CONSTRUCTIONS OF DISJOINT STEINER TRIPLE SYSTEMS

JEAN DOYEN¹

ABSTRACT. Let $D^*(v)$ denote the maximum number of pairwise disjoint and isomorphic Steiner triple systems of order v. The main result of this paper is a lower bound for $D^*(v)$, namely $D^*(6t+3) \ge 4t-1$ or 4t+1 according as 2t+1 is or is not divisible by 3, and $D^*(6t+1) \ge t/2$ or t according as t is even or odd. Some other related problems are studied or proposed for study.

1. Introduction and historical note. Given a finite nonempty set S of v elements (called *points*), a Steiner triple system of order v on S is a collection \mathscr{S} of subsets of S (called *lines*) such that every line has exactly 3 points and every pair of points is contained in one and only one line. Any Steiner triple system is also a balanced incomplete block design with parameters v, k=3 and $\lambda=1$ (see for instance Hall [10, Chapter 15]).

Kirkman [11] proved in 1847 that a necessary and sufficient condition for the existence of a Steiner triple system (briefly STS) of order v is $v \equiv 1$ or 3 (mod 6). An STS of order v is sometimes denoted simply by S(v).

Let \mathscr{S} and \mathscr{S}' be two STS on the same set S of points. \mathscr{S} and \mathscr{S}' are called *disjoint* if $\mathscr{S} \cap \mathscr{S}' = \emptyset$, that is if they have no line in common. According to [8], the construction of disjoint STS might be useful in the design of certain statistical experiments.

Let us denote by D(v) the maximum number of pairwise disjoint S(v) that can be constructed on a set S of v points. As S contains v(v-1)(v-2)/6 subsets of cardinality 3 and as any S(v) contains exactly v(v-1)/6 lines, we have $D(v) \leq v-2$, except of course if v=1. We shall denote by $D^*(v)$ the maximum number of pairwise disjoint and isomorphic S(v) that can be constructed on S. Obviously, $1 \leq D^*(v) \leq D(v)$.

It is clear that

$$D^*(1) = D(1) = 1$$
 and $D^*(3) = D(3) = 1$.

Cayley [6] proved in 1850 that $D^*(7) = D(7) = 2$. The following collections

© American Mathematical Society 1972

409

Received by the editors April 22, 1971.

AMS 1970 subject classifications. Primary 05B05, 05B25; Secondary 62K10.

Key words and phrases. Steiner triple systems, balanced incomplete block designs. ¹ Aspirant du Fonds National belge de la Recherche Scientifique.

 $\begin{aligned} \mathcal{S} &= \{\{a, b, c\}, \{c, d, e\}, \{e, f, a\}, \{a, d, g\}, \{b, e, g\}, \{c, f, g\}, \{b, d, f\}\}, \\ \mathcal{S}' &= \{\{a, b, e\}, \{b, c, f\}, \{c, d, a\}, \{d, e, f\}, \{f, g, a\}, \{b, d, g\}, \{c, e, g\}\}. \end{aligned}$

The same year (1850), Kirkman [12] proved that $D^*(9) = D(9) = 7$. This result was "discovered" again by Sylvester ([18], [19]) in 1861, Walecki in 1883 (see Lucas [14, 161–197]), Bays [4] in 1917 and finally Emch [9] in 1929 (for more historical details, see Ahrens [1, 110–113]). The simplest description of 7 pairwise disjoint S(9) on the set $\{a, b, c, d, e, f, g, h, i\}$ is given by the following square arrays

а	b	С		a	b	d		d	е	g		g	h	а
d	е	f		е	f	g		h	i	а		b	с	d
g	h	i		h	i	с		b	с	f		е	f	i
		g	а	b		а	d	е		d	g	h		
		с	d	е		f	g	h		i	а	b		
		f	h	i		i	b	С		с	е	f		

The 12 lines of each system are simply the 3 rows, the 3 columns and the 6 products involved in the expansion of the "determinant" of each array.

