MATEMATICKO-FYZIKÁLNY ČASOPIS SAV, 16, 3, 1966

POZNÁMKA O CYKLICKÝCH STEINEROVÝCH SYSTÉMOCH TROJÍC

ALEXANDER ROSA, Bratislava

Steinerovým systémom trojíc (SST) rádu n sa nazýva systém $\frac{1}{6}\, n(n-1)$ trojíc utvorených z n daných prvkov tak, že každá z $\frac{1}{2}\, n(n-1)$ možných dvojíc z n prvkov sa nachádza práve v jednej z trojíc systému. Je známe [1], že SST existuje práve vtedy, keď $n \equiv 1$ alebo 3 (mod 6).

Cyklickým SST sa nazýva taký SST, o ktorom platí: ak SST obsahuje trojicu (x, y, z), potom obsahuje aj trojicu $(x+1, y+1, z+1)$, kde sa čísla berú modulo n. V [2] bolo dokázané, že cyklický SST rádu n existuje práve vtedy, keď $n \equiv 1$ alebo 3 (mod 6) s výnimkou $n = 9$ a udaná konštrukcia cyklického SST pre každé takéto n. V tejto poznámke sa podáva iná konštrukcia cyklického SST pre každé prípustné n, pričom sa využívajú kombinatorické výsledky, analogické výsledkom prác [3, 4, 5]. Táto konštrukcia umožňuje zostrojiť istým jednotným spôsobom cyklické SST dvoch príbuzných rádov $6k+3$ a $6k+7$ pre ľubovoľné k s výnimkou $k = 1$.

*

Zavedieme najprv niekoľko definícií.

Def. 1. *Systém k disjunktných dvojíc (p_r, q_r), obsahujúcich čísla $1, 2, \ldots, 2k$ a takých, že $q_r - p_r = r$ pre $r = 1, \ldots, k$, budeme nazývať (A, k)-systémom*(1).

Def. 2. *Systém k disjunktných dvojíc (p_r, q_r), obsahujúcich čísla $1, 2, \ldots, 2k-1, 2k+1$ a takých, že $q_r - p_r = r$ pre $r = 1, \ldots, k$, budeme nazývať (B, k)-systémom.*

Veta 1. *(A, k)-systém existuje práve vtedy, keď $k \equiv 0$ alebo* 1 (mod 4).

Dôkaz pozri v [3].

Veta 2. *(B, k)-systém existuje práve vtedy, keď $k \equiv 2$ alebo* 3 (mod 4).

Dôkaz pozri v [4, 5].

(1) V [3] sa tento systém nazýva 1, + 1 systémom.

Def. 3. *Systém k disjunktných dvojíc (p_r, q_r), obsahujúcich čísla $1, 2, \ldots, k, k+2, k+3, \ldots, 2k+1$ a takých, že $q_r - p_r = r$ pre $r = 1, \ldots, k$, budeme nazývať (C, k)-systémom.*

Def. 4. *Systém k disjunktných dvojíc (p_r, q_r), obsahujúcich čísla $1, 2, \ldots, k, k+2, k+3, \ldots, 2k, 2k+2$ a takých, že $q_r - p_r = r$ pre $r = 1, \ldots, k$, budeme nazývať (D, k)-systémom.*

Označme ešte (A, k)-systém (resp. (B, k)-systém), v ktorom je $p_k = 1$, kvôli stručnosti ako (A^+, k)-systém (resp. (B^+, k)-systém).

Lema 1. *(C, k)-systém existuje práve vtedy, keď existuje $(A^+, k+1)$-systém.*

Dôkaz. Nech je (C, k)-systém tvorený dvojicami (p_r, q_r), $r = 1, \ldots, k$, potom systém dvojíc

$$(1, k+2), (p_r + 1, q_r + 1), r = 1, \ldots, k$$

bude zrejme $(A^+, k+1)$-systémom.

