COLLOQUIUM MATHEMATICUM

VOL. XXII 1971 FASC. 2

# SOME REMARKS ON THE NUMBER OF DIFFERENT TRIPLE SYSTEMS OF STEINER

BY

B. ROKOWSKA (WROCŁAW)

**1. Definitions and results.** Let $S$ be a set of $n$ elements. A family $R$ consisting of three-element subsets of $S$ such that every pair of elements of $S$ is contained in exactly one set from $R$ is called a *triple system on* $S$. For the sake of shortness, a triple system will be called simply a *system.*

It is known that a necessary and sufficient condition for the existence of a system is $n \equiv 1$ or $3 \pmod 6$. There is an open question how many non-isomorphic systems exist for a given set $S$. It is known that for $n = 7$ and $n = 9$ there exist one system only, for $n = 13$ exactly 2, for $n = 15$ exactly 80, and for $n > 13$ at least 2.

If for a system $R$ on $S$ and for a system $R_0$ on $S_0$ we have $S_0 \subset S$ and $R_0 \subset R$, then we say that $R_0$ is a *subsystem* of $R$ on $S_0$.

If $S$ can be put in the form

$$S = \bigcup_{i=1}^{p} S_i \qquad (p > 1)$$

with disjoint $S_1, \ldots, S_p$, and $|S_1| = \ldots = |S_p| > 3$, and if on $S_i$ there exists a subsystem $R_i$ of $R$, then we say that $R$ is *decomposed* into subsystems $R_i$ on $S_i$. Otherwise $R$ is called *indecomposable.*

Let $f(n)$ be the number of non-isomorphic systems on $S$, where $|S| = n$. By $f^*(n)$ we denote the number of non-isomorphic systems $R$ on $S$ with $|S| = n$, which satisfy the following condition:

($*$) *$R$ does not contain any subsystem $R_0$ on any $S_0$ with* $|S_0| \equiv 1 \bmod 6$.

Now let $R$ be a system on $S$, where $|S| = d^*$ and let $R^*$ be a system on $S^*$, where $|S^*| = d$. By $P(R, R^*)$ we shall denote a system on $T$, where $|T| = d\cdot d^*$, constructed as follows (cf. [2]):

Arrange elements of $T$ is a matrix

$$(s_{\alpha\beta}) = \begin{pmatrix} 0 & 1 & \ldots & d^*-1 \\ d^* & 1+d^* & \ldots & 2d^*-1 \\ \vdots & \vdots & & \vdots \\ (d-1)d^* & 1+(d-1)d^* & \ldots & dd^*-1 \end{pmatrix}.$$

Denote the rows of the matrix by $S_1, \ldots, S_d$ and the columns by $S_1^*, \ldots, S_d^*$. Constructing on every row system $R$, we get systems $R_1, \ldots, R_d$ on $S_1, \ldots, S_d$. Similarly constructing on every column system $R^*$, we get systems $R_1^*, \ldots, R_{d^*}^*$ on $S_1^*, \ldots, S_{d^*}^*$. Let $B$ be the family of all triples $\{s_{ab}, s_{cd}, s_{ef}\}$ with $a \neq c$ and $b \neq d$, where $e$ and $f$ are such that the triples $\{s_{1b}, s_{1d}, s_{1f}\}$ and $\{s_{a1}, s_{c1}, s_{e1}\}$ belong to $R_1$ and $R_1^*$, respectively.

The family

$$P(R, R^*) = B \cup \bigcup_{i=1}^{d} R_i \cup \bigcup_{j=1}^{d^*} R_j^*$$

is a triple system on $T$ (cf. [2]).

The main result of this paper is the following

THEOREM. *For* $n \equiv 9 \pmod{18}$ *we have*

$$f(n) \geqslant \sum_{d} f(d) f^*\left(\frac{n}{d}\right) + 2,$$

*where $d$ runs over all divisors of $n$ exceeding* 1 *and congruent to unity* mod 6.

