(k', y', z') \neq w \in C_{B^{**}}$. If $|C_{B^{**}}| = 1$, then three cases arise: (a) $B \in \langle B^{**} - C_{B^{**}} \rangle \subset \mathscr{L}_{xyz}$ (Part 1) if $(x_0, y_0, z_0) \neq (x, y, z) \neq (x_1, y_1, z_1)$ (note if $(x_2, y_2, z_2) = (x, y, z)$, then certainly, $x_0 = x_1 \neq x$, $\psi'_0 = \psi'_1$, $\psi_0 = \psi_1$, $(-k', y', z') \in C_{B^{**}}$, and $|C_{B^{**}}| = 2$); (b) there is v_3 such that $(v_0, v_1, v_2, v_3) \in \mathscr{L}^1$ (Parts 3–5) if $(x_0, y_0, z_0) = (x, y, z)$; and (c) there is v_3 such that $(v_0, v_1, v_2, v_3) \in \mathscr{L}^2$ (Parts 3–5) if $(x_1, y_1, z_1) = (x, y, z)$.

Case ix. $B = B^{**}$ with $|\{x_0, x_1, x_2\}| > 1$. Since $\mathrm{LD}[F_{2^r} \times F_{q'} \times F_q]$ satisfies (C_5) (cf. Section 2), there are only two possibilities: (a) there exists $(x, y, z) \in F_{2^r} \times F_{q'} \times F_q$ such that $B^{**} \in$ Parts 1–4 of $\mathscr{L}^{**}_{xyz}$, (b) there exist $i \in \{1, 2\}$ and v_3 such that $(v_0, v_1, v_2, v_3) \in \mathscr{L}^{**i}$ (Part 1). In (a), if $B^{**} \in$ Part 4 of $\mathscr{L}^{**}_{xyz}$ then $B \in$ Part 2 of $\mathscr{L}_{xyz}$, and if $B^{**} \in$ Parts 1–3 of $\mathscr{L}^{**}_{xyz}$ then $B \in \mathscr{L}_{xyz}$ (Part 1) when $|C_{B^{**}}| \neq 1$, or $B \in \mathscr{L}_w$ (Part 1) when $C_{B^{**}} = \{w\}$. As for (b), we only have to consider $i = 1$, $i = 2$ is similar to it. Then we have $x_{B^{**}} = x_0$, therefore $\infty \notin C_{B^{**}}$, and $|C_{B^{**}}| \leqslant 1$, which can be seen from (C_{16}), (12), (13), and (C_{19}). If $|C_{B^{**}}| = 1$, $C_{B^{**}} = \{(k', y', z')\}$, then $B \in \mathscr{L}_{k'y'z'}$ (Part 1). And if $C_{B^{**}} = \varnothing$, then (v_0, v_1, v_2) cannot take the form $((x_0, y_0, z_0), (x_0 + \theta^k, (e' - \alpha')\, y_0 - y, (e - \alpha)\, z_0 - z), (x_0 + \gamma^{-1}\theta^k, \alpha' y_0 + y, \alpha z_0 + z))$, where $x_0 \in F_{2^r}$, $y_0 \in F_{q'}$, $z_0 \in F_q$, $k \in K$, $y \in Y_k$, and $z \in Z$, otherwise $(k, y, z) \in C_{B^{**}}$—it follows that there exists a v_3 such that $(v_0, v_1, v_2, v_3) \in \mathscr{L}^1$ (Parts 1, 2, 6).

The proof is completed.

8. Proof of Theorems 5 and 6

THEOREM 5. *If q is an odd prime power, $q \geqslant 5$, both r and t are nonnegative integers, $r > 2$, $t \leqslant 2^{r-2} - 1$, $1 + (q-1)t \in D$, and $1 + q \in D$, then $1 + (q-1)t + 2^r q \in D$.*

THEOREM 6. *If q and q' are two prime powers, $q \geqslant 5$, $q' \geqslant 5$, both r and t are nonnegative integers, $r > 2$, $t \leqslant (2^{r-2} - 1)(q' - 3)$, $1 + (q-1)t \in D$ and $1 + q'q \in D$, then $1 + (q-1)t + 2^r q'q \in D$.*

EXAMPLE. We mention an example here, which will be useful in the next paper [6]. We have seen $57 \in D$ and $96 \in D$ in Table II. Taking $q = 5$, $t = 14$, $r = 4$, and $q' = 19$ in Theorem 6, then we get $1577 \in D$. So, if $D(1579) = 1577$, then $D(4731) = 4729$.

