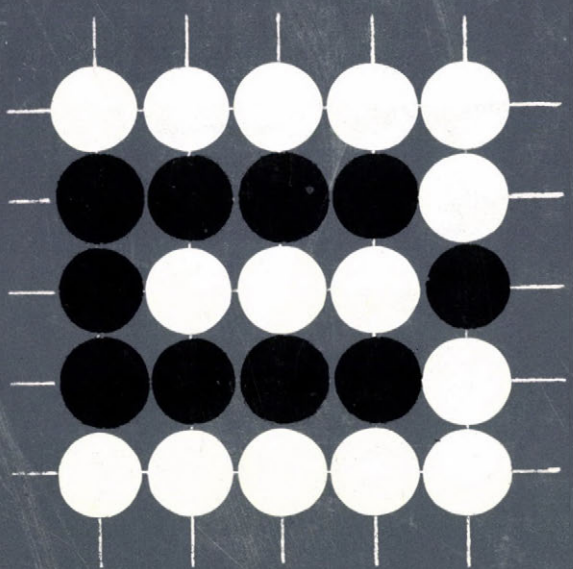
közlemények 16/1976

MTA Számítástechnikai és Automatizálási Kutató Intézet Budapest



MAGYAR TUDOMÁNYOS AKADÉMIA
SZÁMITÁSTECHNIKAI ÉS AUTOMATIZÁLÁSI KUTATÓ INTÉZETE

KÖZLEMÉNYEK

ISBN 963 311 028 9

1976. augusztus

Felelős kiadó:

Dr. Vámos Tibor

igazgató

Technikai szerkesztő:
Solt Jánosné

MTA Számítástechnikai és Automatizálási Kutató Intézete

768214 MTA KESZ Sokszorosító. F. v.: Szabó Gyula

TARTALOMJEGYZÉK

CONTENTS

Proceedings of the Computer and Automation Institute
Hungarian Academy of Sciences

Vol. 16.

СОДЕРЖАНИЕ

Труды Исследовательского Института
Вычислительной Техники и Автоматизации
Венгерской Академии Наук
Выпуск I6.

MTA Számitástechnikai és Automatizálási Kutató Intézete, **Közlemények** 16/1976.

A SZÁMITÓGÉPEK HIERARCHIKUS LAP–TÁROLÁSI ELJÁRÁSAINAK OPTIMALIZÁLÁSÁRÓL

Arató Mátyás

Ahhoz, hogy a számitógépek memória lehetőségeit jól és gyorsan lehessen kihasználni, gyakran alkalmaznak lineáris hierarchikus tárolási eljárásokat. Az ilyen hierarchikus információ–tárolási eljárások esetén meghatározott számu szó alkot egy "lap"–ot. A hierarchia minden szintjén lehetőség van lapok tárolására, és az egyes szinteken belül elhelyezhető lapok száma különböző lehet. Egy futó programban a tárolási helyekre történő hivatkozások minden lépésben kétféle módon történhetnek. Vagy az első szinten elhelyezkedő lapra irányul a hivatkozás, amikor is az elérés közvetlenül megtörténik, vagy egy alsóbb szinten elhelyezkedő lapra, amikor is ezt a lapot automatikusan át kell helyezni az első szintre. Az utóbbi esetben más lapokat alsóbb szintekre kell helyezni. Az alsóbb szinten lévő lapra hivatkozást szokás lapolási hibának (page fault) nevezni. A tárolási eljárás lineárisan hierarchikusnak szokás nevezni, ha a keresett lapot a megtalálási szintről az összes közbenső szinteken keresztül lehet eljuttatni a legelső szintre.

A memória elvi bővitésének lehetőségét először a virtuális memória rendszernek megvalósitása adja (lásd Kilburn [9]), melyet először az ATLAS rendszernél készitettek. A buffer–tárolós memóriákat az IBM 360-as rendszerben alkalmazták. A lapok cserélési eljárásai közül az u.n. megkeresési lapolás (demand paging), amikor is csak akkor van csere a szintek között, ha lapolási hiba fordul elő – a legelterjedtebb. A cserélési algoritmusok közül a következőket emlitjük meg:

1. Az első bekerült kerül ki (FIFO: first in, first out) algoritmus, amely az első szinten legrégebben bennlévő lapot helyezi alacsonyabb szintre lapolási hiba esetén.
2. A legritkábban használt kerül ki (LFU: least frequently used) algoritmus, amely az első szinten – egy bizonyos perióduson belül – legkevesebbszer használt lapot helyezi alacsonyabb szintre lapolási hiba esetén.
3. A legrégebben használt kerül ki (LRU: least recently used) algoritmus, amely az első szinten legrégebben hivatkozott lapot helyezi alacsonyabb szintre lapolási hiba esetén.
4. Optimális algoritmus, amely azt a lapot helyezi az első szintről alacsonyabbra, amelyre a jövőben legkésőbb fognak hivatkozni. Ez utóbbi nyilván használhatatlan a gyakorlatban, mivel a program jövőbeni viselkedését kellene ismerni.
5. Véletlen(RR: random replacement) algoritmus, mely az első szint lapjai közül bármelyiket egyenlő valószinüséggel helyez alsóbb szintre lapolási hiba esetén.

Ebben a cikkben megmutatjuk, hogy bizonyos egyszerü feltevések esetén megadhatók olyan tárolási, illetve cserélési eljárások, amelyek a lapolási hibák átlagos számát minimalizálják. A feladat megoldásánaál a legjelentősebb korlátozás, hogy az egymásutáni hivatkozások függetlenek. Ez a feltevés a gyakorlatban ritkán teljesül, és csak mint durva közelités használható.

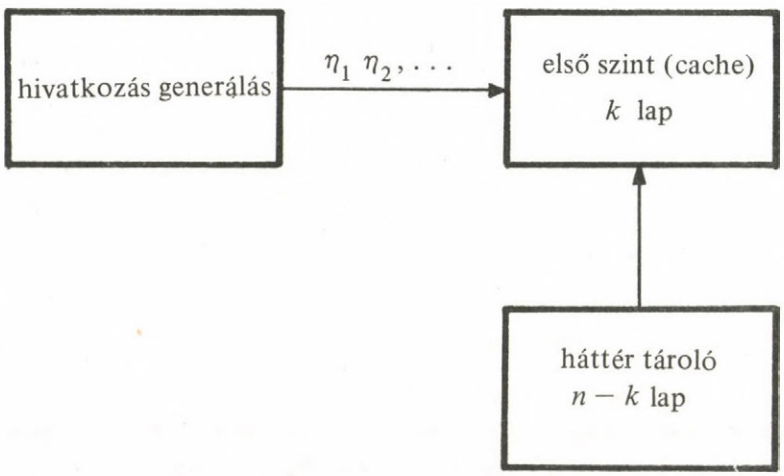
Opderbeck és Chu [11] dolgozatukban a relativ gyakoriságokon alapuló lap–tárolási algoritmust vizsgálják. Ez az algoritmus áll legközelebb a Bayes–féle feltevésen alapuló optimális eljáráshoz, igy nyilvánvaló, hogy szimulációs eredményeik alátámasztják a jelen cikkben bizonyitandó optimális eljárás jóságát. Idézett dolgozatunkban megmutatjuk, hogy az általuk gyakorisági helyettesitési algoritmusnak (PFF: page fault frequency replacement algorithm) nevezett eljárás jobb, mint az LRU (legrégebben használt) algoritmuson alapuló eljárás. Mérési eredményeik egyben azt is igazolják, hogy a lapok független hivására vonatkozó feltevések igen általános feltételek mellett jó közelitésnek tekinthetők.

Megmutatjuk azokat a feltételeket, melyek mellett a megoldás a "kétpisztolyos bandita" (illetve többpisztolyos bandita) problémakör megoldására vezethető vissza. Kitérünk a különböző más feltétel melletti feladat megfogalmazásakor, azok lehetséges megoldásaira és a közelitésekre is.

1.

Mindenekelött egy, a programozás szempontjából elvi jelentőségü feladat megfogalmazásával kezdjük. Multiprogramozásu gép egy programját vizsgálva vetődik fel ezen program két lapja két különböző fokozaton való elhelyezési próblémája. Amennyiben a második fokozaton lévő lapra történő hivatkozás esetén a két lapot azonnal ki kell cserélni, semmilyen optimalizálási feladat nem merül fel. Tegyük fel, hogy lehetőség van mindkét lap első szinten való tartására a hivatkozás befejezéséig, és csak ezután (azaz az ujabb hivatkozás előtt) helyezzük a lapok valamelyikét a második fokozatra.

Az Aho, Denning, Ullman [1] féle kétszintes tárolási eljárás (lásd még: Franaszek, Wagner [5]) esetén, amikor az elérési idők átlagát akarjuk minimalizálni, a fenti megvalósitás reális. Ezért röviden ismertetjük egy ilyen rendszer vázlatát. (1. ábra).



1. ábra Kétszintes tárolás

Az első szint (cache vagy puffer) egy kisebb, de gyors elérésü memória– egység, a második szint (háttér tároló) lassabb elérésü memória– egység. Az $\eta_1, \eta_2, \ldots$ hivatkozási sor generálása a lehetséges $A_1, A_2, \ldots, A_n$ lapokra vonatkozik ($\eta_i = j$, ha az i-edik hivatkozás az A_j lapra történik). Az összes elérés az első szinten történik, ha a hivatkozott lap az első szinten van: az elérési idő T_1 mp., ha a második szinten , akkor előbb az első szintre kell hozni és az elérési idő T_2 mp (általában $T_2 \gg T_1$). Az első szinten egy szabad hely rendszerint rendelkezésre áll az esetleges helyettesités (csere) lebonyolitásához (lásd: Aho, Denning, Ullman [1]). Az itt ismertetett eljárás annyiban uj, hogy a hivatkozás végén kell dönteni a második szintre történő kivitelről (esetleges cseréről).

Visszatérve a két lap esetére az előbbi megfogalmazás alapján jutunk a következő optimalizálási feladatra. Az A_1 és A_2 programrészekre (lapokra) való hivatkozások történjenek függetlenül egymás után, de hivatkozásaik valószinüségeit nem ismerjük. A könnyebb elérésü szint sorszáma legyen 1, a nehezebbé 2. Minden hivatkozás után lehetőség van annak eldöntésére, hogy az A_1 vagy az A_2 programrész kerüljön a könnyebb elérésü helyre. N számu független hivatkozás esetén olyan döntési eljárást kivánunk kidolgozni az A_1 illetve A_2 elhelyezésére, amely minimalizálja a nehezebb elérésü helyre való hivatkozások számát (azaz a lapolási hibák számát). Feltételezzük, hogy az esetleges cserék nem kerülnek költségbe.

Ha az A_1 és A_2 programrészek hivatkozási valószinüségei: p_1 és $1 - p_1$ ismertek, és $p_1 > 1 - p_1$, az A_1 részt kell a könnyebb elérésü 1. helyre helyezni, mivel az 1. helyre történő átlagos hivatkozások száma ekkor Np_1, és az nagyobb, mint az ellenkező elhelyezés esetén. Ha az A_1 és A_2 hivatkozási valószinüségei nem ismertek első közelitésben, feltesszük hogy az egyes programrészekre való hivatkozási valószinüségek p_1 illetve p_2 és $p_1 > p_2$ ismertek ($p_1 + p_2 = 1$, bár ez nem szükséges kikötés), de ismeretlen a hozzárendelés sorrendje.

Jelölje η_t a megfigyelési folyamatot ($t = 1,2, \ldots, N$), lehetséges értékei 1,2 és η_t megadja, hogy a t időpontban az $A_1(\eta_t = 1)$ vagy az $A_2(\eta_t = 2)$ programrészre történt-e hivatkozás.

Az $X_t^{(d)}$ (ahol $d = 1$, ha az A_1 és $d = 2$, ha az A_2 programrész van a 2. (nehezebb) elérésü helyen) valószinüségi változó a d döntés esetén megadja, hogy a t időpontban melyik helyre történt hivatkozás:

$$X_t^{(d)} = \begin{cases} 1 & \text{ha az 1. helyen lévő programrészre történik hivatkozás,} \\ 0 & \text{ha a 2. helyen lévő programrészre történik hivatkozás.} \end{cases}$$

Minden kisérletnél módunkban áll választani (döntést hozni) az előző kisérletek eredményei alapján arról, hogy az $X^{(1)}$ (az A_1 rész kerül a 2. helyre), vagy az $X^{(2)}$ változót figyeljük meg.

Nyilvánvaló hogy

$$X_t^{(d)} = \begin{cases} 0 & \text{ha } \eta_t = d, \\ 1 & \text{ha } \eta_t \neq d. \end{cases}$$

A W valószinüségi változó lehetséges értékei legyenek

1 ha (A_1, A_2) hivási valószinüségei (p_2, p_1),
2 ha (A_1, A_2) hivási valószinüségei (p_1, p_2).

Legyen továbbá az u.n. nem megfigyelhető W komponens apriori eloszlása

$$\boldsymbol{P}(W = 1) = \xi_1, \quad \boldsymbol{P}(W = 2) = \xi_2 = 1 - \xi_1.$$

Feltevéseink szerint tetszőleges t időpontban

$$\begin{aligned} &\boldsymbol{P}\{X_t^{(1)} = 1 \,|W = 1\} = p_1, && \boldsymbol{P}\{X_t^{(1)} = 0|W = 1\} = p_2, \\ &\boldsymbol{P}\{X_t^{(2)} = 1|W = 2\} = p_1, && \boldsymbol{P}\{X_t^{(2)} = 0|W = 2\} = p_2, \\ &\boldsymbol{P}\{X_t^{(1)} = 1|W = 2\} = p_2, && \boldsymbol{P}\{X_t^{(1)} = 0|W = 2\} = p_1, \\ &\boldsymbol{P}\{X_t^{(2)} = 1 \,|W = 1\} = p_2, && \boldsymbol{P}\{X_t^{(2)} = 0|W = 1\} = p_1. \end{aligned}$$

Az optimalizálási feladat megfogalmazása: a $\delta = (d_0, d_1, \ldots, d_{N-1})$ döntési sorozat olyan δ^* megválasztása, melyre

$$E(X_1^{(d_0)} + X_2^{(d_1)} + \ldots + X_N^{(d_{N-1})}) = \max.$$

Hasonló feladat megfogalmazása és megoldása megtalálható DeGroot [2] könyvében (14.7.§), ezt használjuk fel a következő pontban. A dinamikus programozás u.n. Bellman egyenlete segitségével történő megoldást (lásd pl. Prohorov–Rozanov [12] 363.o.) ismertetjük az alábbikaban. Ez a nyereség egy más megfogalmazását igényli. A nyereségfüggvény $V(x)$ definiciója az x megfigyelés esetén a következő:

$$V(x) = \begin{cases} 1 & \text{ha } x = 1, \\ 0 & \text{ha } x = 0. \end{cases}$$

Az optimalizálási feladat a W változó t időpontban adott $\xi(t)$ apriori (vagy a $t-1$ utáni apostreiori) eloszlás estén

$$E_{t,\xi,x} \sum_{s=t}^{N} V(X_s^{(d_{s-1})}) = V(t, \xi(t), X_t = x, \delta^{[t,N]} = (d_{t-1}, \ldots, d_{N-1}))$$

maximalizálása, azaz

$$V(t,\xi(t),x) = \sup_{\delta[t,N]} V(t,\xi(t), X_t = x, \delta^{[t,N]})$$

megadása. Nyilvánvaló, hogy

$$V(N,\xi(N),x) = V(x) \qquad \text{(független a } \xi \text{ eloszlástól)},$$

$$V(N-1),x) = V(x) + \max_{d_{N-1}} \{\boldsymbol{P}(W=1)\,\boldsymbol{P}(X_N^{(d_{N-1})} = 1 \mid W=1)V(N,\xi(N),1) +$$

$$+ \boldsymbol{P}(W=2)\,\boldsymbol{P}(X_N^{(d-1)} = 1 \mid W=2)V(N,\xi(N),1)\},$$

ahol

$$V(N,\xi(N),1) = 1.$$

Az útobbi összefüggés a $d_{N-1} = 1$ esetben a következőt adja

$$V(N-1,\,\xi(N-1),\,x,\,d_{N-1}=1) = V(x) + \{\xi_1(N)p_2 + \xi_2(N)p_1\}$$

mig a $d_{N-1} = 2$ esetben a

$$V(N-1,\,\xi(N-1),\,x,d_{N-1}=2) = V(x) + \{\xi_1(N)p_1 + \xi_2(N)p_2\}$$

adódik. Különbségük (feltevésünk szerint $p_1 > p_2$)

$$\xi_1(N)(p_1-p_2) - \xi_2(N)(p_1-p_2) = (\xi_1(N) - \xi_2(N))(p_1-p_2)$$

alapján a $\xi_1(N) > \xi_2(N)$ esetben $d_{N-1} = 1$, mig a $\xi_1(N) < \xi_2(N)$ esetben a $d_{N-1} = 2$ döntés az optimális. Tehát ebben a lépésben csak a $\xi(N)$ aposteriori eloszlás alapján kell dönteni az eljárás optimalizálásáról. A továbbiakban szükség van a

$$\boldsymbol{P}\{W = 1 \mid X_t^{(d_{t-1})} = x\}$$

valószinüségek meghatározására. A Bayes tétel alapján, (ahol $\boldsymbol{P}\{W=i\}$ jelenti a t időpontbeli apriori valószinüséget)

$$\boldsymbol{P}\{W=1 \mid X_t^{(d_{t-1})} = x\} = \frac{\boldsymbol{P}\{X_t^{(d_{t-1})} = x \mid W=1\}\,\boldsymbol{P}\{W=1\}}{\boldsymbol{P}\{X_t^{(d_{t-1})} = X \mid W=1\}\,\boldsymbol{P}\{W=1\} + \boldsymbol{P}\{X_t^{(d_{t-1})} = x \mid W=2\}\,\boldsymbol{P}\{W=2\}}$$

ahol $\xi_1(1) = \xi_1$ adott, és igy látható, hogy a W változó t-beli aposteriori valószinüsége kifejezhető az apriori valószinüségek segitségével. Az aposteriori valószinüségek segitségével tetszőleges t-re

$$V(t,\xi(t),x) = V(x) + \max_{d_t} \{\xi_1(t+1)\boldsymbol{P}\{X_{t+1}^{(d_t)} = 1 | W = 1\} V(t+1,\xi(t+1),1) + \ldots)$$
$$+ \xi_2(t+1)\boldsymbol{P}\{X_{t+1}^{(d_t)} = 0 | W = 2\} V(t+1,\xi(t+1),0)\} .$$

Innen könnyen leolvasható, hogy az optimális döntési eljárás:

$$d_t = 1 \quad \text{ha} \quad \xi_1(t+1) > \xi_2(t+1),$$
$$d_t = 2 \quad \text{ha} \quad \xi_1(t+1) < \xi_2(t+1).$$

A döntési eljárás tehát az u.n. rövidlátó politika: a t-edik lépésben azt a programrészt (lapot) helyezzük a 2. szintre (nehezebb elérésü helyre), amelynek hivási valószinüsége, aposteriori valószinüsége nagyobb.

2.

Az A_1, A_2, A_3 lapok közül a központi memóriában csak kettő tárolására van lehetőség, a harmadikat háttér tárolóban kell elhelyezni. Feltételezzük, hogy a lapok hivatkozási valószinüségei első közelitésben a következő módon ismeretlenek. A $p_1 > p_2 > p_3$ $(p_1 + p_2 + p_3 = 1)$ valószinüségek ismertek, de számunkra meg nem adott sorrendben vannak hozzárendelve az egyes lapokhoz. Mivel a háttér tárolón lévő lapra történő hivatkozásnál hosszabb adminisztrációs munkára is szükség van, természetesnek tünik minimalizálni N lépés (N hivatkozás) esetén a háttér tárolóban lévő lapra történő hivatkozások átlagos számát.

A programozás technikailag és fizikailag megvalósitható eljárások alapján különböző tipusu feladatok megoldása lehetséges. Ha a d döntés azt jelenti, hogy melyik lap elhelyezése történik a háttér tárolóban ($d = i$, ha A_i kerül a háttér tárolóba, $i = 1,2,3$), akkor elegendő megvizsgálni a háttér tárolóhoz történő hivatkozások száma várható értékének minimumát. Ez a megoldás azonban gyakorlatilag nehezen képzelhető el, mivel azt jelenti, hogy elegendő a lapot a programrész lefutása (a lap felhasználása) után a külső tárolóra visszahelyezni (és ekkor a döntés vonatkozhat bármelyik lapra). Multiprogramozás esetén ez az eljárás használható, mivel a központi memóriában található szabad hely. A valóságban hivatkozás esetén a lapok cseréje azonnal megtörténik. Ennek a feladatnak a megfogalmazásával később foglalkozunk.

Jelölje η_t (lehetséges értékei 1,2,3) a megfigyelhető folyamatot, amelynek értéke a t időpontban megadja, hogy melyik lapra történt hivatkozás.

Legyen $X_t^{(d)}$ az a folyamat, amely megmutatja, hogy a d döntés esetén a központi memóriában vagy a háttér tárolón lévő lapra történt-e hivatkozás. Azaz

$$X_t^{(d)} = \begin{cases} 1 & \text{ha} \quad \eta_t \neq d, \\ 0 & \text{ha} \quad \eta_t = d; \end{cases}$$

Az $X_t^{(d)}$ változókra $(d = 1,2,3)$ vonatkozó kisérleteket úgy kívánjuk elvégezni, azaz a $d_0, d_1, \ldots, d_{N-1}$ sorozatot ugy megválasztani, hogy

$$Z = X_1^{(d_0)} + X_2^{(d_1)} + \ldots + X_N^{(d_{N-1})}$$

várható értéke, $E(Z)$, maximális legyen.

Tegyük fel, hogy a (p_1, p_2, p_3) számhármasnak az (A_1, A_2, A_3) lapokhoz történő hozzárendelése a W valószinüségi változó értékeit jelenti:

	(A_1, A_2, A_3)	
$W = 1,$	$(p_3, p_2, p_1),$	$\boldsymbol{P}(W = 1) = \xi_{11}$
$W = 2,$	$(p_3, p_1, p_2),$	$\boldsymbol{P}(W = 2) = \xi_{22}, \xi_{11} + \xi_{12} = \xi_1,$
$W = 3,$	$(p_2, p_3, p_1),$	$\boldsymbol{P}(W = 3) = \xi_{21},$
$W = 4,$	$(p_1, p_3, p_2),$	$\boldsymbol{P}(W = 4) = \xi_{22}, \xi_{21} + \xi_{22} = \xi_2,$
$W = 5,$	$(p_2, p_1, p_3),$	$\boldsymbol{P}(W = 5) = \xi_{31},$
$W = 6,$	$(p_1, p_2, p_3),$	$\boldsymbol{P}(W = 6) = \xi_{32}, \xi_{31} + \xi_{32} = \xi_3,$

$$\sum_{i,j} \xi_{ij} = \sum_i \xi_i = 1.$$

A $P\{X_t^{(d)} = x, \eta_t = j | W = k\}$ valószinüségek meghatározása azon feltevés alapján történik, hogy tetszőleges t időpontbeli kisérletnél az egyes lapokra történő hivatkozás valószinüsége csak W értékétől függ, és független az előző kisérletek kimenetelétől. Például:

$$\boldsymbol{P}\{X_t^{(1)} = 1, \quad \eta_t = 2 | W = 5\} = p_1,$$
$$\boldsymbol{P}\{X_t^{(1)} = 0, \quad \eta_t = 3 | W = 5\} = 0.$$

Könnyü meghatározni a következő valószinüségeket

$$\boldsymbol{P}\{X_t^{(1)} = 1 | W = 1\} = p_1 + p_2 = 1 - p_3 = \boldsymbol{P}\{X_t^{(1)} = 1 | W = 2\}$$
$$\boldsymbol{P}\{X_t^{(2)} = 1 | W = 3\} = p_1 + p_2 = 1 - p_3 = \boldsymbol{P}\{X_t^{(2)} = 1 | W = 4\}$$
$$\boldsymbol{P}\{X_t^{(3)} = 1 | W = 5\} = p_1 + p_2 = 1 - p_3 = \boldsymbol{P}\{X_t^{(3)} = 1 | W = 6\}$$

A W valószínüségi változó különböző értékei nem függetlenek egymástól, igy az $(X_t^{(d)}, \eta_t)$ megfigyelések W egész aposteriori eloszlását megváltoztatják.

Ha első szinten lévő lapra történik a hivatkozás, az ezen a szinten lévő lapok aposteriori hivatkozási valószinüségei megnőnek és nem kell alsóbb szintüvel felcserélni. Alacsonyabb szinten lévő lapra történő hivatkozás esetén a behivott lap a szükséges hivatkozás után ismét külső tárolóra kerülhet, ha aposteriori hivatkozási valószinüsége nem nőtt eléggé.

A továbbiakban az x kisérleti eredmény (mely megadja, hogy belső vagy külső lapra történt-e hivatkozás) esetén legyen a nyereség a következő

$$V(x) = \begin{cases} 0 & \text{ha} \quad x = 0, \\ 1 & \text{ha} \quad x = 1. \end{cases}$$

Jelölje tetszőleges szekvenciális eljárás esetén M azoknak a hivatkozásoknak a számát (az u.n. "hibás döntések"-nek a számát) a lehetséges N-ből, amelyeknél nem a p_3 valószinüségü lap volt a háttér tárolón. Feltevéseink szerint a megfigyelő nem tudja, hogy melyik $X^{(i)}$ $(i = 1,2,3)$ változóra vonatkozó megfigyelést jelenti a "hibás döntés" (amikor nem a p_3 valószinüségü lap a külső).

M tekinthető a "hibás döntések" számának, mivel az ideális megoldás az lenne, hogy mindig a legkisebb valószinüségü lap legyen a háttér tárolón.

Az előbbi veszteségfüggvény esetén az $E(M)$ várható érték minimalizálása és $E(Z)$ maximalizálása ekvivalens feladat. Ez az optimalizálási feladat speciális esete a következő megfogalmazásu feladatnak.

Legyen ξ a W változó eloszlása. Adott N és ξ esetén jelölje $\tilde{V}_N(\xi)$ az N megfigyelés (hivatkozás) után a különböző döntési eljárásokhoz tartozó lehetséges összegek várható értékének maximumát.

Tekintsük azt az eljárást, amely az első megfigyelést $X_1^{(1)}$ -re (azaz az A_1 lap van háttér tárolon) végzi, majd $N-1$ lépésben optimális. Az $X_1^{(1)}$ megfigyelés után a W változó aposteriori eloszlása $\xi(X_1^{(1)})^*$ és a megmaradó $N-1$ lépésben az összeg maximuma $\tilde{V}_{N-1}(\xi(X_1^{(1)}))$. Ennél az eljárásnál az összeg várható értéke $E(X_1^{(1)} + \tilde{V}_{N-1}(\xi(X^{(1)}))$.

Hasonlóan, ha az első megfigyelés $X_1^{(2)}$ volt (az A_2 lap volt a háttér tárolón) és ezután optimális az eljárás az összeg várható értéke $E(X_1^{(2)} + \tilde{V}_{N-1}(\xi(X_1^{(2)})))$ lesz. Végül az első megfigyelés lehet $X_1^{(3)}$ (az A_3 lap helyezkedik el a háttér tárolón). A $\tilde{V}_N(\xi)$ függvény ki kell elégitse a következő összefüggést

* Ez a valószinüség η_1 értékétől függ, ezt azonban nem jelöljük.

$$\tilde{V}_n(\xi) = \max\{E[X_1^{(1)} + \tilde{V}_{N-1}(\xi(X_1^{(1)}))], E[X_1^{(2)} + \tilde{V}_{N-1}(\xi(X_1^{(2)}))],$$
$$E[X_1^{(3)} + \tilde{V}_{N-1}(\xi(X_1^{(3)}))]\}.$$

Mivel $\tilde{V}_0(\xi) \equiv 0$ a fenti összefüggésből $\tilde{V}_1, \tilde{V}_2, \ldots, \tilde{V}_N$ szukcesszive meghatározható. Más tipusu nyereségfüggvényekre a későbbiekben visszatérünk.

Lemma. *Az $E(M)$ értéket akkor és csak akkor minimalizálja egy szekvenciális eljárás, ha egyben maximalizálja $E(Z)$ értékét.*

Bizonyitás. A bizonyitás hasonlóan végezhető, mint a két lehetséges alternativa esetén (v.ö. DeGroot [2],14.7§1. lemma).

A megfogalmazott feladat optimális döntési eljárása meghatározásához tekintsük ismét Bellman egyenleteit. Adott eloszlás estén nyilvánvalóan teljesülnek a következő összefüggések Legyen

$$V(t,\xi(t),x) = \sup_{\delta[t,N]} V(t,\xi(t),X_t = x,\delta^{[t,N]}) = E_{t,\xi(t),x} \sum_{s=t}^{N} V(X_s^{(d_{s-1})}),$$

akkor

$$V(N,\xi(N),x) = V(x)$$

és

$$V(N-1,\xi(N-1),x) = V(x) + \max_{d_{N-1}} [\xi_{11}(N)\boldsymbol{P}\{X_N^{(d_{N-1})} = 1 | W = 1\} V(N,\xi(N),1) +$$
$$+ \xi_{12}(N)\boldsymbol{P}\{X_N^{(d_{N-1})} = 1 | W = 2\} V(N,\xi(N),1) + \ldots$$
$$+ \xi_{32}(N)\boldsymbol{P}\{X_N^{(d_{N-1})} = 1 | W = 6\} V(N,\xi(N),1)]$$

ahol

$$V(N,\xi(N),1) = 1.$$

Az utóbbi kifejezésre $d_{N-1} = 1$ esetén

$$\tilde{\xi}_1 = V(x) + [\xi_{11}(N)(1-p_3) + \xi_{12}(N)(1-p_3) + \xi_{21}(N)(1-p_2) + \xi_{22}(N)(1-p_1) +$$
$$+ \xi_{32}(N)(1-p_2)],$$

$d_{N-1} = 2$ esetén

$$\tilde{\xi}_2 = V(x) + [\xi_{11}(N)(1-p_2) + \xi_{12}(N)(1-p_1) + \xi_{21}(N)(1-p_3) + \xi_{22}(N)(1-p_3) + \\ + \xi_{31}(N)(1-p_1) + \xi_{32}(N)(1-p_2)],$$

mig $d_{N-1} = 3$ esetén

$$\tilde{\xi}_3 = V(x) + [\xi_{11}(N)(1-p_1) + \xi_{12}(N)(1-p_2) + \xi_{21}(N)(1-p_1) + \xi_{22}(N)(1-p_2) + \\ + \xi_{31}(N)(1-p_3) + \xi_{32}(N)(1-p_3)]$$

adódik.

