O k-posunutiach.

Anton Kotzig, Bratislava.

(Došlo dňa 13. mája 1946.)

Nech sú k, n dané prirodzené čísla, $1 \leq k \leq n$. Vyšetrujme n-rozmerný priestor R_n (ponímaný ako množina všetkých systémov $[x_1, x_2, \ldots, x_n] = \xi$, kde x_i sú t. zv. súradnice bodu ξ). Budeme nazývať k-posunutím také posunutie v priestore R_n, pri ktorom sa zmení najmenej jedna a najviac k súradníc, ktoré sa zmenšia o celé čísla a ostatné súradnice zostanú bez zmeny. Nech je ďalej M množina všetkých bodov, ktorých všetky súradnice sú celé nezáporné čísla, potom platí veta:

Existuje jedna a len jedna množina A, ktorá má tieto tri vlastnosti:

1. $A \subset M$.

2. Ak je $\xi \in M - A$, existuje k-posunutie, ktoré prevádza bod ξ v bod množiny A.

3. Ak je $\xi \in A$ a ak je η bod, vznikajúci z ξ k-posunutím, neleží η v množine A.

Množina A je potom definovaná takto: Nech je $\xi = [x_1, x_2, \ldots, x_n]$ bod o celých nezáporných súradniciach. Rozviňme súradnice v dyadickéj sústave

$$x_i = \sum_{m=0}^{\infty} b_m(x_i)\, 2^m \quad (i = 1, 2, \ldots, n).$$

($b_m(x_i) = 0$ alebo $= 1$, pre každé i je ovšem maximálne konečný počet čísel $b_m(x_i)$ rôzny od nuly). Potom bod ξ patrí do množiny A vtedy a len vtedy, ak je

$$b_m(x_1) + b_m(x_2) + \ldots + b_m(x_n) \equiv 0 \pmod{k+1} \qquad (*)$$

pre každé celé $m \geq 0$.

Def.: Ak bod α ($\alpha \in M$) určitým k-posunutím prejde v bod α', budeme hovoriť, že bod α je počiatočný, α' výsledný bod tohoto k-posunutia. Ak prevedieme postupne viac (napr. s) k-posunutí tak, že výsledný bod jednoho k-posunutia považujeme za počiatočný bod ďalšieho k-posunutia, jednotlivé polohy bodu bude nám udávať postupnosť bodov: $\alpha_0, \alpha_1, \ldots, \alpha_s$. Takejto postupnosti budeme hovoriť *k*-reťaz z bodu α_0.

Dôkaz vety: Dokážeme teraz, že existuje maximálne jedna množina majúca vlastnosti 1., 2., 3.

Dôkaz: Predpokladajme, že existujú dve také množiny A, B, ktoré majú vlastnosti 1., 2., 3. Aby $A \neq B$, musí existovať aspoň jeden bod taký, že je elementom len jednej z týchto množín. Bez újmy všeobecnosti môžeme predpokladať, že existuje bod β_0, o ktorom platí: $\beta_0 \in B$, a zároveň β_0 neleží v A. Skonštruujme k-reťaz z bodu β_0 týmto spôsobom: Prvé k-posunutie preveďme tak, aby platilo $\beta_1 \in A$ (je to možné na základe vlastnosti 2., lebo β_0 neleží v A). Na základe vlastnosti 3. však potom platí: β_1 neleží v B. Môžeme tedy druhé k-posunutie voliť tak, aby $\beta_2 \in B$; na základe vlastnosti 3. bude platiť: β_2 neleží v A a tretie k-posunutie možno voliť tak, aby platilo: $\beta_3 \in A$ neleží v B, atď. Týmto spôsobom docielime toho, že o bodoch tejto k-reťazi bude platiť:

$$\left.\begin{array}{l} \beta_{2l} \in B; \quad \beta_{2l} \text{ neleží v } A \\ \beta_{2l+1} \in A; \ \beta_{2l+1} \text{ neleží v } B \end{array}\right\} \text{ pre všetky } l = 0, 1, 2, \ldots$$

Uvážme, že každým k-posunutím sa najmenej jedna súradnica umenší. Je zrejmé, že pre nejaké j bude najmenej jedná súradnica bodu β_j záporná. Ale to nie je možné, lebo musí byť $\beta_j \in M$; preto je zrejmé, že nemôžu existovať dve rôzne množiny majúce vlastnosti 1., 2., 3. (Že nemôže existovať viac takých množín, je z dôkazu tiež zrejmé.)