The proof of theorem follows immediately from lemmas of section 2 (for the convenience of the reader, proofs of lemmas and theorem are postponed to section 3).

The paper is completed with section 4 containing some remarks on a possibility of strengthening the theorem.

## 2. Lemmas.

LEMMA 1. *Let* $|S| = n$, *where* $n \equiv 3 \pmod 6$. *Then there exists an indecomposable system $R$ on $S$ which satisfies* $(*)$.

LEMMA 2. *Let* $|S| = n$, *where* $n \equiv 9 \pmod{18}$. *Then there exists a system $R$ on $S$ which is decomposable into subsystems $R_i$ on $S_i$ with* $|S_i| = n/3$, *and which satisfies* $(*)$.

LEMMA 3. *The triple system $P(R, R^*)$ is decomposable into subsystems isomorphic to $R^*$ and into subsystems isomorphic to $R$.*

LEMMA 4. *If* $|S| \equiv 1 \pmod 6$, *system $R$ on $S$ satisfies* $(*)$, *and $P(R, R^*)$ contains a subsystem $R_0^*$ on $S_0^*$ with* $|S_0^*| = |S^*|$, *then $R_0^*$ is isomorphic to $R^*$.*

LEMMA 5. *If the system $P(R, R^*)$ on $T$ is isomorphic to $P(\bar{R}, R^*)$ (where both $R$ and $\bar{R}$ are on $S$,* $|S| = d^* = n/d$, *and* $d \equiv 1 \pmod 6$)*, and if $\bar{R}$ satisfies* $(*)$, *then $R$ and $\bar{R}$ are isomorphic.*

LEMMA 6. *If a system $R$ on $S$ satisfies* $(*)$, *then the system $P(R, R^*)$ on $T$ does not contain any subsystem $R_0^*$ on $S_0^*$, where* $|S_0^*| \equiv 1 \pmod 6$ *and* $|S_0^*| > |S^*|$.

## 3. Proofs.

Proof of lemma 1. Let $S = \{0, 1, \ldots, 6k+2\}$. Putting $A_1 = \{0, 1, \ldots, 2k\}$, $A_2 = \{2k+1, \ldots, 4k+1\}$, $A_3 = \{4k+2, \ldots, 6k+2\}$ we shall construct on $S$ three families $B_1, B_2, B_3$ consisting of triples. Namely:

$B_1 = \{\{x, y, z\}: x+y+1 \equiv z \ (\mathrm{mod}(2k+1));\ x \neq y;\ x, y \in A_i$ for some $i$; $z \in A_{(i+1)(\mathrm{mod}\,3)}$; $x, y \not\equiv -1 \ (\mathrm{mod}(2k+1))\}$;

$B_2 = \{\{x, y, z\}: y \equiv -1 \ (\mathrm{mod}(2k+1));\quad z \equiv (2x+1)(\mathrm{mod}(2k+1))$; $x, y \in A_i$ for some $i$; $z \in A_{(i+1)(\mathrm{mod}\,3)}\}$;

$B_3 = \{\{x, x+2k+1, x+4k+2\}: x \in A_1\}$.

First we show that $R = B_1 \cup B_2 \cup B_3$ is a system on $S$. Take $x, y \in A_i$. If $x, y \not\equiv -1 \ (\mathrm{mod}(2k+1))$, then the pair $(x, y)$ lies in a triple from $B_1$ or it lies in a triple from $B_2$. If $x \in A_i$ and, $y \in A_j$ with $i \neq j$, then in the case $x \equiv y \ (\mathrm{mod}(2k+1))$ the pair $(x, y)$ lies in a triple from $B_3$, and in the case $x \not\equiv y \ (\mathrm{mod}(2k+1))$ and $x, y \not\equiv -1 \ (\mathrm{mod}(2k+1))$ it lies in a triple from $B_1$. Finally, if $x \equiv -1 \ (\mathrm{mod}(2k+1))$, then the pair $(x, y)$ lies in a triple from $B_2$ provided $j-i \equiv 1 \ (\mathrm{mod}\ 3)$ or, otherwise, in a triple from $B_1$.