A $\tilde{\xi}_1 - \tilde{\xi}_2, \tilde{\xi}_1 - \tilde{\xi}_3$ és $\tilde{\xi}_2 - \tilde{\xi}_3$ különbségek a következőképpen irhatók

$$\tilde{\xi}_1 - \tilde{\xi}_2 = (1-p_3)(\xi_1(N) - \xi_2(N)) + (1-p_2)[\xi_{21}(N) + \xi_{31}(N) - \xi_{11}(N) - \xi_{32}(N)] + \\ + (1-p_1)[\xi_{22}(N) + \xi_{32}(N) - \xi_{12}(N) - \xi_{31}(N)]$$

$$\tilde{\xi}_1 - \tilde{\xi}_3 = (1-p_3)(\xi_1(N) - \xi_3(N)) + (1-p_2)[\xi_{21}(N) + \xi_{31}(N) - \xi_{12}(N) - \xi_{22}(N)] + \\ + (1-p_1)[\xi_{22}(N) + \xi_{32}(N) - \xi_{11}(N) - \xi_{21}(N)],$$

$$\tilde{\xi}_2 - \tilde{\xi}_3 = (1-p_3)(\xi_2 - \xi_3) + (1-p_2)[\xi_{12} + \xi_{32} - \xi_{21} - \xi_{11}] + \\ + (1-p_1)[\xi_{11} + \xi_{31} - \xi_{22} - \xi_{12}].$$

A jobboldal első tagja – $\xi_1 > \xi_2$ és $\xi_1 > \xi_3$ esetén – pozitiv, mivel $p_3 < p_2 < p_1$. A többi tag rendszerint elhanyagolható (bár lehetnek negativak is), igy a döntési szabály a ξ_1, ξ_2, ξ_3 mennyiségek alapján hozható.

A Bellman egyenletek általános felirása szintén könnyen megtörténhet:

$$V(t,\xi(t),x) = V(x) + \max_{d_t}[\xi_{11}(t+1)\boldsymbol{P}\{X_{t+1}^{(d_t)} = 1 | W = 1\} V(t+1,\xi(t+1),1) \\ + \ldots + \xi_{32}\boldsymbol{P}\{X_{t+1}^{(d_t)} = 0 | W = 6\} V(t+1,\xi(t+1),0)],$$

ahonnan a döntési eljárás rekurzive leolvasható. Mégpedig a max $(\xi_1(t+1), \xi_2(t+1), \xi_3(t+1))$ aposteriori valószinüség értéke alapján hozunk döntést.

Ha $p_1 = p_2 = \frac{1-\epsilon}{2}$, $p_3 = \epsilon$ (ahol $\epsilon \sim 0$) könnyű megmutatni, hogy

$$\tilde{\xi}_1 - \tilde{\xi}_2 = (1/2 - \frac{3}{2}\epsilon)[\xi_1(N) - \xi_2(N)],$$

$$\tilde{\xi}_1 - \tilde{\xi}_3 = (1/2 - 3/2\epsilon)[\xi_1(N) - \xi_3(N)],$$

$$\tilde{\xi}_2 - \tilde{\xi}_3 = (1/2 - 3/2\epsilon)[\xi_2(N) - \xi_3(N)].$$

Innen közvetlenül adódik, hogy $\tilde{\xi}_j = \max_i \tilde{\xi}_i = \max_i \xi_i = \xi_j$, azaz azt a lapot helyezzük a háttér tárolóra melynek ξ aposteriori valószinüsége maximális.

Az aposteriori valószinüségek meghatározása a Bayes képlet segitségével történik*

$$\boldsymbol{P}\{W = i | X_t^{(d_{t-1})} = x\} = \frac{\boldsymbol{P}\{X_t^{(d_{t-1})} = x | W = i\}\boldsymbol{P}\{W = i\}}{\sum_{j=1}^{6} \boldsymbol{P}\{X_t^{(d_{t-1})} = x | W = j\}\boldsymbol{P}\{W = j\}}$$

ahol $\boldsymbol{P}\{W = j\}$ az aposteriori valószinüséget jelenti. Amint azt már korábban láttuk a $\boldsymbol{P}\{X_t^{(d_{t-1})} = 1 | W = i\}$ valószinüségek megadhatók a p_i értékek segitségével, különben a $\boldsymbol{P}\{X_t^{(d)}, \eta_t | W\}$ valószinüségek meghatározására van szükség.

3.

A döntési eljárás és kisérlet (a lapokra történő hivatkozás) következő megfogalmazása (és egyben a döntési tér megszoritása) jobban megfelel a legtöbb gyakorlati követelménynek is. Ha a második szinten lévő lapra történik hivatkozás, az helyet cserél egy első szinten lévő lappal, mig első szinten lévő lapra történő hivatkozás esetén nem történik csere, csak az aposteriori valószinüségek változnak meg. Legyenek a jelölések továbbra is az előző pontban bevezetettek. A döntési eljárás a következő:

$d_t = d_{t-1}$, nincs változás, ha $X_t^{(d_{t-1})} = 1$, azaz első szinten lévő lapra történt hivatkozás;

$d_t = (d_{t-1} + 1$ vagy $d_{t-1} + 2$, mod 3) ha $X_t^{(d_{t-1})} = 0$, azaz első szintü lap kerül ki, és az a lap, amelyik a második szinten volt, felkerül az első szintre.

Feltételezzük, hogy ξ kezdeti eloszlás esetén a max (ξ_1, ξ_2, ξ_3) valószinüségi lap helyezkedik el a második szinten, azaz $d_0 = i$, ha max $(\xi_1, \xi_2, \xi_3) = \xi_i$.
A döntési tér ilyen megszoritása esetén vizsgáljuk a

$$Z = X_1^{(d_0)} + \ldots + X_N^{(d_{N-1})}$$

hibátlan lapolási hivatkozások számának maximalizálását, adott ξ kezdeti eloszlás esetén.

A Bellman egyenletek ebben az esetben a következők

$$V(N,\xi(N),x) = V(X)$$

* Mivel a teljes megfigyelés η_t, X_t-re vonatkozik a Bayes-féle képletben, szükség van a $P(X_t = i, \eta_t = j | W = k)$ feltételes valószinüségekre. A gyakorlatban csak az X_t folyamat megfigyelése történik, ez a feladat azonban új próblémákat vet fel, melyre itt nem térünk ki.

és

$$V(N-1,\xi(N-1),1) = V(1) + [\xi_{11}(N)\boldsymbol{P}\{X_N^{(d_{N-1})} = 1 | W = 1\} V(N,\xi(N),1) +$$

$$+ \ldots + \xi_{32}(N)\boldsymbol{P}\{X_N^{(d_{N-1})} = 1 | W = 6\} V(N,\xi(N),1)],$$

és $d_{N-1} = d_{N-2}$, illetve

$$V(N-1,\xi(N-1),0) = V(0) + \max_{d_{N-1}} [\xi_{11}(N)\boldsymbol{P}\{X_N^{(d_{N-1})} = 1 | W = 1\} V(N,\xi(N),1) +$$

$$+ \ldots + \xi_{32}\boldsymbol{P}\{X_N^{(d_{N-1})} = 1 | W = 6\} V(N,\xi(N),1)],$$

és $d_{N-1} = (d_{N-2} + 1$ vagy $d_{N-2} + 2$, mod 3), $V(0) = 0$.

A $d_{N-1} = 1$ döntés értéke elsősorban a $\xi_i(N)$ valószinüségek viselkedésétől függ. Ha $d_{N-2} = 3$ volt az előző pontban végzett számitásokhoz hasonlóan kiszámitható, hogy $d_{N-1} = 1$, ha

$$(1-p_3)(\xi_1(N) - \xi_2(N)) + (1-p_2)[\xi_{21}(N) + \xi_{31}(N) - \xi_{11}(N) - \xi_{32}(N)] +$$
$$+ (1-p_1)[\xi_{22}(N) + \xi_{32}(N) - \xi_{12}(N) - \xi_{31}(N)] > 0$$

és $d_{N-1} = 2$ ellenkező esetben. Ebből jó közelitéssel

$$d_{N-1} = \begin{cases} 1 & \text{ha} \quad \xi_1(N) > \xi_2(N), \\ 2 & \text{ha} \quad \xi_1(N) < \xi_2(N), \end{cases}$$

amint az várható volt. Abban a speciális esetben, amikor

$$p_1 = p_2 = \frac{1-\epsilon}{2} \quad \text{és} \quad p_3 = \epsilon(\epsilon \sim 0) \quad \text{a}$$

$$V(N-1,\xi(N-1),0,1) - V(N-1,\xi(N-1),0,2)$$

különbségre pontosan

$$\frac{1}{2}(1-3\epsilon)[\xi_1(N) - \xi_2(N)]$$

adódik és az optimális döntés ξ_1 és ξ_2 összehasonlitásából adódik.

Általánosan felirva a Bellman egyenletet belátható, hogy a lapolási hibák számát az az eljárás minimalizálja, amely az első szinten lévő lapok közül szükség esetén azt a lapot viszi a második szintre, amelyhez tartozó legkisebb hivatkozási valószinüségek aposteriori valószinüsége a legnagyobb.

Az aposteriori valószinüségek kiszámitása az előzőekhez hasonlóan történhet. Erre itt külön nem térünk ki.

A legutóbb megfogalmazott döntési eljárás egy lehetséges módositása a következő (az eljárás realizálása elképzelhető, de a gyakorlatban nem ismert hasonló megoldás):
Ha az első szinten lévő lapra történik hivatkozás a nyereség legyen 1, ha a második szinten lévő lapra történik hivatkozás és csak csere történik egy elsőszintü lappal, a nyereség legyen 0, ha a második szinten lévő lapra történik hivatkozás és a hivatkozás befejezése után szükség van a kivitt csere lappal történő visszacserélésre, a nyereség legyen -1. A $\tilde{V}_N(\xi)$ nyereségre vonatkozó előző pontbeli összefüggések érvényben maradnak, azonban az optimális eljárás nem Z várható értékének maximalizálását jelenti.

4.

Az általános esetben feltételezzük, hogy az $A_1, A_2, \ldots, A_n$ lapok közül az első szinten (a központi memóriában) csak $k < n$ tárolható, a továbbiak a másodikon helyezhetők el. A lapok hivatkozási valószinüségeiről feltételezzük, hogy adottak

$$p_1 > p_2 > \ldots > p_n, \sum_{i=1}^{n} p_i = 1$$

de ismeretlen az egyes lapokhoz való hozzárendelés sorrendje. A W valószinüségei változó $n!$ lehetséges értéke a különböző hozzárendeléseket jelenti, eloszlását jelölje

$$\xi = (\xi_{11}, \ldots, \xi_{1(n-1)!}, \xi_{n1}, \ldots, \xi_{n(n-1)!})$$

A ξ_i valószinüség W olyan értékhez rendelt valószinüséget jelent, amelynél az A_i laphoz a minimális p_n valószinüség tartozik.

Az előbbiekhez hasonlóan a Bayes–féle hozzáállás alapján ismét a második szinten (háttér tárolón) lévő lapokra történő hivatkozások átlagos számát kivánjuk minimalizálni.

A d döntés $\frac{n!}{k!(n-k)!}$ lehetséges különböző értéke a háttér tárolón elhelyezendő lapokra vonatkozik. A döntési tér megszoritása abban áll, hogy a háttér tárolón lévő lapra történő hivatkozás esetén a lap az első szintre kerül s vagy azonnali csere történik, vagy – ez a nehezebben realizálható eljárás – a hivatkozás befejezése után történik valamelyik első szinten lévő lap második szintre helyezése.
Multiprogramozás esetén ez utóbbi eljárás használható, mivel a központi memóriában szabad hely rendelkezésre áll.

Az η_t megfigyelhető folyamat, melynek lehetséges értékei $1,2, \ldots, n$ megadja, melyik lapra történik hivatkozás a t időpontban. Az $X_t^{(d)}$ folyamat megadja, hogy d döntés esetén az első vagy második szinten lévő lapra történik-e hivatkozás.

$$X_t^{(d)} = \begin{cases} 1 & \text{ha} \quad \eta_t \in \text{első szint}, \\ 0 & \text{ha} \quad \eta_t \in \text{második szint}. \end{cases}$$

Feltételezzük, hogy tetszőleges t időpontban az egyes lapokra történő hivatkozás valószinüsége csak W értékétől függ, és független az előző kisérletek kimenetelétől. A W változó értékei függőek, igy az $(X_t^{(d)}, \eta_t)$ megfigyelési sorozat megváltoztatja aposteriori eloszlását.
A feladat olyan $\delta = (d_0, d_1 \ldots, d_{N-1})$ döntési sorozat megválasztása, amely maximalizálja

$$Z = X_1^{(d_0)} + \ldots + X_N^{(d_{N-1})}$$

várható értékét.

A feladat ilyen formában történő megfogalmazása általánositása a 2. és 3. pontokban megfogalmazott feladatnak, ahol $n = 3$ volt. Mivel elég nagy n esetén lényeges eltérés nem tapasztalható a 2. és 3. pontbeli feladat megoldása között, elegendő az egyik feladattal foglalkozni.

Bebizonyitható, hogy jó közelitéssel mindig az a lap kerül (szükség esetén) a második szintre, amelyhez tartozó legkisebb hivatkozási valószinüség valószinüsége a legnagyobb. A W segédváltozó bevezetése, mely megadja, hogy az egyes valószinüségek mely lapokhoz tartoznak, itt is szükség és kezdeti eloszlása a megfigyelések során lényegesen változhat.
A $P\{W | X_1^{(d_0)}, \ldots, X_t^{(d_{t-1})}\}$ aposteriori valószinüségeloszlás viselkedése határozza meg a követendő döntési eljárást. A képletek felirását és a számitásokat mellőzzük, mivel azok az $n = 3$ eset formális általánositásai.

Az eddigiekben tárgyalás során lényeges megszoritás volt, hogy az η_t folyamat (a lapokra történő hivatkozások) egy független valószinüségi változó sorozatot jelentett. Feltételezve η_t-ről markovitást, vagy bizonyos periodicitást, a feladat megfogalmazása csak formálisan válik kezelhetővé. Amint erről az olvasó meggyőződhet Ingargiola és Korsh [8] cikkéből, ahol általános Markov hivatkozás esetén felirják a dinamikus programozásból adódó összefüggéseket, de egyetlen általános elvű megoldást nem sikerül adniok.

A Markov tipusú hivatkozások pedig természetesek, különösen a Denning-féle munkamezőkkel történő programleirás mutatja ennek jelentőségét. A szükséges megfigyelésszám – N – megválasztása a p_i valószinüségektől függ. A gyakorlatban, mivel az optimális eljárás igen bonyolult számitásokat igényel, a következőképpen tanácsos eljárni.
A p_i valószinüségektől függő N megadása után elvégezve az optimális eljárást, felvilágositást kapunk az egyes lapok hivatkozási valószinüségeire is. A nagy számok törvénye alapján, amint ezt több cikkben is teszik (lásd pl. Gyires [7]) ezután a relativ gyakoriságok alapján történik a lapok besorolása a különböző szintekre.

Az optimális és közelitő eljárások összehasonlitását elvégző szimulációs eredmények ismertetésére egy másik dolgozatban kivánunk visszatérni.

Irodalom

[1] Aho, A.V., Denning, P.J., Ullman, J.D., Principles of optimal page replacement. Journ. ACM, 18 (1) 80-93, 1971.

[2] DeGroot, M.H., Optimal Statistical Decisions. McGraw-Hill, 1970.

[3] Denning, P.J., Virtual memory. – Computing Surveys, 2 (3) 153-189, 1970.

[4] Doyle, M.S. and Grahman, J.W., Some parameters affecting performance of paged storage hierarchies. INFOR 13 (2) 197-207, 1975.

[5] Franaszek, P.A., and Wagner, T.J., Some distribution–free aspects of paging algorithm performance. Journ. ACM, 21 (1) 31-39, 1974.

[6] Freiberger, W.F., Grenander, U., Sampson, P.D., Patterns in program references. IBM J. Res. Development, 23-243, May 1975.

[7] Gyires T., A virtuális memóriáról. MTA SzTAKI Közlemények, 15 1975. (s.a.)

[8] Ingargiola, G. and Korsh, J.F., Finding optimal demand paging algorithms. Journ. ACM, 21 (1) 40-53, 1974.

[9] Kilburn, T., Edwards, D., Lanigan, M., Sümner, F., One–level storage system. IEEE Transactions on Electronic Computers, EC-11 (2) 223-235, 1962.

[10] Mattson, R.L. et al., Evaluation techniques for storage hierarchies. IBM Syst. Journ., 9, (2) 78-117, 1970.

[11] Opderbeck, H. and Chu, W.W., Performance of the page fault frequency replacement algorithm in a multiprogramming environment. IFIP Congress, 1974., Inform. Proc. 235-241.

[12] Prohorov, J.V. and Rozanov, J.A., Probability theory (in Russian) Nauka, Moszkva, 1967.

Summary

On optimal performance of page storage hierarchies

M. Arató

The Bayes sequential design is obtained for an optimization problem involving the choice of page replacement. In the most elementary case given are two pages A_1, A_2, request probabilities $p_1 > p_2$ $(p_1 + p_2 = 1)$, a positive integer N and a number ξ. A sequence of N references is to be made and at each stage either A_1 or A_2 is on the second level, the loss being 1 if a page fault occurs (a reference to the second level), 0 otherwise. ξ is the apriori probability that A_1 has the less request probability, p_2. The replacement of one page to the second level occurs after delivering the contents of the demanded page. The reference string is an independent, identically distributed random sequence. The principal result of this paper is a proof of optimality for the sequential procedure which at each stage puts the page to the second level with higher posterior probability of having the smaller request probability p_2. The solution is similar to the solution of "two–armed bandit problem". The general case when the number of pages, $n \geqslant 2$ and the number of pages on the first level, $k(1 \leqslant k < n)$ are given and the apriori probability distribution $\xi = (\xi_1, \ldots, \xi_n)$ of the request probabilities $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_n (\sum_1^n p_i = 1)$ is given the optimal sequential procedure is constructed. Special cases are examined when the solution does not depend on the request probabilities.

The results of the paper give general mathematical foundation of the "least frequency used" and "page fault frequency replacement" algorithms in the case of independent reference string.

Р е з ю м е

Оптимальная процедура для хранения станиц

М. Арато

Рассматривается Байесовская постановка задачи для оптимизации хранения и перестановки страниц в вычислительной машине с виртуальной памятью и с мультипрограммированием. В самой простой постановке задачи предполагается, что имеется две страницы A_1, A_2 с вероятностями обращения $p_1>p_2$ ($p_1+p_2=1$), целое положительное число N и число $0\leq\xi\leq1$. Последовательность N обращений к страницам является независимой и в каждый момент времени или A_1 или A_2 находится на втором уровне памяти /другая на первом/. Если обращение происходит к странице на втором уровне потерь равен 1 и о в другом случае. ξ вероятность что страница A_1 имеет вероятность обращения p_2. Посылка одной из страниц на второй уровень происходит после доставки содержания требуемой страницы.

Главный результат статьи состоит в следующем: оптимальная процедура в каждый момент времени посылает ту страницу на второй уровень памяти которая имеет наибольшую aposteriori вероятность иметь меньшую вероятность обращения p_2. Результаты обобщаются на случай $n(\geq3)$ страниц, где $2\leq k<n$ могут находиться на первом уровне памяти. Рассматриваются специальные случаи когда оптимальное решение не зависит от вероятностей обращения $p_1\geq p_2\geq\ldots\geq p_n$ ($\Sigma p_i=1$).

Результаты статьи дают математическое обоснование ранее разработанных альгоритмов где последовательность обращения является независимой.

MTA Számitástechnikai és Automatizálási Kutató Intézete, **Közlemények** 16/1976.

LINEÁRIS OSZTÁLYOK SZERKEZETE PRIMSZÁM ÉRTÉKÜ LOGIKÁBAN

Bagyinszki János – Demetrovics János

0. Bevezetés

E. Post 1921-ben megoldotta a P_2 kétértékü logika strukturális vizsgálatát [3,4,8]. P_2-vizsgálatánál elvi nehézség nem merült fel, mivel a P_2-ben megszámlálható sok zárt osztály van. A k-értékü logika ($k \geqslant 3$) [1,6] zárt osztályainak tartalmazás szerinti parciális rendezését elvileg nem lehet teljesen leirni, mert a P_k-ban kontinuum sok megszámlálható zárt osztály van [9].

Sz. V. Jablonszkij megadta 1952-ben a P_3 [7], Rosenberg pedig 1965-ben a P_k $k \geqslant 3$ struktura első szintjét [5], vagyis leirták a P_k-beli maximális osztályokat.

Ebben a dolgozatban a P_k strukturáját teljes mélységében vizsgáljuk. Ugy gondoljuk, hogy az elvi nehézségek ellenére a strukturát "majdnem teljesen" le lehet irni. Véleményünk szerint "néhány sokszor" kontinuum sok zárt osztály – amelyek vizsgálatára egyszerü és nem is érdekes – ugy helyezkedik el, hogy a körülöttünk levő osztályokat teljes egészében le lehet irni. Elgondolásainkat a lineáris maximális osztályon illusztráljuk.

A jelen dolgozatban bebizonyitjuk, hogy a primszám-értékü logikában:

a.) Véges sok lineáris zárt osztály van. Ezen osztályok pontos számát is meghatározzuk.
b.) Minden egyes lineáris osztály bázisát és rendjét meghatározzuk. Bebizonyitjuk, hogy minden osztály bázisa véges és a rendje $\leqslant 2$.
c.) Megadjuk a lineáris osztályok strukturáját; maximális és minimális láncainak hosszát.

1. Alapfogalmak, lemmák

Legyen $k \geqslant 2$ egész szám, $E_k = \{0,1, \ldots ,k-1\}$ k-elemü halmaz, s az $E_k x E_k x \ldots x E_k$ n-szeres Descartes-szorzatot jelölje E_k^n, $n \geqslant 1$. Az E_k halmazon definiált n-változós függvények halmazát jelölje $P_k^{(n)} : P_k^{(n)} = \{f | f = f(x_1, x_2, \ldots ,x_n) : E_k^{(n)} \to E_k\}$ $n \geqslant 1$ esetén, és legyen $P_k^{(0)}$ a 0-változós függvények – azaz a konstans függvények halmaza. (Itt "$\to$" egyértelmü leképezést jelöl.)

A $P_k = \bigcup_{n=0}^{\infty} P_k^{(n)}$ halmazt – a benne értelmezett szuperpozició müvelettel együtt – *k-értékü logikának* nevezzük. Ebben a dolgozatban függvényen mindig P_k valamely elemét értjük, p mindig valamely primszámot, a "+" és "·" müveleti jelek pedig a mod k összeadást illetve szorzást jelölik. Az $\tilde{x} = (x_1, x_2, \ldots ,x_n)$ rövid jelölést is gyakran fogjuk használni.

1.1 **Definició.** Legyen $E_0(\tilde{x}) = \{e | e = e_j(\tilde{x}) = x_j, n \geqslant 1,\ 1 \leqslant j \leqslant n\}$ és $P \subseteq P_k$. P halmazon definiált *szuperpozíciók* a következő rekurzive definiált függvények:

1.) minden $f \in P$ szuperpozició P felett;

2.) ha $f_0 = f_0(x_1, x_2, \ldots, x_n)$ szuperpozició P felett és $f_i = f_i(x_{i_1}, x_{i_2}, \ldots, x_{im_i})$ $(i = 1,2, \ldots, n)$ függvények mindegyike vagy P-feletti szuperpozició, vagy $E_0(\tilde{x})$ eleme (azaz $f_i(x_{i_1}, x_{i_2}, \ldots, x_{im_i}) = x_{ij_i}$, $1 \leqslant j_i \leqslant m_i$), akkor az $f_0(f_1, f_2, \ldots, f_n) \in P_k$ is szuperpozició P felett. (A változók az egyes függvényekben nem feltétlenül különbözőek).

3.) az 1.) és 2.) minden P-feletti szuperpozíciót megad.

1.2. **Definició.** A $P \subseteq P_k$ *zárt függvényosztály* a szuperpozicióra nézve, ha $f,g \in P$ esetén bármely $\{f,g\}$ halmaz feletti szuperpozició is eleme P-nek.
A $P \subseteq P_k$ *lezárása*: $[P]$, a P feletti szuperpozíciók összesége. Világos, hogy P pontosan akkor zárt, ha $[P] = P$, továbbá az itt definiált lezárási müvelet algebrai értelemben lezárási operáció, s igy teljesülnek a következő relációk:

$$P \subseteq [P], \quad [[P]] = [P], \quad P' \subset P \Rightarrow [P'] \subseteq [P].$$

1.3. **Definició.** Legyen $P \subseteq P_k$ zárt függvény-osztály, és $P' \subseteq P$. P' *teljes P-ben*, ha $[P'] = P$. P' *bázis P-ben*, ha $[P'] = P$, és bármely $P'' \subset P'$ esetén $[P''] \neq P$.
A $P'' \subseteq P$ zárt függvény osztály *maximális* (*részosztály*) *P-ben*, ha bármely $P' \neq P''$, $P'' \subset P' \subset P \subseteq P_k$ esetén $[P'] = P$.

1.4. **Definició.** Azt mondjuk, hogy az $f(x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n)$ függvény x_i változója *valódi*, ha létezik olyan $\tilde{\alpha}, \tilde{\beta}$ értékpár kombináció, hogy

$f(\tilde{\alpha}) \neq f(\tilde{\beta})$, ahol
$\tilde{\alpha} = (\alpha_1, \ldots, \alpha_{i-1}, \alpha, \alpha_{i+1}, \ldots, \alpha_n)$,
$\tilde{\beta} = (\alpha_1, \ldots, \alpha_{i-1}, \beta, \alpha_{i+1}, \ldots, \alpha_n)$, ahol $\alpha \neq \beta$.

Itt és a továbbiakban mindig $f(\tilde{\alpha})$ illetve $f(\tilde{x})$ az $f(\alpha_1, \ldots, \alpha_n)$ illetve $f(x_1, \ldots, x_n)$ röviditett alakja.

1.5. **Definició.** Azt mondjuk, hogy az $f(x_1, \ldots, x_n)$ *függvény rendszáma* $l (0 \leqslant l \leqslant n)$, ha valódi a változóinak a száma l.

1.6. **Definició.** Az $f(x_1, \ldots, x_n)$ függvény nem valódi változóit *fiktiv változóknak* nevezzük. Két függvény egyenlő, ha az egyiket a másikból fiktiv változóknak a hozzáadásával illetve elvételével meg lehet kapni.

A továbbiakban az $f(x_1, \ldots, x_n)$ függvény megadásával az f-el egyenlő függvényeket is adottaknak tekintjük.

Legyen B a P zárt osztály tetszőleges bázisa. $l(B)$-vel jelöljük a B-ben levő függvények rendszámának a maximumát.

1.7. **Definició.** A P véges bázisú zárt *osztály rendszáma* az $l(B) = \min_B l(B)$ természetes szám, ahol a P összes bázisára vesszük a minimumot.

1.8. **Definició.** Azt mondjuk, hogy az $f(x_1, \ldots, x_n)$ függvény α-őrző, $\alpha \epsilon E_k$, ha $f(\alpha, \alpha, \ldots, \alpha) = \alpha$.

Általánosságban nyitott kérdés, hogy mely P_k-beli függvények irhatók polinom-alakban az $f_1(x,y) = x + y$, $f_2(x,y) = x \cdot y \; \epsilon P_k^{(2)}$ müvelet-párra nézve.
A következő megállapitás mutatja, hogy általában nem minden függvény irható polinom-alakban.

Megállapitás. Legyen $k = q \cdot k'$, $q, k' \geqslant 2$, és jelölje a mod k összeadást és szorzást $+$ illetve $\cdot$. Az

$$f(x) = \begin{cases} 0, & \text{ha} \quad x = 0 \\ & \text{függvény nem irható} \\ q + 1, & \text{ha} \quad x \neq 0 \end{cases}$$

$$c_0 + c_1 x + c_2 x^2 + \ldots + c_m x^m, \qquad m \geqslant 1$$

polinom alakban.