Ide ešte o dôkaz, že množina definovaná podmienkami (*) má vlastnosti 1., 2., 3.:

Každé celé nezáporné číslo x dá sa rozvinúť v dvojkovej (dyadickej) sústave, pri čom budeme stále užívať označenia

$$x = \sum_{m=0}^{\infty} b_m(x)\, 2^m \quad (b_m(x) = 0, \text{ alebo } = 1).^{1)} \tag{1}$$

Ak je daná ľubovolná skupina A, skladajúca sa z celých nezáporných čísel

$$a_1, a_2, \ldots, a_p,^{2)} \tag{2}$$

---

[1]) Pre každé také x je ovšem opäť maximálne konečný počet čísel $b_m(x)$ rôzny od nuly.

[2]) Tieto čísla $a_1, \ldots, a_p$ nemusia byť navzájom rôzne, bude záležať na tom, koľkokrát sa každé z nich v tej skupine vyskytuje. Naproti tomu nám nebude záležať na tom, v jakom poriadku sú čísla $a_1, a_2, \ldots, a_p$ napísané. Teda napr.: 2, 2, 0, 7, 7, 2 bude tá istá skupina ako 0, 2, 7, 2, 7, 2, ale iná než 2, 0, 7, alebo 2, 2, 2, 0, 7. Ačkoľvek teda „skupina" (užívam úmyselne tohoto neutrálneho slova) je niečo trochu iného než „množina", budeme užívať symboliky obvyklej z teorie množín: Keď je A skupina $a_1, \ldots, a_p$, ak je B skupina $b_1, \ldots, b_q$ a ak označíme C skupinu $a_1, \ldots, a_p, b_1, \ldots, b_q$, budeme písať $C = A + B$, $B = C - A$, $A \subset C$ (A je „časťou" C), $a_1 \in A$, $a_2 \in A, \ldots, a_p \in A$ (a_i je „prvkom" skupiny A) atď. Nedorozumenie je iste vylúčené.

budeme znakom $\sigma_m(A)$ označovať zbytok čísla

$$b_m(a_1) + b_m(a_2) + \ldots + b_m(a_p) = \sum_{x \in A} b_m(x)^{3)} \tag{3}$$

podľa modulu $k + 1$, takže $0 \leq \sigma_m(A) \leq k$.

Nech je teraz S_0 ľubovolná skupina n celých nezáporných čísel

$$x_1, x_2, \ldots, x_n. \tag{4}$$

Budem hovoriť, že skupina T_0 celých nezáporných čísel

$$y_1, y_2, \ldots, y_n \tag{5}$$

vzniká z S_0 k-posunutím, ak je $y_p \leq x_p$ pre $p = 1, 2, \ldots, n$ a ak nerovnosť $y_p < x_p$ platí najmenej pre jednu a najviac pre k hodnôt p.