The other values of $D^*(v)$ and D(v) are unknown. Besides a few isolated lower bounds such as $D(13) \ge 3$, $D(15) \ge 2$ (Kirkman [13]), $D(31) \ge 6$ (Assmus and Mattson ([2], [3])), the only known general results are $D^*(2^n-1) \ge 2$ for every odd integer $n \ge 3$ (Assmus and Mattson [2]) and $D^*(6t+1) \ge 2$ for every t > 0: indeed, as was shown by Rosa [16] and Di Paola [7], it is not difficult to construct two disjoint and isomorphic cyclic STS of order 6t+1 (an S(v) is called cyclic if one of its automorphisms is a cycle of length v).

In 1917, Bays [4] conjectured that $D(v) \ge (v-1)/2$ for every $v \equiv 1$ or 3 (mod 6), v > 7. Our first theorem shows that this conjecture is true for every $v \equiv 3 \pmod{6}$, even if D(v) is replaced by $D^*(v)$.

2. A lower bound for $D^*(v)$.

THEOREM 1. For every nonnegative integer t,

 $D^*(6t+3) \ge 4t+1$ if $2t+1 \not\equiv 0 \pmod{3}$,

and

$$D^*(6t+3) \ge 4t-1$$
 if $2t+1 \equiv 0 \pmod{3}$.

PROOF. Let $G = \{1, a, a^2, \dots, a^{2t}\}$ be a multiplicative cyclic group of order 2t+1 and let us consider the Cartesian product $S = G \times \{0, 1, 2\}$. For every $e \in \{0, 1, 2\}$, the subset $G \times \{e\}$ of S will be denoted by G_e and any

410

element (x, e) of G_e by $(x)_e$ or, when there is no danger of confusion, simply by x_e .

The set \mathscr{S} consisting of (i) all subsets $\{x_0, x_1, x_2\}$ of S for any $x \in G$, (ii) all subsets $\{x_0, y_0, z_1\}$, $\{x_1, y_1, z_2\}$, $\{x_2, y_2, z_0\}$ of S for any $x, y, z \in G$, where $x \neq y$ and $xy = z^2$, is easily verified to be an STS of order 6t+3; this construction is essentially due to Bose [5].

(a) Let $\varphi_0, \varphi_1, \dots, \varphi_{2t}$ be 2t+1 permutations of the set S defined as follows: for every $x \in G$ and every $i=0, 1, \dots, 2t$,

$$\varphi_i(x_0) = x_0, \quad \varphi_i(x_1) = (a^i x)_1, \quad \varphi_i(x_2) = (a^{2t-i} x)_2.$$

Let \mathscr{S}_i be the STS whose lines are the images of the lines of \mathscr{S} by the permutation φ_i . The systems $\mathscr{S}_0, \mathscr{S}_1, \dots, \mathscr{S}_{2t}$ obtained in this way are clearly isomorphic; we are going to prove that they are also pairwise disjoint.

Let \mathscr{S}_i , \mathscr{S}_j be any two of the above systems, with $i \neq j$ $(i, j=0, 1, \cdots, 2t)$.

Any line of \mathscr{S}_i having a point in G_0 , G_1 and G_2 is of the form $\{x_0, (a^i x)_1, (a^{2t-i} x)_2\}$; in \mathscr{S}_j , such a line is $\{x'_0, (a^j x')_1, (a^{2t-j} x')_2\}$. If these lines coincide, we must have

$$x = x', a^i x = a^j x', a^{2t-i} x = a^{2t-j} x'$$

which implies $a^i = a^j$, a contradiction since $i \neq j$.

Any line of \mathscr{S}_i having two points in G_0 is of the form $\{x_0, y_0, (a^i z)_1\}$ where $z^2 = xy$; in \mathscr{S}_j , such a line is $\{x'_0, y'_0, (a^j z')_1\}$ where $z'^2 = x'y'$. If they coincide, we have either

$$x = x', \qquad x = y',$$

$$y = y', \quad \text{or} \quad y = x',$$

$$a^{i}z = a^{j}z', \qquad a^{i}z = a^{j}z'.$$

As G is abelian of odd order, we find in both cases $a^i = a^j$, a contradiction.

By similar straightforward computations, one can easily check that no line of \mathscr{S}_i having two points in G_1 or G_2 can coincide with a line of \mathscr{S}_j and therefore \mathscr{S}_i and \mathscr{S}_j are disjoint.

