13. Az asszociativitás következményei

Félcsoporton egy asszociativ müvelettel rendelkező algebrai struktu-rát értünk. A továbbiakban félcsoportról általában beszélve, müveletét mindig szorzásnak nevezzük és ennek megfelelő beszédmódot (pl. tényező, szorzat, hatvány) valamint jelölést alkalmazunk.

Tömören szólva, a szorzás asszociativitása azt jelenti, hogy három tényező esetén a szorzás eredménye független attól, hogy a két lehetséges "értelmes" zárójelzés közül melyiket alkalmazzuk. Bár intuitive eléggé világos, hogy mit értünk "értelmes" zárójelzésen - pl. az S félcsoportbeli a,b,c, elemek $a(bc)$ zárójelezése értelmes, mig az $a)bc$ zárójelezés nem - mégis szükség van arra, hogy ezt a fogalmat pontosabbá tegyük (hiszen pl. már abban mindenképpen meg kell állapodnunk, hogy az $(a(bc))$ zárójelezést értelmesnek tekintsük-e, mert itt a külső zárójelpár felesleges, azaz elhagyása a szorzat egyértelmü meghatározottságát és eredményét nem befolyásolja).

Rövidség kedvéért, értelmesen zárójelezett szorzat helyett a következőkben a szabályos szorzat kifejezést használjuk. Legyen S tetszőleges félcsoport. Az S elemeiből és zárójelekből képezett sorozatok szabályosságát a következőképpen definiáljuk:

(1) Az ab $(a,b\in S)$ sorozat (amely tehát kételemü és nem tartalmaz zárójelet) szabályos szorzat.

(2) Ha A egy szabályos szorzatot jelöl és $c\in S$, akkor $c(A)$ és $(A)c$ is szabályos szorzatok.

(3) Ha A,B szabályos szorzatokat jelölnek, akkor $(A)(B)$ is szabályos szorzat.

(4) Minden szabályos szorzat előáll (1) alaku szabályos szorzatokból a (2) és (3) képzési törvények véges számu alkalmazásával.

Tekintsünk egy S elemeiből és zárójelekből képzett (röviden: S-beli) szabályos szorzatot, melyben S-nek $a_1,\dots,a_n$ elemei - ebben a sorrendben - szerepelnek (az elemek között megegyezők is lehetnek). Mivel e szabályos szorzatnak az (1)-(4) törvények alkalmazásával való előállitásánál minden lépésben két S-beli elem szorzatát kell képeznünk - az pedig egyértelmüen meghatározott - azért az $a_1,\dots,a_n$ elemeket e sorrendben tartalmazó bármely szabályos szorzat S-nek egy egyértel-

müen meghatározott elemét jelenti. Nevezzük ezt az elemet az adott szabályos szorzat értékének.

Legyen most a,b,c az S félcsoportnak három tetszőleges eleme. Könnyen meggondolható, hogy csak két olyan különböző szabályos szorzat létezik, amely ezeket az elemeket ebben a sorrendben tartalmazza, éspedig $a(bc)$ és $(ab)c$. Eszerint az S-beli szorzás asszociativitása azt jelenti, hogy bármely $a,b,c\in S$ esetén két, az a,b,c elemeket ebben a sorrendben tartalmazó szabályos szorzat értéke megegyezik.

Megmutatjuk, hogy tetszőleges S félcsoport bármely $a_1,\dots,a_n$ elemei esetén is (ahol n ugyancsak tetszőleges természetes szám) két, az $a_1,\dots,a_n$ elemeket ebben a sorrendben tartalmazó szabályos szorzat értéke megegyezik. Az $n=1$ esetben az állitás üres, az $n=2$ esetben triviális, mig az $n=3$ esetben a szorzás asszociativitását jelenti, amit a félcsoport definiciója magában foglal. Legyen most $n>3$ és tegyük fel, hogy n-nél kevesebb tényezős szabályos szorzatokra állitásunk igaz. Képezzünk az $a_1,\dots,a_n\in S$ elemekből két szabályos szorzatot, mely őket ebben a sorrendben tartalmazza. Jelölje a két szorzatot π és ϱ. Szorzataink az 1. - 3. képzési törvények véges számu alkalmazásával keletkeznek; emellett utoljára mindig a 2. vagy a 3. törvényt használjuk. Legyen pl. $\pi=(a_1,\dots,a_{n-1})a_n$ és $\varrho=(a_1\dots a_i)(a_{i+1}\dots a_n)$.