Bizonyitás. Bármely $g(x) = c_0 + \sum_{i=1}^{m} c_i x^i$ polinomra igaz, hogy

$$g(x + q) = c_0 + \sum_{i=1}^{m} c_i (x + q)^i = g(x) + \sum_{i=1}^{m} c_i \sum_{j=1}^{i} \binom{i}{j} x^{i-j} q^j = g(x) + q \cdot Q(x),$$

ahol $Q(x)$ az x egész-együtthatós polinom ja. Ezért $f(x)$-re $x = 0$ esetén ebből $q + 1 = f(q) = f(0) + q \cdot Q(0) = q \cdot Q(0)$ adódna, s ez lehetetlen, mert q és $q + 1$ relativ primek, $k = q \cdot k'$. ■

Legyen $s(x) \epsilon P_k^{(1)}$ k számú, értéket felvevő függvény, azaz permutáció E_k felett, $\overset{s}{+}$, $\overset{s}{\cdot}$ a $+$ és $\cdot$ müveletek s-duálja, azaz $x \overset{s}{+} y = s^{-1}(s(x) + s(y))$, $x \overset{s}{\cdot} y = s^{-1}(s(x) \cdot s(y))$. Jelölje a P_k-beli, $\{\overset{s}{+}, \overset{s}{\cdot}\}$ müveletpárra *lineáris függvények osztályát* L_s, $s(x) = x$ esetén $L_x = L$. Könnyen látható, hogy

$$L_s = \{f(\tilde{x}) \mid f(\tilde{x}) = c_0 \overset{s}{+} c_1 \overset{s}{\cdot} x_1 \overset{s}{+} \ldots \overset{s}{+} c_n \overset{s}{\cdot} x_n, \; c_i \epsilon E_k, \quad i = 0,1, \ldots, n; \; n \geqslant 0\} =$$
$$= \{f(\tilde{x}) \mid f(\tilde{x}) \epsilon L^s\}, \text{ ahol } L^s = \{f(\tilde{x}) \mid f(\tilde{x}) = s^{-1}(g(s(x_1), \ldots, s(x_n))), g(\tilde{x}) \epsilon L\}.$$

Ezért elegendő az L szerkezetét vizsgálni (ld. részletesebben [5])

Jól ismert a következő tétel [6]:

1.1. **Tétel.** *L akkor és csak akkor maximális P_k-ban, ha $k = p$ primszám.* ■

Egyes bizonyitásokban gyakran egyszerübb a kérdéses függvényosztály bázisát generálni, mint a zárt osztály minden elemének előállithatóságát kimutatni. Ezért a következő 1.2. tételben megadjuk L-nek egy bázisát, majd az 1.3. tételben leirjuk az összes olyan bázisit, amely

$$f(x,y)\in P_k^{(2)} \setminus P_k^{(1)} \quad \text{és} \quad d_1(x), d_2(x)\in P_k^{(0)}$$

függvényeket tartalmaz.

1.2. **Tétel.** *Legyen $h(x,y) = x + y$, $g(x) = x + 1$. Az L lineáris osztálynak bázisa a $B_L = \{ h(x,y), g(x) \}$ halmaz.*

Bizonyitás. Legyen

$$h_1(x) = x, \quad h_2(x,y) = h(x,y) = x + y,$$
$$h_m(x_1, \ldots, x_m) = h(h_{m-1}(x_1, \ldots, x_{m-1}), x_m) = x_1 + x_2 + \ldots + x_m, \quad m \geqslant 2;$$
$$g_1(x) = g(x) = x + 1; \; g_m(x) = g(g_{m-1}(x)) = x + m, \quad m \geqslant 1.$$

A konstans függvények $L^{(0)}$ halmazának előállitása:

$$h_k(x, \ldots, x) = 0, \; g_m(0) = m, \quad m = 1,2, \ldots, k-1.$$

Az 1- változós lineáris függvények szintén generálhatók, mert

$$a\in\{1,2 \ldots, k-1\}, \; b\in\{0,1,2, \ldots, k-1\} \text{ esetén } f(x) = ax + b = g_b(h_a(x, \ldots, x$$

Legyen

$$n \geqslant 1, \; L^{(n)} \ni f(\tilde{x}) = c_0 + c_1x_1 + \ldots + c_nx_n, \text{ és } f'(x_1, \ldots, x_{n-1}) = c_0 + \sum_{j=0}^{n-1} c_jx_j \in L^($$

Feltéve, hogy $L^{(n-1)}$ elemeit már előállitottuk, $f(\tilde{x}) = h(f', c_n \cdot x_n)$ és ezzel n-re vonatkozó indukcióval bizonyitottuk az állitást. ■

A későbbiekben gyakran fogjuk felhasználni az itt következő öt lemmát, valamint teljes változó-azonositásra az $(If)(x) = f(x,x, \ldots, x)$ operátoros irásmódot.

1.1. **Lemma.** *Legyenek*

$$f_1(\tilde{x}) = f_1(x_1, x_2, \ldots, x_{n_1}) = c_{10} + c_{11}x_1 + \ldots + c_{1n_1}x_{1n_1} \epsilon L^{(n_1)},$$
$$f_2(\tilde{y}) = f_2(y_1, y_2, \ldots, y_{n_2}) = c_{20} + c_{21}y_1 + \ldots + c_{2n_2}y_{n_2} \epsilon L^{(n_2)},$$
$$f(y_1, y_2, \ldots, y_{n_2}, x_2, \ldots, x_2, \ldots, x_{n_1}) = f_1(f_2(y_1, \ldots, y_{n_2}), x_2, \ldots, x_{n_1}) \; n_1, n_2 \geqslant 1.$$

Az $f \epsilon L$ *szuperpozicióra igazak a következő állitások:*

(α) $(If)(x) = (If_1)(x) + (c_{11}(If_2)(x) + (k-1)c_{11} \cdot x;$
(β) *ha* $(If_2)(l) = l$ $(l \epsilon E_k)$, *akkor* $(If)(l) = (If_1)(l);$
(γ) *ha* $(If_1)(l) = (If_2)(l) = l$, *akkor* $(If)(l) = l.$

Bizonyitás. Az f_1 és f_2 lineáris függvények szuperpoziciója:

$$f_1(f_2(\tilde{y}), x_2, \ldots, x_{n_1}) = f_1(\tilde{x}) + c_{11}f_2(\tilde{y}) + (k-1)c_{11}x_1,$$

s ebből változó-azonositással adódik az (α) állitása. A (β) és (γ) állitások pedig (α)-ból közvetlenül leolvashatók. ■

1.2. **Lemma.** *Legyen* p *tetszőleges primszám,* $p > a \geqslant 1$ *egész. Igazak a következő állitások:*

(α) $a^{p-1} = 1 (\mathrm{mod} p)$
(β) $ax = 1 (\mathrm{mod} p)$ *egyenletet kielégiti az* $x = a^{p-2}$ *érték.*

Bizonyitás. Az (α) állitás a jól ismert Euler-Fermat tétel következménye, a (β) állitás pedig (α)-ból közvetlenül adódik. ■

A következő 1.3. lemmában egy speciális szuperpozició-sorozat néhány – a későbbiekben felhasznált – tulajdonságát mondjuk ki, az 1.4. lemma pedig az egyváltozós függvények szuperpoziciójára vonatkozik. Végül az 1.5. lemma az egyváltozós függvényeket érték-megőrzés szempontjából jellemzi.

1.3. **Lemma.** *Legyen* $k = p$ *primszám,*

$1 \leqslant a < p,\ b,\ c_i \epsilon E_p \qquad (i = 0,1,2, \ldots n),$
$h(y,z,x_1, \ldots, x_n) = ay + bz + r(\tilde{x}),$ ahol $r(\tilde{x}) = c_0 + c_1x_1 + \ldots + c_n \cdot x_n.$

Legyenek továbbá

$$h^1(y_1,z,\tilde{x}) = h(y_1,z,\tilde{x}),$$
$$\ldots\ldots\ldots\ldots$$
$$h^m(y_1,y_2, \ldots, y_m,z,\tilde{x}) = h(h^{m-1}(y_1, \ldots, y_m,\tilde{x}),z,\tilde{x}).$$

Igazak a következő állitások:

$$(\alpha)\quad h^m(\tilde{y},z,\tilde{x}) = a^m y_1 + b(a^{m-1}y_2 + \ldots + ay_m + z) + (a^{m-1} + a^{m-2} + \ldots + a + 1)r(\tilde{x}), \quad \text{ha} \quad 2 \leqslant m \leqslant p-1$$

továbbá, a $h^1, h^2, \ldots, h^{p-1}$ *függvények páronként különbözőek.*

$$(\beta)\quad h^{p-1} = (\tilde{y},z,\tilde{x}) = \begin{cases} y_1 + b(a^{p-2}y_2 + \ldots + ay_{p-1} + z), & \text{ha} \quad a > 1 \\ y_1 + b(y_2 + \ldots + y_{p-1} + z) + (p-1)r(\tilde{x}), & \text{ha} \quad a = 1. \end{cases}$$

$$(\gamma)\quad y_1 = y, y_2 = y_3 = \ldots = y_m = z \quad \text{esetén}$$

$$(\alpha'): h^m(y,z,\tilde{x}) = a^m y + (a^{m-1} + a^{m-2} + \ldots + a + 1)(bz + r(x))$$

$$(\beta'): h^p(y,z,\tilde{x}) = \begin{cases} y, & \text{ha} \quad a > 1, \\ y + (p-1)(bz + r(\tilde{x})), & \text{ha} \quad a = 1. \end{cases}$$

Bizonyitás. $(\alpha)Ah^m(\tilde{y},z,\tilde{x})$ szuperpozició rekurziv definiciójából m-re vonatkozó indukcióval adódik a direkt formula, az állitás második része pedig nyilvánvaló, hiszen a változók száma is páronként különböző, s $a^l \neq 0$, ha $a \neq 0$. A (β) állitás az (α)-ból $m = p-1$ esetén, az 1.2. lemma figyelembe vételével adódik, a (γ) állitás pedig az (α) illetve (β) megfelelő speciális esetenként, az

$$a^{p-2} + \ldots + a + 1 = \begin{cases} \dfrac{a^{p-1}-1}{a-1} = 0, & \text{ha} \quad a > 1 \\ p-1, & \text{ha} \quad a = 1. \end{cases}$$

azonosság alkalmazásával, az 1.2. lemma szerint nyerhető. ■

1.4. **Lemma.** *Legyen* $k = p$ *primszám,* $g(x) = a_0 + ax \epsilon L^{(1)}$. *Igaz a következő két állitás:*

(α) *ha* $a = 1$, $a_0 \neq 0$, *akkor* $[\{g(x)\}] = \{x, x+1, \ldots, x+p-1\} = [\{x+1\}]$

(β) *ha* $a > 1$, *akkor* $[\{g(x)\}] = \{a^m x + a_0(a^{m-1} + \ldots + a + 1) \mid m = 1,2,\ldots,p-1\}$.

Bizonyitás. (α) Legyen $a = 1, a_0 \neq 0$, igy $g(x) = a_0 + x$. Világos, hogy $m_1 \neq m_2$ esetén

$$g^{m_1}(x) = m_1 \cdot a_0 + x \neq m_2 \cdot a_0 + x = g^{m_2}(x),$$

mert $a_0 \neq 0$ következtében az $m_1 a_0 = m_2 \cdot a_0$ egyenlőségből az 1.2. lemma szerint $m_1 = m_2$ adódik.

A (β) állítás az 1.3. lemma alapján adódik. ■

1.5. **Lemma.** *Legyen* $f(\tilde{x}) \in L$, $(If)(x) = a_0 + ax$. *Igazak a következő állítások:*

1.) *ha* $a = 1, a_0 = 0$ *akkor* $f(\tilde{x}) \in L_\alpha$ *minden* $\alpha \in E_p$ *értékre teljesül;*

2.) *ha* $a = 1$, $a_0 \neq 0$ *akkor* $f(\tilde{x}) \in L_\alpha$ *egyetlen* $\alpha \in E_p$ *értékre sem teljesül;*

3.) *ha* $a \neq 1$, *akkor* $f(\tilde{x}) \in L_\alpha$ *pontosan egy* $\alpha \in E_p$ *értékre teljesül.*

Bizonyitás. $(If)(x) = a_0 + ax = a(x - \alpha) + a\alpha + a_0$; $f(\tilde{x})$ α-őrző, ha $\alpha = (If)(\alpha) = a\alpha + a_0$, azaz, ha $(a - 1)\alpha = (p - 1)a_0$. Az (1) esetben ez bármely $\alpha \in E_p$ értékre teljesül, a (2) esetben nem létezik a feltételnek megfelelő $\alpha \in E_p$, mig a (3) esetben az egyetlen megfelelő $\alpha \in E_p$ érték:

$$\alpha = (p - 1)\, a_0 \cdot (a - 1)^{p-2}. \blacksquare$$

A 1.1., 1.3., 1.4., és 1.5. lemmák felhasználásával bebizonyitjuk, hogy igaz a következő

1.3. **Tétel.** *Legyen* $f(x,y) = ax + by + c$, $a \neq 0 \neq b$, $d_1(x) = d_1 \neq d_2 = d_2(x)$ *konstans függvények,* $d(x) \in \{d_1(x), d_2(x)\}$. *Igazak a következő állitások:*

1.) *ha* $a + b = 1$, $c = 0$, *akkor* $\{f(x,y), d_1(x), d_2(y)\}$ *bázis L-ben.*

2.) *ha* $a + b = 1$, $c \neq 0$, *akkor* $\{f(x,y), d(x)\}$ *bázis L-ben*

3.) *ha* $a + b \neq 1$, $d(x) = d \neq (p - c)(a + b - 1)^{p-2}$, *akkor* $\{f(x,y), d(x)\}$ *bázis L-ben.*

Bizonyitás. Először megmutatjuk, hogy mindhárom esetben generálható az L rendszer $B_L = \{x + y, x + 1\}$ bázisa (ld. 1.2. tétel), majd a rendszerek minimális, azaz bázis voltát igazoljuk.

1. Az 1.3. lemma (γ) szerinti speciális szuperpozicióra adódik:

$$f^m(x,y) = a^m x + b(a^{m-1} + \ldots + 1)y.$$

Az $m_0 = p - 2$ értékre ebből (minthogy $a \neq 1$):

$$f_1(x,y) = f^{p-2}(f(x,d_1),y) = a^{p-2}(ax + bd_1) + b\frac{a^{p-2} - 1}{a - 1}\, y =$$

$$= x + a^{p-2} \cdot b(d_1 - y) = x + b_1 y + c_1,$$

$$b_1 = (a - 1)a^{p-2}, \qquad c_1 = a^{p-2} \cdot b \cdot d_1.$$

A $d_1 \neq d_2$ feltétel következtében $f_1(x,d_2) = x + a^{p-2} \cdot b(d_1 - d_2)$ az 1.4. lemma szerint előállitja a $g(x) = x + 1$ függvényt. Minthogy

$$[\{f_1(x,y), g(x)\}] \ni f_2(x,y) = x + b_1 y,$$

adódik, hogy

$$f_2^{b_2}(x,y) = x + b_2 \cdot b_1 \cdot y = x + y, \text{ ha } b_2 = (a-1)^{p-2} \cdot a.$$

2. $f(x,x) = x + c$, $c \neq 0$ következtében $[\{f(x,x)\}] \ni g(x) = x + 1$ (1.4. lemma), s minthogy $g^{p-c}(f(x,y)) = ax + by$, az 1. részben látott módon származtatható $h(x,y) = x + y$.

3. Ha $a = 1$, azaz $f(x,y) = x + by + c$, akkor a $d \neq (p-c)b^{p-2}$ feltétel következtében $f(x,d) = x + bd + c \neq x$, s igy $[\{f(x,d)\}] \ni g(x) = x + 1$, s ezért a 2. rész bizonyitása szerint származtatható $h(x,y) = x + y$.
Ha $a \geqslant 2$, képezzük a következő szuperpoziciót:

$$f(f^{p-2}(x,y),d) = x + (a^{p-2} + \ldots + a)(by + c) + bd + c = x + b(d - y).$$

(Közben az $a^{p-2} + \ldots + a + 1 - 1 = \frac{a^{p-1} - 1}{a - 1} - 1 = -1$ azonosságot alkalmaztunk). Minthogy

$$f(d,d) = (a + b)d + c = (a + b - 1 + 1)d + c = (a + b - 1)d + c + d \neq d$$

a $d(x)$-re vonatkozó feltétel szerint, igy $[\{x + b(d - f(d,d))\}] \ni g(x) = x + 1$. A $h(x,y) = x + y$ előállitása mindkét esetben az előbbiek szerint történik.
Végül, a tételben szereplő három teljes rendszer valóban bázis. Ugyanis, az $f(x,y)$ kétváltozós függvény nem hagyható el belőle, hiszen a maradó egyváltozós függvényekből kétváltozósakat nem lehet előállitani. Ha viszont egyváltozós függvényt hagynánk el a rendszerből, akkor:

1. az 1.1. és 1.5. lemma 1. állitása szerint $f(x,y)$ minden $\alpha \in E_p$ értéket megőriz, $d(x) = d$ konstans függvény viszont az $\alpha = d$ értéket megőrzi, s igy az 1.1. lemma szerint a megmaradó rendszer is megőrzi a d értéket, tehát a d_1, d_2 konstansok közül az egyiket nem generálja.

2. az 1.1. lemma (α) állitása szerint $f(x,y)$ csak olyan f_1 függvényeket generál, amelyekre $(If_1)(x) = x + c_0$, s igy $d(x) \notin [\{f(x,y)\}]$.

3. az 1.1. és 1.5 lemma szerint $[\{f(x,y)\}] \subseteq L_\alpha, \alpha = (p-c)(a+b-1)^{p-2}$, s igy $d(x) \notin L_\alpha$ nem állitható elő $f(x,y)$-ból.■

2. Maximális függvényosztályok L-ben ($k = p$)

Legyen a továbbiakban $k = p \geqslant 3$ primszám, rögzitett érték. Megadunk $p + 2$ számu zárt osztályt, mindegyik osztályhoz megadunk egy-egy bázist, és bizonyitjuk, hogy ezek maximálisak L-ben, és ezeken kivül nincs maximális osztály L-ben.

A következő tétel az egyelemü $\{\alpha\}$ részhalmazt megőrző lineáris függvények osztályának L-ben maximális voltát állitja: $\alpha = 0,1,\ldots,p-1$ értékeknek megfelelően "p" szá-

mú L-ben maximális osztályt ir le.

2.1. **Tétel.** *Legyen* $L_\alpha = \{f(\tilde{x}) \mid f(\alpha, \ldots, \alpha) = \alpha\} \subseteq L, \alpha \in E_p$. *Az* L_α *részosztály maximális az* L*-ben.*

Bizonyitás. L_α zártsága az 1.1. lemma (γ) állitásából következik. Továbbá, L_α nem teljes, mert $x + 1 \in L \setminus L_\alpha$. Legyen $f(x_1, x_2, \ldots, x_n) \in L \setminus L_\alpha$. Az $(If)(x) = a_0 + ax$ függvényre $f \in L_\alpha$ következtében teljesül a következő feltétel:

(A) $\qquad a_0 + a \cdot \alpha \neq \alpha.$

Három esetet különböztetünk meg.

1. eset: $a = 0$. Az $(If)(x) = a_0$ és $x + y + (p-1)\alpha \in L_\alpha$ függvények szuperpoziciójából $x + a_0 + (p-1)\alpha$ adódik, s az A-feltétel következtében $a_0 + (p-1)\alpha \neq 0$.

2. eset: $a = 1$. $(If)(x) = a_0 + x$, $a_0 \neq 0$ szintén az A-feltétel szerint.

3. eset: $a > 1$. Az 1.4. lemma (β) szerint $m = p - 2$ esetén adódó

$$(If)^{p-2}(x) = a^{p-2}x + a_0(a^{p-3} + \ldots + a + 1) \text{ és az } f_\alpha(x) = a(x - \alpha) + \alpha \in L_\alpha$$

függvények szuperpoziciója:

$$f\alpha((If)^{p-2}(x)) = a(a^{p-2}x + a_0(a^{p-3} + \ldots + a + 1) - \alpha) + \alpha = a^{p-1}x + \\ + \frac{a^{p-1} - 1}{a - 1} a_0 - (a_0 + \alpha a - \alpha) = x - (a_0 + a\alpha - \alpha),$$

s az A-feltétel szerint $a_0 + a\alpha - \alpha \neq 0$.

Mindhárom esetben az 1.4. lemma (α) szerint $g(x) = x + 1$ és $g^\alpha(x) = x + \alpha$ generálható, továbbá $x + y + (p-1)\alpha \in L_\alpha$ szuperpoziciójából $g^\alpha(x + y + (p-1)\alpha) = x + y$ adódik, s igy generáltuk L-nek az 1.2. tételben megadott $B_L = \{x + y, x + 1\}$ bázisát. ■

A most következő L_* maximális osztály az $x + 1 \in L_*^{(1)}$ függvényre *önduális lineáris* függvények osztálya.

2.2. **Tétel.** *Legyen* $L_* = \{f(\tilde{x}) \mid f(\tilde{x}) = c_0 + \sum_{i=1}^{n}{}' c_i x_i,\ n = 1,2, \ldots, (If)(x) = c_0 + x\}$.

L-ben maximális az $L_* \subseteq L$ *részosztály.*

Bizonyitás. L_* zártsága az 1.1. lemmából következik. L_* nem teljes, mert pl. $x + y \notin L_*$.

Legyen $f(\tilde{x}) \in L \setminus L_*$. Az $(If)(x)$ és $x + p - a_0 \in L_*$ szuperpoziciójából adódik az $f_1(x) = ax$ függvény. Minthogy $(If)(x) = a_0 + ax$, $a \neq 1$, két eset lehetséges.

1. eset: $a = 0$. Ekkor $f_1(x) = 0$ konstans függvény és $f_2(x,y,z) = x + y + (p-1)z \in L_*$ szuperpoziciója: $f_2(x,y,0) = x + y$.

2. eset: $a > 1$. Legyen $b_1 = (p-1)(a-1)^{p-2}$, $b_2 = p - b_1 + 1$, s képezzük a $z_1 = f_1(t) = at$, $z_2 = t \in L_*$ és a $b_1 z_1 + b_2 z_2 \in L_*$ függvények alábbi szuperpozicióját: $b_1 \cdot at + b_2 t = t(b_1(a-1) + 1) = 0$. Minthogy ismét a $f_0(x) = 0$ konstans függvény adódott, az 1. esethez hasonlóan nyerhető $x + y$.
Minthogy $x + 1 \in L_*$, mindkét esetben előállitottuk az L osztály B_L bázisát. ■

A következő maximális osztályra vonatkozó tétel a Slupecki-tétel L-beli analógjának tekinthető.

2.3. **Tétel.** *L-ben maximális az 1-változós függvények* $L^{(1)} = \{ax + b \mid a \in E_p,\ b \in E_p\}$ *halmaza.*

Bizonyitás. Hogy $L^{(1)}$ zárt és nem teljes L-ben, az nyilvánvaló, mert többváltozós függvény nem állitható elő $L^{(1)}$-ből és az összes l-változós lineáris függvényt tartalmazza a definiciója szerint.
Legyen $f(\tilde{x}) \in L \setminus L^{(1)}$. Az $\{f(\tilde{x})\} \cup L^{(1)}$ feletti alkalmas szuperpozició a pontosan két változótól függő $ax + by \in L^{(2)}$ $(a \neq 0 \neq b)$ függvényt eredményezi $(0, x + 1 \in L^{(1)}$ felhasználásával).
Az $ax + by$ függvényből viszont már $a^{p-2} \cdot x$, $b^{p-2} \cdot y \in L^{(1)}$ helyettesitésével adódik $x + y$, s igy ismét generáltuk a B_L bázist. $(x + 1 \in L^{(1)})$. ■

A következő tételekben minden maximális osztályhoz megadjuk az összes minimális elemszámú bázist. Ezek az eredmények magukban is érdekesek, de a teljességi tétel bizonyitásánál, valamint a Post-strúktúra következő, második szintjének vizsgálatához is szükségesek.

2.4. **Tétel.** 1.) *Az* $f_\alpha(x,y) = x + y + (p-1)\alpha$ *függvény az* L_α*-ban bázis, ahol* $\alpha = 0,1,\ldots,p-1$.

2.) *Bármely* $f(x_1,x_2,\ldots,x_n) \in L_\alpha \setminus (L_* \cup L^{(1)})$ *függvény bázis* L_α*-ban, és* L_α*-ban más egy elemü bázis nincs.*

A tétel bizonyitásához szükségünk lesz a következő lemmára.

2.1. **Lemma.** *Az n-változós* α*-őrző függvények halmaza*

$$L_\alpha^{(n)} = \left\{ \sum_{i=1}^{n} c_i(x_i - \alpha) + \alpha \mid c_i \in E_k, \quad i = 1,2,\ldots,n \right\}$$

Bizonyitás. Könnyen látható, hogy a jobboldalon felsorolt k^n számú függvények páronként különbözőek, és mindegyike α-őrző. Azonban több α-őrző n-változós függvény nincs is, mert

$$|L_\alpha^{(n)}| = \frac{1}{k} |L^{(n)}| = \frac{1}{k} k^{n+1} = k^n. \blacksquare$$

2.4. **tétel bizonyitása.** Először az (1) állitást bizonyitjuk. n-re vonatkozó indukcióval kimutatjuk, hogy $L_\alpha^{(n)}$ minden elemét generálja $f_\alpha(x,y) \epsilon L_\alpha^{(2)} \setminus L_\alpha^{(1)}$. A (2) állitás bizonyitásához az ott szereplő $f(\tilde{x})$ függvényből generáljuk az $f_\alpha(x,y)$ bázis-függvényt.

1.) Az 1.3. lemmában definiált hatványozás szerint, ha $a = b = 1$, $r(\tilde{x}) = (p-1)\alpha$, akkor f_α m-edik hatványa:

$$f_\alpha^m = y_1 + y_2 + \ldots + y_m + z + m(p-1)\alpha, \qquad m \geqslant 1.$$

Ebből $m = p - 1$ esetén változó-azonositással adódik az $L_\alpha^{(0)} = \{\alpha\}$ halmaz:

$$(If_\alpha^{p-1})(x) = px + (p-1)^2\alpha = \alpha.$$

Az L_α 1-változós elemei $L_\alpha^{(1)} = \{a(x-\alpha) + \alpha \mid a \epsilon E_p\}$ halmazának előálli - tása ($a = 0$ esetén $\{\alpha\} = L_\alpha^{(0)}$ már szerepelt):

$a = 1$ esetén $(If_\alpha^p)(x) = x$,

$a \geqslant 2$ esetén $(If_\alpha^{a-1})(x) = ax + (a-1)(p-1)\alpha = a(x-\alpha) + \alpha$.

Feltéve, hogy az $L_\alpha^{(n-1)}$ halmazt már előállitottuk, az

$\alpha + \sum_{i=1}^{n} c_i(x_i - \alpha) = f(\tilde{x}) \epsilon L_\alpha^{(n)}$ előállitása az

$f_\alpha^{c_n}(\tilde{y}, z)$ és $f'(\tilde{x}) = \alpha + \sum_{i=1}^{n-1} c_i(x_i - \alpha) \epsilon L_\alpha^{(n-1)}$ függvényekből az

$f_\alpha^{c_n}(\tilde{y}, f'(\tilde{x}))$ szuperpozicióból az $y_1 = y_2 = \ldots = y_{c_n} = x_n$ azonositással adódik.

2.) Legyen $f(\tilde{x}) = c_0 + \sum_{i=1}^{n} c_i x_i \epsilon L_\alpha \setminus (L_* \cup L^{(1)})$ azaz $c_1 \neq 0 \neq c_2$, $(If)(x) = c_0 + cx$, ahol $c \neq 1$, és $c_0 = (c-1)(p-1)\alpha$. Az $r(\tilde{x}) = \sum_{i=3}^{n} c_i x_i + c_0$ jelölést bevezetve, képezzük $f(\tilde{x}) = c_1 x_1 + c_2 x_2 + r(\tilde{x})$ m-edik hatványát:

$f^m = c_1^m \cdot y_1 + c_2(c_1^{m-1} y_2 + c_1^{m-2} y_3 + \ldots + c_1 y_m + z) + (c_1^{m-1} + \ldots + c_1 + 1) r(\tilde{x})$. Az $y_1 = x, y_2 = \ldots = y_m = y$ azonositással $c_1 \geqslant 2$ esetben $m = p - 1$, a $c_1 = 1$ .esetben $m = p$ választással adódik f^m-ből a $t(x,y,z) = x + c_2(y - z)$ függvény.

Képezzük a $t_1(x,y,z) = t(x,y,z)$, $t_m(x,y,z) = t(t_{m-1}(x,y,z),y,z)$, $m = 2,3, \ldots$ sorozatot. Látható, hogy $t_m(x,y,z) = x + mc_2(y - z)$.

Legyen $m_0 = ((c-1)c_2)^{p-2}$; ez esetben $t_{m_0}(x,(If)(y),y) = x + m_0 \cdot$

$$\cdot c_2(c_0 + cy - y) = x + m_0 c_2(c-1)y +$$

$$+ m_0 c_0 c_2 = x + y + (p-1)\alpha,$$

amely függvény bázis L_α-ban .■

2.5. **Tétel.** *Legyen* $L'_* = \{ f' \mid f' \epsilon L_* \setminus L^{(1)}, (If')(x) \neq x \}$, $L'_{*0} = L_* \setminus (L'_* \cup L^{(1)})$. *Igazak a következő állitások:*

1.) *az* $f'_0 \epsilon L_{*0}$ *akkor és csak akkor bázis* L_{*0}*-ban, ha* $f'_0 \epsilon L'_{*0}$;

2.) *az* $f' \epsilon L_*$ *akkor és csak akkor bázis* L_**-ban, ha* $f' \epsilon L'_*$.

Bizonyitás. A szükségesség mindkét esetben nyilvánvaló, mert egyváltozós függvény többváltozósat nem állithat elő. Legyen

$$f'(\tilde{x}) = c'_0 + \sum_{i=1}^{n} c'_i x_i, \quad n \geqslant 2, \quad 1 \leqslant c'_i \leqslant p-1, \quad i = 1,2,\ldots,n$$

esetén, és $c' = \sum_{i=1}^{n} c'_i = 1$. Az (1) és (2) esetet egyidejüleg tárgyalhatjuk, mert $c'_0 = 0$ esetén $[\{f'(\tilde{x})\}]$ bármely eleme 0-őrző, $c'_0 \neq 0$ esetén pedig az 1.4. lemma alapján

$$[L_{*0} \cup \{x + c'_0\}] = L_*$$

Az 1.3. lemma (α) állitása szerint

$$f'^m(y_1,y_2,\ldots,y_m,x_2,x_3,\ldots,x_n) = c'^m_1 \cdot y_1 + c'_2(c'^{m-1}_1 \cdot y_2 + \ldots + c'_2 y_m + x_2)$$
$$+ (c'^{m-1}_1 + \ldots + c'_1 + 1)r(\tilde{x}), \quad \text{ahol } r(\tilde{x}) = c'_3 x_3 + \ldots + c'_n x_n + c'_0$$

Ezért

$$f_1(y_1,y_2,x,\tilde{x}) = f'^{p-1}(y_1,y_2,\ldots,y_2,x,\tilde{x}) =$$
$$= y_1 + c'_2(c'^{p-2}_1 + \ldots + c'_1)y_2 + x) + (c'^{p-2}_1 + \ldots + c'_1 + 1)r(\tilde{x}) =$$
$$= \begin{cases} y_1 + c'_2((p-2)y_2 + x) + (p-1)r(\tilde{x}), & \text{ha} \quad c'_1 = 1, \\ y_1 + c'_2((p-1)y_2 + x) & \text{ha} \quad c'_1 \geqslant 2. \end{cases}$$

Azt kell tehát megmutatni, hogy $g(x,y,z) = x + ay + (p - a)z$ generálja az L_{*0} osztályt.