To show that every pair is contained in at most one triple from $R$, it is enough to compute the cardinalities of $B_1, B_2$ and $B_3$. As it is easy to check, $|B_1| = 3k(2k-1)$, $|B_2| = 6k$ and $|B_3| = 2k+1$, whence $|B_1|+|B_2|+|B_3| = |R| = n(n-1)/6$, as needed.

Now we show that system $R$ on $S$ satisfies (*). Let $R_0$ on $S_0$, where $|S_0| \equiv 1 \ (\mathrm{mod}\ 6)$, be a subsystem of $R$. Clearly, $S_0$ can be a subset of no $A_i$ and of no union $A_i \cup A_j$. Thus $|S_0 \cap A_j| \neq 0$ for $j = 1, 2, 3$. Let $|S_0 \cap A_1| = e$, $|S_0 \cap A_2| = f$, $|S_0 \cap A_3| = g$. We shall show that $f \leqslant e \leqslant g \leqslant f$.

Let $x_0 \in A_1 \cap S_0$. Since there are $e-1$ pairs $x_0, x$ with $x_0 \neq x_1 \in A_1 \cap S_0$, we have $e-1$ distinct triples $\{x_0, x, y\} \in R_0$ with $y \in A_2 \cap S_0$. If $y \not\equiv x_0$ $(\mathrm{mod}\ (2k+1))$, $y$ must be an element of such a triple, hence $f = e-1$. And if $y \equiv x_0 \ (\mathrm{mod}(2k+1))$, then $f = e$. Therefore $f \leqslant e$. Proofs of the remaining inequalities are analogous and we come to the equality $e = f = g$.

Hence $S_0$ is divisible by 3 and so $|S_0| \not\equiv 1 \ (\mathrm{mod}\ 6)$. Finally, we shall show that the system $R$ on $S$ is indecomposable. Assume to the contrary that $R$ is decomposed into some subsystems. Let $S_0$ be one of $S_i$'s. From the equality $e = f = g$ we infer that if $x \in A_1 \cap S_0$, then there is an $y \in A_2 \cap S_0$ and a $z \in A_3 \cap S_0$ such that $x \equiv y \equiv z \ (\mathrm{mod}\ (2k+1))$. To focus our attention, we may assume that $S_0$ contains 0. Hence if $x \in A_1 \cap S_0$ and $x \not\equiv -1 \ (\mathrm{mod}(2k+1))$, then $x+1, x+2, \ldots, 2k$ belong to $S_0$ and, consequently, $1, 2, \ldots$ are also in $S_0$. Hence all elements of $S$ are in $S_0$.

Remarks. 1. It is easy to prove that in the case $n \equiv 9 \ (\mathrm{mod}\ 18)$ the system $R$ on $S$ contains a subsystem $R_0$ on $S_0$ for which

$$S_0 = \{a: a \in S \wedge a \equiv 2 (\mathrm{mod} 3)\}.$$

2. If $S = n \equiv 1 \ (\mathrm{mod}\ 6)$, then there exists a system on $S$, which does not contain any subsystem at all. Such are the triple systems constructed by Skolem in [1] for an arbitrary $n$ of this kind.

Proof of lemma 2. Let $S = \{0, 1, \ldots, 18k+8\}$. Putting $A_1 = \{0, 1, \ldots, 6k+2\}$, $A_2 = \{6k+3, \ldots, 12k+5\}$, and $A_3 = \{12k+6, \ldots, 18k+8\}$, we construct two families $B_1$ and $B_2$ of triples of $S$. Namely, set

$$B_1 = \{\{x, y, z\}\colon x+y \equiv 2z\big(\mathrm{mod}(6k+3)\big);\ x, y \in A_i;\ z \in A_{(i+1)(\mathrm{mod}\ 3)};\ x \neq y\},$$
$$B_2 = \{\{x, x+6k+3, x+12k+6\}\colon x \in A_1\}.$$

This is a construction of Skolem [1].