Itt tehát π képzésének utolsó lépéseként a 2. törvény második részét, ϱ képzésének utolsó lépéseként pedig a 3. törvényt alkalmaztuk. A zárójelekben levő szabályos szorzatokat további zárójelek felhasználása nélkül irhattuk, mert az indukciófeltevés szerint értékük a zárójelezéstől független. Ugyanezen ok miatt a zárójeleken belüli szabályos szorzatokban további zárójeleket is kitehetünk a szorzatok értékének megváltozása nélkül. Ezért irhatjuk: $\pi=((a_1\dots a_i)(a_{i+1}\dots a_{n-1}))a_n=$ $=(a_1\dots a_i)((a_{i+1}\dots a_{n-1})a_n)$. Ekkor az asszociativitás következtében $\pi=\varrho$. Ehhez hasonlóan nyerjük a $\pi=\varrho$ egyenlőséget a lehetséges további esetekben is.

Eredményünket röviden ugy fejezhetjük ki, hogy félcsoportban szorzat értéke független a zárójelezéstől. A félcsoportbeli szorzás e tulajdonságát általános asszociativitásnak nevezzük. Az általános asszociativitás tehát az asszociativitásnak következménye. Az általános asszociativitást figyelembe véve a továbbiakban a félcsoportbeli szorzatokat rendszerint zárójelek nélkül irhatjuk, másrészt pedig, ha ez szükséges, zárójeleket bármilyen módon ki is tehetünk. (Igy pl. megengedjük az $(a_1a_2)a_3a_4$ alaku szorzatot is, bár ez nem szabályos. E szorzat értéke ugyanis mindenképpen egyértelmüen meghatározott, az alkalmazott zárójelezés viszont lehetővé teszi, hogy szorzatunkat átmenetileg háromtényezősnek tekintsük, ami bizonyos meggondolásoknál előnyös lehet.)

Tekintsük most az S kommutatív félcsoportot. A szorzás kommutativitása azt jelenti, hogy két tényező esetén a szorzat értéke független attól, hogy a két tényezőnek a szorzatban mi a sorrendje. Megmutatjuk, hogy kommutatív félcsoportban tetszőleges számú tényezőt tartalmazó szorzat értéke is független a tényezők sorrendjétől.

Legyen $a_1,\dots,a_n\in S$. Tegyük fel, hogy $n>2$ és n-nél kevesebb tényezőt tartalmazó szorzatokra állításunkat - mely kéttényezős szorzatokra éppen a kommutativitást jelenti - már igazoltuk. Legyen φ az $\langle 1,\dots,n\rangle$ halmaz permutációja. Azt kell megmutatnunk, hogy $a_{1\varphi}\dots a_{n\varphi}=a_1\dots a_n$. Van olyan i $(1\le i\le n)$, hogy $1=i\varphi$ Ekkor

$$a_{1\varphi}\dots(a_{(i-1)\varphi}\,a_{i\varphi})\dots a_{n\varphi}=a_{1\varphi}\dots(a_{i\varphi}\,a_{(i-1)\varphi})\dots a_{n\varphi}\,.$$

Ilyen átalakítás $i-1$-szeri alkalmazásával elérjük, hogy $a_{i\varphi}(=a_1)$ a szorzat első helyére kerül; azaz $a_{1\varphi}\dots a_{n\varphi}=a_1(a_{1\varphi}\dots a_{(i-1)\varphi}\,a_{(i+1)\varphi}\dots a_{n\varphi})$.

Az indukciófeltevés szerint a zárójelben levő $n-1$-tényezős szorzat értéke megegyezik az $a_2\dots a_n$ szorzatéval. Ezért $a_{1\varphi}\dots a_{n\varphi}=a_1\dots a_n$, amit bizonyítani akartunk. A kommutatív félcsoportbeli szorzás most igazolt tulajdonságát <u>általános kommutativitás</u>nak nevezzük. Az általános kommutativitás tehát a kommutativitásnak következménye.