(b) Let σ be the permutation of S defined by $\sigma(x_0) = x_2$, $\sigma(x_1) = x_1$ and $\sigma(x_2) = x_0$ for every $x \in G$. Let \mathscr{S}'_i $(i=0, 1, \dots, 2t)$ be the STS whose lines are the images of the lines of \mathscr{S}_i by the permutation σ . It is clear that $\mathscr{S}_0, \mathscr{S}_1, \dots, \mathscr{S}_{2t}, \mathscr{S}'_0, \mathscr{S}'_1, \dots, \mathscr{S}'_{2t}$ are isomorphic and that $\mathscr{S}'_0, \mathscr{S}'_1, \dots, \mathscr{S}'_{2t}$ are pairwise disjoint.

If a system \mathscr{S}'_i has a line in common with a system \mathscr{S}_j , this line must necessarily have a point in G_0 , G_1 and G_2 . In \mathscr{S}_j , any such line is of the form $\{x_0, (a^j x)_1, (a^{2t-j} x)_2\}$; in \mathscr{S}'_i , it is $\{(a^{2t-i} x')_0, (a^i x')_1, x'_2\}$. If these

1972]

lines coincide, we have

 $x = a^{2t-i}x', \quad a^{j}x = a^{i}x', \quad a^{2t-j}x = x',$

which gives $a^{2t-2i+j}=1$ and $a^{4t-i-j}=1$, that is $a^{3i}=a^{6t}$. Let us exclude the systems \mathscr{S}'_i which may have a line in common with one of the systems \mathscr{S}_0 , $\mathscr{S}_1, \dots, \mathscr{S}_{2t}$. As the number of distinct cube roots of a^{6t} in the group G is three or one according as the order of G is or is not divisible by 3, the number of excluded systems will be three or one, and the theorem follows immediately.

COROLLARY 1. $D^*(v) \ge 2$ for every $v \ge 7$, $v \equiv 1$ or 3 (mod 6).

This follows from Theorem 1 and from Rosa's result mentioned in the introduction.

COROLLARY 2. For every $v \ge 7$, $v \equiv 1$ or 3 (mod 6), there exists a balanced incomplete block design with parameters v, k = 3 and $\lambda = 2$, all of whose blocks are distinct (compare with Theorem 15.4.4 in Hall [10]).

THEOREM 2. For every nonnegative integer t,

$$D^*(6t+1) \ge t/2 \quad \text{if } t \equiv 0 \pmod{2},$$

and

$$D^*(6t+1) \ge t$$
 if $t \not\equiv 0 \pmod{2}$.

PROOF. Let $G = \{1, a, a^2, \dots, a^{2t-1}\}$ be a multiplicative cyclic group of order 2t and let us consider the set $S = (G \times \{0, 1, 2\}) \cup \{\infty\}$ of cardinality 6t+1, where ∞ is a new symbol. For every $e \in \{0, 1, 2\}$, the element (x, e) of the subset $G \times (e\}$ will be denoted by $(x)_e$ or, when there is no danger of confusion, by x_e . Finally, let $L = \{1, a, a^2, \dots, a^{t-1}\}$, $R = \{a^t, a^{t+1}, \dots, a^{2t-1}\}$ and let \mathscr{S} be the set consisting of

(i) all subsets $\{x_0, x_1, x_2\}$ of S for any $x \in L$,

(ii) all subsets $\{\infty, x_0, (a^t x)_2\}$, $\{\infty, x_1, (a^t x)_0\}$, $\{\infty, x_2, (a^t x)_1\}$ of S for any $x \in L$,

(iii) all subsets $\{x_0, y_0, z_1\}$, $\{x_1, y_1, z_2\}$, $\{x_2, y_2, z_0\}$ of S for any x, $y \in G$ with $x \neq y$ and

(1) $z \in L$ and $z^2 = xy$ if $xy = a^{2j}$,

(2) $z \in R$ and $az^2 = xy$ if $xy = a^{2j+1}$.

It is not difficult to verify that \mathscr{S} is an STS of order 6t+1; this construction is due to Skolem [17].