Nech je $(A^+, k+1)$-systém tvorený dvojicami (p_r, q_r), $r = 1, \ldots, k+1$. Daný $(A^+, k+1)$-systém obsahuje dvojicu $(1, k+2)$. Potom systém dvojíc

$$(p_r - 1, q_r - 1), r = 1, \ldots, k$$

bude zrejme (C, k)-systémom.

Lema 2. *(D, k)-systém existuje práve vtedy, keď existuje $(B^+, k+1)$-systém.*

Dôkaz je celkom analogický dôkazu lemy 1.

Veta 3. *(C, k)-systém existuje práve vtedy, keď $k \equiv 0$ alebo $3 \pmod 4$.*

Dôkaz. I. Nutnosť podmienky vyplýva z vety 1 a lemy 1.

II. Nech je $k \equiv 0 \pmod 4$, $k = 4m$. Potom stačí podľa lemy 1 dokázať existenciu $(A^+, 4m+1)$-systému. Takýto $(A^+, 4m+1)$-systém tvoria dvojice:

(1) $(r, 4m + 3 - r)$ pre $r = 1, \ldots, m$;
(2) $(3m + 1, 5m + 2)$;
(3) $(m + r, 3m + 1 - r)$ pre $r = 1, \ldots, m$;
(4) $(3m + 2, 7m + 2)$;
(5) $(4m + 2 + r, 8m + 2 - r)$ pre $r = 1, \ldots, m - 1$;
(6) $(6m + 2, 8m + 2)$;
(7) $(5m + 2 + r, 7m + 2 - r)$ pre $r = 1, \ldots, m - 1$

(pri $m = 1$ sa (5) a (7) vynechajú).

Dvojice (7) dávajú párne rozdiely $2, 4, \ldots, 2m - 2$, dvojica (6) rozdiel $2m$, dvojice (5) rozdiely $2m + 2, 2m + 4, \ldots, 4m - 2$ a dvojica (4) zvyšný párny rozdiel $4m$; dvojice (3) dávajú nepárne rozdiely $1, 3, \ldots, 2m - 1$, dvojica (2) rozdiel $2m + 1$ a dvojice (1) zvyšné nepárne rozdiely $2m + 3, 2m + 5, \ldots, 4m + 1$.

III. Nech je $k \equiv 3 \pmod 4$, $k = 4m - 1$. Potom stačí podľa lemy 1 dokázať existenciu $(A^+, 4m)$-systému. Takýto $(A^+, 4m)$-systém tvoria dvojice:

(1) $(r, 4m + 2 - r)$ pre $r = 1, 2, \ldots, 2m$;
(2) $(2m + 1, 6m)$ a $(4m + 2, 6m + 1)$;
(3) $(4m + 2 + r, 8m + 1 - r)$ pre $r = 1, 2, \ldots, m - 1$;
(4) $(7m + 1, 7m + 2)$;
(5) $(5m + 1 + r, 7m - r)$ pre $r = 1, 2, \ldots, m - 2$;

(pri $m = 1$ sa vynechá (3) a (5), pri $m = 2$ sa vynechá (5)).

Dvojice (1) dávajú všetky párne rozdiely $2, 4, \ldots, 4m$; dvojice (2) dávajú nepárne rozdiely $2m - 1$ a $4m - 1$, dvojica (4) rozdiel 1 a dvojice (3) zvyšné nepárne rozdiely $2m + 1, 2m + 3, \ldots, 4m - 3$.

Tým je veta 3 dokázaná.

Poznámka. $(A^+, 4m)$-systém z časti III. dôkazu vety 3 dostaneme z $(A, 4m)$-systému skonštruovaného v [3], ak v dvojici (p_r, q_r) pre $r = 1, \ldots, k$ namiesto p_r, resp. q_r položíme $2k - q_r + 1$, resp. $2k - p_r + 1$.

Veta 4. *(D, k)-systém existuje práve vtedy, keď $k \equiv 1$ alebo $2 \pmod 4$, $k \neq 1$.*

Dôkaz. I. Nutnosť podmienky vyplýva z lemy 2 a vety 2.