Definiáljuk félcsoportelem <u>hatványait</u> a következőképpen: a első hatványa, a^1 legyen maga a, s ha már a $n-1$-edik hatványa (a^{n-1}) definiálva van, legyen a n-edik hatványa, a^n egyenlő $(a^{n-1})a$-val. Teljes indukció mutatja, hogy ily módon a^n minden n természetes számra értelmeztük. Észrevesszük, hogy bármely m,n természetes számra igaz $a^{m+n}=a^m a^n$ (ezt bármely m-re n szerinti teljes indukcióval igazolhatjuk, felhasználva az általános asszociativitást). Ugyancsak teljesül $(a^m)^n=a^{mn}$ is; ha pedig az S félcsoport kommutatív, minden $a,b\in S$-re és minden m természetes számra igaz $(ab)^m=a^m b^m$.

Definiciónk a^0-nak nem tulajdonit értelmet. Ha a^0-t értelmezni akarjuk, kívánatos ezt ugy tennünk, hogy a hatványozás törvényei (pl. az $a^{m+n}=a^m a^n$ törvény) érvényben maradjanak. Speciálisan, bármely a félcsoportelemre teljesülnie kell az $aa^0=a^1a^0=a^1a^0=a$, s hasonlóan az $a^0a=a$ egyenlőségnek. Ha félcsoportunk egységelemes, ezt elérhetjük, ha minden elem nulladik hatványának a félcsoport egységelemét nevezzük. Ilyen megállapodás mellett az $(a^m)^n=a^{mn}$ törvény, kommutatív félcsoportokra pedig az $(ab)^m=a^m b^m$ törvény is érvényben marad.

Megjegyezzük, hogy minden S félcsoport beágyazható egységelemes félcsoportba, mégpedig egyszerüen ugy, hogy tekintjük az $S\cup\langle e\rangle$ halmazt, ahol e az S elemei között nem szereplő szimbólum, s ezen a halmazon a szorzást a következő módon értelmezzük: az S-hez tartozó elemek szorzását változatlanul végezzük (ez biztositja, hogy S a keletkező félcsoportnak részfélcsoportja legyen), továbbá, ha $s\in S$, legyen $se=es=s$, végül legyen $ee=e$. Ekkor $(S\cup\langle e\rangle;\cdot)$ egységelemes félcsoport.

Példák

1. $(ab)((cd)e)=(a(bc))(de)$; részletesen
$(ab)((cd)e)=(ab)(c(de))=((ab)c)(de)=(a(bc))(de)$.

2. Kommutatív félcsoportban
$aecbd=bedac$; részletesen
$bedac=beadc=baedc=abedc=aecbd$.

Gyakorlatok

1. Határozzuk meg az egyelemü generátorrendszerrel rendelkező félcsoportokat!

2. Nevezzük az egymüveletes algebrai struktura a elemét idempotensnek, ha $a^2=a$. Minden véges félcsoportban van idempotens elem.

3. Kommutativ félcsoportban az idempotens elemek részfélcsoportot alkotnak.

4. Határozzuk meg a természetes számok additiv félcsoportjának összes kompatibilis osztályzásait!

14. Transzformációfélcsoport

Legyen M nemüres halmaz. M összes transzformációinak halmaza a leképezés-szorzás müvelettel félcsoportot alkot. Valóban, M két transzformációjának szorzata maga is transzformációja M-nek; másrészt a transzformációk szorzása asszociativ, ugyanis, ha $m\in M$, α,β,γ pedig M-nek transzformációi, akkor $m(\alpha(\beta\gamma))=(m\alpha)(\beta\gamma)=((m\alpha)\beta)\gamma=(m(\alpha\beta))\gamma=m((\alpha\beta)\gamma)$, ezért $\alpha(\beta\gamma)=(\alpha\beta)\gamma$.
A tekintett félcsoport neve: M <u>teljes transzformációfélcsoportja</u>, jelölése: $\mathcal{T}_M$. $\mathcal{T}_M$ mindig egységelemes: egységeleme az ι identikus leképezés.

A teljes transzformációfélcsoportok részfélcsoportjait <u>transzformációfélcsoportnak</u> nevezzük.

Tétel: Minden félcsoport izomorf egy transzformációfélcsoporttal.

Bizonyitás: Legyen S félcsoport, s először tegyük fel, hogy S-nek van e egységeleme. Jelölje φ S-nek $\mathcal{T}_S$-be való ama leképezését, amely $s \in S$-nek az $x\varphi_s = xs$ összefüggéssel $(x \in S)$ definiált $\mathcal{T}_S$-beli φ_s transzformációt feleltei meg. Megmutatjuk, hogy φ S-nek $\mathcal{T}_S$-be való olyan kölcsönösen egyértelmü leképezése, amely a müvelettel felcserélhető. Ebből már következik, hogy φ S-nek a $\mathcal{T}_S$-beli $S\varphi$ részfélcsoportra való izomorf leképezése, azaz $S \cong S\varphi$.