Ak skupina (4) splňuje rovnice

$$\sigma_m(S_0) = 0 \quad \text{pre } m = 1, 2, 3, \ldots \tag{6}$$

a ak skupina (5) (označme ju T_0) vzniká k-posunutím z S_0, nemôžu byť splnené všetky rovnice

$$\sigma_m(T_0) = 0 \quad (m = 1, 2, 3, \ldots). \tag{7}$$

Lebo nech je m_0 najväčšia hodnota m taká, že je $b_m(y_p) < b_m(x_p)$ aspoň pre jedno p $(1 \leq p \leq n)$. Zo vzťahov $y_q \leq x_q$, $b_m(y_q) = b_m(x_q)$, platných pre $m > m_0$, $q = 1, 2, \ldots, n$ plynie, že je nutne $b_{m_0}(y_q) \leq b_{m_0}(x_q)$ pre $q = 1, 2, \ldots, n$, takže $\sum_{y \in T_0} b_{m_0}(y)$ je menšie než $\sum_{x \in S_0} b_{m_0}(x)$ aspoň o 1 a najviac o k. Nakoľko $\sigma_{m_0}(S_0) = 0$, nemôže byť $\sigma_{m_0}(T_0) = 0$.

Aby sme dokázali základnú vetu, stačí teda, keď dokážeme ešte toto:

Nech je daná skupina (4) celých nezáporných čísel — označme ju S_0, ktorá nesplňuje všetky rovnice (6). Potom existuje skupina T_0, vznikajúca z S_0 k-posunutím a taká, že platia všetky rovnice (7).

Dôkaz: Budeme definovať celé číslo $\pi > 0$, skupiny

$$S_\pi \subset S_{\pi-1} \subset \ldots \subset S_1 \subset S_0, \tag{8}$$

$$P_i = S_{i-1} - S_i \quad (i = 1, 2, \ldots, \pi) \tag{9}$$

celé čísla

$$m_1 > m_2 > \ldots > m_\pi > m_{\pi+1} = -1.^{4)} \tag{10}$$

a celé kladné čísla

$$\overset{0}{\sigma}_{m_1}, \overset{1}{\sigma}_{m_2}, \ldots, \overset{\pi-1}{\sigma}_{m_\pi} \tag{11}$$

spôsobom, ktorý teraz popíšeme.

---

[3]) Smysel symbolu je jasný. Obecne, ak je A skupina $a_1, a_2, \ldots, a_p$ a ak je $f(x)$ ľubovolná funkcia, značí symbol $\sum_{x \in A} f(x)$ číslo $f(a_1) + f(a_2) + \ldots + f(a_p)$.

[4]) Číslo $m_{\pi+1}$ zavádzam len pre pohodlie.

Z (8), (9) plynie, že

$$S_0 = P_1 + P_2 + \ldots + P_i + S_i \quad (i = 1, 2, \ldots, \pi), \tag{12}$$

obecnejšie

$$S_j = P_{j+1} + \ldots + P_i + S_i \quad (0 \leqq j < i \leqq \pi), \tag{13}$$

špeciálne

$$S_0 = P_1 + P_2 + \ldots + P_\pi + S_\pi. \tag{14}$$

Pre všetky dostatočne veľké m je $b_m(x_p) = 0$, teda $\sigma_m(S_0) = 0$; podľa predpokladu existuje však m_1 také, že

$$\sigma_{m_1}(S_0) > 0. \tag{15}$$

Zvolme za m_1 najväčšie číslo, pre ktoré platí (15). Položme $\sigma_{m_1}(S_0) = \sigma^0_{m_1}$ a z čísel $x_1, x_2, \ldots, x_n$ vyberme $\sigma^0_{m_1}$ čísel

$$x_{1,1}, x_{1,2}, \ldots, x_{1,\sigma^0_{m_1}}, \tag{16}$$

pre ktoré je $b_{m_1}(x) = 1$; čísla (16) nech tvoria skupinu P_1, kladieme potom $S_1 = S_0 - P_1$, takže $P_1 = S_0 - S_1$, $0 < \sigma^0_{m_1} \leqq k$. Predpokladajme, že sme už definovali pre isté $p \geqq 1$ skupiny

$$S_p \subset S_{p-1} \subset \ldots \subset S_0, \tag{17}$$

$$P_i = S_{i-1} - S_i \quad (i = 1, 2, \ldots, p) \tag{18}$$

celé čísla

$$m_1 > m_2 > \ldots > m_p \geqq 0 \tag{19}$$

a celé kladné čísla

$$\sigma^0_{m_1}, \ldots, \sigma^{p-1}_{m_p} \tag{20}$$

tak, že

$$\sigma^0_{m_1} + \ldots + \sigma^{p-1}_{m_p} \leqq k \tag{21}$$

a že každá skupina P_i sa skladá z $\sigma^{i-1}_{m_i}$ čísel; pre $p = 1$ sme to práve učinili.