Legyen $f(x_1,\ldots,x_n) = \sum_{i=1}^{n} c_i x_i$, $c_i \geqslant 1$, $c = \sum_{i=1}^{n} c_i = 1$. Minthogy $g_1(x,y,z) = g(x,y,z)$, $g_m(x,y,z) = g(g_{m-1}(x,y,z),y,z) = x + m(ay + (p-a)z)$, az $m_0 = a^{p-2}$ esetén $g_{m_0}(x,y,z) = x + y + (p-1)z$ adódik.

Képezzük a $g_{m_0}(x,y,z)$ függvény $s = c_1 \oplus c_2 \oplus \ldots \oplus c_n$ – 2-edik hatványát, és azonositsuk az első c_1 számú változót x_1-gyel, a következő c_2 számú változót x_2-val, általában legyen

$$x_{s_{i-1}\oplus 1} = x_{s_{i-1}\oplus 2} = \ldots = x_{s_{i-1}\oplus c_i} = x_i, \qquad i = 1,2,\ldots,n.$$

Itt $s_0 = 0$, $s_i = s_{i-1} \oplus c_i$ és a "$\oplus$" jel az aritmetikai összeadást jelöli. Igy valóban az

$$f(x_1,\ldots,x_n) = \sum_{i=1}^{n} c_i x_i$$

függvényt állitottunk elő. ■

Az egyváltozós lineáris függvények osztálya bázisainak vizsgálatához szükség van az $E_p \setminus \{0\}$ halmazon a "$\cdot$" (modp szorzás") müvelettel definiált strúktura néhány tulajdonságára. Ismeretes (ld. [2], 289. old), hogy ez az algebrai strúktura ciklikus csoport, továbbá, hogy pontosan $\varphi(p-1)$ számú generátor eleme van. Az $a \epsilon E_p \setminus \{0\}$ elem multiplikativ rendjén azt a legkisebb $r(a) = r \geqslant 1$ egész számot értjük, amelyre $a^r = 1$ teljesül. (A $\varphi(x)$ az Euler-féle φ-függvény). Általánosabban igaz a következő

2.2. **Lemma.** *Ha m osztója $(p-1)$-nek, akkor az $E_p \setminus \{0\}$ halmaznak $\varphi(m)$ számú olyan eleme van, amelynek rendje m. Továbbá ha "a" egy m-rendü elem, akkor*

$$\left\{ a^r \mid r = s \cdot \frac{p-1}{m}, \quad 1 \leqslant s \leqslant m, \quad (s,m) = 1 \right\} = M$$

az m-edrendü elemek halmaza.

Bizonyitás. A lemma a [2] 12. fejezet, 9. tételének következménye. ■

Megjegyezzük továbbá, hogy a generátor-elemek egyszerü jellemzése nem várható, mert az a "p" primszám számelméleti tulajdonságainak függvénye. Viszont – mint látni fogjuk – az $L^{(1)}$ szerkezete éppen a 2.2. lemmában szereplő "m" renddel van szoros kapcsolatban. Tekintsük először $L^{(1)}$ bázisait.

Ehhez szükségünk lesz a következő, könnyen belátható lemmára:

2.3. **Lemma.** *Ha $f(\tilde{x})$ α-őrző függvény, $g(\tilde{y})$ nem α-őrző függvény, akkor a $g(y_1, \ldots, y_{i-1}, f(\tilde{x}), y_{i+1}, \ldots y_n)$ szuperpozició nem α-őrző függvény.*

Megjegyezzük, hogy a lemma állitása nem csak a k-értékü logikában igaz. ■

A következő tétel $L^{(1)}$ bázisaira vonatkozik. Legyen $l_0(x) = c_0 \epsilon L^{(0)}$, $l_i(x) = a_i x + c_i \epsilon L^{(1)} \setminus L^{(0)}$, $i \geqslant 1$ egész. Jelölje $r(a_i) = r_i$ az $a_i \epsilon E_p \setminus \{0\}$ elem multiplikativ rendjét és $lkkt\{r_1, r_2, \ldots\}$ az $r_1, r_2, \ldots$ számok legkisebb közös többszörösét.

2.6. **Tétel.**

A.) *A következő állitások ekvivalensek:*

1.) $B_s = \{l_1(x), l_2(x), \ldots, l_s(x)\}$ *halmaz bázis* $L^{(1)} \setminus L^{(0)}$*-ban.*

2.) $B_{s0} = \{l_0(x)\} \cup B_s$ *halmaz bázis* $L^{(1)}$*-ben.*

3.) B_s *elemeire teljesül a következő három feltétel:*

(a) $lkkt\{r_1, r_2, \ldots, r_s\} = p - 1$

(b) *egyetlen* $\alpha \epsilon E_p$ *értékre sem üres a* $B_s \setminus L_\alpha^{(1)}$ *halmaz.*

(c) B_s *egyetlen valódi részhalmazára sem teljesül* (a) *és* (b) *egyidejüleg.*

B.) *A minimális elemszámu bázis hossza* $L^{(1)} \setminus L^{(0)}$ *illetve* $L^{(1)}$ *halmazokra rendre* 2 *illetve* 3.

Bizonyitás.

A.) (2) ⇒ (1): Nyilvánvaló, hogy a B_{s0} elemeiből képzett szuperpozició akkor és csak akkor nem konstans függvény, ha abban $l_0(x)$ nem vesz részt. Ezért B_s bázis $L^{(1)} \setminus L^{(0)}$-ban.

(1) ⇒ (2): $[B_s] = (L^{(1)} \setminus L^{(0)}) \ni x + 1$ következtében

$$(L^{(1)} \supseteq)[B_{s0}] \supseteq [B_s] \cup [\{x + 1, l_0(x)\}] = (L^{(1)} \setminus L^{(0)}) \cup (L^{(0)} \cup L_*^{(1)}) = L^{(1)}.$$

(1) ⇒ (3): Legyen $l(x) = ax + c \in L^{(1)}$, amelyre $r(a) = p - 1$. Ha az (a) feltétel nem teljesülne B_s-re, akkor $l(x) \in [B_s]$ sem teljesülhetne. Ugyanis $\{a_1, a_2, \ldots, a_s\}$ által generált (modp, multiplikativ) csoport rendje $lkkt\{r_1, r_2, \ldots, r_s\} \neq p - 1$ esetén $p - 1$-nél határozottan kisebb lenne, s igy a Lagrange-tétellel kerülnénk ellentmondásba.

Ha viszont a (b) feltétel nem teljesülne, azaz valamely α értékre $B_s \subseteq L_\alpha^{(1)} \setminus \{\alpha\}$, akkor $L^{(1)} \setminus (L^{(0)} \cup L_\alpha^{(1)}) \neq \emptyset$ halmaz elemeit $[B_s]$ nem tartalmazná, s ez ellentmond (1)-nek. A (c) feltétel közvetlenül következik B_s bázis-voltából.

(3) ⇒ (1): Tegyük fel, hogy B_s-re teljesül az (a) és (b) feltétel. Az (a) feltétel szerint előállitható egy $l(x) = ax + c$ függvény, amelyre $r(a) = p - 1$, s ez pontosan egy értéket, az $\alpha = \frac{p - c}{a - 1}$ értéket őrzi meg (ld. 1.5. lemma), mert $r(a) = p - 1 > 1$ következtében $a \geqslant 2$.

A (b) feltétel szerint valamely $1 \leqslant i \leqslant s$ értékre $l_i(x) \notin L_\alpha^{(1)}$, s igy az $a_i \cdot a^j = 1$ egyenletnek eleget tevő j értékre: $l_i(l^j(x)) = x + b$, ahol $b = a_i c(a^{j-1} + \ldots + 1) + c_i \neq 0$ a 2.3. lemma alapján. Tetszőleges $f(x) = Ax + B \in L^{(1)} \setminus L^{(0)}$ függvény egy előállitása: $f(x) = g^B((g^{p-c}(l(x)))^i)$, ahol i az $a^i = A$ egyenletnek tesz eleget.

Végül a bázis definiciójából következik, hogy egy teljes rendszer pontosan akkor bázis, ha a (c) feltétel teljesül.

B.) A (b) állitás nyilvánvaló, mert $l_1(x) = x + 1$, $l_2(x) = l(x) = ax + c$, $r(a) = p - 1$ taljesitik az (a), (b), (c), feltételeket és $s \leqslant 1$ esetén ez lehetetlen. (1.5. lemma) ■

Végül e rész befejezéseként bebizonyitjuk, hogy az előbbiekben megadott $p + 2$ számú maximális osztályon kivül nincs más maximális osztály L-ben.

2.7. **Tétel.** *Minden zárt osztály L-ben, amely különbözik az összes lineáris függvény L halmazától, benne van legalább egyikében az $L_0, L_1, \ldots, L_{p-1}, L_*, L^{(1)}$-gyel jelölt $p + 2$ számú maximális osztálynak.*

Bizonyitás. Tegyük fel, hogy a P osztály, amely L-ben zárt, nincs benne az előbbiekben definiált $p + 2$ maximális osztály egyikében sem. Akkor P tartalmaz minden $\alpha = 0,1, \ldots, p$ értékre egy-egy $f_\alpha(\tilde{x})$ lineáris függvényt, amely nem α-őrző, azaz

$$z_\alpha(x) = (If_\alpha)(x) = c_{\alpha 0} + c_\alpha(x - \alpha), \quad c_{\alpha 0} \neq \alpha, \quad \alpha = 0,1, \ldots, p - 1.$$

P tartalmaz továbbá egy $f_n(\tilde{x}) \in L$ függvényt, amely nem L_* -beli, azaz

$$z_p(x) = (If_p)(x) = c_{p0} + c_p \cdot x, \qquad c_p \neq 1,$$

és egy $f_{p+1}(\tilde{x}) \in L$ függvényt, amely nem $L^{(1)}$ -beli, azaz

$$f_{p+1}(\tilde{x}) = c_{p+1\ 0} + \sum_{i=1}^{n}{}' c_{p+1\,i} x_i, \quad 1 \leqslant c_{p+1\,i} \leqslant p-1, \quad i = 1,2,\ldots,n; \quad n \geqslant 2.$$

Legyen

$$z_{p+1}(x) = (If_{p+1})(x) = c_{p+1\ 0} + x \cdot \sum_{i=1}^{n}{}' c_{p+1\,i} = c_{p+1\ 0} + c_{p+1} \cdot x.$$

Három esetet különböztetünk meg. Mindhárom esetben generáljuk a $p+2$ számú maximális osztály egyikét, s igy az a P megfelelő elemével teljes lesz.

1.) $c_{p+1} = 1, c_{p+1\ 0} = 0$. Az 1.5. lemma szerint $f_{p+1}(\tilde{x}) \in (L_* \cap\cap_{\alpha \in E_p} L_\alpha) \setminus L^{(1)}$.

Ha $z_0(x) \in L_*$, azaz $c_0 = 1$, akkor $z_0(f_{p+1}(\tilde{x})) = f'$ teljesiti a 2.5. tétel (2). feltételét, s igy $[\{f'\}] = L_*, [\{f', f_p\}] = L$. A 2.5. tétel (1) feltétele szerint $[\{f_{p+1}(\tilde{x})\}] = L_{*0}$, s az $L_{*0} \ni x + y + (p-1)z$ függvényből $c_0 = 0$ esetén $x + y + (p-1)c_{00}$ előállitható. Minthogy $[\{x + y + (p-1)c_{00}\}] = L_{c_{00}}$, igy $[L_{c_{00}} \cup \{f_{c_{00}}\}] = L$

Ha viszont $c_0 > 1$, legyen $a = (p-1)(c_0 - 1)^{p-2}$; az $ay + (p-a-1)x \in L_{*0}$ és $c_0 x + c_{00}$ szuperpoziciója:

$$a(c_0 x + c_{00}) + (p - a + 1)x = (a(c_0 - 1) + 1)x + ac_{00} = ac_{00}$$

konstans függvény, s igy az előbbihez hasonlóan származtatható az $L_{ac_{00}}$ maximális osztály, és igy $[L_{ac_{00}} \cup \{f_{ac_{00}}\}] = L$.

2.) $c_{p+1} = 1, c_{p+1\ 0} \neq 0$. A 2.5. tétel szerint $[\{f_{p+1}(\tilde{x})\}] = L_*$, mert $f_{p+1}(\tilde{x}) \in L'_*$.
Minthogy L_* maximális osztály, $f_p(\tilde{y}) \notin L$, ezért $[\{f_p(\tilde{y}), f_{p+1}(\tilde{x})\}] = L$.

3.) $c_{p+1} \neq 1$. Az 1.5. lemma szerint pontosan egy $\alpha_0 \in E_p$ létezik, amelyre $f_{p+1}(\tilde{x}) \in L_{\alpha_0} \setminus (L_* \cup L^{(1)})$ s ezért a 2.4. tétel alapján $[\{f_{p+1}(\tilde{x})\}] = L_{\alpha_0}$,
Minthogy L_{α_0} maximális osztály, és $f_{\alpha_0}(\tilde{x}) \in L_{\alpha_0}$, igy $[\{f_{p+1}, f_{\alpha_0}\}] = L$. ■

Az előbbiekben bizonyitott 2.1., 2.2., 2.3., és 2.7. tételek együttesen teljesen leirják az L-beli maximális osztályokat. A következő pontban e $p+2$ számú zárt osztály maximális osztályait irjuk le.

3. Az $L_0, L_1, \ldots, L_{p-1}, L_*, L^{(1)}$ zárt függvény-osztályok maximális osztályai

Legyen $\alpha, \beta \in E_p$, $L_{\alpha,\beta} = L_\alpha \cap L_\beta$, $L_{\alpha *} = L_\alpha \cap L_*$, $L_\alpha^{(1)} = L_\alpha \cap L^{(1)} = \{f(x) \mid f(x) = cx + (1-c)\alpha, c = 0,1,\ldots,p-1\}$, $L_*^{(1)} = L_* \cap L^{(1)} = \{f(x) \mid f(x) = x + c_0, c_0 = 0,1,\ldots,p-1\}$. A 2.1. és az 1.5. lemmák alapján $L_{\alpha,\beta} \subseteq L_{*0}$, másrészt ugyanezen

lemmák szerint $L_{\alpha,\beta} \supseteq \bigcap_{\gamma=0}^{p-1} L_\gamma \supseteq L_{*0}$, tehát $L_{\alpha,\beta} = L_{*0}$. Hasonlóan könnyen belátható, hogy $L_{\alpha *} = L_{*0}$. Megvizsgáljuk, hogy $L_0, L_1, \ldots, L_{p-1}, L_*, L^{(1)}$ zárt osztályok mely zárt részosztályai maximálisak és mindegyikhez megadunk egy minimális elemszámú bázist.

3.1. **Tétel.**

1.) L_{*0} *maximális az* $L_0, L_1, \ldots, L_{p-1}$ *zárt függvényosztályokban*

2.) *Minden* $\alpha \in E_p$ *esetén* $L_\alpha^{(1)}$ *maximális az* L_α *zárt osztályban.*

Bizonyitás.

1.) Legyen $f(\tilde{x}) \in L_\alpha \setminus L_{*0}$, azaz $f(\tilde{x}) = \sum_{i=1}^{n} c_i(x_i - \alpha) + \alpha_1$ és teljesül a következő feltétel: $c = \sum_{i=1}^{n} c_i \neq 1$. (Ugyanis $L_{\alpha *} = L_{*0}$ következtében $c = 1$ esetén $c_0 = \alpha(1 - c) = 0$ lenne.)
Ha $c = 0$, akkor $(If)(x) = c_0 = \alpha$ és $x + y + (p-1)z \in L_{*0}$ szuperpozíciójából $x + y + (p-1)\alpha$ adódik, s ez a 2.4. tétel szerint bázis az L_α osztályban.
Ha $c > 1$, legyen $a = (p-1)(c-1)^{p-2}$. Az $ay + (p - a + 1)x \in L_{*0}$ és $(If)(x) = cx + c_0$ ($c_0 = \alpha(1-c)$.) szuperpozíciójából adódik: $a(cx + c_0) + (p - a + 1)x = (a(c-1) + 1)x + ac_0 = ac_0 = \alpha'$, konstans függvény, s igy az előbb látott módon generálható L_α.

Megjegyzés. Formálisan nem szükséges az eset-szétválasztás, mert az utóbbi esetben képezett szuperpozició $c = 0$ értékre is kiadja az α konstans függvényt.

2.) Legyen $f(\tilde{x}) \in L_\alpha \setminus L_\alpha^{(1)}$. Ha $f(\tilde{x}) \in L_{\alpha *} \setminus L_\alpha^{(1)} = L_{*0} \setminus L_\alpha^{(1)}$, akkor a 2.5. tétel alapján $[\{f(\tilde{x})\}] = L_{*0}$, s minthogy (1) szerint L_{*0} maximális az L_α osztályban, ezért $2x + (p-1)\alpha \in L_\alpha^{(1)} \setminus L_{*0}$ következtében $[L_{*0} \cup \{2x + (p-1)\alpha\}] = L_\alpha$. Ha viszont $f(\tilde{x}) \notin L_{*0} \setminus L_\alpha^{(1)}$, akkor $f(\tilde{x}) \in L_\alpha \setminus (L_* \cup L^{(1)})$ s igy a 2.4. tétel alapján $[\{f(\tilde{x})\}] = L_\alpha$. ■

3.2. **Tétel.** *Legyen* $\alpha \in E_p$. *Ha* $P \subseteq L_\alpha$*-tól különböző zárt osztály, akkor* P *az* L_{*0}, $L_\alpha^{(1)}$ *maximális osztályok legalább egyikének része.*

Bizonyitás. Tegyük fel, hogy létezik az L_α-ban P zárt osztály, amelyre $P \setminus L_{*0} \neq \emptyset$ és $P \setminus L_\alpha^{(1)} \neq \emptyset$. Bizonyitani fogjuk, hogy ez esetben $P = L_\alpha$. Ugyanis, ha $P' = (P \setminus L_{*0}) \cap (P \setminus L_\alpha^{(1)}) \neq \emptyset$, akkor létezik a 2.4. tétel szerint bármely $f(\tilde{x}) \in P'$ esetén $[\{f(\tilde{x})\}] = L_\alpha$. Ha viszont $P' = \emptyset$, akkor létezik $f_1(\tilde{x}) \in (L_{*0} \setminus L_\alpha^{(1)}) \cap P$, $f_2(\tilde{y}) \in (L_\alpha^{(1)} \setminus L_{*0}) \cap P$. A 2.5. tétel szerint $[\{f_1(\tilde{x})\}] = L_{*0}$, s igy valóban $[\{f_1(\tilde{x}), f_2(\tilde{y})\}] = L_\alpha$. ■

3.3. **Tétel.**

1.) L_{*0} *maximális az* L_* *zárt függvény-osztályban.*

2.) $L_*^{(1)}$ *maximális az* L_* *zárt függvény-osztályban.*

Bizonyitás.

1.) Legyen $f(\tilde{x}) \epsilon L_* \setminus L_{*0}$; ekkor $(If)(x) = x + c_0$, $c_0 \neq 0$. Minthogy az 1.4. lemma szerint $x + a_0 \epsilon [\{x + c_0\}]$ bármely $a_0 \epsilon E_p$ esetén, igy bármely $g(\tilde{x}) = \sum_{i=1}^{n} a_i x_i + a_0 \epsilon L_*$ előállitható $g'(\tilde{x}) = \sum_{i=1}^{n} a_i x_i$ és $x + a_0$ szuperpoziciójából.

2.) Legyen $f(\tilde{x}) \epsilon L_* \setminus L_*^{(1)}$. Minthogy $f(\tilde{x})$ legalább kétváltozós és bármely $a_0 \epsilon E_p$ esetén $x + a_0 \epsilon L_*^{(1)}$, igy alkalmas a_0 választással $x + a_0$ és $f(\tilde{x})$ szuperpoziciójából nyerhető $f'(\tilde{x}) \epsilon L'_*$, amely a 2.5. tétel szerint generálja az L_* osztályt. ■

3.4. **Tétel.** *Ha* $P \subseteq L_*$ *zárt osztály,* $P \neq L_*$, *akkor* P *az* L_{*0}, $L_*^{(1)}$ *maximális osztályok legalább egyikének része.*

Bizonyitás. Tegyük fel, hogy a $P \subseteq L_*$ zárt osztályra teljesülnek: $P \setminus L_{*0} \neq \emptyset$, $P \setminus L_*^{(1)} \neq \emptyset$. Bizonyitani fogjuk, hogy ez esetben $P = L_*$. Legyen

$$f_1(\tilde{x}) \epsilon P \setminus L_*^{(1)}, \quad f_2(\tilde{y}) \epsilon P \setminus L_{*0}, \quad \text{azaz} \quad (If_2)(y) = y + c_0, \quad c_0 \neq 0.$$

Az eddigiekhez hasonlóan látható, hogy létezik $f'(\tilde{z}) \epsilon [\{f_1(\tilde{x}), y + c_0\}]$ amely teljesiti a 2.5. tétel feltételeit, és igy $[\{f'(\tilde{z})\}] = L_*$. ■

A 2.6. tételből kiindulva, meghatározhatjuk $L^{(1)}$ maximális részhalmazait. A 2.5. és 2.6. tételekhez hasonlóan, a bizonyitások hasonlósága miatt $L^{(1)}$ és $L^{(1)} \setminus L^{(0)}$ maximális osztályait együtt tárgyaljuk. Könnyen ellenőrizhető, hogy $L^{(1)} \setminus L^{(0)}$ egy $p(p-1)$ rendü (nem-kommutativ) csoport.

Legyen $p - 1 = q_1^{\kappa_1} \cdot q_2^{\kappa_2} \cdot \ldots \cdot q_u^{\kappa_u}$, $p_i = \frac{p-1}{q_i}$, $i = 1,2,\ldots,u$ és

$$L^{(1,i)} = \{l(x) \mid l(x) = ax + b, \quad r(a) (\geqslant 1) \text{ osztója } p_i\text{-nek}\}.$$

3.5. **Tétel.**

A.) *Az* $L^{(1)} \setminus L^{(0)}$ *zárt függvényosztályban maximális a következő* $p + u$ *számu zárt függvényosztály:*

1.) $L^{(1,i)}$, $i = 1,2,\ldots,u$

2.) $L_\alpha^{(1)} \setminus \{\alpha\}$, $\alpha = 0,1,\ldots,p-1$

B.) *Az* $L^{(1)}$ *zárt függvényosztályban maximális a következő* $p + u + 1$ *számú zárt függvényosztály:*

1.) $L^{(1,i)} \cup L^{(0)}$, $i = 1,2,\ldots,u$

(2) $L_\alpha^{(1)} \cup L^{(0)}$, $\alpha = 0,1, \ldots, p-1$

(3) $L^{(1)} \setminus L^{(0)}$.

Bizonyitás.

A.)

1.) Az $L^{(1,i)}$ zártsága világos, mert $r(a_1 \cdot a_2) = lkkl\{r(a_1), r(a_2)\}$ osztója p_i-nek. Továbbá $L^{(1,i)}$ valódi részhalmaz $L^{(1)} \setminus L^{(0)}$-ban, mert $r(a) = p-1$ esetén $ax + b \notin L^{(1,i)}$. Végül $L^{(1,i)}$ maximális, mert bármely $ax + b \in (L^{(1)} \setminus L^{(0)}) \setminus L^{(1,i)}$ függvényre az $L^{(1,i)}$ definiciója szerint $r(a)$ osztható $q_i^{\kappa_i}$ értékkel és igy az $r(a') = p_i$ feltételt teljesitő $a'x + b' \in L^{(1,i)}$ függvénnyel az $\{ax + b,\ a'x + b'\}$ halmazra teljesül a 2.6. tétel (3.a.) feltétele. Továbbá $L^{(1,i)}$ nyilvánvalóan teljesiti a 2.6. tétel (3.b.) feltételét is.

2.) Hogy $L_\alpha^{(1)} \setminus \{\alpha\}$ zárt és valódi részhalmaz, az könnyen látható. Legyen $f(x) = ax + b \in (L^{(1)} \setminus L^{(0)}) \setminus L_\alpha^{(1)}$. $(L_\alpha^{(1)} \setminus \{\alpha\}) \cup \{f(x)\}$ könnyen láthatóan teljesiti a 2.6. tétel (3.a.) és (3.b.) feltételét. Ugyanis $L_\alpha^{(1)} \setminus \{\alpha\} = \{x, 2x + (p-1)\alpha, \ldots, (p-1)x + 2\alpha\}$, és pl. $\{2x + (p-1)\alpha, f(x)\}$ egyetlen értéket sem őriz meg.

B.)

1.) Az állitás A. (1)-ből következik, mert

$L^{(1)} \setminus (L^{(1,i)} \cup L^{(0)}) = (L^{(1)} \setminus L^{(0)}) \setminus L^{(1,i)}$.

2.) Az (1)-hez hasonlóan, $L^{(1)} \setminus (L_\alpha^{(1)} \cup L^{(0)}) = (L^{(1)} \setminus L^{(0)}) \setminus (L_\alpha^{(1)} \setminus \{\alpha\})$ egyenlőség és A (2) állitás közvetlen következménye.

3.) Legyen $c \in L^{(0)}$. $[\{c\} \cup L_*^{(1)}] = L^{(0)} \cup L_*^{(1)}$ következtében $[\{c\} \cup (L^{(1)} \setminus L^{(0)})] = L^{(1)}$, mert $L_*^{(1)} \subset L^{(1)} \setminus L^{(0)}$. ■

3.6. **Tétel.**

A.) *Ha* $P \subseteq L^{(1)} \setminus L^{(0)}$ *zárt osztály,* $P \neq L^{(1)} \setminus L^{(0)}$, *akkor* P *a* 3.5. A. *tételben megadott* $p + u$ *számú maximális osztály legalább egyikének része.*

B.) *Ha* $P' \subseteq L^{(1)}$ *zárt osztály,* $P' \neq L^{(1)}$, *akkor* P *a* 3.5. B. *tételben megadott* $p + u + 1$ *számú maximális osztály legalább egyikének része.*

Bizonyitás.

A.) Tegyük fel, hogy P a felsorolt maximális osztályok egyikének sem része. Megmutatjuk, hogy a 2.6. tételben szereplő B_s-tipusú bázis előállitható P-ből, s igy az indirekt feltevésből a $P = L^{(1)} \setminus L^{(0)}$ ellentmondás adódik, amely a tétel állitását bizonyitja. Legyen $l_i(x) \in P \setminus L^{(1,i)}$, $i = 1,2, \ldots, u$, és $t_\alpha(x) \in P \setminus L_\alpha^{(1)}$, $\alpha = 0,1, \ldots, p-1$.

Az $\{l_1(x), l_2(x), \ldots, l_u(x)\}$ halmaz teljesiti a 2.6. tétel (3)(a) feltételét, a $\{t_\alpha(x) \mid \alpha \in E_p\}$ halmaz pedig a (3)(b) feltételnek tesz eleget.

Ezért az egyesitett halmaz a 2.6. tétel alapján valóban generálja az $L^{(1)} \setminus L^{(0)}$ halmazt.

B.) Az A.) rész bizonyitásánál alkalmazott gondolatmenet megismétlése adja az állitás igaz voltát. Ugyanis, az

$$l_i(x) \in P' \setminus (L^{(1,i)} \cup L^{(0)}) = (P' \setminus L^{(1,i)}) \setminus L^{(0)}, \quad i = 1,2, \ldots, u \text{ és}$$
$$t_\alpha(x) \in P' \setminus (L_\alpha^{(1)} \cup L^{(0)}) = (P' \setminus L_\alpha^{(1)}) \setminus L^{(0)}, \quad \alpha \in E_p$$

függvények az A.) rész bizonyitása szerint generálják az $L^{(1)} \setminus L^{(0)}$ halmazt. Ehhez hozzávetve a $c \in P' \setminus (L^{(1)} \setminus L^{(0)})$ konstans függvényt, a 3.5. tétel B.) (3) állitása szerint lezárással valóban $L^{(1)}$ adódik. ■

A 3.1., 3.3. és 3.5. tételekben megadott maximális osztályok bázisainak vizsgálatával zárjuk a 3. részt. Az L_{*0} bázisait a 2.5. tételben, az $L^{(1)} \setminus L^{(0)}$ bázisait a 2.6. tételben vizsgáltuk. Az 1.4. lemmából leolvasható, hogy igaz a következő

3.7. **Tétel.** *Az* $L_*^{(1)}$ *zárt osztály bázisai egy elemüek:* $L_*^{(1)} \setminus \{x\}$ *minden eleme bázis.* ■ *Az* $L_\alpha^{(1)}$ *és* $L_\alpha^{(1)} \cup L^{(0)}$, illetve $L^{(1,i)}$ *és* $L^{(1,i)} \cup L^{(0)}$ *bázisait szintén célszerü együtt tárgyalni.*

3.8. **Tétel.**

A.) $ax + (1 - a)\alpha \in L_\alpha^{(1)} \setminus \{\alpha\}$ *akkor és csak akkor bázis elem, ha* $r(a) = p - 1$.

B.) $L_\alpha^{(1)}$ *minimális elemszámú bázisai két elemüek:* $\{\alpha, ax + (1 - a)\alpha\}$ *akkor és csak akkor bázis* $L_\alpha^{(1)}$*-ben, ha* $r(a) = p - 1$.