II. Nech je $k \equiv 1 \pmod 4$, $k = 4m + 1$. Potom stačí podľa lemy 2 dokázať existenciu $(B^+, 4m + 2)$-systému. Takýto $(B^+, 4m + 2)$-systém tvoria dvojice:

a) $m = 1$

$(4, 5), (9, 11), (10, 13), (2, 6), (3, 8), (1, 7)$;

b) $m \geqq 2$

(1) $(r, 4m + 4 - r)$ pre $r = 1, 2, \ldots, 2m + 1$;
(2) $(2m + 2, 6m + 3)$;
(3) $(6m + 2, 8m + 5)$;
(4) $(5m + 1 + r, 7m + 4 - r)$ pre $r = 1, \ldots, m$;
(5) $(7m + 4, 7m + 5)$;
(6) $(4m + 3 + r, 8m + 4 - r)$ pre $r = 1, \ldots, m - 2$

(pri $m = 2$ sa (6) vynechá).

Dvojice (1) dávajú všetky párne rozdiely $2, 4, \ldots, 4m + 2$, dvojica (5) dáva rozdiel 1, dvojice (4) rozdiely $3, 5, \ldots, 2m + 1$, dvojica (3) rozdiel $2m + 3$, dvojice (6) rozdiely $2m + 5, 2m + 7, \ldots, 4m - 1$ a dvojica (2) zvyšný nepárny rozdiel $4m + 1$.

Ostáva prípad $m = 0$. Ľahko sa zistí, že neexistuje nijaký $(B^+, 2)$-systém. Existuje totiž jediný $(B, 2)$-systém

$$(1, 2),\ (3, 5),$$

ktorý však nie je $(B^+, 2)$-systémom. Podľa lemy 2 potom neexistuje ani $(D, 1)$-systém.

III. Nech je $k \equiv 2 \pmod 4$, $k = 4m + 2$. Potom stačí podľa lemy 2 dokázať existenciu $(B^+, 4m + 3)$-systému. Takýto $(B^+, 4m + 3)$-systém tvoria dvojice:

a) $m = 0$

$(2, 3), (5, 7), (1, 4)$;

b) $m \geqq 1$

(1) $(r, 4m + 5 - r)$ pre $r = 1, 2, \ldots, 2m + 1$;

(2) $(2m + 2, 6m + 4)$ a $(2m + 3, 6m + 3)$;

(3) $(7m + 4, 7m + 5)$;

(4) $(8m + 5, 8m + 7)$;

(5) $(4m + 5, 6m + 5)$;

(6) $(4m + 5 + r, 8m + 5 - r)$ pre $r = 1, \ldots, m - 1$;

(7) $(5m + 4 + r, 7m + 4 - r)$ pre $r = 1, \ldots, m - 2$

(pri $m = 1$ sa vynechá (5), (6), (7), pri $m = 2$ sa vynechá (7)).

Dvojica (4) dáva rozdiel 2, dvojice (7) rozdiely $4, 6, \ldots, 2m - 2$, dvojica (5) rozdiel $2m$, dvojice (6) rozdiely $2m + 2, 2m + 4, \ldots, 4m - 2$ a dvojice (2) zvyšné párne rozdiely $4m$ a $4m + 2$; dvojica (3) dáva rozdiel 1 a dvojice (1) dávajú ostatné nepárne rozdiely $3, 5, \ldots, 4m + 3$.

Veta 4 je dokázaná.

Veta 5. *Cyklický SST rádu n existuje práve vtedy, keď $n \equiv 1$ alebo $3 \pmod 6$, $n \neq 9$.*

Dôkaz. I. Nech je najprv daných $n = 6k + 1$ prvkov $0, 1, 2, \ldots, 6k$. V tomto prípade existuje vždy (A, k)-systém alebo (B, k)-systém. Nech tento systém tvoria dvojice (p_r, q_r), $r = 1, \ldots, k$. Potom bude zrejme každé z $3k$ čísel $1, 2, \ldots, 3k$ v prípade (A, k)-systému a každé z $3k$ čísel $1, 2, \ldots, 3k - 1, 3k + 1$ v prípade (B, k)-systému obsiahnuté práve raz v systéme trojíc $(r, p_r + k, q_r + k)$, $r = 1, \ldots, k$.