Skupina $S_p = S_0 - (P_1 + \ldots + P_p)$ sa skladá z $n - \sigma^0_{m_1} - \ldots - \sigma^{p-1}_{m_p} \geqq n - k \geqq 0$ čísel. Ak neexistuje žiadne číslo m, pre ktoré by platilo

$$m_p > m \geqq 0, \; 0 < \sigma_m(S_p) \leqq k - \sum_{i=1}^{p} \sigma^{i-1}_{m_i}, \tag{22}$$

položme $\pi = p$, $m_{p+1} = -1$ a sme s indukciou hotoví. Ak však existuje také číslo m, pre ktoré platí (22) — nech je m_{p+1} najväčšie také číslo m — položme $\sigma_{m_{p+1}}(S_p) = \sigma^p_{m_{p+1}}$, takže podľa (22) je

$$\sigma^p_{m_{p+1}} > 0, \quad \sum_{i=1}^{p+1} \sigma^{i-1}_{m_i} \leqq k.$$

Vyberme ďalej zo skupiny S_p skupinu $\sigma^p_{m_{p+1}}$ čísel

$$x_{p+1,1},\ x_{p+1,2},\ \ldots,\ x_{p+1,\sigma^p_{m_{p+1}}},\tag{23}$$

pre ktoré je $b_{m_{p+1}}(x) = 1$, túto skupinu označme P_{p+1} a položme $S_{p+1} = S_p - P_{p+1}$. Vidíme, že vzťahy (17) až (21) budú teraz platiť s indexom $p + 1$ namiesto p. Nakoľko každá skupina obsahuje aspoň jedno číslo, je vidieť, že sa postup musí najneskoršie po n krokoch zastaviť, takže dospejeme takto k systému s vlastnosťami (8) až (13).

Z toho, ako bol indukčný krok (prvý a $(p + 1)$-ý) prevedený, je zrejmé ešte toto: Predovšetkým je

$$\sigma^0_{m_1} + \sigma^1_{m_2} + \ldots + \sigma^{\pi-1}_{m_\pi} \leqq k,\tag{24}$$

teda istotne

$$1 \leqq \pi \leqq k.$$

Za druhé: P_i sa skladá z $\sigma^{i-1}_{m_i}$ čísel, pri čom pre $x \in P_i$ je $b_{m_i}(x) = 1$, teda $\sigma_{m_i}(P_i) = \sigma^{i-1}_{m_i}$.

Za tretie:

$$\sigma^{i-1}_{m_i} = \sigma_{m_i}(S_{i-1}) \quad (i = 1, 2, \ldots, \pi),\tag{25}$$

takže podľa vlastnosti druhej je

$$\sigma_{m_i}(S_i) = \sigma_{m_i}(S_{i-1} - P_i) = 0 \quad (i = 1, 2, \ldots, \pi).\tag{26}$$

Za štvrté:

$$\sigma_m(S_0) = 0\tag{27}$$

pre $m > m_1$.