C.) $L_\alpha^{(1)} \cup L^{(0)}$ *minimális elemszámu bázisai három-elemüek:* $\{\alpha, \beta, ax + (1 - a)\alpha\}$ *akkor és csak akkor bázis* $L_\alpha^{(1)} \cup L^{(0)}$*-ban, ha* $\beta \neq \alpha$ *és* $r(a) = p - 1$.

Bizonyitás.

A-B.) Az $r(a) < p - 1$ esetén $|[\{ax + (1 - a)\alpha\}]| = r(a) < p - 1$ igy $\{ax + (1 - a)\alpha\}$ nem teljes $L_\alpha^{(1)} \setminus \alpha$ halmazban. Ha viszont $r(a) = p - 1$, akkor $[\{ax + (1 - a)\alpha\}] = L_\alpha^{(1)} \setminus \alpha$, s igy valóban teljes $L_\alpha^{(1)}$-ben az $\{\alpha, ax + (1 - a)\}$ halmaz, s részhalmazára ez nyilván nem lehet igaz.

C.) A-B.) állitásból és az $[L_\alpha^{(1)} \cup \{\beta\}] = L_\alpha^{(1)} \cup \{\beta, 2\beta + (p - 1)\alpha, 3\beta + (p - 2)\alpha, \ldots$ $\ldots, (p - 1)\beta + 2\alpha\} = L_\alpha^{(1)} \cup L^{(0)}$ egyenlőségből következik. (Ugyanis $a_1 \cdot \beta + (1 - a_1)\alpha = a_2\beta + (1 - a_2)\alpha$ egyenlőségből $(a_1 - a_2)(\alpha - \beta) = 0$, azaz $a_1 \neq a_2$ esetén $\alpha = \beta$ adódik.) ■

A következő tétel a 2.6. tétel megfelelője; csak a teljesség kedvéért mondjuk ki. Legyen

$$l_0(x) = c_0 \in L^{(0)}, \quad l_i(x) = a_i x + c_i \in L^{(1,j)}, \quad i \geqslant 1.$$

3.9. **Tétel.**

A.) *A következő állitások ekvivalensek:*

1.) $B_s = \{l_1(x), l_2(x), \ldots, l_s(x)\}$ *halmaz bázis* $L^{(1,j)}$*-ben*

2.) $B_{s_0} = \{l_0(x)\} \cup B_s$, *halmaz bázis* $L^{(1,j)} \cup L^{(0)}$*-ban*

3.) B_s *elemeire teljesül a következő három feltétel:*

a.) $lkkt\{r_1, r_2, \ldots, r_s\} = p_j$

b.) *egyetlen* $\alpha \epsilon E_p$ *értékre sem üres a* $B_s \setminus L_\alpha^{(1)}$ *halmaz*

c.) B_s *egyetlen valódi részhalmazára sem teljesül* a.) *és* b.) *egyidejüleg.*

B.) *A minimális elemszámú bázis hossza* $L^{(1,j)}$ *illetve* $L^{(0)} \cup L^{(1,j)}$ *halmazokra rendre* 2 *illetve* 3.

A bizonyitás is a 2.6. tétel bizonyitásához hasonlóan megy, ezért elhagyjuk. ■

A most következő 4. pontban a L szerkezetének leirását teljessé tesszük. Rámutatunk bizonyos hasonlóságok (mint pl. a 2.6. és 3.9 tételek) mélyebb okaira, megadjuk a szerkezetet leiró háló láncainak maximális hosszát és a háló pontjainak (zárt osztályok) számát.

4. A további zárt függvény-osztályok leirása

Az előző három pontban az L-ben maximális osztályokat és ezen osztályokban maximális osztályokat irtuk le. Az 1. ábrán megadott háló-diagramon minden osztály-tipusból csak egyet tüntettünk fel – az áttekinthetőség érdekében. E diagram a különböző tipusú zárt osztályok kapcsolatát irja le oly módon, hogy az irányitott él az illető osztályban maximális osztály felé mutat.

Feltüntettük még a diagramon a 2.5. és 3.7. közvetlen következményeként adódó következő eredményt:

4.1. **Tétel.**

1.) L_{*0} *zárt osztályban egyetlen maximális osztály van, és ez az egy elemü* $\{x\}$ *halmaz.*

2.) $L_*^{(1)}$ *zárt osztályban egyetlen maximális osztály van és ez az egy elemü* $\{x\}$ *halmaz.* ■

A 3. pontban megjegyeztük, hogy $L^{(1)} \setminus L^{(0)}$ $p(p-1)$-rendü nem-kommutativ csoport. Igy természetesen ebben részcsoportok az $L^{(1,i)}$, $L_\alpha^{(1)} \setminus \{\alpha\}$ zárt osztályok, és a már vizsgált $L_*^{(1)}$. Legyen $\alpha \epsilon E_p$ rögzitett érték.

4.2. **Tétel.**

1.) $L_\alpha^{(1)} \setminus \{\alpha\}$ $(p-1)$*-rendü ciklikus csoport, amelynek* α *fix-pontja.*

2.) $L_\alpha^{(1)} \setminus \{\alpha\}$ *maximális* $L_\alpha^{(1)}$*-ben*

3.) $L_\alpha^{(1)}$ *maximális* $L_\alpha^{(1)} \cup L^{(0)}$*-ban*

Bizonyitás. A 3.8. tételből könnyen leolvasható az állitások helyessége. ■

Bevezetve az $L^{(1,i)} \cap L_\alpha^{(1)} = L_\alpha^{(1,i)} = L_\alpha^{(1,i)}$ jelölést, az eddigiekhez hasonlóan látható be, hogy $\{\alpha\} \cup L_\alpha^{(1,i)}$ maximális $L_\alpha^{(1)}$-ben, és $L_\alpha^{(1,i)} \setminus \{\alpha\}$ maximális $L_\alpha^{(1)} \setminus \{\alpha\}$ halmazban. A 3.5. és 3.6. tételek által leirt $L^{(1)}$-beli maximális osztályok mindegyike $G \cup F$ alakú, ahol G részcsoport az $L^{(1)} \setminus L^{(0)}$ csoportban, és $F \subseteq L^{(0)}$. Világos, hogy $G \cup F$ bármely zárt részosztálya $G' \cup F'$ alakú, $F' \subseteq F$, és $G' \subseteq G$ zárt, azaz részcsoport. Az $L^{(1)}$ és $L^{(1)} \setminus L^{(0)}$ szerkezetének leirását a 3.5. tételhez hasonlóan egybekapcsoljuk. A Lagrange-tétel szerint $L^{(1)} \setminus L^{(0)}$ minden részcsoportjának rendje osztója $p(p-1)$-nek. Látni fogjuk, hogy minden lehetséges rendhez létezik részcsoport, és ezeket két osztályba sorolja a következő:

4.1. **Lemma.** *Az $L^{(1)} \setminus L^{(0)}$ csoport G részcsoportja akkor és csak akkor tartalmazza az $L_*^{(1)}$ részcsoportot, ha G rendje $\geqslant p$.*

Bizonyitás. A szükségesség nyilvánvaló, mert $L_*^{(1)}$ p-edrendü csoport. Az elégségesség bizonyitásához tegyük fel, hogy teljesül a $|G| \geqslant p$ feltétel. Ha G tartalmaz $x + c$, $c \neq 0$ alakú elemet, akkor az 1.4. lemma alapján $L_*^{(1)} \subseteq G$ teljesül. Ha viszont $G \setminus \{x\}$ bármely eleme $ax + b$, $a > 1$ alakú, akkor az 1.5. lemma szerint minden x-től különböző elem pontosan egy értéket őriz meg. Ez az érték nem lehet G minden elemére azonos, mert $G \subseteq L_\alpha^{(1)} \setminus \{\alpha\}$ esetén $|G| \leqslant |L_\alpha^{(1)} \setminus \{\alpha\}| = p - 1$. És minthogy $G \cap L_\alpha \setminus \{x\}$ bármely két elemére az x együtthatója nem lehet azonos, szintén számossági okokból valamely $\alpha_1 \neq \alpha_2$ értékpárra létezik $ax + b_1 \in L_{\alpha_1}^{(1)} \setminus \{x\}$, $ax + b_2 \in L_{\alpha_2}^{(1)} \setminus \{x\}$, $b_i = (1-a)\alpha_i$, $i = 1,2$.

Ez esetben $a^{p-2} \cdot (x - b_2) \in L_{\alpha_2}^{(1)} \setminus \{x\}$ és $ax + b_1$ szuperpoziciója:

$$a(a^{p-2}(x - b_2)) + b_1 = x + b_1 - b_2,$$

ahol

$$b_1 - b_2 = (1-a)(\alpha_1 - \alpha_2) \neq 0,$$

és igy ismét az 1.4. lemma alapján adódik, hogy $L_*^{(1)} \subseteq G$. ■

4.2. **Lemma.** *A $|G| \leqslant p - 1$ rendü $G \subseteq L^{(1)} \setminus L^{(0)}$ részcsoport ciklikus csoport, és részcsoportja valamely $L_\alpha^{(1)} \setminus \{\alpha\}$, $\alpha \in E_p$ osztálynak.*

Bizonyitás. A 4.1. lemma bizonyitásából leolvasható, hogy $G \subseteq L_\alpha^{(1)} \setminus \{\alpha\}$, s minthogy $L_\alpha^{(1)} \setminus \{\alpha\}$ ciklikus csoport, bármely részcsoportja ciklikus. ■

A ciklikus csoportok szerkezete (azaz részcsoport-hálója) az Abel-csoportok alaptétele alapján felirható, Ugyanis $L_\alpha^{(1)} \setminus \{\alpha\}$ részcsoport-hálója azonos a $p - 1 = q_1^{\kappa_1} \ldots q_u^{\kappa_u}$ osztóinak oszthatósága szerinti, vagyis a $(\lambda_1, \ldots, \lambda_u)$,$(0 \leqslant \lambda_i \leqslant \kappa_i$ egészek) kitevő-sorozatok szerinti parciális rendezés által definiált hálóval. Látni fogjuk, hogy ez az $L^{(1)} \setminus L^{(0)}$ csoportra is igaz, mert $p - 1$ bármely osztójához pontosan egy $p - 1$-nél nagyobbrendü és bár-

mely 1-nél nagyobb osztójához minden $\alpha \epsilon E_p$-re pontosan egy α-őrző részcsoport tartozik. Ugyanis igaz a következő:

4.3. **Lemma.** *Legyen* G_α *α-őrző,* G_β *β-őrző részcsoport.* $[G_\alpha \cup \{x+1\}] = [G_\beta \cup \{x+1\}]$ *akkor és csak akkor igaz, ha* $|G_\alpha| = |G_\beta|$. *Továbbá* $|[G_\alpha \cup \{x+1\}]| = p \cdot |G_\alpha|$.

Bizonyítás. A G_α csoport rendje, $|G_\alpha|$ azonos a G_α-beli függvények x együtthatóiból képezett H mod p multiplikativ csoport rendjével, minthogy e két ciklikus csoport izomorf a következő megfeleltetéssel:

$$Ha \leftrightarrow ax + (1-a)\alpha \epsilon G_\alpha.$$

Ebből mindkét állítás helyessége leolvasható. ■

A kölcsönös egyértelmüség következtében a $p \cdot q_1^{\lambda_1} \cdot \ldots \cdot q_u^{\lambda_u}$ rendü G részcsoportnak megfeleltethetjük a $\lambda_1 \lambda_2 \ldots \lambda_u$ sorozatot. Általánosabban, a $p^{\lambda_0} \cdot q_1^{\lambda_1} \cdot \ldots q_u^{\lambda_u}$ rendü részcsoporthoz rendeljük hozzá a $p+u$ hosszuságú $\mu_0 \mu_1 \ldots \mu_{p-1} \lambda_1 \ldots \lambda_u$ sorozatot a következő, kölcsönösen egyértelmü módon $(i \epsilon E_p)$:

$$\mu_i = \begin{cases} 1, & \text{ha} \quad \lambda_0 = 1 \\ 0, & \text{ha} \quad \lambda_0 = \lambda_1 = \ldots = \lambda_u = 0 \\ 1 - (i-\alpha)^{p-1} \ (\mathrm{mod} p), & \text{egyébként.} \end{cases}$$

Legyen G_α α-őrző, $g = |G_\alpha| \leqslant p-1$ rendü részcsoport, $\frac{p-1}{g} = h$. Képezzük az

$$F_0 = \{\alpha\} \cup G_\alpha, \ F_1 = [\{\beta_1\} \cup F_0], \ldots, F_i = [\{\beta_i\} \cup F_{i-1}], \ldots, F_h = [\{\beta_h\} \cup F_{h-1}] = G_\alpha \cup L^{(0)}.$$

sorozatot, ahol $\beta_1 \neq \alpha$, $\beta_i \epsilon L^{(0)} \setminus F_{i-1}$, $i = 1,2,\ldots,h$. Világos, hogy F_i maximális F_{i+1}-ben, $i = 0,1,\ldots,h-1$. Hogy a $G_\alpha \subset F_0 \subset F_1 \subset \ldots \subset F_h = G_\alpha \cup L^{(0)}$ láncok $\frac{p-1}{g} + 2$ elemüek, az abból következik, hogy G_α bármely bázis-elemének elem-idegen ciklus-felbontása ugyanazt a $\frac{p-1}{g} + 1$ elemü particiót indukálja az E_p halmazon. Ebben $\{\alpha\}$ egyelemü halmaz, a többi h számú halmaz mindegyike g elemü. Ugyanigy képezhetők az $F_i' = F_i \setminus \{\alpha\}$, $i = 0,1,\ldots,h$ halmazok.

Hasonló módon $|G| \geqslant p$ esetén G-hez csak a kételemü $G \subset G \cup L^{(0)}$ lánc tartozik. Az $\{x\}$ triviális csoporthoz viszont E_p részhalmaz-hálójának bármely lánca hozzárendelhető, igy az $\{x\} \subset \{x\} \cup \{0\} \subset \{x\} \cup \{0,1\} \subset \ldots \subset \{x\} \cup L^{(0)}$ tipusú láncok hossza $p+1$. (összhangban azzal, hogy $\{x\}$ α-őrző és $h = p-1$).

Rendeljünk minden $F = G \cup K \subseteq L^{(1)}$ zárt osztályhoz bináris sorozatot, amelynek az első $p+u$ eleme a G-hez rendelt $\mu_0 \mu_1 \ldots \mu_{p-1} \lambda_1 \ldots \lambda_u$ sorozat, a következő p számú elem pedig a $K \subseteq L^{(0)}$ karakterisztikus sorozata, azaz $\nu_i = 1$, ha $i \epsilon K$ és $\nu_i = 0$, ha

$i \notin K$, $i = 0,1, \ldots, p-1$. Végeredményben bármely $G \subseteq L^{(1)} \setminus L^{(0)}$ részcsoport esetén annak maximális rendü ciklikus részcsoportja által indukált partició elemeiből egyesitéssel adódnak a megfelelő K halmazok. Igy minden F zárt halmaz előáll és más halmaz nem adódik. Ezért $\{x\}$ esetén tetszőleges $\nu_0\nu_1 \ldots \nu_{p-1}$ bináris sorozat megfelelő, G_α α-őrző g-rendü csoprt esetén $\nu_\alpha = 1$ minden F_i és F_i'-ben, továbbá F_i-ben $1 + i \cdot g$ számú ν értéke 1, a többi zérus, F_i'-ben $i \cdot g$ számú ν értéke 1, a többi zérus.

Végül $|G| \geqslant p$ esetén $G \cup L^{(0)}$-hoz a $\nu_i = 1$, $i = 0,1, \ldots, p-1$ sorozat, s általában $G \subseteq L^{(1)} \setminus L^{(0)}$-hoz a $\nu_i = 0$, $i = 0,1, \ldots, p-1$ sorozat tartozik.

Az F zárt osztályhoz tartozó $\mu\lambda\nu = \mu_0\mu_1 \ldots \mu_{p-1}\lambda_1 \ldots \lambda_u\nu_0\nu_1 \ldots \nu_{p-1}$ sorozatok konstruálásánál az volt a célunk, hogy a sorozatok szokásos rendezése a zárt osztályok tartalmazás szerinti rendezését megőrizze.
A parciális rendezés: $\gamma_1\gamma_2 \ldots \gamma_k \leqslant \delta_1\delta_2 \ldots \delta_k$, ha $\gamma_j \leqslant \delta_j$, $j = 1,2, \ldots, k$.
Nevezzük a γ bináris sorozat súlyának és jelöljük $s(\gamma)$-val a benne előforduló 1-ek számát. Definiáljuk a μ sorozattól függően az N_μ halmazt a következőképpen:

$$N_\mu = \begin{cases} \{0,p\}, & \text{ha } s(\mu) = p; \\ \left\{l \cdot g,\ l \cdot g + 1 \mid g = p_1^{\lambda_1} \ldots p_u^{\lambda_u},\ l = 0,1, \ldots, \frac{p-1}{g}\right\}, & \text{ha } s(\mu) = 1, \\ \{0,1, \ldots, p\} & \text{ha } s(\mu) = 0. \end{cases}$$

Most már megfogalmazhatjuk az $L^{(1)}$ szerkezetét leiró tételt.

4.3. **Tétel.**

A.) *Az* $L^{(1)} \setminus L^{(0)}$ *csoport részcsoport hálója izomorf a*

$$\Gamma = \{\mu\lambda \mid \mu_i \in \{0,1\},\ 0 \leqslant \lambda_j \leqslant \kappa_j,\ i \in E_p,\ j = 1,2, \ldots, u;\ s(\mu) \in \{0,1,p\}\}$$

parciálisan rendezett halmazt leiró hálóval.

B.) *Az* $L^{(1)}$ *félcsoport részfélcsoport-hálója izomorf a*

$$\Delta = \{\mu\lambda\nu \mid \mu\lambda \in \Gamma,\ s(\nu) \in N_\mu,\ \text{és} \quad \nu_i \geqslant \mu_i,\ \text{ha } s(\mu) = 1\}$$

parciálisan rendezett halmazt leiró hálóval.

Bizonyitás. A konstrukcióból következik, hogy $L^{(1)}$ minden zárt osztályához pontosan egy Δ-beli sorozat tartozik és megforditva, Δ minden eleméhez pontosan egy $L^{(1)}$-beli zárt osztályt rendeltünk. Ezért csak a rendezés-tartást kell megmutatni. Legyen $G_2 \cup K_2$ maximális osztály a $G_1 \cup K_1$ zárt osztályban. Ha $|G_1| \geqslant p$, akkor $K_1 = L^{(0)}$ és G_2 maximális G_1-ben (4.1. lemma). Ezért $\mu_i^{(1)} = 1 = \nu_i^{(1)}$, $i \in E_p$, és $\lambda^{(2)} \leqslant \lambda^{(1)}$ a Lagrange-tétel következtében.
Ha $|G_1| \leqslant p-1$, akkor $G_1 = G_2$ esetén $K_2 \subset K_1$ és igy $\mu^{(1)}\lambda^{(1)} = \mu^{(2)}\lambda^{(2)}$, $\nu^{(2)} < \nu^{(1)}$. A $G_2 \subset G_1$ esetben viszont $\mu^{(2)} \leqslant \mu^{(1)}$, $s(\mu^{(1)}) = 1$ és $\lambda^{(2)} < \lambda^{(1)}$ nyilvánvaló, s $K_2 \subseteq K_1$ következtében $\nu^{(2)} \leqslant \nu^{(1)}$ is teljesül. Ezért valóban $\mu^{(2)}\lambda^{(2)}\nu^{(2)} < \mu^{(1)}\lambda^{(1)}\nu^{(1)}$ minden esetben teljesül. ■

A 4.3. tételből kiindulva, meghatározhatjuk az $L^{(1)} \setminus L^{(0)}$ illetve $L^{(1)}$-beli zárt osztályok számát. Jelölje $d(a)$ az "a" szám pozitiv osztóinak számát.

4.4. **Tétel.**

A.) *Az* $L^{(1)} \setminus L^{(0)}$ *csoport részcsoportjainak száma*:

$$|\Gamma| = (p + 1)d(p - 1) - p + 1.$$

B.) *Az* $L^{(1)}$ *félcsoport részfelcsoportjainak száma*:

$$|\Delta| = 2d(p - 1) - (p - 1)2^p + 2p \cdot \sum_{g|p-1} 2^g.$$

Bizonyitás.

A.) Az $s(\mu) = 0$ súlyhoz egyetlen, $\mu\lambda = 00 \ldots 0$ sorozat, $s(\mu) = p$ súlyhoz egyetlen μ és $d(p - 1)$ számú λ sorozat, $s(\mu) = 1$ súlyhoz p számú μ-sorozat és mindegyikhez $d(p - 1) - 1$ számú λ sorozat tartozik.
Ezek összege:

$$|\Gamma| = 1 + 1 \cdot d(p - 1) + p \cdot (d(p - 1) - 1) = (p + 1)d(p - 1) - p + 1.$$

B.) Az $s(\nu) = 0$ súlyhoz tartoznak az A.) részben számitott zárt osztályok, $s(\mu) = p = s(\nu)$ súlypárnak $d(p - 1)$ számú λ sorozat felel meg. Az $s(\mu) = 0 \neq s(\nu)$ kombinációhoz $2^p - 1$ számú sorozat tartozik. Legyen most $s(\mu) = 1$, $s(\nu) \neq 0$.
(Ez esetben az $L^{(1)} \setminus L^{(0)}$-hez tartozó rész mindegyik zárt osztályban α-őrző részosztály s ez ciklikus csoport.)
Az $s(\mu) = 1$ súlyú sorozatok száma p s ezek mindegyikéhez – rögzitett g esetén $\sum_{l=0}^{h} \binom{h}{l}$ féleképpen választható $1 + l \cdot g$ tipusú $s(\nu)$ súlyoknak megfelelő sorozat és hasonlóan $\sum_{l=1}^{h} \binom{h}{l}$ számú lesz az $s(\nu) = l \cdot g (l = 1,2, \ldots, h)$ súlyú ν sorozatok száma. Ezek összege:

$$\Delta = |\Gamma| + d(p - 1) + (2^p - 1) + p \cdot \sum_{\substack{g|p-1 \\ g \neq 1}} (2 \cdot \sum_{l=0}^{h} \binom{h}{l} - 1) =$$

$$= (p + 2)d(p - 1) - p + 2^p + p \cdot (\sum_{g|p-1} (2^{h+1} - 1) - (2^p - 1)) =$$

$$= (p + 2)d(p - 1) - (p - 1)2^p - p \sum_{g|p-1} 1 + 2p \sum_{g|p-1}' 2^h =$$

$$= 2d(p - 1) - (p - 1)2^p + 2p \cdot \sum_{g|p-1} 2^g. \blacksquare$$

5. Számosság, és néhány záró megjegyzés

A 4.4. tétel és az 1. ábrán összefoglalt rész-szerkezet alapján könnyen megadhatjuk az L-beli zárt osztályok teljes számát. Az L lineáris osztály szerkezetét leiró hálóhoz rendelt irányitott gráf láncain irányitott utakat értünk. Világos, hogy a maximális hosszúságú lánc hossza az (L) gyökérpont feletti magasság. Legyen most is $p-1$ kanonikus felbontása

$$p-1 = q_1^{\kappa} \cdot \ldots \cdot q_u^{\kappa u}.$$

5.1. **Tétel.**

1.) Az L lineáris osztály zárt osztályainak száma:

$$p+3-(p-1)2^p + 2d(p-1) + 2p \sum_{g/p-1} 2^g.$$

2.) *Az L lineáris osztály maximális illetve minimális láncainak hossza*:

$$p+2+\sum_{i=1}^{u} \kappa_i, \text{ illetve } 3.$$

Bizonyitás.

1.) Az L lineáris osztály többváltozós függvényeket is tartalmazó osztályai: $L, L_0, L_1, \ldots, L_{p-1}, L_*, L_{*0}$, igy ezek száma $p+3$. Ezért a 4.4. tétellel együtt ez bizonyitja az állitást.

2.) Könnyen látható, hogy a maximális lánc tartalmazza az $(L^{(1)})$ pontot. Világos, hogy $L^{(1)}$-ben minden lépésnél vagy a $p(p-1)$ kanonikus felbontásához tartozó $1+\sum_{i=1}^{u} \kappa_i$ kitevő-összeg, vagy a zárt osztályhoz tartozó konstansok száma csökken.

Ezért a lánc-hosszakra felső korlát az

$$1+|L^{(0)}|+\quad 1+\sum_{i=1}^{u} \kappa_i \quad = p+2+\sum_{i=1}^{u} \kappa_i.$$

Ez a korlát elérhető, mert az

$$\to (L^{(1)}) \to \ldots \to (G \cup L^{(0)}) \to \ldots \to (L_*^{(1)} \cup L^{(0)}) \to (\{x\} \cup L^{(0)}) \to (\{x\} \cup L^{(0)} \setminus \{0\}) \to \ldots \to (\{x\})$$

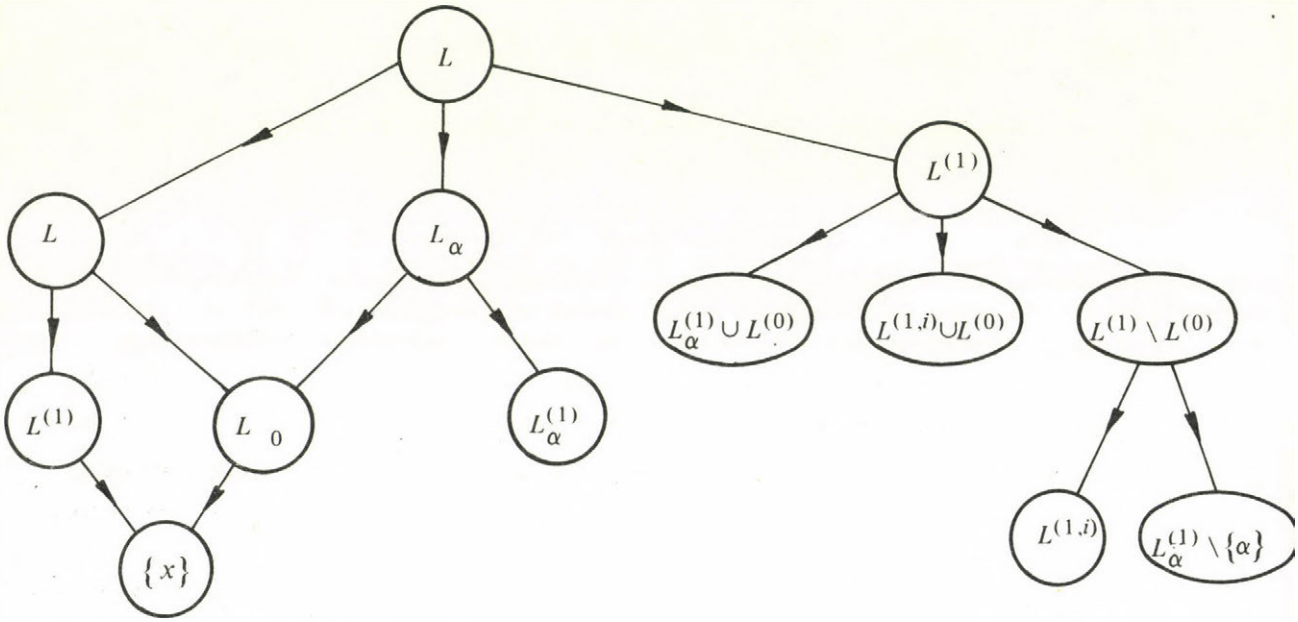
utvonal hossza éppen ezzel egyezik.

A minimális lánc:

$$(L) \to (L_*) \to (L_{*0}) \to (\{x\}). \blacksquare$$

Végül az 1. ábra a különböző tipusú zárt osztályok tartalmazás szerinti rendezését mutatja.

Megjegyzés a korrekturánál. A kézirat leadása után jutott tudomásunkra, hogy az L_α, L_* , L_{*0} ($\alpha = 0,1, \ldots p-1$) zárt osztályokat A.Salomaa meghatározta a P_k-beli zárt osztályok halmazának számosságát vizsgáló alábbi dolgozatában : "On infinitely generated sets of operations infinite algebras", Ann. Univ. Turkuensis, ser. A. I. 74. (1964) 1-13.



1. ábra

Osztály	Bázis	Rendszám
L	$\{x + 1, x + y\}$	2
L_α $(0 \leqslant \alpha \leqslant p-1)$	$\{x + y + (p-1)\alpha\}$	2
L_*	$\{2x + (p-1)y + 1\}$	2
$L^{(1)}$	$0, x + 1, ax$, ha $r(a) = p - 1$	1
L_{*0}	$2x + (p-1)y$	2
$L^{(1)}_\alpha$ $0 \leqslant \alpha \leqslant p-1$	$\alpha, ax + (1-a)\alpha$ ha $r(a) = p - 1$	1
$L^{(1)}_*$	$x + 1$	1
$L^{(1)} \setminus L^{(0)}$	$x + 1, ax$ ha $r(a) = p - 1$	1

Táblázat

I r o d a l o m

[1] Bagyinszki, J., Az m-értékü logika függvényrendszereinek funkcionális teljessége KFKI-tanulmány KFKI-73-55.

[2] Birkhoff, G., Bartee, T.C., A modern algebra a számitógép-tudományban M.K. (1974)

[3] Demetrovics, J., A kétértékü logika strukturális vizsgálata, Alkalmazott Matematikai Lapok 2 (1975)

[4] Post, E., The two-valued iterative systems of mathematical logic, Annals of Math. Studies, 5 (1941).

[5] Rosenberg, I., La structure des funktions de plusieurs variables sur un ensemble fini, C.r. Acad. Sci. Paris 14 (1969) 413-438.

[6] Salomaa, A., Some compleleteness criteria for sets of funktions over a finite domain I.-II. Ann. Univ. Turkuensis Ser. A. I 53 (1962) 1-9. 63 (1963) 1-19.

[7] Яблонский С.В., Функциональные построения в k-значной логике, Труды МИАН СССР 51 /1958/ 5-142.

[8] Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б., Функции алгебры логики и классы Поста, М., "Наука", /1966/

[9] Янов Ю.И., Мучник А.А., О существовании k-значных замкнутых классов, не имеющих конечного базиса, ДАН СССР 127, /1959/ 1, 44-46.