Let $\varphi_0, \varphi_1, \dots, \varphi_{t-1}$ be t permutations of the set S defined as follows; for every $x \in G$ and every $i=0, 1, \dots, t-1$,

$$\varphi_i(x_0) = x_0,$$
 $\varphi_i(x_1) = (a^i x)_1,$
 $\varphi_i(x_2) = (a^{2t-1-i}x)_2,$ and $\varphi_i(\infty) = \infty.$

Let \mathscr{G}_i be the STS whose lines are the images of the lines of \mathscr{G} by the permutation φ_i . The systems $\mathscr{G}_0, \mathscr{G}_1, \cdots, \mathscr{G}_{t-1}$ are clearly isomorphic. Moreover a proof similar to that of the preceding theorem shows that $\mathscr{G}_0, \mathscr{G}_1, \cdots, \mathscr{G}_{t/2-1}$ are pairwise disjoint if t is even and that $\mathscr{G}_0, \mathscr{G}_1, \cdots, \mathscr{G}_t$ are pairwise disjoint if t is odd. The computations involved in this proof being quite straightforward, they will not be reproduced here.

3. A lower bound for D(v). The two preceding theorems obviously give a lower bound for D(v), since $D^*(v) \leq D(v)$. We want to prove now that this lower bound is not best possible and can be improved in certain cases. For instance, Theorem 2 gives $D(19) \geq 3$; our next result will show that $D(19) \geq 9$.

THEOREM 3. For every $v \ge 7$ with $v \equiv 1$ or 3 (mod 6),

$$D(2v+1) \ge D(v) + 2$$

PROOF. Let D(v) = d and let S, S' be two disjoint sets of cardinality v. We shall denote by $\mathscr{S}_1, \mathscr{S}_2, \dots, \mathscr{S}_d d$ pairwise disjoint STS of order von the set S, and by $\mathscr{S}'_{d+1}, \mathscr{S}'_{d+2}$ two disjoint STS of order v on the set S'(the existence of at least two such systems follows from Corollary 1 and our hypothesis $v \ge 7$).

Let α be any permutation of S consisting of a single cycle of length v and let φ be any bijection from S' onto S. Finally let us consider the set $T=S\cup S'\cup\{\infty\}$ of cardinality 2v+1, where ∞ is a new symbol.

We are going to construct d+2 Steiner triple systems $\mathcal{F}_1, \mathcal{F}_2, \cdots, \mathcal{F}_{d+2}$ on the set T. For every $i=1, 2, \cdots, d$, the lines of \mathcal{F}_i will be

(i) all lines of \mathscr{S}_i ,

(ii) all subsets $\{\infty, x, \alpha^{i-1}(\varphi(x))\}$ of T, where x is any point of S',

(iii) all subsets $\{x, y, \alpha^{i-1}(\varphi(z))\}$, $\{x, \alpha^{i-1}(\varphi(y)), z\}$, $\{\alpha^{i-1}(\varphi(x)), y, z\}$ of T, where $\{x, y, z\}$ is any line of \mathscr{S}'_{d+1} .

For i=d+1 or d+2, the lines of \mathcal{T}_i will be

(i) all lines of \mathscr{G}'_i ,

(ii) all subsets $\{\infty, x, \alpha^{i-1}(\varphi(x))\}$ of T, where x is any point of S',

(iii) all subsets $\{x, \alpha^{i-1}(\varphi(y)), \alpha^{i-1}(\varphi(z))\}, \{\alpha^{i-1}(\varphi(x)), y, \alpha^{i-1}(\varphi(z))\}, \{\alpha^{i-1}(\varphi(x)), \alpha^{i-1}(\varphi(y)), z\}$ of T, where $\{x, y, z\}$ is any line of \mathscr{S}'_{d+1} .

It is easy to check that each \mathcal{T}_i is an S(2v+1) and that $\mathcal{T}_1, \mathcal{T}_2, \cdots, \mathcal{T}_{d+2}$ are pairwise disjoint. This verification is rather tedious and will be omitted here.