Za piate: Pre

$$m_i > m > m_{i+1} \quad (i = 1, 2, \ldots, \pi)$$

neplatí (22), t. j. je

$$\text{buďto } \sigma_m(S_i) = 0, \text{ alebo } \sigma_m(S_i) > k - \sum_{j=1}^{i} \sigma^{j-1}_{m_j}\tag{28}$$

$$(m_i > m > m_{i+1};\ i = 1, 2, \ldots, \pi).$$

Teraz nahradím skupinu S_0 novou skupinou S'_0 (složenou tiež z n celých nezáporných čísel) takto: Skupinu S_π nechám bez zmeny, kdežto čísla každej skupiny P_i $(i = 1, 2, \ldots, \pi)$ zmením takto:

Ak je $x \in P_i$, nahradím číslo x číslom

$$x' = \sum_{\substack{0 \leqq m \leqq m_i \\ m \neq m_\pi, m_{\pi-1}, \ldots, m_{i+1}, m_i}} 2^m + \sum_{m > m_i} b_m(x)\, 2^m.\tag{29}$$

T. j. koeficienty pri 2^m $(m > m_i)$ nechám bez zmeny, koeficienty pri $2^{m_i}, 2^{m_{i+1}}, \ldots, 2^{m_\pi}$ nahradím nulami (vieme, že v x bol koeficient pri 2^{m_i} rovný 1), ostatné koeficienty nahradím jedničkami. Nakoľko prvý súčet v (29) je menší než 2^{m_i}, je $x' < x$. Skupinu čísel x', ktorú takto dostaneme zo skupiny P_i, označme P'_i; položme ešte

$$S'_\pi = S_\pi,\ S'_i = P'_{i+1} + \ldots + P'_\pi + S'_\pi \quad (i = 0, 1, \ldots, \pi - 1). \tag{30}$$

Čísla z S'_0 vznikly teda z čísel skupiny S_0 tak, že sme čísla skupiny $P_1 + P_2 + \ldots + P_\pi$ zmenšili, ostatné nechali bez zmeny.

Je zrejmé toto:

1. Ak je $m > m_1$, je:

$$\sigma_m(S'_0) = \sigma_m(S_0) = 0. \tag{31}$$

2. Ak je $m = m_p$ $(p = 1, 2, \ldots, \pi)$, je podľa (29) $b_{m_p}(x') = 0$ pre $x' \in P'_i$, akonáhle $i \leq p$

t. j.

$$\sigma_{m_p}(P'_1 + P'_2 + \ldots + P'_p) = 0,$$

t. j.

$$\sigma_{m_p}(S'_0) = \sigma_{m_p}(S'_p).$$

Ale pre $x' \in S'_p$, t. j. $x' \in P'_{p+1} + \ldots + P'_\pi + S'_\pi$[5]) je podľa (29) a v dôsledku rovnice $S_\pi = S'_\pi$ zrejme $b_{m_p}(x') = b_{m_p}(x)$,[6]) takže $\sigma_{m_p}(S'_p) = \sigma_{m_p}(S_p) = 0$ [viď (26)].

Teda:

Pre $m = m_p$ $(p = 1, 2, \ldots, \pi)$ je

$$\sigma_{m_p}(S'_0) = 0. \tag{32}$$

3. Ak je $m_p > m > m_{p+1}$ $(p = 1, 2, \ldots, \pi)$, platí toto: keď je $x' \in P'_{p+1} + \ldots + P'_\pi + S'_\pi$, t. j. $x' \in S'_p$, je podľa (29) a v dôsledku rovnice $S_\pi = S'_\pi$ zrejme $b_m(x') = b_m(x)$, tedy

$$\sigma_m(S'_p) = \sigma_m(S_p). \tag{33}$$

Nahradíme konečne čísla skupiny $S'_0 = P'_1 + P'_2 + \ldots + P'_\pi + S'_\pi$ novými číslami, ktoré budú tvoriť novú skupinu S''_0 o n číslach a budú sostrojené takto:

1. Čísla z S'_π necháme bez zmeny.

2. Koeficienty $b_m(x')$ pre $m > m_1$ a práve tak koeficienty $b_{m_1}(x')$, $b_{m_2}(x')$, $\ldots$, $b_{m_\pi}(x')$ nechám bez zmeny pre každé $x' \in S'_0$.