Systém $k(6k + 1)$ trojíc $(x, x + r, x + q_r + k)$, $r = 1, 2, \ldots, k$; $x = 0, 1, \ldots, 6k$, pričom sa čísla v trojiciach berú modulo $6k + 1$, bude potom tvoriť cyklický SST. Skutočne, ľubovoľnú dvojicu z prvkov $0, 1, \ldots, 6k$ možno zapísať jediným spôsobom (a, b) tak, že $a - b \equiv c \pmod{6k + 1}$, pričom $1 \leqq c \leqq 3k$. K ľubovoľnému c existuje teda jediné r tak, že c sa rovná jednému z troch čísel $r, p_r + k, q_r + k$ a k tomuto r jediné x tak, že (a, b) sa zhoduje s dvoma z troch čísel $x, x + r, x + q_r + k$. Cykličnosť tohto SST je zrejmá.

II. Nech je daných $n = 6k + 3$ $(k \neq 1)$ prvkov $0, 1, 2, \ldots, 6k + 2$. V tomto prípade existuje vždy (C, k)-systém alebo (D, k)-systém. Nech tento systém tvoria dvojice (p_r, q_r), $r = 1, \ldots, k$. Potom bude zrejme každé z $3k$ čísel $1, 2, \ldots, 2k, 2k + 2, 2k + 3, \ldots, 3k + 1$ v prípade (C, k)-systému a každé z $3k$ čísel $1, 2, \ldots, 2k, 2k + 2, 2k + 3, \ldots, 3k, 3k + 2$ v prípade (D, k)-systému obsiahnuté práve raz v systéme trojíc $(r, p_r + k, q_r + k)$, $r = 1, \ldots, k$.

Systém $k(6k + 3)$ trojíc $(x, x + r, x + q_r + k)$, $r = 1, \ldots, k$, $x = 0, 1, \ldots, 6k + 2$ a systém $(2k + 1)$ trojíc $(x, x + 2k + 1, x + 4k + 2)$, $x = 0, 1, \ldots, 2k$, pričom sa čísla v trojiciach berú modulo $6k + 3$, budú potom spolu tvoriť cyklický SST. Skutočne, ľubovoľnú dvojicu z prvkov $0, 1, \ldots, 6k + 2$ možno zapísať jediným spôsobom (a, b) tak, že $a - b \equiv c \pmod{6k + 3}$, pričom $1 \leqq c \leqq 3k + 1$. K ľubovoľnému $c \neq 2k + 1$ existuje teda jediné r tak, že c sa rovná jednému z troch čísel $r, p_r + k, q_r + k$ a k tomuto r jediné x tak, že (a, b) sa zhoduje s dvoma z troch čísel $x, x + r, x + q_r + k$, a k $c = 2k + 1$ existuje jediné x tak, že (a, b) sa zhoduje s dvoma z troch čísel $x, x + 2k + 1, x + 4k + 2$. Cykličnosť tohto SST je zrejmá.

III. Nutnosť podmienky $n \equiv 1$ alebo $3 \pmod 6$ je zrejmá. Neexistencia cyklického SST v prípade $k = 1$, $n = 9$ vyplýva napr. z [1], str. 221.

Veta 5 je dokázaná.

Poznámka. Časť I. dôkazu vety 5 vyplýva už aj z prác [3, 4, 5].

Na záver by sme spomenuli v súvislosti s cyklickými SST ešte dve úlohy.

1. Dva cyklické SST toho istého rádu sú rôzne, ak sa líšia aspoň v jednej trojici. Označme počet rôznych cyklických SST rádu n znakom $R(n)$. Ľahko sa zistí, že platí $R(7) = 2$, $R(13) = 4$, $R(15) = 4$, $R(19) = 24$. Pri $n = 6k + 1$ alebo $n = 6k + 3$, $n \neq 9$ platí triviálne $R(n) \geqq 2^k$.