Legyen $s_1, s_2 \in S$ és $s_1\varphi = s_2\varphi$, vagyis $\varphi_{s_1} = \varphi_{s_2}$. Akkor $e\varphi_{s_1} = es_1 = s_1$, $e\varphi_{s_2} = es_2 = s_2$, tehát $s_1 = s_2$. Ezért φ kölcsönösen egyértelmü. Továbbá bármely $x \in S$-re $x((s_1\varphi)(s_2\varphi)) =$

$= x(\varphi_{s_1}\varphi_{s_2}) = xs_1s_2 = x\varphi_{s_1 s_2} = x((s_1s_2)\varphi)$, tehát $(s_1\varphi)(s_2\varphi) =$

$= (s_1s_2)\varphi$. Nyertük, hogy φ a szorzással felcserélhető.

Ha S-nek nincs egységeleme, ágyazzuk be egy S_1 egységelemes félcsoportba; ezután minden változtatás nélkül alkalmazva az előző meggondolásokat, nyerjük, hogy $\mathcal{T}_{S_1}$-nek van S_1-gyel izomorf részfélcsoportja. Ebből az egységelemet (az identikus leképezést) elhagyva, $\mathcal{T}_{S_1}$-nek S-sel izomorf részfélcsoportját kapjuk.

Ezt a tételt a félcsoportok reprezentációtételének nevezzük, a következő meggondolás alapján. Tekintsük félcsoportok tetszőleges H halmazát; tudjuk, hogy ezen az izomorfia ekvivalenciareláció. A hozzátartozó osztályozás minden egyes osztályához létezik olyan transzformációfélcsoport, mely izomorf az adott osztályba tartozó félcsoportokkal. Egy-egy ilyen transzformációfélcsoportot kiválasztva - feltehetjük, hogy H ezeket eleve tartalmazza - az osztályozás teljes reprezentánsrendszerét kapjuk. Hasonló reprezentációtételeket más strukturafajtákra is fogunk bizonyitani, s ezek lényege mindig az, hogy izomorfia-osztályok reprezentánsainak bizonyos speciális strukturák tekinthetők.

Legyen S az M halmaznak egységelemes transzformációfélcsoportja. Segitségével M-en egy $\sim$ relációt értelmezünk a következőképpen: $a, b \in M$-re $a \sim b$ akkor és csak akkor, ha van olyan $\sigma \in S$, hogy $a\sigma = b$. Ha $\sim$ az univerzális reláció - más szóval M bármely eleme bármely elembe átvihető S-beli transzformációval - akkor azt mondjuk, hogy S tranzitiv M-en. Általánosabban, ha $M' \subseteq M$, azt mondjuk, hogy S tranzitiv M'-n, ha M' bármely eleme bármely elemébe átvihető S-beli transzformációval.

Vegyük észre, hogy $(M;S)$ automata, ti. az S-beli transzformációk - mint általában minden transzformáció - M-nek egyváltozós müveletei. S akkor és csak akkor tranzitiv M-en, ha $(M;S)$-nek nincs tőle különböző részautomatája. Valóban, tegyük fel, hogy S tranzitiv M-en, és legyen K $(M;S)$-nek részautomatája. Ha $k \in K$ és m M-nek tetszőleges eleme, akkor létezik olyan $\sigma \in S$, hogy $k\sigma = m$, ezért $m \in K$, tehát $K = M$. Ha pedig S nem tranzitiv M-en, akkor van olyan

$m_1, m_2 \in M$, hogy bármely $\sigma \in S$-re $m_1\sigma \neq m_2$, tehát $M_1 = \langle m_1\sigma : \sigma \in S \rangle$ valódi része M-nek. Emellett M_1 részautomatája $(M;S)$-nek, mert ha $\sigma_1, \sigma_2 \in S$ és $m_1\sigma_1$ M_1-nek tetszőleges eleme, akkor $(m_1\sigma_1)\sigma_2 = m_1(\sigma_1\sigma_2) \in M_1$ (t.i. S zárt a szorzásra nézve). Létezik tehát $(M;S)$-nek valódi részautomatája.