The proof that $R = B_1 \cup B_2$ is a system on $S$ is given in [1]. Now we prove that it is decomposable into subsystems $R_i$ on $S_i$, where $|S_i| = n/3$. Let

$$S_1 = \{a\colon a \in S \wedge a \equiv 0 \pmod 3\},$$
$$S_2 = \{a\colon a \in S \wedge a \equiv 1 \pmod 3\},$$
$$S_3 = \{a\colon a \in S \wedge a \equiv 2 \pmod 3\}.$$

If $\{x, y, z\} \in B_1$ and $x, y \equiv i(\mathrm{mod} 3)$, then $z \equiv i(\mathrm{mod} 3)$. If $\{x, y, z\} \in B_2$ and $x \equiv i(\mathrm{mod} 3)$, then $y$ and $z$ are congruent to $i(\mathrm{mod} 3)$.

Now we show that $R$ satisfies $(*)$. Let $R_0$ on $S_0$ be a subsystem of $R$ such that $S_0 \equiv 1\ (\mathrm{mod} 6)$. It is evident that $|A_k \cap S_0| \neq 0$ for $k = 1, 2, 3$. Let $|S_0 \cap A_1| = e$, $|S_0 \cap A_2| = f$ and $|S_0 \cap A_3| = g$. We show that $f \leqslant e \leqslant g \leqslant f$.

Let $x_0 \in A_1 \cap S_0$. Since there are $e-1$ different pairs $(x_0, x)$, where $x \in A_1 \cap S_0$, $x \neq x_0$, we have $e-1$ different triples $\{x_0, x, y\}$ such that $y \in A_2 \cap S_0$. If every $y \not\equiv x_0\ \big(\mathrm{mod}\ (6k+3)\big)$ is an element of such a triple, then $f = e-1$, and if $y \equiv x_0\ \big(\mathrm{mod}\ (6k+3)\big)$, then $f = e$, whence $f \leqslant e$. Proofs of the remaining inequalities are analogous and in this way we come to the equality $e = f = g$. Hence 3 divides $|S_0|$ and so $|S_0| \not\equiv 1$ (mod 6).

Proof of lemma 3. The proof follows directly from the construction of $P(R, R^*)$ (see section 1).

Proof of lemma 4. Let us construct $P(R, R^*)$ as in 1 with $T = \{0, 1, \ldots, 18k+8\}$. Put $n = |T| = d \cdot d^*$, where $d \equiv 1\ (\mathrm{mod}\ 6)$ and $d > 1$. Assume that a system $R$ on $S$ satisfies $(*)$. The existence of such a system $R$ on $S$ follows from lemmas 1 and 2.

Now let $P(R, R^*)$ contain a subsystem $R_0^*$ on $S_0^*$ with $|S_0^*| = |S^*| = d$. Assuming that there exists an index $i_0$ such that $\varepsilon = |S_{i_0} \cap S_0^*| \geqslant 2$ we have $\varepsilon \geqslant 3$ and this implies that for no $i$ there is $|S_i \cap S_0^*| = 1$. In fact, if $|S_i \cap S_0^*| \neq 0$ and, for some $k$, $\{s_{i_0 1}, s_{i_1 1}, s_{k1}\} \in R_1$, then at least $\varepsilon$ elements from the row $S_k$ belong to $S_0^*$ and $\varepsilon$ elements from the row $S_i$ belong to $S_0^*$. Hence, for some $i$, there is $|S_i \cap S_0^*| = 0$, and for some other $i$, $|S_i \cap S_0^*| \geqslant 3$. Choose an $i$ such that the latter inequality holds and let $S_i \cap S_0^* = S_{i0}$. Clearly, either $|S_{i0}| = 3$ or a system $R_{i0}$ (i.e. subsystem of $R_i$) can be constructed on the set $S_{i0}$. Consequently, $|S_{i0}| \equiv 3\ (\mathrm{mod}\ 6)$.