Podľa (31), (32) bude potom

$$\sigma_m(S''_0) = 0 \text{ pre } m > m_1 \text{ a práve tak pre } m = m_1,\ m = m_2, \ldots, m = m_\pi. \tag{34}$$

3. Nech je konečne m číslo, splňujúce nerovnosť $m_p > m > m_{p+1}$ $(1 \leq p \leq \pi)$. Potom zmením koeficienty $b_m(x')$ takto:

[5]) Pre $p = \pi$ odpadne ovšem $P'_{p+1} + \ldots + P'_\pi$, podobne v analogických prípadoch.

[6]) Znakom x značím to číslo z S_p, z ktorého vzniklo číslo x' zmenou, udanou v (29).

I. Buď je $\sigma_m(S_p) = 0$. Potom všetky koeficienty $b_m(x')$ pre všetky $x' \in P'_1 + \ldots + P'_p$ nahradím nulami [u x' boly tieto koeficienty rovné 1, viď (29)], kdežto u všetkých $x' \in P'_{p+1} + \ldots + P'_\pi + S'_\pi = S''_p$ nechám $b_m(x')$ bez zmeny.

Potom bude teda:

$$\sigma_m(S''_0) = \sigma_m(S'_p) = \sigma_m(S_p) = 0 \tag{35}$$

[viď (33)].

II. Alebo neni $\sigma_m(S_p) = 0$. Potom je podľa (28)

$$\sigma_m(S_p) > k - \sum_{j=1}^{p} \sigma_{m_j}^{j-1};$$

nakoľko $\sigma_m(S_p) \leqq k$ a nakoľko platí (24), je istotne

$$k + 1 \leqq \sum_{j=1}^{p} \sigma_{m_j}^{j-1} + \sigma_m(S_p) \leqq 2k. \tag{36}$$

Je

$$\sigma_m(S'_0) \equiv \sum_{x' \in P'_1 + \ldots + P'_p} b_m(x') + \sum_{x' \in P'_{p+1} + \ldots + P'_\pi + S'_\pi} b_m(x') \pmod{(k+1)}. \tag{37}$$

Ale podľa (29) a v dôsledku rovnice $S'_\pi = S_\pi$ je

$$\sum_{x' \in P'_{p+1} + \ldots + P'_\pi + S'_\pi} b_m(x') = \sum_{x \in P_{p+1} + \ldots + P_\pi + S_\pi} b_m(x) \equiv \sigma_m(S_p) \pmod{(k+1)},$$

kdežto prvý súčet v (37) sa skladá zo samých jedničiek. Teda

$$\sigma_m(S'_0) \equiv \sigma_{m_1}^{0} + \ldots + \sigma_{m_p}^{p-1} + \sigma_m(S_p) \pmod{(k+1)}. \tag{38}$$

Nakoľko $0 \leqq \sigma_m(S'_0) \leqq k$, plynie z (36), (38) zrejme

$$\sigma_m(S'_0) + k + 1 = \sum_{j=1}^{p} \sigma_{m_j}^{j-1} + \sigma_m(S_p) < \sum_{j=1}^{p} \sigma_{m_j}^{j-1} + k + 1,$$

t. j.

$$\sigma_m(S_0') < \sum_{j=1}^{p} \sigma_{m_j}^{j-1}. \tag{39}$$

Nakoľko ďalej všetky čísla

$$x' \in P'_1 + P'_2 + \ldots + P'_p$$

(ktorých počet je práve rovný $\sum_{j=1}^{p} \sigma_{m_j}^{j-1}$) majú koeficient $b_m(x') = 1$, môžem tieto koeficienty podľa (39) zmeniť tak, že u $\sigma_m(S'_0)$ týchto čísel $x' \in P'_1 + P'_2 + \ldots + P'_p$ koeficient $b_m(x') = 1$ nahradím nulou, u ostatných čísel $x' \in P'_1 + \ldots + P'_p$ jako aj u všetkých čísel $x' \in S'_p$ nechám $b_m(x')$ bez zmeny. Potom bude zrejme

$$\sigma_m(S''_0) = 0. \tag{40}$$