Summary

The structure of linear classes in prime valued logics

J. Bagyinszki, J. Demetrovics

In the present paper the following are stated for logics with a prime number of values:

a.) there is a finite number of closed linear classes; their exact number is given.
b.) the base and the rank of each linear class are given.
c.) the structure of the linear classes are given, including the lenght of their minimal chains.

Р е з ю м е

СТРУКТУРА ЛИНЕЙНЫХ КЛАССОВ В P_k
ПРИ k РАВНО ПРОСТОМУ ЧИСЛУ

Я. Бадьинский – Я. Деметрович

В этой работе доказывается, что в k-значной логике, при k=простое число, имеют места следующие утверждения:

а/ имеется конечное число линейных классов и определяется их точные числа,

б/ определяется порядок и базис каждого линейного класса,

в/ определяем структуру линейных классов и длину максимальных и минимальных цепей.

MTA Számitástechnikai és Automatizálási Kutató Intézete, **Közlemények** 16/1976.

TETSZŐLEGESEN NAGY EGÉSZ SZÁMOKKAL VALÓ PONTOS SZÁMOLÁS SZÁMITÓGÉPPEL

Gesztelyi Ernő – Jékel Pál
(Debrecen, KLTE Számitástudományi Tanszék)

0. Bevezetés

Adott számitógéppel rendelkező számolóközpont kerülhet olyan feladat elé, hogy olyan nagy egész számokkal kellene aritmetikai müveleteket pontosan végezni, amelyek nagyobbak mint a gépen ábrázolható legnagyobb egész szám. Természetesen sok esetben megoldható a probléma, ha dupla, tripla, stb. hosszuságu számokkal dolgozunk, az ALGOL 68 terminológiájával kifejezve: ha rátérünk a *long integer*, vagy *long long integer*, stb. módu számokkal való számolásra. Természetesen adott gépi reprezentáció esetén a *long*-ok száma korlátozott, és ezért adott gépen igy nem minden feladat végezhető el. (Tudomásunk szerint nagy teljesitményü számitógépekkel végeznek olyan vizsgálatokat, amelyekkel igen nagy számokra vonatkozó, számelméleti érdekességgel biró kérdéseket döntenek el.)

Jelen dolgozatnak az a célja, hogy megmutassunk egy módszert arra, hogy hogyan lehet bármilyen nagy egész számokkal pontos számitásokat végeztetni rekeszek összekapcsolása nélkül. Természetesen módszerünk akkor is alkalmazható, ha mód van rekeszek összekapcsolására, ebben az esetben a programok futási ideje rövidül le.

A módszer alapgondolata a következő: Tekintsünk valamilyen b alapot, és az egész számokat b alapú számrendszerben megadva képzeljük el. Akkor adott szám esetén minden számjegyet elhelyezhetünk egy egy memória rekeszben. Ilyen módon igen nagy egész számok ábrázolhatók a gépben, tekintve, hogy még az operativ memória rekeszeinek a száma is tekintélyes, nem is beszélve arról, hogy dobra is vihetők. Általában azonban nincs szükség a számoknak a memóriában való tárolására, konkrét esetekben elegendő a számjegyeket előállitó valamilyen eljárás algoritmusát tárolni a memóriában.

Legyen tehát $f(n)$ és $g(n)$ két függvényeljárás, melyek egy-egy pozitiv egész szám b alapu számjegyeit generálják ugy, hogy a függvényértékek a b^n együtthatóját szolgáltatják. (Megjegyezzük, hogy ha egy számot a fentebb leirt módon tároljuk a memóriában, akkor célszerü egy vektorban elhelyezni, és akkor (az ALGOL 60 terminológiáját használva) $f[n]$-et és $g[n]$-et irunk). Akkor felirhatunk egy eljárást, mely az $f(n) + g(n)$ értékeket generálja. Mivel általában $f(n) + g(n) > b$ ezért $f(n) + g(n)$ nem adja meg általában valamilyen egész szám b alapu számjegyeit. A dolgozatban megadunk egy Tb nevü eljárást, melynek alkalmazásával $Tb(f(n) + g(n))$ már olyan függvény lesz, amely megadja a

$$\sum_{n=0}^{N} (f(n) + g(n))b^n$$

szám b alapu számjegyeit, ahol N egy bizonyos szám ugy, hogy $f(n) = 0$ ha $n > N$.

Ha az f eljárás és a g eljárás által meghatározott egész számok szorzatát akarjuk megkapni akkor képezni kell a

$$\sum_{k=0}^{N} f(n-k)g(k)$$

konvolueiót, és azután alávetni a Tb eljárásnak, hogy megkapjuk a szorzat számjegyeit.

Ha rekeszeket kapcsolunk össze, akkor valamilyen módon (hardware, vagy software eszközökkel) meg kell oldani az átvitel próbjémáját. A mi esetünkben tehát a müveletek végzése és az átvitel külön van választva. Ha több müveletet kell egy feladat kapcsán elvégezni, akkor nem szükséges minden művelet elvégzése után alkalmazni a Tb eljárást. Ha túlcsordulás veszélye nem áll fenn, akkor elég csak a müveletsor végén alkalmazni a Tb eljárást, hogy a végeredményt megkapjuk.

Célszerü b-t minél nagyobbra választani, és nagyságát csak a túlcsordulás korlátozza. Ugyanis minél nagyobb a b annál jobban kihasználhatjuk a gép gyors aritmetikáját.

Gyakorlatilag célszerü az is, ha $b = 10^m$ (m pozitiv egész) mert ekkor nincs szükség olyan algoritmusra, mely a b alapu számrendszerből a 10-es alapu számrendszerbe alakit át. Ugyanis a kiiratásnál elegendő a rekeszek tartalmát a legnagyobb helyértékü tagtól kezdve visszafelé kiiratni egymás mellé, és akkor megkapjuk a szám 10-es számrendszerbeli alakját.

A dolgozat tárgyalásmódja a matematikai precizitás követelményeit igyekszik megvalósitani. Enélkül ugyanis nem lehetünk biztosak abban, hogy a gép valóban azt számolja-e ki, amit akarunk.

A dolgozat végén egy programot közlünk ALGOL 60 nyelven, amelyet az ODRA 1204 gépen le is futtattunk. A program táblázatot készit a pozitiv egész számok faktoriálisairól 1-től kezdve folyamatosan.

1. Egész értékeket felvevő véges tartószámú aritmetikai függvények

1.1 **Definició.** I-vel jelöljük azoknak az f függvényeknek a halmazát, melyek a következő tulajdonságoknak tesznek eleget.

a.) f értelmezési tartománya a nem negativ egész számok halmaza.
b.) Az f értékkészlete az egész számok halmazának részhalmaza.
c.) Minden $f \neq 0$ függvényhez f-től függően tartozik egy N nemnegativ egész úgy, hogy $f(N) \neq 0$, de ha $n > N$ akkor $f(n) = 0$.
d.) Az azonosan zérus értéket felvevő függvény I-be tartozik.

1.2 **Definició.** Legyen $f \in I$ és $f \neq 0$. Azt a N számot, amelyre $f(N) \neq 0$ de minden $n > N$ mellett $f(n) = 0$, az f függvény felső tartó számának nevezzük és Supp$f$-fel jelöljük, vagyis:

(1) $N = \text{Supp}f$, ha $f(N) \neq 0$, de minden $n > N$ mellett $f(n) = 0$.

1.3. **Definició.** *I-ben* értelmezzük az összeadást és a konvolúciós szorzást a következő módon: Legyen $f,g \in I$, akkor

(2) $(f + g)(n) = f(n) + g(n)$

(3) $(f * g)(n) = \sum_{k=0}^{n} f(n - k)g(k).$

1.1. **Tétel.** *Ha* $f,g \in I$ *akkor* $f + g \in I$ *és* $f * g \in I$ *és ha* $f,g,f + g \neq 0$ *akkor*

(4) $\text{Supp}(f + g) \leqslant \max(\text{Supp}f, \text{Supp}g)$ *és ha* $f,g \neq 0$ *akkor* $f * g \neq 0$ *és*

(5) $\text{Supp}(f * g) = \text{Supp}f + \text{Supp}g.$

Bizonyitás. Az 1.1. definició *a* és *b* tulajdonságának nyilván eleget tesz $f + g$ is és $f*g$ is, ha $f,g \in I$. Mivel az is triviális, hogy ha f és g közül legalább az egyik azonosan zérus, akkor $f + g$ is és $f*g$ is I-be tartozik, elég csak a (4) és (5) tulajdonságot igazolni, mert ezekből a c) tulajdonság az összegre és a konvolúcióra már következik.
Legyen tehát $f,g \in I$. Ha $f + g = 0$, akkor az 1. definició d) miatt $f + g \in I$.

Tegyük fel, hogy $f + g \neq 0$, és legyen $N = \max(\text{Supp}f, \text{Supp}g)$. Ha $n > N$, akkor igy $f(n) = 0$ és $g(n) = 0$, tehát

(6) $(f + g)(n) = f(n) + g(n) = 0 \qquad (n > N).$

Mivel $f + g \neq 0$, ezért van olyan legnagyobb N_0 melyre $(f + g)(N_0) \neq 0$ és (6) miatt nyilván $N_0 \leqslant N$.

Mivel igy $N_0 = \text{Supp}(f + g)$, ezért a (4) egyenlőtlenséget igazoltuk.

Most rátérünk az (5) egyenlőség igazolására, ahol feltesszük, hogy $f,g \neq 0$ és $f,g \in I$. $f,g \neq 0$ miatt létezik

(7) $N_1 = \text{Supp}f$

és

(8) $N_2 = \text{Supp}g.$

Először megmutatjuk, hogy ha

(9) $N_0 = N_1 + N_2$

akkor

(10) $(f * g)(N_0) = \sum_{k=0}^{N_0} f(N_0 - k)g(k) \neq 0,$

mert, mint igazolni fogjuk,

(11) $\quad (f * g)(N_0) = f(N_1)g(N_2),$

és mivel (7) és (8) miatt $f(N_1) \neq 0$ és $g(N_2) \neq 0$, igy $(f*g)(N_0) = f(N_1)g(N_2) \neq 0$. Ha $k = N_2$, akkor $f(N_0 - k)g(k) = f(N_1)g(N_2)$. Tehát (10) belátásához azt kell kimutatni, hogy ha $k \neq N_2$, akkor

(12) $\quad f(N_0 - k)g(k) = 0.$

Valóban, ha $k < N_2$, akkor $N_0 - k > N_1$ és igy (7) miatt $f(N_0 - k) = 0$ következtében teljesül (12). Ha pedig $k > N_2$, akkor (8) miatt $g(k) = 0$ és igy megint igaz a (12) egyenlőség. Tehát a (10) egyenlőség valóban fennáll.

Most azt igazoljuk, hogy ha $n > N_0$, akkor $(f * g)(n) = 0$. Valóban, ha a $\sum_{k=0}^{n} f(n-k)g(k)$ összegben $k \leqslant N_2$, akkor $n - k > N_1$ és akkor $f(n-k) = 0$, ha pedig $k > N_2$, akkor $g(k) = 0$, és igy $(f * g)(n) = 0$. Tehát $N_0 = \mathrm{Supp}(f * g)$ és igy az (5) egyenlőség (7), (8) és (9) következménye.

1.2. **Tétel.** *Az I halmaz a* (2) *és* (3) *alatt értelmezett műveletekre nézve nullosztómentes kommutativ gyűrűt alkot.**

Bizonyitás. Az 1.1. tételben igazoltuk, hogy a (2) és (3) alatti müveletek nem vezetnek ki az I-ből. Könnyen igazolható, hogy I az összeadásra nézve Ábel-csoportot alkot. Ismeretes, hogy a (3) alatti konvolúció kommutativ, associativ és az összeadásra nézve disztributiv művelet. Igy tehát I valóban kommutativ gyürü. A nullosztómentesség (5) következménye.

2. A szummációs transzformáció

2.1. **Definició.** Legyen $b > 1$ egész szám. I-ben értelmezünk egy S_b-vel jelölt transzformációt, melyet "b-re vonatkozó szummációs transzformációnak" nevezünk, és igy értelmezzük:

(1) $$(S_b f)(n) = \begin{cases} \sum_{k=0}^{\mathrm{Supp}f} f(k)b^k, & \text{ha } n = 0 \\ 0, & \text{ha } n > 0 \end{cases} \qquad (f \epsilon I)$$

Megjegyzés. Mivel $f(k) = 0$, ha $k > \mathrm{Supp}f$, ezért azt is irhatjuk, hogy

(2) $\quad (S_b f)(0) = \sum_{k=0}^{\infty} f(k)b^k.$

* L.BERG: EINFÜHRUNG IN DIE OPERATORENRECHNUNG, Berlin, 1962.

Megjegyzés. Világos, hogy ha $f \in I$, akkor $S_b f \in I$, azaz $S_b : I \longrightarrow I$.

Megjegyzés. Nyilvánvaló az is, hogy ha $(S_b f)(0) \neq 0$, akkor

(3) $\quad \mathrm{Supp}(S_b f) = 0.$

2.1.**Tétel.** *Az* S_b *transzformáció additiv*:

(4) $\quad S_b(f + g) = S_b f + S_b g \qquad (f, g \in I).$

Bizonyítás. Ha $n > 0$, nyilván igaz, hogy

(5) $\quad (S_b(f + g))(n) = (S_b f)(n) + (S_b g)(n),$

mert mindkét oldal zérus. Ha $n = 0$, akkor pedig

$$(S_b(f + g))(0) = \sum_{k=0}^{\infty} (f + g)(k) b^k = \sum_{k=0}^{\infty} f(k) b^k + \sum_{k=0}^{\infty} g(k) b^k =$$

$$= (S_b f)(0) + (S_b g)(0),$$

és igy (5) minden $n = 0,1,2, \ldots$ egészre teljesül, ami (4)-et igazolja.

2.2.**Tétel.** Az S_b transzformáció multiplikativ:

(6) $\quad S_b(f * g) = (S_b f) * (S_b g) \qquad (f, g \in I)$

és

(7) $\quad (S_b(f * g))(0) = (S_b f)(0) \cdot (S_b g)(0).$

Bizonyítás. Először a (7) egyenlőséget igazoljuk, vagyis azt, hogy

(8) $$\sum_{n=0}^{\mathrm{Supp}(f * g)} (f * g)(n) b^n = \sum_{n=0}^{\mathrm{Supp}\, f} f(n) b^n \cdot \sum_{n=0}^{\mathrm{Supp}\, g} g(n) b^n.$$

Legyen $N_1 = \mathrm{Supp} f$ és $N_2 = \mathrm{Supp} g$ (feltehetjük ugyanis, hogy $f, g \neq 0$, mert ha f és g egyike is azonosan zérus, akkor (6) és (7) nyilvánvalóan teljesül). Akkor $N_0 = N_1 + N_2$ jelöléssel

$$\sum_{n=0}^{\mathrm{Supp}(f*g)} (f*g)(n)b^n = \sum_{n=0}^{N_0}\sum_{k=0}^{n} f(n-k)g(k)b^n = \sum_{k=0}^{N_0}\sum_{n=k}^{N_0} f(n-k)g(k)b^n =$$

$$= \sum_{k=0}^{N_0} g(k) \sum_{n=k}^{N_0} f(n-k)b^n = \sum_{k=0}^{N_2} g(k) \sum_{m=0}^{N_0-k} f(m)b^{k+m} =$$

$$= \sum_{k=0}^{N_2} g(k)b^k \sum_{m=0}^{N_0-k} f(m)b^m = \sum_{k=0}^{N_2} g(k)b^k \cdot \sum_{m=0}^{N_1} f(m)b^m .$$

Tehát (8) és igy (7) is teljesül. A (6) egyenlőség (7)-ből a következő tételből közvetlenül következik.

2.3. **Tétel.** *Legyen*

$$\delta(n) = \begin{cases} 1, & \text{ha } n = 0 \\ 0, & \text{ha } n > 0 \end{cases} \tag{9}$$

és legyen a tetszőleges szám. Akkor bármely $f \in I$-re

$$(f * a\delta)(n) = af(n). \tag{10}$$

Bizonyitás.

$$(f*a\delta)(n) = \sum_{k=0}^{n} f(n-k)a\delta(k) = f(n)a\delta(0) = af(n).$$

Megjegyzés. A fenti tétel alapján (7)-ből (6) igy következik: A (9) alatt értelmezett δ függvény felhasználásával kapjuk minden $n \geqslant 0$ mellett, hogy

$$\left.\begin{aligned} &(S_b f)(n) = (S_b f)(0)\delta(n) \quad \text{és} \quad (S_b g)(n) = (S_b g)(0)\delta(n) \quad \text{és} \\ &(S_b(f*g))(n) = (S_b(f*g))(0)\delta(n) \end{aligned}\right\}$$

és igy (10) és (7) felhasználásával:

$$((S_b f) * (S_b g))(n) = (((S_b f)(0) \cdot \delta) * ((S_b f)(0) \cdot \delta))(n) =$$

$$= (S_b f)(0) \cdot (S_b g)(0)\delta(n) = (S_b(f*g))(0)\delta(0) = (S_b(f*g))(n).$$

Tehát valóban igaz a (6) egyenlőség.

Megjegyzés. Ha (10)-ben $a = 1$ akkor speciálisan kapjuk, hogy

$$f*\delta = f, \tag{11}$$

vagyis a δ függvény a konvolúciós szorzás egységeleme.

Tehát I egységelemes kommutatitv gyürü de nem test, mint arról könnyen meggyőződhetünk.

3. Az egészértékü aritmetikai függvények ekvivalenciája

3.1. **Definició.** I-ben bevezetünk egy ekvivalencia relációt, melyet a következőképpen értelmezünk: Legyen $f_1, f_2 \epsilon I$. f_1 ekvivalens f_2-vel, jelben: $f_1 \overset{b}{\sim} f_2$, akkor és csak akkor ha

$$S_b f_1 = S_b f_2 .$$

Megjegyzés. A 3.1. definicióból rögtön következik, hogy annak a szükséges és elégséges feltétele, hogy $f_1 \overset{b}{\sim} f_2$ legyen az, hogy

$$(1) \qquad \sum_{k=0}^{\mathrm{Supp} f_1}{}' f_1(k) b^k = \sum_{k=0}^{\mathrm{Supp} f_2}{}' f_2(k) b^k$$

teljesüljön.

Megjegyzés. A 3.1. definició alatt értelmezett ekvivalencia reláció természetesen b-től függ.
Ha két I-beli függvény egy adott b-re vonatkozóan ekvivalens, egy másik b-re vonatkozóan álatlában nem ekvivalens.
Ha például $f_1(0) = 1$, $f_1(1) = 1$, $\mathrm{Supp} f_1 = 1$ és $f_2(0) = 3$, $\mathrm{Supp} f_2 = 0$, akkor $f_1 \overset{2}{\sim} f_2$, de ha $b = 10$, akkor nem ekvivalensek, mert

$$\sum_{k=0}^{1}{}' f_1(k) 10^k = 11 \neq 3 = \sum_{k=0}^{0}{}' f_2(k) 10^k .$$

Ha a félreértés lehetősége kizárt, akkor az egyszerübb $\sim$ jelölést használjuk.

Megjegyzés. A 3.1. definicióban értelmezett reláció valóban ekvivalencia reláció, könnyen látható, hogy reflex, szimmetrikus, és tranzitiv, azaz

1.) $f \overset{b}{\sim} f$
2.) Ha $f_1 \overset{b}{\sim} f_2$ akkor $f_2 \overset{b}{\sim} f_1$
3.) Ha $f_1 \overset{b}{\sim} f_2$ és $f_2 \overset{b}{\sim} f_3$, akkor $f_1 \overset{b}{\sim} f_3$

A következőkben, mint eddig is, egy adott b-t mindig lerögzitettnek képzelünk, és igy a $\overset{b}{\sim}$ jelölés helyett a $\sim$ jelölést félreértés nélkül használhatjuk.

3.1. **Tétel.** *A* 3.1. *definicióban értelmezett ekvivalencia reláció kompatibilis az összeadásra és a konvolucios szorzásra nézve, vagyis, ha* $f_1 \sim f_2$ *és* $g_1 \sim g_2$,

$(f_1, f_2, g_1, g_2 \epsilon I)$, akkor

$$(2) \qquad f_1 + g_1 \sim f_2 + g_2$$

és

$$(3) \qquad f_1 * g_1 \sim f_2 * g_2 .$$

Bizonyitás. Mivel

$$(4) \qquad \sum_{k=0}^{\infty} f_1(k)b^k = \sum_{k=0}^{\infty} f_2(k)b^k$$

és

$$(5) \qquad \sum_{k=0}^{\infty} g_1(k)b^k = \sum_{k=0}^{\infty} g_2(k)b^k$$

ezért (4) és (5) alapján

$$\sum_{k=0}^{\infty} (f_1 + g_1)(k)b^k = \sum_{k=0}^{\infty} f_1(k)b^k + \sum_{k=0}^{\infty} g_1(k)b^k = \sum_{k=0}^{\infty} f_2(k)b^k + \sum_{k=0}^{\infty} g_2(k)b^k = \sum_{k=0}^{\infty} (f_2 + g_2)($$

azaz teljesül (2).

Most igazolni fogjuk, hogy (3) is fennáll. Mivel $f_1 \sim f_2$ és $g_1 \sim g_2$ ezért

$$(6) \qquad S_b f_1 = S_b f_2$$

és

$$(7) \qquad S_b g_1 = S_b g_2.$$

A 2.2 tétel felhasználásával (2-6 képlet) (6) és (7) miatt

$$S_b(f_1 * g_1) = (S_b f_1) * (S_b g_1) = (S_b f_2) * (S_b g_2) = S_b(f_2 * g_2),$$

vagyis (3) valóban igaz.

3.2. **Definició.** A 3.1. definició értelmében vett ekvivalencia meghatározza I-nek egy osztályozását, amennyiben egy osztályba soroljuk azokat az I-beli függvényeket, amelyek egymással ekvivalensek. Ilyen módon I felbomlik nem üres, páronként diszjunkt osztályok halmazára. Az osztályok halmazát I/b-vel jelöljük. Ha $f \in I$, akkor azt az osztályt melyben f benne van $\{f(n)\}_b$-vel jelöljük. Ha nem okoz félreértést, akkor $\{f(n)\}_b$ helyett rövidebben $\{f(n)\}$ -et is irhatunk.

3.3. **Definició.** Az I/b halmazban értelmezzük az összeadás és a szorzás müveletét a következőképpen:

Legyen $\{f(n)\}$ és $\{g(n)\}$ két tetszőleges I/b-be tartozó osztály, akkor az összeadást a

$$(8) \qquad \{f(n)\} + \{g(n)\} = \{f(n) + g(n)\}$$

és a szorzást a

$$(9) \qquad \{f(n)\}\{g(n)\} = \Big\{\sum_{k=0}^{n} f(n-k)g(k)\Big\} = \{(f * g)(n)\}$$

képlettel értelmezzük.

Megjegyzés. A (8) és (9) alatt értelmezett müveletek a 3.1. tétel következtében egyértelmüen vannak meghatározva.

3.2. **Tétel.** *Az I/b halmaz a* (8) *és* (9) *alatti müveletekre nézve kommutativ gyürüt alkot, mely az egész számok gyürüjével izomorf.*

Bizonyitás. Az hogy I/b kommutativ gyürü, az 1.2. tétel alapján könnyen látható. Azt kell tehát csak igazolni, hogy I/b leképezhető az egész számok E gyürüjére úgy, hogy a leképzés kölcsönösen egyértelmü és müvelettartó.

Megadjuk a leképzést: Ha $\{f(n)\} \in I/b$, akkor ehhez az osztályhoz az $(S_b f)(0) \in E$ egész számot rendeljük. Jelöljük az $\{f(n)\}$ osztályhoz rendelt számot $\overline{\{f(n)\}}$ -sal, akkor tehát azt irhatjuk:

$$(10) \qquad \overline{\{f(n)\}} = (S_b f)(0) = \sum_{k=0}^{\infty} f(k)b^k \in E.$$

A (10) leképzés egyértelmü, mert $\overline{\{f(n)\}}$ nem függ attól, hogy az $\{f(n)\}$ osztályból melyik f elemet választottuk ki.

Tegyük fel, hogy $\{f(n)\} = \{f_1(n)\}$. Akkor $f_1 \sim f$, vagyis a 3.1. megjegyzés alapján

$$\sum_{k=0}^{\infty} f_1(k)b^k = \sum_{k=0}^{\infty} f(k)b^k, \text{ tehát } \overline{\{f_1(n)\}} = \overline{\{f(n)\}}.$$

De a leképezés kölcsönösen egyértelmü is, mert ha valamilyen $\{f_1(n)\}$ és $\{f_2(n)\}$ osztályra $\overline{\{f_1(n)\}} = \overline{\{f_2(n)\}}$ teljesül, akkor (10) értelmezés szerint

$$\sum_{k=0}^{\infty} f_1(k)b^k = \sum_{k=0}^{\infty} f_2(k)b^k$$

teljesül, amiből a 3.1. megjegyzés alapján $f_1 \sim f_2$, azaz $\{f_1(n)\} = \{f_2(n)\}$ következik.

Megmutatjuk, hogy a (10) alatti leképezés müvelettartó, azaz

$$(11) \qquad \overline{\{f(n)\} + \{g(n)\}} = \overline{\{f(n)\}} + \overline{\{g(n)\}}$$

és

$$(12) \qquad \overline{\{f(n)\}\{g(n)\}} = \overline{\{f(n)\}} \cdot \overline{\{g(n)\}}.$$

Valóban, a 2.1. tétel és (8) és (10) felhasználásával kapjuk, hogy

$$\overline{\{f(n)\}} + \overline{\{g(n)\}} = \overline{\{f(n) + g(n)\}} = (S_b(f + g))(0) =$$
$$= (S_b f)(0) + (S_b g)(0) = \overline{\{f(n)\}} + \overline{\{g(n)\}},$$

tehát (11) igaz.

(12) igazolásához a 2.2 tétel (7) képletét, valamint (9)-et és (10)-et használjuk fel:

$$\overline{\{f(n)\}\{g(n)\}} = \overline{\{(f * g)(n)\}} = (S_b(f * g))(0) = (S_b f)(0) \cdot (S_b g)(0) =$$
$$= \overline{\{f(n)\}} \cdot \overline{\{g(n)\}},$$

tehát (12) is igaz. Ezzel megmutattuk, hogy I/b és E izomorf.

4. Az átvitelt végrehajtó Tb transzformáció

4.1. **Definició.** Aritmetikai függvénynek nevezzük az f függvényt, ha f értelmezési tartománya a nem negativ egész számok halmaza és $f(n)$ valós számértéket vesz fel minden n mellett. Az aritmetikai függvények halmazát A-val jelöljük.

4.2. **Definició.** Az A halmazon értelmezünk egy T_b transzformációt, mely minden $f \epsilon A$ függvényhez egy $T_b f \epsilon A$ függvényt rendel. A T_b transzformációt a következő egyenletrendszer segitségével értelmezzük:

$$\text{(1)} \quad \begin{aligned} &\text{a)} \quad s(0) = f(0) \\ &\text{b)} \quad s(n+1) = f(n+1) + \left[\frac{s(n)}{b}\right] \\ &\text{c)} \quad (T_b f)(n) = s(n) - b\left[\frac{s(n)}{b}\right], \end{aligned}$$

ahol $s(n)$ egy egész értékeket felvevő segédfüggvény, melyet az f ismeretében az (1.a.) ill. (1.b.) egyenletek egyértelmüen meghatároznak. s-et az f-hez tartozó állapotfüggvénynek nevezzük.

4.3. **Definició.** Jelöljük I_+-szal azoknak a függvényeknek a halmazát, melyek értelmezési tartománya a nemnegativ egészek halmaza, és ezen egész számértékeket vesznek fel és a következő tulajdonságoknak tesznek eleget:

I. Minden $f \epsilon I_+$ függvényre $0 \leqslant f(n) < b \quad (n = 0,1,2, \ldots)$

II. Minden $f \epsilon I_+$ függvényhez létezik Supp$f$, ha $f \neq 0$, vagyis minden $f \neq 0$, $f \epsilon I$-hez – f-től függően – létezik N nemnegativ egész, hogy $f(N) \neq 0$, de minden $n > N$ egész számra $f(n) = 0$.

III. Ha $f = 0$, akkor $f \epsilon I_+$.

Megjegyzés. Világos, hogy $I_+ \subset I$.

4.4. **Definició.** Jelöljük I_--szal azoknak a nemnegativ egész számok halmazán értelmezett, egész értékeket felvevő függvényeknek a halmazát, amelyek a következő tulajdonságoknak tesznek eleget:

(*i*) Minden $g \in I_-$-függvényre $0 \leqslant g(n) \leqslant b$.

(*ii*) Minden $g \in I_-$-hoz – g-től függően – létezik olyan M nemnegativ egész szám, hogy ha $n \geqslant M$, akkor $g(n) = b - 1$.

Megjegyzés. Világos, hogy $I_- \cap I = \emptyset$, vagyis az I_--ba tartozó függvények nem I-beliek és forditva, ha $f \in I$ akkor $f \notin I_-$.

4.1. **Tétel.** Legyen $f \in I$. Ha $(S_b f)(0) \geqslant 0$, akkor $T_b f \in I_+$ ha $(S_b f)(0) < 0$, akkor $T_b f \in I_-$.

Bizonyitás. Először megmutatjuk, hogy ha $f \in I$, akkor minden n-re

$$0 \leqslant (T_b f)(n) < b \,. \tag{2}$$

Valóban, mivel minden valós x-re $0 \leqslant x - [x] < 1$, ezért az (1.c.) egyenletből adódó

$$\frac{(T_b f)(n)}{b} = \frac{s(n)}{b} - \left[\frac{s(n)}{b}\right]$$

összefüggésből $0 \leqslant \dfrac{(T_b f)(n)}{b} < 1$ adódik, ahonnan (2) következik.