Thus

$$|S_0^*| = \sum_{i=1}^{d} |S_i \cap S_0^*| \equiv 3 \pmod 6 \not\equiv 1 \pmod 6,$$

contrary to the assumption of lemma 4. Hence $|S_i \cap S_0^*| = 1$ for every $i = 1, \ldots, d$. For any indices $b, d, f$ we have $\{s_{ab}, s_{cd}, s_{ef}\} \epsilon P(R, R^*)$ if and only if $\{s_{a1}, s_{c1}, s_{e1}\} \epsilon R_1^*$. Since $|S_i \cap S_0^*| = 1$, for any $a$ there is exactly one $b = b(a)$ such that $s_{ab} \epsilon S_0^*$ and so the one to one correspondence $s_{a1} \to s_{ab(a)}$ $(1 \leqslant a \leqslant d)$ determines an isomorphism between $R_1^*$ and $R_0^*$.

Proof of lemma 5. Since $P(R, R^*)$ and $P(\bar{R}, R^*)$ are isomorphic, $P(R, R^*)$ can be decomposed into subsystems isomorphic to $\bar{R}$. Let the system $\bar{R}_0$ on $\bar{S}_0$ be one of them.

If, for some $i$, $|S_0 \cap S_i^*| = 1$, then this equality holds for every $i = 1, \ldots, d^*$. Hence, repeating the last part of the preceding proof, we infer that $\bar{R}_0$ and $R$, and so $\bar{R}$ and $R$ are isomorphic in this case.

We now prove that the inequality $|\bar{S}_0 \cap S_i^*| \geqslant 2$ can occur for no $i$. For suppose that it occurs for some $i$. In such a case we infer as in the proof of lemma 4, that for every $i$ either $|\bar{S}_0 \cap S_i^*| \geqslant 3$ or $|\bar{S}_0 \cap S_i^*| = 0$. Now let $\bar{S}_0 \cap S_{i0}^* = S_{i0}^*$.

Hence a system $R_{i0}^*$ (a subsystem of $R_i^*$ and $\bar{R}_0$) can be constructed on the set $S_{i0}^*$. Since $R_{i0}^*$ is a subsystem of the system $\bar{R}_0$, which is isomorphic with $\bar{R}$, and since the only subsystems $R_0$ of $\bar{R}$ are such that $|S_0| \equiv 3 \pmod 6$, $|S_{i0}^*| \equiv 0 \pmod 3$.

Furthermore, since $P(R, R^*)$ can be decomposed into subsystems isomorphic with $\bar{R}$ (let it be $P_1, \ldots, P_d$ on sets $Q_1, \ldots, Q_d$), there exist for each $a \epsilon T$, $i$ and $j$, such that $a \epsilon S_{ij}^*$, where $S_{ij}^* = Q_j \cap S_i^*$. Hence for each $a \epsilon S_i^*$ there exists $j$, such that $a \epsilon S_{ij}^*$ and $S_i^*$ is a union of disjoint sets $S_{ij}^*$. On each of those sets one can construct a subsystem of $P_j$. In view of the isomorphism between $P_j$ and $\bar{R}$, and of the hypothesis of lemma it follows that $|S_{ij}^*| \equiv 3 \pmod 6$, and so that $|S_i^*| = d \equiv 3 \pmod 6$, contrary to the assumption $d \equiv 1 \pmod 6$.

Proof of lemma 6. If, for some $i$, $|S_0^* \cap S_i| = 1$, then this equality holds for every $i = 1, \ldots, d$, and $|S_0^*| = |S^*|$. We now prove that the inequality $|S_0^* \cap S_i| \geqslant 2$ cannot occur for any $i$. In fact, suppose that it occurs for some $i$. Hence, as in the proof of lemma 4, we infer that, or every $i$, either $|S_0^* \cap S_i| \geqslant 3$ or $|S_0^* \cap S_i| = 0$. But if $|S_0^* \cap S_i| \geqslant 3$ for some $i$, then $|S_0^* \cap S_i| \equiv 0 \pmod 3$, whence $|S_0^*| \equiv 0 \pmod 3$.