Ak možno čísla $1, 2, \ldots, 3k$ (resp. čísla $1, 2, \ldots, 2k, 2k + 2, 2k + 3, \ldots, 3k + 1$) rozdeliť do k trojíc tak, že v každej trojici je alebo súčet všetkých troch čísel rovný $6k + 1$ (resp. $6k + 3$), alebo súčet niektorých dvoch čísel sa rovná tretiemu (porovnaj [1], str. 224 a [2]), potom nazveme tento systém trojíc (α, k)-systémom (resp. (β, k)-systémom). Označme počet rôznych (α, k)-systémov, resp. počet rôznych (β, k)-systémov ako f_k, resp. g_k.

Ľahko sa zistí, že potom budú platiť rovnosti

$$R(6k + 1) = f_k \,.\, 2^k,$$
$$R(6k + 3) = g_k \,.\, 2^k.$$

Úloha nájsť čísla $R(n)$ sa teda redukuje na úlohu nájsť čísla f_k a g_k.

2. Dva SST toho istého rádu sa nazývajú disjunktné, ak neexistuje trojica obsiahnutá v oboch SST. Označme znakom $\mu(n)$ maximálny počet po dvoch disjunktných SST rádu n. Je známe, že $\mu(7) = 2$, $\mu(9) = 7$, ale vo všeobecnosti nie je o $\mu(n)$ nič známe. Možno preto skúmať špeciálnejšiu úlohu:

Nech $\mu^*(n)$ označuje maximálny počet po dvoch disjunktných cyklických SST rádu n. Ak je $n \equiv 3 \pmod 6$, $n \neq 9$, potom je $\mu^*(n) = 1$ $(\mu^*(9) = 0)$.

Toto tvrdenie vyplýva napríklad z toho, že každý cyklický SST rádu $6k + 3$ musí obsahovať trojicu $(0, 2k + 1, 4k + 2)$. Analogické tvrdenie pre $n \equiv 1 \pmod 6$ neplatí. Tak napríklad $\mu^*(7) = \mu^*(13) = 2$, $\mu^*(19) = 6$. Čo možno povedať všeobecne o $\mu^*(6k + 1)$?

LITERATÚRA

[1] Netto E., *Lehrbuch der Combinatorik*, Zweite Aufl., Berlin 1927. Reprint New York 1958.
[2] Peltesohn R., *Eine Lösung der beiden Heffterschen Differenzenprobleme*, Compositio Math. *6* (1939) 251—257.
[3] Skolem Th., *On certain distributions of integers in pairs with given differences*, Math. Scand. *5* (1957) 57—68.
[4] Skolem Th., *Some remarks on the triple systems of Steiner*, Math. Scand. *6* (1958) 273—280.
[5] O'Keefe E. S., *Verification of a conjecture of Th. Skolem*, Math. Scand. *9* (1961) 80—82.

Došlo 20. 8. 1965.

ČSAV, Matematický ústav Slovenskej akadémie vied, Bratislava

A NOTE ON CYCLIC STEINER TRIPLE SYSTEMS

Alexander Rosa

Summary

A Steiner triple system of order n with elements $1, 2, \ldots, n$ is called cyclic if containing the triple (x, y, z), it contains also the triple $(x + 1, y + 1, z + 1)$ with numbers taken modulo n. In the first part of this note combinatorial results analogous to those in [3, 4, 5] are given. These results are used in the second part of this note for a new construction of a cyclic Steiner triple system of order n for every admissible n, i. e. a new proof of following theorem (proved first in [2]) is given:

Theorem 5. A cyclic Steiner triple system of order n exists if and only if $n \equiv 1$ or $3 \pmod 6$, $n \neq 9$.

The given construction permits to construct cyclic Steiner triple systems of two adjacent orders $6k + 3$ and $6k + 7$ for $k \neq 1$ in a certain uniform manner.

At the end of this note two problems related to cyclic Steiner triple systems are formulated.