COROLLARY 3. For every odd integer $t \ge 1$,

 $D(6t+1) \ge 2t-1.$

JEAN DOYEN

PROOF. If t=1, the result is trivial. If $t=2t'+1\geq 3$, then 6t+1=2(6t'+3)+1 and so, by Theorems 3 and 2,

$$D(6t+1) \ge D(6t'+3) + 2 \ge 4t'+1 = 2t-1.$$

4. Disjoint and isomorphic cyclic Steiner triple systems. Let us denote by $D_c^*(v)$ the maximum number of pairwise disjoint and isomorphic cyclic STS of order v. So for instance $D_c^*(1) = D_c^*(3) = 1$, $D_c^*(7) = 2$ and $D_c^*(9) = 0$. The following result is essentially due to Rosa [16].

The following result is essentially use to Rosa

THEOREM 4. For every positive integer t,

$$D_c^*(6t+1) \ge 2.$$

PROOF. Peltesohn [15] has established the existence of a cyclic S(v) for every $v \equiv 1$ or 3 (mod 6), except v=9. Let \mathscr{S} be a cyclic S(6t+1) constructed on the set $S=\{0, 1, \dots, 6t\}$ in such a way that the permutation $\alpha = (0, 1, \dots, 6t)$ be an automorphism of \mathscr{S} . The distance d_{ij} of the points *i* and *j* (*i*, *j*=0, 1, \dots , 6*t*) will be defined as

$$d_{ii} = \min\{|i - j|, 6t + 1 - |i - j|\}.$$

For every line $\{i, j, k\}$ of \mathscr{S} , the 3 distances d_{ij} , d_{jk} , d_{ki} are distinct. Indeed, suppose for instance that $d_{ij}=d_{jk}$ and let α_{ij} be the power of α mapping *i* onto *j*. As $d_{ij}=d_{jk}$, α_{ij} maps *j* onto *k* and therefore also *k* onto *i*, otherwise the points *j* and *k* would belong to two distinct lines of \mathscr{S} . We conclude that $d_{ij}=d_{jk}=d_{ki}=(6t+1)/3$, which is clearly impossible.

Let \mathscr{S}' be the STS whose lines are the images of the lines of \mathscr{S} by the involution $\sigma = (0)(1, 6t)(2, 6t-1) \cdots (i, 6t+1-i) \cdots (3t, 3t+1)$. \mathscr{S}' is isomorphic to \mathscr{S} . Moreover \mathscr{S} and \mathscr{S}' are disjoint. Indeed, let $\{i, j, k\}$ (resp. $\{i, j, k'\}$) be the line of \mathscr{S} (resp. \mathscr{S}') containing the points *i* and *j*; it is easily seen that $d_{ik} = d_{jk'}$. Therefore these two lines are distinct, otherwise k = k' and $d_{ik} = d_{jk}$, a contradiction.

REMARK. If \mathscr{S} is any cyclic S(6t+3) constructed on the set $S=\{0, 1, \dots, 6t+2\}$ and admitting the permutation $\alpha = (0, 1, \dots, 6t+2)$ as an automorphism, then \mathscr{S} necessarily contains the lines $\{i, 2t+1+i, 4t+2+i\}$ for every $i=0, \dots, 2t$, and so \mathscr{S} and its image \mathscr{S}' by the permutation $\sigma = (0)(1, 6t+2)(2, 6t+1) \cdots (3t+1, 3t+2)$ are never disjoint.

THEOREM 5. For every positive integer $t \not\equiv 1 \pmod{3}$,

$$D_c^*(6t+3) \ge 4t+1.$$

PROOF. Let \mathscr{S} be the S(6t+3) constructed in the proof of Theorem 1. The permutations π_1 and π_2 of S such that for every $x \in G$

$$\pi_1(x_0) = x_1, \qquad \pi_1(x_1) = x_2, \qquad \pi_1(x_2) = x_0, \pi_2(x_i) = (ax)_i \qquad (i = 0, 1, 2),$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

[April

414

are clearly two automorphisms of \mathscr{S} . Moreover if $2t+1 \not\equiv 0 \pmod{3}$, the permutation $\pi_1 \pi_2$ consists of a single cycle of length 6t+3 and \mathscr{S} is a cyclic STS. The above inequality is then an immediate consequence of Theorem 1.

5. **Open problems.** (1) Given a Steiner triple system \mathscr{S} of order $v \ge 7$ on a set S of cardinality v, is there always another Steiner triple system \mathscr{S}' isomorphic to \mathscr{S} and disjoint from \mathscr{S} ? In other words, is there always a permutation α of S such that the image of any line of \mathscr{S} by α is never a line of \mathscr{S} ?