Ezzel megmutattuk, hogy $T_b f$ eleget tesz a 4.3. definició I. és a 4.4. definició (*i*) tulajdonságának minden n-re. Azt könnyü látni (1)-ből hogy $(T_b f)(n)$ egész szám minden n-re.

Most megmutatjuk, hogy ha $(S_b f)(0) \geqslant 0$, akkor $T_b f$-re 4.3. definició I. tulajdonsága mellett teljesül a 4.3. definició II. tulajdonsága is, és igy $T_b f \in I_+$, ha pedig $(S_b f)(0) < 0$, akkor $T_b f$-re teljesül a 4.4. definició (*i*) tulajdonsága mellett a 4.4. definició (*ii*) tulajdonsága is, és igy $T_b f \in I_-$.

Ehhez szükségünk van a következő lemmára:

4.1. **Lemma.** *Legyen* $f \in I$ *és legyen* $s = s(n)$ *az* (1.b.) *egyenletnek az* (1.a.) *kezdeti feltétel melletti megoldása. Ha* $s(\mathrm{Supp} f) \geqslant 0$, *akkor létezik olyan* N_1, *hogy ha* $n \geqslant N_1$, *akkor* $s(n) = 0$, *ha pedig* $s(\mathrm{Supp} f) < 0$, *akkor létezik olyan* N_2 *egész szám, hogy ha* $n \geqslant N_2$, *akkor* $s(n) = -1$.

Bizonyitás. Legyen $N_0 = \mathrm{Supp} f$. Akkor $f(N_0 + 1) = 0$ miatt (1.b)- ből azt kapjuk, hogy

$$s(N_0 + 1) = \left[\frac{s(N_0)}{b}\right] \leqslant \frac{s(N_0)}{b} \,. \tag{3}$$

Megmutatjuk teljes indukcióval, hogy tetszőleges k természetes számra

$$s(N_0 + k) \leqslant \frac{s(N_0)}{b^k} \,. \tag{4}$$

$k = 1$-re (4) a már igazolt (3) egyenlőtlenségbe megy át. Tegyük fel, hogy (4) teljesül $k \geqslant 1$-re. Akkor $f(N_0 + k + 1) = 0$, (1.b.) és (4) felhasználásával kapjuk:

$$s(N_0 + k + 1) = \left[\frac{s(N_0 + k)}{b}\right] \leqslant \frac{s(N_0 + k)}{b} \leqslant \frac{s(N_0)}{b^{k+1}},$$

tehát igaz (4). Ha $s(N_0) \geqslant 0$, akkor teljes indukcióval (1.b.) alapján beláthatjuk, hogy $s(N_0 + k) \geqslant 0$ minden k természetes számra. Ha K olyan nagy, hogy $\frac{s(N_0)}{b^K} < 1$, akkor (4)-ből $0 \leqslant s(N_0 + K) < 1$ következik, és mivel $s(N_0 + K)$ egész szám, ez csak úgy teljesülhet, hogy $s(N_0 + K) = 0$. Legyen $N_1 = N_0 + K$. Akkor $s(N_1) = 0$ és igy minden $k \geqslant 0$ egész szám (1.b.)-ből $s(N_1 + k) = 0$ következik, vagyis, ha

$$n \geqslant N_1, \text{ akkor } s(n) = 0.$$

Legyen most $s(N_0) < 0$. Akkor minden k természetes számra

$$(5) \qquad \frac{s(N_0)}{b^k} - s(N_0 + k) < \frac{b}{b-1}.$$

$k = 1$-re ugyanis (5) az $\frac{s(N_0)}{b} - s(N_0 + 1) < \frac{b}{b-1}$ egyenlőtlenségbe megy át, ami $s(N_0 + 1) = \left[\frac{s(N_0)}{b}\right]$ miatt nyilván igaz. Tegyük fel, hogy (5) igaz $k \geqslant 1$-re, akkor (5)-ből kapjuk:

$$(6) \qquad \frac{s(N_0)}{b^{k+1}} - \frac{s(N_0 + k)}{b} < \frac{1}{b}\,\frac{b}{b-1} = \frac{1}{b-1}$$

Mivel $\left[\frac{s(N_0 + k)}{b}\right] = s(N_0 + k + 1)$, ezért

$$(7) \qquad \frac{s(N_0 + k)}{b} - s(N_0 + k + 1) < 1.$$

A (6) és (7) egyenlőtlenségek megfelelő oldalainak az összeadása után kapjuk, hogy

$$\frac{s(N_0)}{b^{k+1}} - s(N_0 + k + 1) < 1 + \frac{1}{b-1} = \frac{b}{b-1}.$$

Tehát (5) igaz minden k-ra. (5)-ből azt kapjuk, hogy

$$\frac{s(N_0)}{b^k} - s(N_0 + k) < \frac{b}{b-1} = 1 + \frac{1}{b-1}, \text{ és innen}$$

$$(8) \qquad s(N_0 + k) > -1 - \frac{1}{b-1} + \frac{s(N_0)}{b^k} \geqslant -2 + \frac{s(N_0)}{b^k} .$$

Ha most K olyan nagy, hogy $\frac{s(N_0)}{b^K} > -1$, akkor

$$s(N_0 + K) > -2 + \frac{s(N_0)}{b^K} > -3,$$

ahonnan

$$\frac{s(N_0 + K)}{b} > -\frac{3}{b} \geqslant -\frac{3}{2},$$

tehát

$$(9) \qquad s(N_0 + K + 1) = \left[\frac{s(N_0 + K)}{b}\right] \geqslant -2.$$

(9)-ből (1.b.) alapján felhasználva, hogy $s(n) < 0$, ha $s(N_0) < 0$, és $n \geqslant N_0$, továbbá azt, hogy

$$\frac{s(N_0 + K + 1)}{b} \geqslant -\frac{2}{b} \geqslant -1,$$

kapjuk, hogy

$$(10) \qquad 0 > s(N_0 + K + 2) = \left[\frac{s(N_0 + K + 1)}{b}\right] = -1.$$

Legyen $N_2 = N_0 + K + 2$. Akkor $s(n+1) = \left[\frac{s(n)}{b}\right]$, $(n \geqslant N_2)$ egyenlőségből teljes indukcióra kapjuk, hogy $s(n) = -1$. Ugyanis az állitás $n = N_2$-re igaz. Tegyük fel, hogy $n \geqslant N_2$ mellett $s(n) = -1$. Igy

$$\left[\frac{s(n)}{b}\right] = \left[\frac{-1}{b}\right] = -1.$$

Tehát, ha $n \geqslant N_2$, akkor $s(n) = -1$.

Ezzel a lemmát igazoltuk.

A 4.1. tétel bizonyitásának a folytatása:
Az (1) egyenletek felhasználásával kapjuk, hogy

$$\sum_{n=0}^{N} (T_b f)(n) b^n = \sum_{n=0}^{N} s(n) b^n - \sum_{n=0}^{N} b^{n+1} \left[\frac{s(n)}{b} \right] =$$

$$= f(0) + \sum_{n=1}^{N} f(n) b^n + \sum_{n=1}^{N} b^n \left[\frac{s(n-1)}{b} \right] - \sum_{n=0}^{N} b^{n+1} \left[\frac{s(n)}{b} \right] =$$

$$= \sum_{n=0}^{N} f(n) b^n + \sum_{n=0}^{N-1} b^{n+1} \left[\frac{s(n)}{b} \right] - \sum_{n=0}^{N-1} b^{n+1} \left[\frac{s(n)}{b} \right] - b^{N+1} \left[\frac{s(N)}{b} \right]$$

vagyis

$$(11) \qquad \sum_{n=0}^{N} (T_b f)(n) b^n = \sum_{n=0}^{N} f(n) b^n - b^{N+1} \left[\frac{s(N)}{b} \right].$$

Tegyük fel, hogy $(S_b f)(0) = \sum_{k=0}^{Supp\, f} f(k) b^k \geqslant 0$, és legyen a rövidség kedvéért $Supp f = N_0$. Akkor $s(N_0) \geqslant 0$. Ha ugyanis $s(N_0) < 0$, akkor van olyan N_2, hogy ha $n \geqslant N_2$, akkor $s(n) = -1$. Legyen $N > \max(N_0, N_2)$, akkor (11) átmegy a

$$(12) \qquad \sum_{n=0}^{N} (T_b f)(n) b^n = \sum_{n=0}^{N} f(n) b^n + b^{N+1} = (S_b f)(0) + b^{N+1}$$

egyenlőségbe. Mivel (2) miatt $(T_b f)(n) \leqslant b - 1$, (12)-ből a következő egyenlőtlenséget kapjuk

$$(13) \qquad (S_b f)(0) + b^{N+1} \leqslant \sum_{n=0}^{N} (b-1) b^n = b^{N+1} - 1,$$

ahonnan az $(S_b f)(0) \leqslant -1$ ellentmondásra jutunk.
Tehát, ha $(S_b f)(0) \geqslant 0$, akkor $s(N_0) \geqslant 0$. De akkor van a 4.1. lemma szerint olyan N_1, hogy ha $n \geqslant N_1$, akkor $s(n) = 0$. De akkor (1.c.) alapján azt kapjuk, hogy $n \geqslant N_1$ esetén

$$(T_b f)(n) = 0$$

Ezzel megmutattuk, hogy $T_b f \in I_+$.

Tegyük most, fel hogy $(S_b f)(0) < 0$. Akkor $s(Supp f) < 0$. Ha ugyanis $s(Supp f) \geqslant 0$ volna, akkor a 4.1. lemma szerint létezne N_1, hogy $s(N) = 0$, ha $N \geqslant N_1$. Legyen $N \geqslant \max(N_1, N_0)$, akkor igy (11) átmenne a

$$(14) \qquad \sum_{n=0}^{N} (T_b f)(n) b^n = \sum_{n=0}^{N} f(n) b^n = (S_b f)(0)$$

egyenlőségbe. Azonban (2) szerint $(T_b f)(n) \geqslant 0$ és igy (14)-ből az $(S_b f)(0) \geqslant 0$ ellentmondásra jutnánk. Tehát $s(Supp f) < 0$. De akkor a 4.1. lemma alapján létezik N_2, hogy minden $n \geqslant N_2$ mellett $s(n) = -1$. Igy tehát $n \geqslant N_2$ esetén (1c)-ből kapjuk, hogy

$$(T_b f)(n) = s(n) - b\left[\frac{s(n)}{b}\right] = -1 + b = b - 1.$$

Tehát $(S_b f)(0) < 0$ esetén $T_b f \epsilon I_-$.

4.2. **Tétel.** *Legyen* $f, g \epsilon I$. *Akkor* $f \overset{b}{\sim} g$ *akkor és csak akkor teljesül, ha*

$$T_b f = T_b g \tag{15}$$

Bizonyítás. A 3.1. megjegyzés alapján azt kell igazolni, hogy ha $f,g \epsilon I$, akkor

$$(S_b f)(0) = (S_b g)(0) \tag{16}$$

akkor és csak akkor igaz, ha (15) igaz.

Tegyük fel először, hogy (16) teljesül. Legyen s_1, az f-hez, s_2 a g-hez tartozó állapotfüggvény. A 4.1. lemma értelmében létezik olyan N_1^* és N_2^*, hogy $n > N_1^*$ esetén $s_1(n) = 0$ vagy $s_1(n) = -1$ aszerint, hogy $(S_b f)(0) \geqslant 0$ vagy $(S_b f)(0) < 0$.

Ugyanigy, g-hez is létezik egy N_2^* úgy, hogy $s_2(n) = 0$, ha $(S_b g)(0) \geqslant 0$ és $n \geqslant N_2^*$, vagy ha $(S_b g)(0) \leqslant 0$, akkor $s_2(n) = -1$ minden $n \geqslant N_2^*$ mellett. Legyen $N^* = \max(N_1^*, N_2^*)$, akkor (16) miatt $N \geqslant N^*$ esetén vagy $s_1(N) = s_2(N) = 0$ vagy $s_1(N) = s_2(N) = -1$.

Tehát minden esetben

$$\left[\frac{s_1(N)}{b}\right] = \left[\frac{s_2(N)}{b}\right]. \tag{17}$$

Legyen $N \geqslant \max(N^*, \mathrm{Supp} f, \mathrm{Supp} g)$ és ilyen N mellett tekintsünk a (11) egyenlőséget f-re és g-re:

$$\sum_{n=0}^{N} (T_b f)(n) b^n = (S_b f)(0) - b^{N+1}\left[\frac{s_1(N)}{b}\right] \tag{18}$$

$$\sum_{n=0}^{N} (T_b g)(n) b^n = (S_b g)(0) - b^{N+1}\left[\frac{s_2(N)}{b}\right]. \tag{19}$$

A (18)-ból és (19)-ből (16)-ra és (17)-re való tekintettel kapjuk, hogy

$$\sum_{n=0}^{N} (T_b f)(n) b^n = \sum_{n=0}^{N} (T_b g)(n) b^n. \tag{20}$$

Mivel a 4.1. tétel miatt $T_b f, T_b g \epsilon I_+ \cup I_-$, a (20) baloldala is meg a jobboldala is ugyanannak a számnak a b alapú számrendszerben felírt alakja. Ez a felírás egyértelmű, ezért (20)-ból

$$(T_b f)(n) = (T_b g)(n) \tag{21}$$

következik minden $0 \leqslant n \leqslant N$ számra. Mivel N tetszőleges nagy lehet, (21) igaz minden n-re,

és igy igaz (15).

Tegyük most fel, hogy (15) igaz, vagyis (21) teljesül minden n-re. Akkor (1.c.) és (21) alapján

$$(22) \qquad s_1(n) - b\left[\frac{s_1(n)}{b}\right] = s_2(n) - b\left[\frac{s_2(n)}{b}\right] \qquad (n = 0,1,2,\ldots)$$

ahol s_1, az f-hez, s_2 a g-hez tartozó állapotfüggvény, (22)-ből kapjuk:

$$(23) \qquad \frac{s_1(n) - s_2(n)}{b} = \left[\frac{s_1(n)}{b}\right] - \left[\frac{s_2(n)}{b}\right] \qquad (n = 0,1,2,\ldots)$$

Legyen $N > \max(N_1^*, N_2^*, \mathrm{Supp}f, \mathrm{Supp}g)$. Akkor ilyen N mellett tekintve a (18) és (19) egyenlőségeket (21) figyelembevételével kapjuk:

$$(S_b f)(0) - b^{N+1}\left[\frac{s_1(N)}{b}\right] = (S_b g)(0) - b^{N+1}\left[\frac{s_2(N)}{b}\right],$$

ahonnan átrendezéssel adódik

$$(S_b f)(0) - (S_b g)(0) = b^{N+1}\left(\left[\frac{s_1(N)}{b}\right] - \left[\frac{s_2(N)}{b}\right]\right)$$

és innen (23)-ra való tekintettel

$$(24) \qquad (S_b f)(0) - (S_b g)(0) = b^N(s_1(N) - s_2(N)).$$

Mivel (24) bal oldala nem függ a N számtól, ezért a jobboldal sem függ N-től. De mivel a N-re tett feltevés miatt $s_1(N) - s_2(N)$ sem függ N-től, (24) jobboldala csak akkor lehet konstans, ha $s_1(N) - s_2(N) = 0$. De akkor viszont (24)-ből (16) következik, amit bizonyitani kellett.

4.3. **Tétel.** *Minden* $n \geqslant 0$ *egészre és minden* $f \in A$ *függvényre igaz*

$$(25) \qquad (T_b^2 f)(n) = (T_b f)(n), \qquad \textit{azaz } T_b \textit{ idempotens operátor :}$$

$$(26) \qquad T_b^2 = T_b.$$

Bizonyitás. Legyen $f \in A$, akkor a $g(n) = (T_b^2 f)(n) = (T_b(T_b f))(n)$ függvény értékeit az (1) egyenletrendszerből kaphatjuk meg:

$$(27) \qquad s(0) = (T_b f)(0)$$

$$(28) \qquad s(n+1) = (T_b f)(n+1) + \left[\frac{s(n)}{b}\right]$$

$$(29) \qquad (T_b^2 f)(n) = s(n) - b\left[\frac{s(n)}{b}\right]$$

Teljes indukcióval bebizonyitjuk, hogy

(30) $\quad s(n) = (T_b f)(n) \quad (n = 0,1,2,\ldots)$

$n = 0$-ra (27) miatt igaz az álllitás.

Tegyük fel, hogy (30) igaz $n \geqslant 0$ mellett. Mivel (2) szerint $0 \leqslant (T_b f)(n) < b$, igy $\left[\frac{(T_b f)(n)}{b}\right] = 0$

Tehát (28)-ból (30) felhasználásával kapjuk, hogy

$$s(n+1) = (T_b f)(n+1) + \left[\frac{s(n)}{b}\right] = (T_b f)(n+1) + \left[\frac{(T_b f)(n)}{b}\right] = (T_b f)(n+1).$$

Ezzel igazoltuk a (30)-egyenlőséget. Akkor viszont (29) alapján

$$(T_b^2 f)(n) = (T_b f)(n) - b\left[\frac{(T_b f)(n)}{b}\right] = (T_b f)(n).$$

Ezzel igazoltuk a (25) egyenlőséget és igy a (26)-ot is.

4.4.**Tétel.** *Ha* $f,g \in I$, *akkor*

(31) $\quad T_b(f+g) = T_b(T_b f + T_b g)$

és

(32) $\quad T_b(f * g) = T_b(T_b f * T_b g).$

Bizonyitás. Elöszőr megmutatjuk, hogy ha $f \in I$, akkor $f \overset{b}{\sim} T_b f$.

A 4.3. tétel alapján $T_b f = T_b^2 f = T_b(T_b f)$ és innen a 4.2 tétel alkalmazásával kapjuk, hogy

(33) $\quad f \overset{b}{\sim} T_b f$

Mivel $g \in I$, ugyanigy fennáll

(34) $\quad g \overset{b}{\sim} T_b g$

is. Igy a 3.1. tétel alkalmazásával kapjuk, hogy

(35) $\quad f + g \overset{b}{\sim} T_b f + T_b g$

és

(36) $\quad f * g \overset{b}{\sim} T_b f * T_b g$

(35) és (36)-ból a 4.2. tétel alkalmazásával kapjuk (31) és (32)-t.

4.5.**Tétel.** *Ha* $f \in I_+ \cup I_-$, *akkor*

(37) $\quad T_b f = f.$

Bizonyitás. Legyen $f \epsilon I_+ \cup I_-$. Akkor minden $n \geqslant 0$ egész számra

(38) $\quad 0 \leqslant f(n) < b.$

Tehát ha s az f-hez tartozó állapotfüggvény, akkor

$$\left[\frac{s(0)}{b}\right] = \left[\frac{f(0)}{b}\right] = 0.$$

Megmutatjuk

(39) $\quad \left[\frac{s(n)}{b}\right] = 0.$

$n = 0$-ra a (39) egyenlőséget már beláttuk. Tegyük fel, hogy (38) igaz $n \geqslant 0$ esetén. Akkor (1.b.) alapján

$$s(n + 1) = f(n + 1)$$

tehát (38) miatt $\left[\frac{s(n+1)}{b}\right] = \left[\frac{f(n+1)}{b}\right] = 0$. Tehát (39) igaz minden n-re. De akkor (1.b.) és (1.c.) alapján minden n-re

$$(T_b f)(n) = s(n) = f(n)$$

vagyis (37) valóban fennáll.

5. Algoritmus hosszú egész számnak rövid számmal való osztására

5.1. **Tétel.** *Legyen* $f \epsilon I_+$ *és valamilyen egész szám legyen* $a \neq 0$. *Akkor az*

$$ax(0) - bt(0) = f(0)$$

(1)

$$ax(n) - bt(n) = f(n) - t(n - 1)$$

egyenletrendszernek a

(2) $\quad 0 \leqslant x(n) < b \qquad (x(n), t(n) \epsilon E^*) \qquad (n = 0,1,2, \ldots)$

feltételek mellett legfeljebb egyetlen $x(n)$ *és* $t(n)$ *függvény megoldáspárja létezik.*

Bizonyitás. Tegyük fel, hogy az $x(n)$ és $t(n)$ függvénypár mellett az $x'(n), t'(n)$ függvénypár is megoldása (1)-nek ugy, hogy

(3) $\quad 0 \leqslant x'(n) < b \qquad (n = 0,1,2, \ldots)$

teljesül. Mivel $x'(n)$ és $t'(n)$ is megoldása (1)-nek, ezért

$$(4)\qquad \begin{cases} ax'(0) - bt'(0) = f(0) \\ \\ ax'(n) - bt'(n) = f(n) - t'(n-1) \end{cases} \qquad (n = 1,2,\ldots)$$

Legyen $y(n) = x(n) - x'(n)$, $z(n) = t(n) - t'(n)$ $(n = 0,1,2,\ldots)$. Akkor az (1) és (4) egyenletekből kapjuk, hogy

$$(5)\qquad \begin{cases} ay(0) - bz(0) = 0 \\ \\ ay(n) - bz(n) = -z(n-1) \end{cases} \qquad (n = 1,2,\ldots)$$

Mivel az $ay - bz = 0$ diofantikus egyenlet álatlános megoldása $y = kb$ és $z = ka$, ahol $k = 0, \pm 1, \pm 2, \ldots$ ezért az (5) egyenletrendszer első egyenletéből $y(0) = kb$ és $z(0) = ka$ alaku lehet.

A (2) és (3) feltételből következik, hogy

$$(6)\qquad |y(n)| < b \qquad (n = 0,1,2,\ldots)$$

Tehát speciálisan $n = 0$ mellett

$$|k|b = |kb| = |y(0)| < b$$

ahonnan azt kapjuk, hogy $|k| < 1$. Ez csak $k = 0$ mellett lehetséges, és igy $y(0) = 0$, és $z(0) = 0$. Megmutatjuk, hogy

$$(7)\qquad y(n) = 0$$

és

$$(8)\qquad z(n) = 0$$

teljesül minden $n = 0,1,2,\ldots$ mellett. $n = 0$ esetre beláttuk az állitást. Tegyük fel, hogy valamilyen $n \geqslant 1$ mellett $y(n-1) = 0$ és $z(n-1) = 0$. Az indukciós bizonyitáshoz azt kell megmutatni, hogy akkor (7) és (8) is teljesül. Valóban, az indukciós feltevés miatt az (5) alatti második egyenlet ilyen alaku lesz;

$$(9)\qquad ay(n) - bz(n) = 0$$

Tehát $y(n) = kb$ és $z(n) = ka$ és (6) miatt $k = 0$, vagyis valóban igaz (7) és (8). Igy tehát azt kapjuk, hogy $x(n) = x'(n)$ és $t(n) = t'(n)$ minden n-re. Ezzel a tételt igazoltuk.

Megjegyzés. Jól ismert, hogy az

$$ax - bt = c$$

diofanatikus egyenletnek akkor és csak akkor van megoldása, ha a és b legnagyobb közös osztója c-nek is osztója. Igy tehát az (1) egyenletrendszernek biztosan nincs megoldása, ha (a,b) nem osztója $f(c)$-nak. Az (1) egyenletrendszernek mindig van megoldása, ha a és b relativ prim, mert akkor $(a,b) = 1$ minden szám osztója.

5.2. **Tétel.** *Legyen* $f \epsilon I_+$ *és* $M = \sum_{k=0}^{\mathrm{Supp} f} f(k)b^k \geqslant 0$.

Ha $a > 0$ osztója M-nek, akkor létezik az 5.1. tétel szerint

$$ax(0) - bt(0) = f(0)$$

$$(n = 1,2, \ldots)$$

$$ax(n) - bt(n) = f(n) - t(n-1)$$

egyenletrendszernek olyan $x(n)$, $t(n)$ megoldáspárja, amelyre a

$$0 \leqslant x(n) < b$$

feltétel teljesül. Ekkor $x \epsilon I_+$ és

$$(10) \qquad \sum_{k=0}^{\mathrm{Supp} x} x(k)b^k = \frac{M}{a}$$

Bizonyitás. Legyen $m = \frac{M}{a}$ és $\mu \epsilon I_+$ olyan, hogy

$$(11) \qquad m = \sum_{k=0}^{\mathrm{Supp}\mu} \mu(k)b^k$$

vagyis (11) az m szám b alapu számrendszerben felirt alakja. De akkor $a > 0$ miatt

$$S_b(a\mu)(0) = \sum_{k=0}^{\mathrm{Supp}\mu} a\mu(k)b^k = am = M = \sum_{k=0}^{\mathrm{Supp} f} f(k)b^k = (S_b f)(0),$$

tehát $f \overset{b}{\sim} a\mu$. Igy a 4.2. tétel alkalmazásával kapjuk, hogy

$$(13) \qquad T_b f = T_b(a\mu).$$

$f \epsilon I_+$ miatt a 4.5. tétel alapján $T_b f = f$ és igy

$$(14) \qquad f = T_b(a\mu)$$

Legyen s az $a\mu$ függvényhez tartozó állapotfüggvény. Megmutatjuk, hogy akkor $x(n) = \mu(n)$ és $t(n) = \left[\frac{s(n)}{b}\right]$ kielégiti az (1) egyenletrendszert, és a (2) egyenlőtlenség is teljesül. Valóban a 4.2. definició szerint

(15) $s(0) = a\mu(0)$

(16) $s(n+1) = a\mu(n+1) + \left[\frac{s(n)}{b}\right]$

(17) $T_b(a\mu)(n) = s(n) - b\left[\frac{s(n)}{b}\right]$

Igy tehát (14)-re való tekintettel kapjuk, hogy

$$f(0) = T_b(a\mu)(0) = s(0) - b\left[\frac{s(0)}{b}\right] = a\mu(0) - b\left[\frac{s(0)}{b}\right] = ax(0) - bt(0),$$

vagyis, az (1) első egyenlete teljesül. Legyen $n \geqslant 1$. Akkor (14), (16) és (17) miatt

$$f(n) = T_b(a\mu)(n) = s(n) - b\left[\frac{s(n)}{b}\right] = a\mu(n) + \left[\frac{s(n-1)}{b}\right] - b\left[\frac{s(n)}{b}\right] =$$
$$= ax(n) + t(n-1) - bt(n),$$

ahonnan átrendezéssel kapjuk az (1) egyenleteit $n = 1,2,\ldots$ esetére. Az, hogy a (2) egyenlőtlenség $x = \mu$ esetén fennáll, az $a\mu \epsilon I_+$ feltétel miatt nyilván teljesül. Az is nyilvánvaló, hogy $x = \mu$ mellett (10) is fennáll (a (11) egyenlőség és $m = \frac{M}{a}$ miatt). Ezzel a tételt igazoltuk.

6. Algoritmus hosszú egész számnak hosszú egész számmal való osztására

A következőkben adott f és g mellett vizsgáljuk a

(1) $(g * x)(n) - bt(n) = f(n) - t(n-1) \qquad (t(-1) = 0;\ n = 0,1,\ldots)$

egyenleteknek a

(2) $0 \leqslant x(n) < b \qquad (x(n),\ t(n)$ egész; $n = 0,1,2,\ldots)$

feltételek melletti megoldásait. Az (1) egyenletrendszer az (5.1.) egyenletrendszer általánositása. Ugyanis, ha speciális $g(0) = a$ és $Suppg = 0$ akkor (1) átmegy az (5.1) egyenletrendszerbe.

6.1. **Tétel.** *Legyenek f és g egész értékeket felvevő függvények. Ha $g \neq 0$, akkor legfeljebb egy olyan $x(n)$, $t(n)$ függvénypár létezik, amelyre az* (1) *egyenletek fennállnak és ugyanakkor a* (2) *feltételek is teljesülnek.*

Bizonyitás. Tegyük fel, hogy $x(n)$-re és $t(n)$-re teljesül (1) és (2) és ugyanakkor $x'(n)$ és $t'(n)$-re is fennáll, hogy

(3) $(g * x')(n) - bt'(n) = f(n) - t'(n-1) \qquad (t'(-1) = 0;\ n = 0,1,\ldots)$

és

(4) $0 \leqslant x'(n) < b \qquad (x'(n),\ t'(n)$ egész; $n = 0,1,\ldots)$

Legyen $y = x - x'$ és $z = t - t'$. Akkor (1)-ből és (3)-ból kapjuk, hogy

(5) $\qquad (g * y)(n) - bz(n) = - z(n - 1) \qquad (z(- 1) = 0; n = 0,1, \ldots)$

és (2)-ből (4)-ből kapjuk:

(6) $\qquad |y(n)| < b \qquad (n = 0,1, \ldots)$

Az (5) egyenletet részletesen kiirva kapjuk, hogy

(7) $\qquad \sum_{k=0}^{n} g(n - k)y(k) - bz(n) = - z(n - 1) \qquad (z(- 1) = 0; n = 0,1, \ldots)$

$n = 0$ esetén a (7) egyenlet a

(8) $\qquad g(0)y(0) - bz(0) = 0$

egyneletbe megy át. Megmutatjuk, hogy $y(0) = z(0) = 0$. Ez $g(0) \neq 0$ esetén (8)-ból (6) miatt következik. Ha $g(0) = 0$, akkor (8)-ból egyenlőre csak az következik, hogy $z(0) = 0$. Tegyük fel, hogy $g(0) = 0$. Mivel $g \not\equiv 0$, létezik olyan $r > 0$, hogy $g(r) \neq 0$, de ha $0 \leqslant n < r$, akkor $g(n) = 0$. Ha tehát $0 \leqslant n < r$, akkor a (7) egyenlet a

(9) $\qquad - bz(n) = - z(n - 1) \qquad (n = 0, \ldots, r - 1)$

egyenletbe megy át, ahonnan (teljes indukcióval) következik, hogy

(10) $\qquad z(n) = 0, \qquad$ ha $\qquad 0 \leqslant n < r.$

Helyettesitsük (7)-be n helyébe r-et, akkor (10)-re való tekintettel azt kapjuk, hogy

(11) $\qquad g(r)y(0) - bz(r) = - z(r - 1) = 0.$

Innen $g(r) \neq 0$ és (6) miatt az következik, hogy

(12) $\qquad y(0) = z(r) = 0$

Azt akarjuk teljes indukcióval megmutatni, hogy $y(n) = z(n + r) = 0$ minden n-re igaz. Ezt $n = 0$ esetére már beláttuk.