Proof of the theorem. In virtue of lemmas 1 and 2 there exists a system $R$ on $S$, where $|S| = d^* \equiv 9 \pmod{18}$ satisfying $(*)$. From lemmas 4 and 5 we infer that, having fixed $R$ in $P(R, R^*)$ and letting $R^*$ assume distinct values, we receive for each $d/n$ $(d \equiv 1 \pmod 6)$ so many non-isomorphic systems on a set of cardinality $n$, how many such systems exist on a set of cardinality $d$, i.e. $f(d)$. And having fixed $R^*$ with condition $(*)$ and letting $R$ assume distinct values, we receive so many non-isomorphic systems on a set of cardinality $n$, how many such systems satisfying $(*)$ exist on a set of cardinality $n/d$, i.e. $f^*(n/d)$. Hence $f(n) \geqslant f(d)\cdot f^*(n/d)$. And if, in addition, we let $d$ assume distinct values, then, taking yet lemma 6 into consideration we come to the inequality

$$f(n) \geqslant \sum_d f(d)\cdot f^*(n/d).$$

Lemmas 1, 2 and 3 allow to prove that, besides systems $P(R, R^*)$ constructed in the manner described in 1, there exists on a set of cardinality $n$ at least 2 more systems non-isomorphic to each other and non-isomorphic to any of $P(R, R^*)$. In fact, systems $R$ of lemmas 1 and 2 are evidently non-isomorphic and satisfy $(*)$. From lemma 3 we infer that system $P(R, R^*)$ contains a subsystem isomorphic with $R^*$, and so a subsystem an a set of cardinality $d \equiv 1 \pmod 6$, whence it follows that $P(R, R^*)$ does not satisfy $(*)$. Hence

$$f(n) \geqslant \sum_d f(d)\cdot f^*(n/d)+2.$$

**4. Conjecture.** We conjecture that the estimation given in the theorem can be strengthened considerably to the following $f(n) \geqslant n\cdot \sum_d f(d)\cdot f^*(n/d)$. This conjecture is based upon the following modification of the construction of $P(R, R^*)$ from 1.

Arrange the elements of the set $T$ into the matrix

$$\begin{pmatrix} 0 & 1 & \ldots & d^*-1 \\ d^* & 1+d^* & \ldots & 2d^*-1 \\ \vdots & \vdots & & \vdots \\ (d-1)d^* & 1+(d-1)d^* & \ldots & dd^*-1 \end{pmatrix}.$$

Divide $T$ into subsets $S_i$ and $S_j^*$ as in 1. On sets $S_1$ and $S_1^*$ construct systems $R_1$ and $R_1^*$, respectively, in a way that $R_1$ satisfies $(*)$ otherwise arbitrary. On the other $S_i$'s construct systems as follows: choose some $a$ of them $(0 \leqslant a \leqslant d-1)$ and construct systems on them which satisfy $(*)$ and are all isomorphic to each other, but not isomorphic to the system $R_1$ on $S_1$; on the remaining $S_i$'s construct systems $R_i$ isomorphic to $R_1$.

Similarly, on $S_j^*$'s construct $b$ $(0 \leqslant b \leqslant d^*-1)$ systems $R_j^*$ non-isomorphic to $R_1^*$ and $d^*-b-1$ systems isomorphic to $R_1^*$. Finally add to all those systems the set of triples $B$ from 1. Since $a = 0, 1, \ldots, d-1$ and $b = 0, 1, \ldots, d^*-1$, we obtain $d\cdot d^* = n$ systems $P(R, R^*)$.

To prove the above conjecture one has only to show that all these systems are pairwise non-isomorphic. The author was unable to do this.

## *REFERENCES*

[1] Th. Skolem, *Some remarks on the triple systems of Steiner*, Mathematica Scandinavica 6 (1958), p. 273-280.

[2] E. Witt, *Über Steinersche Systeme*, Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität 12 (1938), p. 265-275.

*Reçu par la Rédaction le 4. 11. 1968*