(2) Is it true that $D_c^*(6t+3) \ge 2$ for every $t \ge 2$?

(3) The lower bounds for D(v) given in this paper can certainly be improved. It is tempting to conjecture that D(v)=v-2 for every $v \ge 9$, $v \equiv 1$ or 3 (mod 6).

(4) Given an integer *n* such that $0 \le n \le v(v-1)/6$, let us denote by D(v, n) the maximum number of STS of order *v* that can be constructed on a set of cardinality *v* in such a way that any two of them have exactly *n* lines in common, these *n* lines being moreover in each of the D(v) systems. It is an easy exercise to check that D(7, 0) = D(7) = 2, D(7, 1) = 3, D(7, 2) = 0, D(7, 3) = 2, D(7, 4) = D(7, 5) = 0, $D(7, 7) = \infty$. Kirkman [12] proved in 1850 that $D(15, 5) \ge 15$, but almost nothing is known in general about the function D(v, n). For example, is it true that $D(v, 1) \ge 2$ for every $v \ge 3$, $v \equiv 1$ or 3 (mod 6)?

References

1. W. Ahrens, Mathematische Unterhaltungen und Spiele. Vol. 2, Teubner, Leipzig, 1918.

2. E. F. Assmus, Jr. and H. F. Mattson, Jr., *Steiner systems and perfect codes*, University of North Carolina Institute of Statistics Mimeo Series, No. 484–1, 1966.

3. ——, Research problem, J. Combinatorial Theory 3 (1967), 307.

4. S. Bays, Une question de Cayley relative au problème des triades de Steiner, Enseignement Math. 19 (1917), 57–67.

5. R. C. Bose, On the construction of balanced incomplete block designs, Ann. Eugenics 9 (1939), 353–399. MR 1, 199.

6. A. Cayley, On the triadic arrangements of seven and fifteen things, London, Edinburgh and Dublin Philos. Mag. and J. Sci. (3) 37 (1850), 50–53 (Collected Mathematical Papers, I, 481–484).

7. J. W. Di Paola, *Steiner triples and totally non-symmetric loops*, Combinatorial Structures and their Applications (Proc. Calgary Internat. Conf., Calgary, Alta., 1969), Gordon and Breach, New York, 1970, pp. 59–61. MR **41** #8260.

8. D. H. Doehlert, Balanced sets of balanced incomplete block designs of block size three, Technometrics 7 (1965), 561–577.

9. A. Emch, Triple and multiple systems, their geometric configurations and groups, Trans. Amer. Math. Soc. 31 (1929), 25-42.

10. M. Hall, Jr., Combinatorial theory, Blaisdell, Waltham, Mass., 1967. MR 37 #80.

11. T. P. Kirkman, On a problem in combinations, Cambridge and Dublin Math. J. 2 (1847), 191-204.

JEAN DOYEN

12. ——, Note on an unanswered prize question, Cambridge and Dublin Math. J. 5 (1850), 255-262.

13. ——, Theorems on combinations, Cambridge and Dublin Math. J. 8 (1853), 38-45.

14. E. Lucas, Récréations mathématiques. Vol. 2, Gauthier-Villars, Paris, 1883.

15. R. Peltesohn, Eine Lösung der beiden Heffterschen Differenzenprobleme, Compositio Math. 6 (1939), 251-257.

16. A. Rosa, A note on cyclic Steiner triple systems, Mat.-Fyz. Časopis Sloven. Akad. Vied 16 (1966), 285–290. (Slovak) MR 35 #2759.

17. Th. Skolem, Some remarks on the triple systems of Steiner, Math. Scand. 6 (1958), 273-280. MR 21 #5582.

18. J. J. Sylvester, *Remark on the tactic of nine elements*, London, Edinburgh and Dublin Philos. Mag. and J. Sci. (4) 22 (1861), 144–147 (Collected Mathematical Papers, II, 286–289).

19. ——, Note on a nine schoolgirls problem, Messenger Math. (2) 22 (1892/93), 159–160; correction, 192 (Collected Mathematical Papers, IV, 732–733).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRUSSELS, 1050 BRUSSELS, BELGIUM