Proof of the theorems. In fact, we can take the constructions of Theorems 3 and 4 for those of Theorems 5 and 6, respectively. But here we should take $K \subseteq \{-2^{r-1} + 3, -2^{r-1} + 5, \ldots, -1, 1, \ldots, 2^{r-1} - 5, 2^{r-1} - 3\}$. It should be pointed out that if q or $q' = 5$, then there exists no $\beta \in F_q$ or no $\beta' \in F_{q'}$ satisfying the corresponding conditions mentioned in Section 3. These β and β' are not necessary in the present case, however. For any given block B^* (B^{**}), there exists no pair of two distinct elements $k', k'' \in K$ satisfying the simultaneous Eqs. (7), (8), and (9) ((11), (12), and (13)). If these equations were satisfied, then we should have $\theta^s(\theta^{-k'} + \theta^{-k''}) = \theta^{-s}(\theta^{k'} + \theta^{k''})$, which requires $\theta^{2s} = \theta^{k'+k''}$ (namely, $k' + k'' \equiv 2s \equiv -1 \pmod{2^r - 1}$) if $\theta^{k'} \neq \theta^{k''}$. It can be verified easily that there exists no pair of two distinct elements $k', k'' \in K$ satisfying this requirement, in light of the stipulation about the set K. Hence, all that relates to β and β' in conditions (C_8), (C_{10}), (C_{15}), and (C_{17}) does not work now, and both β and β' are not necessary indeed. Thus, one sees Theorems 5 and 6 can be established.

9. Proof of Theorem 1

Let us denote by C^* the set of integers m which take the form $m = 2^r$ or $m = 2^r q$, where r is a nonnegative integer and q is an odd prime power greater than 3. Let $m \in C^*$, we define $f(m) = 2^{r+2} - 3$ if $m = 2^r$, $f(m) = (2^{r+2} - 3)(q - 3)$ if $m = 2^r q$ and q is an odd prime power greater than 5, and $f(m) = 2(2^{r+1} - 1)$ if $m = 2^r \cdot 5$, where r is a nonnegative integer. Thus, if $m \in C^*$, from the above definition we can immediately deduce that $4m \in C^*$ and

$$f(4m) \geqslant 4f(m) + 6. \tag{19}$$

We may regard the following theorem as a corollary of Theorems 3, 4, and 6, but Theorem 7 is more convenient for many applications.

THEOREM 7. *If* $m \in C^*$, *t is an odd number, and* $0 < t \leqslant f(m)$, *then* $1 + 6t + 56m \in D$.

Proof. From Lemma 1 we know $1 + 6t \in D$. And by Lemmas 3 and 4 we have $8 \in D$ and $1 + q'7 \in D$, where q' is an odd prime power greater than 3. Hence, taking $q = 7$ in Theorems 3, 4 and 6, we get Theorem 7 immediately.

LEMMA 5. *If there exists a sequence of* $m+1$ *steadily increasing integers* $a_1, a_2, \ldots, a_{m+1}$, *each term of which belongs to* C^*, *satisfying* $a_{m+1} = 4a_1$, $a_i \equiv 2 \pmod 3$, *and* $3f(a_i) \geqslant 28(a_{i+1} - a_i)$ *for* $i = 1, 2, \ldots, m$, *then* $n \in D$ *whenever* $n \equiv 11 \pmod{12}$ *and* $n \geqslant 7 + 56a_1$.