Tegyük fel, hogy valamilyen $n > 0$ esetén

(13) $\qquad y(0) = y(1) = \ldots = y(n - 1) = 0, \qquad z(0) = z(1) = \ldots = z(n + r - 1) = 0$

igaz. Helyettesitsünk (7)-be n helyébe $n + r$-et akkor

(14) $\qquad g(n + r - k)y(k) = 0,$

ha $k < n$, mert akkor $y(k) = 0$. Ha pedig $n < k \leqslant n + r$, akkor $0 \leqslant n + r - k < r$ és igy $g(n + r - k) = 0$, aminek következtében (14) ismét fennáll. Igy tehát a (7) egyenlet a következő egyenletre redukálódik:

(15) $\quad g(r)y(n) - bz(n + r) = - z(n + r) = - z(n + r - 1)$

Az indukciós feltevés miatt $z(n + r - 1) = 0$, és igy a (15) egyenletből $g(r) \neq 0$ és (6) miatt $y(n) = 0$ és $z(n + r) = 0$ következik. Ezek megmutaták, hogy minden n-re

$$x(n) - x'(n) = y(n) = 0 \quad \text{és és} \quad t(n) - t'(n) = 0,$$

vagyis igazoltuk a tételt.

Megjegyzés. A 6.1 tétel egyik következménye: Adott f és g mellett, ha $g \neq 0$, akkor legfeljebb egyetlen olyan $x \in I_+ \cup I_-$ létezik, hogy valamely $t = t(n)$ mellett az (1) egyenletek teljesüljenek.

6.2 **Tétel.** *Legyen* $f,g \in I$, $g \neq 0$. *Ha van olyan* $x \in I$, *amely megoldása* (1)*-nek es teljesülnek a* (2) *feltételek is, akkor*

$$\sum_{k=0}^{\mathrm{Supp}f} f(k)b^k \quad \textit{osztható az} \quad \sum_{k=0}^{\mathrm{Supp}g} g(k)b^k \quad \textit{számmal, és}$$

(16) $$\sum_{k=0}^{\mathrm{Supp}x} x(k)b^k = \frac{\sum_{k=0}^{\mathrm{Supp}f} f(k)b^k}{\sum_{k=0}^{\mathrm{Supp}g} g(k)b^k}$$

Bizonyitás. Legyen x az (1) egyenlet megoldása, és legyen

(17) $\quad N > \max(\mathrm{Supp}f, \mathrm{Supp}\ (g * x))$.

Az (1) egyenlet mindkét oldalát megszorozva b^n-vel és összegezve $n = 0$-tól $n = N$-ig, azt kapjuk, hogy

(18) $\quad (S_b g)(0) \cdot (S_b x)(0) = (S_b f)(0) + b^{N+1} t(N)$

Innen viszont következik, hogy

(19) $\quad b^{N+1} t(N) = c = \text{konstans} \quad N > \max(\mathrm{Supp}f, \mathrm{Supp}\ (g * x))$.

Legyen $N_0 > \max(\mathrm{Supp}f, \mathrm{Supp}\ (g * x))$ olyan nagy, hogy már

$$\frac{|c|}{b^{N_0+1}} < 1.$$

Akkor (19) következtében $|t(N_0)| = \dfrac{|c|}{b^{N_0+1}} < 1$. Mivel $|t(N_0)|$ egész, $|t(N_0)| < 1$ csak ugy teljesülhet, ha $t(N_0) = 0$. De akkor (19) miatt

$$0 = b^{N_0+1} t(N_0) = c$$

és igy (19)-re való tekintettel

(20) $\quad t(N) = 0, \quad$ ha $\quad N > \max(\mathrm{Supp} f, \mathrm{Supp}(g * x))$

De akkor (18)-ból a bizonyitandó (16) egyenlőség is következik, és mivel $(S_b x)(0)$ egész szám, az is következik (16)-ból, hogy $(S_b f)(0)$ osztható $(S_b g)(0)$-val.
Ezzel a tételt igazoltuk.

6.3. **Tétel.** *Legyen* $f,g \in I, (S_b f)(0) \geqslant 0, (S_b g)(0) > 0$. *Ha* $(S_b f)(0)$ *osztható* $(S_b g)(0)$*-val akkor létezik az* (1) *egyenletrendszernek a* (2) *feltételek melletti* $x(n), t(n)$ *megoldása. Ekkor* $x \in I_+$ *és*

$$(21) \qquad (S_b x)(0) = \frac{(S_b f)(0)}{(S_b g)(0)}$$

Bizonyitás. Legyen

$$(22) \qquad m = \frac{(S_b f)(0)}{(S_b g)(0)} \qquad \text{és}$$

legyen $\xi = \xi(n) \in I_+$ olyan, hogy

$$(23) \qquad m = \sum_{k=0}^{\mathrm{Supp}\xi} \xi(k) b^k = (S_b \xi)(0),$$

vagyis (23) az m számnak b alapu számrendszerben felirt alakja. Azt fogjuk igazolni, hogy $x = \xi$ a (2) feltételek mellett megoldása az (1) egyenletrendszernek.

Az, hogy $0 \leqslant \xi(n) < b \quad (n = 0,1,2, \ldots)$ rögtön következik (23)-ból.

Helyettesitsük be az (1) egyenletek mindegyikében x helyébe a ξ függvényt. Akkor $t(-1) = 0$ ismeretében a $t(0), t(1), \ldots$ értékek szukcesszive meghatározhatók a

$$(24) \qquad (g * \xi)(n) - bt(n) = f(n) - t(n-1) \qquad (n = 0,1,2, \ldots)$$

egyenletekből. A tétel bizonyitásához azt kell igazolni, hogy a $t(n)$ számok mind egész számok.

Legyen N olyan egész szám, amelyre

$$(25) \qquad N \geqslant \max(\mathrm{Supp} f, \mathrm{Supp}(g * \xi)) = N_0$$

teljesül. Adjuk össze a (24) alatti egyenlőségek mindkét oldalát 0-tól N-ig, akkor kapjuk, hogy

$$\sum_{n=0}^{N} \Big(\sum_{k=0}^{n} g(n-k)\xi(k) \Big) b^n - \sum_{n=0}^{N} t(n) b^{n+1} = \sum_{n=0}^{N} f(n) b^n - \sum_{n=0}^{N} t(n-1) b^n,$$

ahonnan (25) következtében kapjuk, hogy

$$(26) \qquad (S_b g)(0) \cdot (S_b \xi)(0) - t(N)b^{N+1} = (S_b f)(0),$$

ugyanis

$$\sum_{n=0}^{N} t(n-1)b^n = \sum_{n=1}^{N} t(n-1)b^n = \sum_{n=0}^{N-1} t(n)b^{n+1},$$

De akkor (22) és (23) figyelembe vételével (26)-ból kapjuk, hogy

$$(27) \qquad t(N) = 0.$$

Minden $N \geqslant N_0$ mellett. Azt kell még belátni, hogy ha $n \leqslant N_0$, akkor is egész szám lesz $t(n)$. Az állitást N_0-ra már beláttuk. Tegyük fel az indukciós bizonyitáshoz, hogy $t(n)$ egész szám, ha $0 < n \leqslant N_0$. Akkor (24)-ből következik, hogy

$$t(n-1) = f(n) + bt(n) - (g * \xi)(n)$$

is egész szám. Tehát minden $n = 0,1, \ldots$ mellett $t(n)$ egész szám, és fennáll (24) is és ezzel igazoltuk a tételt.

7. A faktorális táblázatot készitő program

A következőkben megmutatjuk, hogy a fenti elméleti meggondolások hogyan alkalmazhatók a gyakorlatban. Mivel $k!$ értéke rohamosan nő az k értékével nagy egész számokkal való számolásra adott módszerünk bemutatására faktoriális tábálzatot készitő ALGOL 60 programot irtunk.

Az eredményt egy fix felső korlátu w vektor tároloja. A vektor elemei az eredményt bináris kodolásu 10^d alapu ábrázolásban tartalmazzák. Az egyes faktoriálisok kiszámitásánál a vektor ténylegesen felhasznált hossza csak az értékes számjegyeket tartalmazó Supp w, amit az egymás utáni értékek kiszámitásánál a program határoz meg. Az eredményben gyorsan halmozódó számvégi nullákat a program csak megjegyzi, de nem számol velük. Ezt a Norm w eljárás oldja meg.

A $k!$-ból a $(k+1)!$ kiszámitása három lépésben történik:

I. A $k!$ jegyeit tartalmazó w vektort beszorozza $(k+1)$-gyel a hosszu egész számnak rövid egész számmal való szorzásra vonatkozó 2.3 tétel alapján.

II. Az igy kialakult w vektor ekvivalens $(k+1)!$-sal, de elemei $(k+1)!$-nak nem a 10^d alapu számrendszerbeli jegyeit tartalmazzák. A w vektort alávetjük a Tb transzformációnak, hogy a keletkezett vektorban megkapjuk $(k+1)!$-nak 10^d alapu számrendszerbeli jegyeit.

III. A Supp w és a Norm w eljárások alkalmazása.

A kiszámitott érték kiiratása egy előre megadott "kezd" értéktől, vagy egy kényszerités hatására történik.

A számolás során a 10^d alapszámot változtatjuk abból a célból, hogy az adott gép hardware sajátosságaiból adódó tulcsordulást kivédjük.

Esetünkben $k = 838$-ig 10^4, utána 10^3 az alapszám. Az adott programba a további csökkenést nem épitettük be, ezért 8388!-nál nagyobb, számot a program már nem számol helyesen (még akkor sem ha a w vektort a kellő hosszuságura kb. 10 000-re deklaráljuk).

A "RAJT" cimkéjü feltételes utasitás kis módositásával azonban a jelen program 847 344! értékét még ki tudja számitani a háttér tár felhasználásával. Ha ezen is túl akarunk menni, akkor másik programot kell irni, amelyben már két hosszú szám szorzatára kell eljárást készitení a konvolucios szorzás felhasználásával.

A programot ténylegesen 1003! kiszámitásáig futtattuk le. (1003! egy 2577 jegyü szám. Annak érzékeltetésére, hogy ez milyen nagy szám, legyen szabad megemliteni, hogy egy olyan sugarú gömbben, amely a földtől az Ursa Ma II. galaxishalmazig terjed, ami kb. félmilliárd fényév, legfeljebb annyi atom van, amelynek számjegyeinek száma 100-nál kevesebb.) A futási idő 10 perc 29 sec volt, amiből látszik, hogy egy szám faktoriálisának a kiszámitásra kb. 1/2 sec időre volt a gépnek szüksége átlagban (persze az elején kevesebb a végén több idő kellett).

Megjegyezzük, hogy ha assembler nyelv szintjéig mennénk le, vagy méginkább, ha gépi kódban 2^m alapu számrendszerben dolgoznánk, lényegesen gyorsabb lenne a program lefutása.

Ha a számitógép gyárak a fentiekben vázolt hosszú aritmetikát a gép alap-software-jébe épitenék be, akkor a jelenleg használatos programnyelvek némi módositásával még kis számitógépek esetén is tetszőlegesen előre adott pontossággal lehetne számolni viszonylag gyorsan.

Irodalom

[1] L. Berg,: Einführung in die Operatorenrechnung, Berlin 1962.

```
begin comment FAKT;
 integer korlaat;
 korlaat=9500;
 begin
  integer i,j,k,l,m,n,r,s,a,b,c,d,e,f,g,kezd,norm;
  Boolean nagy;
  integer array w[0:korlaat];
  procedure kiir(k,w,s,norm,c,d,f);
   integer k,s,norm,c,d,f;
   integer array w;
   begin
    integer i,r,l,g;
    r=10;
    for i=1 step 1 until d do
     if w[0]÷r×r≠w[0] then go to ki else r=r×10;
ki: if r>10 then
     begin r=r÷10;
      for i=0 step 1 until s do
       w[i]=w[i]÷r+(w[i+1]-w[i+1]÷r×r)×(c÷r);
      norm=norm+ln(r)/ln(10.0);
      if w[s]=0 then s=s-1;
     end pontos normirozaas;
    comment itt helyezkedik el a kiiroo programreesz;
   end kiir;
L0:k=s=norm=w[0]=0;
  copy(korlaat,w[0],w[1]);
  nagy=false; c=10000; d=4; f=60; e=f÷d; w[0]=1;
  comment egyeeb programkezdeti szervezeesek;
  kiir(k,w,s,norm,c,d,f);
RAJT:k=k+1;
  if k=838 then
rend:begin
       nagy=true; c=1000; d=3; e=f÷d;
       l=r=(s+1)/3+.2; s=3×r-1;
```

```
      for i:=s step -3 until 2 do
       begin m:=w[i+r]:=w[i]÷10; j:=w[i-1]÷100;
        w[i+r-1]:=(w[i]-m×10)×100+j; m:=w[i-2]÷1000;
        w[i+r-2]:=(w[i-1]-j×100)×10+m;
        w[i+r-3]:=w[i-2]-m×1000;
        r:=r-1;
       end i;
      s:=s+1;
     end bin. kod. 10^4-es aabr.-rool 10^3-asra aatteerees;
  b:=0;
  for i:=0 step 1 until s do
   begin l:=w[i]×k+b; b:=l÷c; w[i]:=l-b×c;
   end i;
ST:if b≠0 then
    begin l:=b÷c; w[i]:=b-l×c; b:=l; i:=i+1;
     go to ST;
    end 2.3 tetel es Tb transzformacio;
  s:=i-1; comment Supp w;
  i:=-1;
  for i:=i+1 while w[i]=0 do ;
  if i>0 then
   begin copy(s+1,w[i],w[0]); s:=s-i; norm:=norm+d×i;
   end durva normirozaas;
  kiir(k,w,s,norm,c,d,f);
  comment a befejezeest eloeiro felteetelek vizsgaalata;
  go to RAJT;
 end;
end FAKT;
```

Summary

Accurate calculation with arbitrary large integers by means of digital computers

E. Gesztelyi – P. Jékel

The paper deals with the theoretical background of an integer arithmetic applicable for accurate calculation with large integers independent of the specific hardware feature of the given digital computer.

A function is called arithmetical when it is defined on the set of nonnegative integers. The arithmetical function f is said to be an integral valued function if $f(n)$ is an integer for every n and such that $f(n) = 0$ for $n > N$ where the number N depends on f. In the set I of integral valued arithmetical functions let the addition be defined in the usual way and the multiplication as the convolution

$$(1) \qquad \sum_{k=0}^{n} f(n-k)g(k)$$

This way I becomes an integral domain.

Let $b \geqslant 0$ be a fixed integer that we consider the base of a number system. We define in I an equivalence relation (depending on b) as follows. We say that the functions $f,g \in I$ are equivalent with respect to b (written $f \overset{b}{\sim} g$) iff

$$(S_b f)(0) = (S_b g)(0)$$

where S_b is such a transformation that

$$(S_b f)(n) = \begin{cases} \sum_{k=0}^{N} f(k)b^k & \text{if} \quad n = 0 \\ 0 & \text{if} \quad n > 0 \end{cases}$$

This equivalence relation is compatible with respect to the addition and multiplication (defined by (1)). Thus we can construct the corresponding factor ring I/b in the usual way. The ring I/b is isomorphic to the ring of integers.

We define a transformation T_b as follows

$$s(0) = f(0)$$

$$s(n+1) = f(n+1) + [\frac{s(n)}{b}]$$

$$(T_b f)(n) = s(n) - b[\frac{s(n)}{b}]$$

where [ ] = entier ( ).

Let

$$I_+ = \{ f \mid f \epsilon I,\ 0 \leqslant f(n) < b,\ n = 0,1, \ldots \}$$

and

$$I_- = \{ g \mid b - 1 - g \epsilon I_+ \} .$$

Then the following statements are true.

1. If $f \epsilon I_+$ then $(T_b f)(n)$ is the $(n+1)$-th digit of $(S_b f)(0)$ with respect to the base b.
2. $f \overset{b}{\sim} g$ iff $T_b f = T_b g$ $(f,g \epsilon I)$ (Theorem 4.2.)
3. If $f \epsilon I$ and $(S_b f)(0) \geqslant 0$ then $T_b f \epsilon I_+$ and if $(S_b f)(0) < 0$ then $T_b f \epsilon I_-$ (Theorem 4.1.).
4. $T_b^2 = T_b$ (Theorem 4.3.).
5. Theorem 4.4.: $T_b(f + g) = T_b(T_b f + T_b g)$,
   $T_b(f * g) = T_b(T_b f * T_b g)$.
6. If $f \epsilon I_+ \cup I_-$ then $T_b f = f$.

If follows from the above facts that we are able to write programs for the computation of algebraic expressions consisting of integers even if they are very large. Let f and g be two integer procedures which generate the digits of $(S_b f)(0)$ and $(S_b g)(0)$, respectively, in the number system of base b. Since $f,g \epsilon I$, if we take the sum or the convolution of f and g we obtain a result h which is also in I. If we submit h to the procedure T_b then we get functions which are in I_+ or I_- depending on the sign of $(S_b h)(0)$.

Thus the values of $T_b h$ provide the digits of $(S_b h)(0)$ if $T_b h \epsilon I_+$ and if $T_b h \epsilon I_-$ then the complement of $T_b h$ gives the digits of the number $-(S_b h)(0)$.

We have also presented algorithms for the division.

To show the applicability of the theory we have written a program in ALGOL 60 for the computation of the factorials. We have flowed the program by the computer ODRA 1204 to calculate the factorials from 1 to 1003.

Р е з ю м е

Точные расчеты с произвольно большими числами на ЭВМ

Е. Гестельи – П. Йекель

В настоящей работе обсуждаются теоретические основы целой машинной арифметики, с помощью которой на любой ЭВМ, независимо от ее технического обеспечения, могут быть реализованы точные расчеты с произвольно большими целыми числами.

Функции определенные на множестве неотрицательных чисел назовем арифметическими функциями.

Арифметическую функцию назовем целой функцией если ее значения целые числа, за исключением, быть может, конечного числа значений функции равных нулю.

На множестве I целых функций определим обычным образом операцию сложения, а также операцию умножения со сверткой:

$$(f * g)(n) = \sum_{k=0}^{n} f(n-k)g(k) \qquad (f,g \in I) \tag{1}$$

Таким образом I область целостности.

Пусть $b \geq 2$ фиксированное целое число, которое принимаем за основание системы счисления.

Определим на I отношение эквивалентности:
будем говорить, что f и $g \in I$ эквивалентны относительно $f \overset{b}{\sim} g/$, если

$$\sum_{n=0}^{\infty} f(n)b^n = \sum_{n=0}^{\infty} g(n)b^n \tag{2}$$

отношение эквивалентности (2) совместимо на I.

Покажем, что соответствующая фактор-структура I/b изоморфна кольцу целых чисел.

Определим T_b – преобразование следующим образом:

Пусть f некоторая арифметическая функция, и пусть

$$\Delta(0) = f(0)$$
$$\Delta(n+1) = f(n+1) + \left[\frac{\Delta(n)}{b}\right]$$
$$(T_b f)(n) = s(n) - b\left[\frac{\Delta(n)}{b}\right],$$

где [ ] = entier ( ).

Обозначим через

$$I_+ = \{ f / f \epsilon I,\ 0 \leqslant f(n) < b, n = 0,1,2, \ldots \}$$

и через

$$I_- = \{ g / b - 1 - g \epsilon I_+ \} .$$

Тогда справедливы следующие утверждения

1/ Если $f \epsilon I_+$, тогда в системе счисления с основанием b $f(n)$ дает $n+1$ -ий знак числа $(S_b f)(0) = \sum_{n=0}^{N} f(n) b^n$

2/ $f \overset{b}{\sim} g$ в том и только в том случае, если $T_b f = T_b g$ /теорема 4.2/

3/ Если $f \epsilon I$ и $(S_b f)(0) \geqslant 0$, тогда $T_b f \epsilon I_+$, а также если $(S_b f)(0) < 0$, тогда $T_b f \epsilon I_-$ /теорема 4.1/

4/ $T_b^2 = T_b$ /теорема 4.3/

5/ $T_b(f + g) = T_b(T_b f + T_b g)$,

$T_b(f * g) = T_b(T_b f * T_b g), f, g \epsilon I$ /теорема 4.4/

6/ Если $f \epsilon I_+ \cup I_-$, тогда $T_b f = f$.

Из вышесказанного следует, что сумма и умножение со сверткой функций f и g, при помощи которых мы генерируем цифры целых чисел $(S_b f)(0)$ и $(S_b g)(0)$ в b -ричной системе счисления, принадлежат I .

Применяя к сумме или произведению (2) указаных функций преобразование T_b получаем функции лежащие в I_+ или в I_- , в зависимости от знака преобразования S_b .

Таким образом, мы получаем b-ричные цифры результата S_b непосредственно, если результат преобразования T_b лежит в I_+ , дополнение до $b-1$ дает нам цифры результата S_b со знаком минус, в том случае, если результат преобразования T_b лежит в I_- .

Программа на АЛГОЛе-60, написанная с использованием вышеописанного метода за эффективное время рассчитала, например, значение 1003! на ЭВМ ODRA 1204.

MTA Számítástechniaki és Automatizálási Kutató Intézete, **Közlemények** 16/1976.

REGULÁRIS, OPERÁTOR EGYÜTTHATÓS STURM-LIOUVILLE EGYENLET SPEKTRUMÁNAK DISZKRÉTSÉGÉRŐL

Juhász Ferenc

Legyen H szeparábilis Hilbert tér. $\overline{H}$ álljon azon $f(x)$ $(0 \leqslant x \leqslant \pi)$ vektor értékü, Bochner szerint mérhető függvényekből, amelyekre

$$\int (f(x), f(x))dx < \infty.$$

$\overline{H}$ szintén szeparábilis Hilbert tér, melyben

$$\|f\|^2 = \int_0^{\pi} |f(x)|^2 dx.$$

Legyen $D \subset H$ mindenütt sűrű halmaz, $Q(x) : D \to H$ önadjungált, diszkrét spektrumú, egynél nagyobb operátor *mm.* x-re. Minden $h \epsilon D$-re $Q(x)h$ legyen $\overline{H}$-beli. Legyen $ly = -y'' + Q(x)y$, ahol a vessző erős deriváltat jelöl. P_0 és P_π legyen pozitiv, önadjungált operátor H-n. Értelmezzük l-et az összes olyan

$$y(x) = \sum_{l=1}^{m} \sum_{k=1}^{n} h_k \varphi_e(x)$$

függvényen, amely kielégiti az $y'(0) - P_0 y(0) = 0$, $y'(\pi) + P_\pi y(\pi) = 0$ peremfeltételeket, ahol $h_k \in D$, $\varphi_l(x) \epsilon C_2(0,\pi)$. Jelöljük L-lel l Friedrichs féle önadjungált kiterjesztését. Ekkor igaz a következő:

Tétel: *L spektruma diszkrét.*

Levitán és Szuvorcsenkova [2]-ben bizonyitotta a tételt azzal a további megszoritással, hogy Q inverze gyengén mérhető. Mászlov [1]-ben foglalkozik a szinguláris feladattal. Jelen dolgozat célja annak megmutatása, hogy az ott alkalmazott módszer milyen könnyedén elintézi a reguláris feladatot.

A bizonyitás a következő lemmán és annak Maszlov által közölt megforditásán alapul. Igazolásuk [1]-ben található.

Lemma: *Tegyük fel, hogy A teljesen folytonos operátor, A^{-1} létezik és értelmezési tartománya sürü. Ekkor minden A^{-1} értelmezési tartományában levő, gyengén nullához tartózo $y_n \to 0$ sorozatra.*

$$\sigma_n^2 = \frac{|y_n|^2}{\max\{|A^{-1} y_n|, \alpha\}} \to 0, \quad \text{ahol } \alpha > 0 \text{ rögzitett.}$$

Lemma. *Tegyük fel, hogy A korlátos operátor H-n, A^{-1} létezik és értelmézesi tartománya sürü. A akkor és csak akkor teljesen folytonos, ha A^{-1} minden, az értelmézési tartományában lévö, egy normáju, gyengén nullához tartozó sorozatot a végtelenbe visz.*

Tételünk bizonyitásához elegendő megmutatni, hogy $\sqrt{L}^{-1}$ teljesen folytonos, ebből következik, hogy $\sqrt{L}$ és igy L spektruma is diszkrét. A második lemmát felhasználva tegyük fel indirekte, hogy létezik olyan $\{y_n\}$ sorozat, $\|y_n\| = 1$, $y_n \rightharpoonup 0 \in \overline{H}$, melyre

$$(\sqrt{L}y_n, \sqrt{L}y_n) = (P_0 y(0), y(0)) + (P_\pi y(\pi), y(\pi)) +$$

$$+ \int_0^\pi ((y_n', y_n') + (y_n, Qy_n)) \leqslant C_1$$

Megmutatjuk először, hogy $|y_n(x)| \leqslant C_2$ minden n-re és x-re.

$$(1) \qquad \left| |y_n(x_2)|^2 - |y_n(x_1)|^2 \right| \leqslant 2 \left| \int_{x_1}^{x_2} (y_n', y_n) \right| \leqslant \int_0^\pi (|y_n'|^2 + |y_n|^2) \leqslant C_1$$

Ha $|y_n(x)| \leqslant C_2$ nem teljesülne, akkor létezne olyan $\{x_i\}$ sorozat, melyre $|y_{n_i}(x_i)| \to \infty$. Ekkor azonban (1) miatt $y_{n_i}(x) \to \infty$ minden x-re, ami ellentmond az $y_{n_i} \in \overline{H}$ feltételnek.

Mivel $\|y_n'\| \leqslant C_1$ ezért legyen az $\{y_{n_i}'\}$ sorozat olyan, hogy $y_{n_i}' \rightharpoonup f \in \overline{H}$. Minthogy $y_{n_i} \rightharpoonup 0 \in \overline{H}$, ezért $f = 0 \in \overline{H}$. Legyen $X(\xi)$ a $[0,x]$ intervallum karakterisztikus függvénye. Ekkor tetszőleges $h \in H$-ra

$$(2) \qquad (h, y_{n_i}(x) - y_{n_i}(0)) = (h, \int_0^x y'_{n_i}) = \int_0^\pi (hX(\xi), y'_{n_i}(\xi)) d\xi \to 0$$

mivel $y'_{n_i} \rightharpoonup 0 \in \overline{H}$.

Válasszunk ki az $\{y_{n_i}(0)\}$ sorozatból egy $y_{n_{i_k}}(0) \rightharpoonup g \in H$ sorozatot. Ekkor (2) miatt $y_{n_{i_k}}(x) \rightharpoonup g \in H$ és minthogy $y_{n_{i_k}} \rightharpoonup 0 \in \overline{H}$, a Lebesque tétel felhasználásával kapjuk, hogy $g = 0 \in H$. $\{y_{n_{i_k}}\}$ tehát olyan sorozat, melyre $y_{n_{i_k}}(x) \rightharpoonup 0 \in H$ *mm.* x-re.

A továbbiakban az $\{y_{n_{i_k}}\}$ sorozatot jelöljük egyszerüen $\{y_n\}$ -nel.

Minthpgy $\sqrt{Q}^{-1}$ teljesen folytonos *mm.* x-re, ezért

$$\sigma_n^2 = \frac{|y_n|^2}{\max\{(y_n, Qy_n), \alpha\}} \to 0 \qquad \textit{mm. } x\text{-re.}$$

Minthogy mérhető, ezért mértékben is tart 0-hoz. Ilymódon bármely $\epsilon > 0$, $\delta > 0$ számhoz található olyan $N = N(\epsilon,\delta)$, hogy $n > N$ esetén az F_n halmaz pontjaiban $\sigma_n^2 \leqslant \delta$ továbbá

$\text{mes}\overline{F_n} \leqslant \epsilon$.

Ekkor

$$\int_{F_n'} (y_n, y_n) \leqslant \delta \int_{F_n} \max\{(\sqrt{Q}yn,\ \sqrt{Q}yn), \alpha\} \leqslant$$

$$\leqslant \delta \int_{F_n} ((y_n, Qy_n) + \alpha) \leqslant \delta(C_1 + \alpha)\pi, \text{ továbbá}$$

$$\int_{F_n} (y_n, y_n) \leqslant c_1 \text{mes}\overline{F_n} \leqslant C_1 \epsilon$$

Ha $\delta < \frac{1}{2(c_1 + \alpha)\pi}$ és $\epsilon < \frac{1}{2c_1}$, akkor $\int_0^{\pi} (y_n, y_n) < 1$, ami ellentmond feltételünknek.

I r o d a l o m

[1] Маслов, В.П.: О критерии дискретности спектра уравнения Штурма - Лиувилля с операторным коэффициентом. Ф.А. 2.вып. 2. 1968, 63-67.

[2] Левитан, Б.М. - Суворченкова, Г.А.: Достаточные условия дискретности спектра уравнения Штурма - Лиувилля с Операторным коэффициентом. Ф.А. 2 вып. 2. 1968, 56-62.

[3] Рисс, Ф. - Секефальви-Надь, Б.: Лекции по функциональному анализу /1954/.

[4] Hille,E. - Phillips R.S.: Functional analysis and semigroups /1957/.

[5] Achieser, N.I. - Glasmann, I.M.: Theorie der linearen Operatoren im Hilbert-Raum /1954/.

[6] Данфорд, Н. - Шварц, Дж.Т.: Линейные операторы II. /1966/.

S u m m a r y

On the discreetness of spectrum of regular
Sturm–Liouville equation with operator coefficient

F. Juhász

The statement of this paper is proved in [2], with an additional condition of measurability. V. P. Maslov studied the singular equation in [1]. The aim of this paper is to show how usefully that method can be applied for the regular case.

Р е з ю м е

О дискретности спектра регулярного уравнения
Штурма-Лиувилля с операторным коэффициентом

Ф. Юхас:

Утверждение данной работы доказана в [2] с добавочным условием измеримости. В [1] В.П.Маслов изучал сингулярную задачу. Наша цель - показать, что метод Маслова полезно применяется также в случае регулярной задачи.