Proof. The integer n as stated in this lemma can be expressed as $n = 1 + 6t' + 56n'$, where t' is an odd number, $0 < t' \leqslant 27$, and n' is an integer satisfying $n' \equiv 2 \pmod 3$ and $n' \geqslant a_1$. Certainly, there exist two integers r and i, $r \geqslant 0$, $m \geqslant i \geqslant 1$, such that $4^r a_i \leqslant n' < 4^r a_{i+1}$. Setting $t = t' + \frac{28}{3}(n' - 4^r a_i)$ (clearly, t is an odd number), we have $0 < t \leqslant t' + \frac{28}{3}(4^r a_{i+1} - 3 - 4^r a_i) < \frac{28}{3} \cdot 4^r(a_{i+1} - a_i) \leqslant 4^r f(a_i) \leqslant f(4^r a_i)$ (note the formula (19)). Then the number n can be expressed as $n = 1 + 6t + 56 \cdot 4^r a_i$, and $n \in D$ follows from the Theorem 7.

Put $T = \{23, 47, 59, 83, 107, 167, 179, 227, 263, 299, 347, 383, 719, 767, 923, 1439\}$. We again state

THEOREM 1. *If n is a positive integer*, $n \equiv 11 \pmod{12}$, *and* $n \notin T$, *then* $n \in D$.

Proof. The following eight integers fulfill the requirements in Lemma 5:

i	1	2	3	4	5	6	7	8
a_i	32	44	53	56	68	86	104	128
$f(a_i)$	125	104	50	116	182	200	290	509

Therefore, by Lemma 5, if n is a positive integer, $n \equiv 11 \pmod{12}$ and $n \geqslant 1799$, then $n \in D$. We enumerate the cases $n < 1799$ ($n \equiv 11 \pmod{12}$, $n \notin T$) in decreasing order as follows:

$n = 1787$ (see Table II); $1775 \geqslant n \geqslant 1463$: use Theorem 7, taking $m = 26$, 29; $n = 1451$, 1427, 1415 (see Tables I and II; $1403 \geqslant n \geqslant 1295$: use Theorem 7, taking $m = 23$; $n = 1283$: use Theorem 4, taking $q = 11$, $q' = 7$,

$r = 4$, and $t = 5$ $(51, 78 \in D$, see Table II); $1271 \geqslant n \geqslant 1211$ (see Tables I and II); $1199 \geqslant n \geqslant 1127$: use Theorem 7, taking $m = 20$; $1115 \geqslant n \geqslant 1043$ (see Tables I and II); $1031 \geqslant n \geqslant 959$: use Theorem 7, taking $m = 17$; $n = 947$, 935, 911 (see Tables I and II; $899 \geqslant n \geqslant 791$: use Theorem 7, taking $m = 14$; $n = 779$: use Theorem 6, taking $q = 19$, $q' = 5$, $r = 3$ and $t = 1$ $(96 \in D$, see Table II); $755 \geqslant n \geqslant 731$ and $707 \geqslant n \geqslant 671$ (see Tables I and II); $659 \geqslant n \geqslant 455$: use Theorem 7, taking $m = 8, 11$; $443 \geqslant n \geqslant 395$ and $n = 371$ (see Tables I and II); $n = 359$: use Theorem 3, taking $q = 19$, $r = 4$ and $t = 3$ $(20 \in D$, see Table I); $335 \geqslant n \geqslant 311$ (see Tables I and II); $n = 287$: use Theorem 7, taking $m = 5$; $n = 275$, 251, 239, 215, 203, 191, 155 (see Tables I and II); $143 \geqslant n \geqslant 119$: use Theorem 7, taking $m = 2$; $n = 95$, 71, 35, 11 (see Tables I and II).

The proof of Theorem 1 is completed.

REFERENCES

1. A. HEDAYAT, A generalization of sum composition: self orthogonal Latin square design with sub-self orthogonal Latin square designs, *J. Combin. Theory Ser. A* **24** (1978), 202–210.
2. J. X. LU, On large sets of disjoint Steiner triple systems, I, *J. Combin. Theory Ser. A* **34** (1983), 140–146.
3. J. X. LU, On large sets of disjoint Steiner triple systems, II, *J. Combin. Theory Ser. A* **34** (1983), 147–155.
4. J. X. LU, On large sets of disjoint Steiner triple systems, III, *J. Combin. Theory Ser. A* **34** (1983), 156–182.
5. J. X. LU, On large sets of disjoint Steiner triple systems, IV, *J. Combin. Theory Ser. A* **37** (1984), 136–163.
6. J. X. LU, On large sets of disjoint Steiner triple systems, VI, *J. Combin. Theory Ser. A* **37** (1984), 189–192.