M-en egy további $\approx$ relációt is értelmezünk a következő módon: $a, b \in M$-re $a \approx b$ akkor és csak akkor, ha $a \sim b$ és $b \sim a$. Észrevesszük, hogy a $\approx$ reláció reflexiv és tranzitiv (e tulajdonságokkal már $\sim$ is rendelkezett), valamint szimmetrikus, ezért ekvivalencia. A hozzátartozó osztályozáson, $M/\approx$-n pedig egy $\leq$ relációt vezetünk be: $\bar{a}, \bar{b} \in M/\approx$-re legyen $\bar{a} \leq \bar{b}$ akkor és csak akkor, ha van olyan $a_1 \in \bar{a}$, $b_1 \in \bar{b}$, hogy $a_1 \sim b_1$. Megmutatjuk, hogy $\leq$ részbenrendezés. Bármely $a \in H$-re $\bar{a} \leq \bar{a}$, mert $a \sim a$, t.i. $a\iota = a$. Legyen $\bar{a} \leq \bar{b}$ és $\bar{b} \leq \bar{a}$, akkor alkalmas $a_1, a_2 \in \bar{a}$ és $b_1, b_2 \in \bar{b}$ elemekre $a_1 \sim b_1$ és $b_2 \sim a_2$. Figyelembe véve, hogy $b_1 \sim b \sim b_2$ és $a_2 \sim a \sim a_1$, s a $\sim$ reláció tranzitiv, nyerjük, hogy $a \sim b$ és $b \sim a$, tehát $\bar{a} = \bar{b}$. Ha pedig $\bar{a} \leq \bar{b}$ és $\bar{b} \leq \bar{c}$, akkor alkalmas $a_1 \in \bar{a}$, $b_1, b_2 \in \bar{b}$ és $c_1 \in \bar{c}$ elemekre $a_1 \sim b_1$, $b_2 \sim c_1$. Ismét a $b_1 \sim b \sim b_2$ összefüggésre és $\sim$ tranzitivitására támaszkodva nyerjük, hogy $a_1 \sim c_1$, tehát $\bar{a} \leq \bar{c}$.

Megfigyeléseinket szemléletesebben a következőképpen fogalmazhatjuk meg: egy M halmazon, annak bármely S transzformáció félcsoportja segitségével megadható egy osztályozás, az osztályok között pedig egy részbenrendezés ugy, hogy egy-egy osztálynak bármely eleméből bármely elemét megkaphatjuk S-beli transzformáció segitségével, továbbá egy osztály bármely eleméből a részbenrendezésben nagyobb osztályok (és csak ezek) elemeit ugyancsak megkaphatjuk S-beli transzformáció segitségével. Ezt az észrevételt az automaták elméletében fogjuk felhasználni.

Példák

1. Az összes (mindenütt értelmezett) valós függvények az összetett függvény képzésének müveletével tranzitiv transzformációfélcsoportot alkotnak. Hasonlóképpen a folytonos, valamint a differenciálható valós függvények.

2. A nemnegativ valós számokon értelmezett, (nem szigoruan) monoton, minden x-re $x \leq f(x)$ feltételnek eleget tevő valós függvények transzformációfélcsoportot alkotnak. A $\sim$ reláció az összes (a,b) pá-

rokból áll, ahol $a \leq b$; $a \approx$ reláció az egyenlőség; a szövegben értelmezett $\leq$ reláció a nemnegativ valós számok közönséges rendezése.

3. Tekintsük egy M nemüres halmazt, s rendeljük minden $a \in M$ elemhez M-nek azt a φ_a transzformációját, melyet $M\varphi_a = \langle a \rangle$ definiál. Az összes φ_a alaku transzformációk M-nek tranzitiv transzformáció-félcsoportját alkotják.

4. Legyen A tetszőleges automata. Az A halmaz mindazon transzformációi, melyek előállnak A véges számu müveletének szorzataként, A-nak transzformációfélcsoportját alkotják.

Gyakorlatok

1. Tetszőleges M halmaz bármely részbenrendezése megkapható alkalmas transzformációfélcsoportja segitségével. (Általánositsuk a 2. példát!)

2. Legyen o tetszőleges asszociativ müvelet a természetes számok $\mathcal{N}$ halmazán. Létezik folytonos valós függvényeknek olyan halmaza, amely az összetett függvény képzésének müveletével ellátva az $(\mathcal{N}; o)$ félcsoporttal izomorf félcsoportot alkot.

3. Minden halmaznak van idempotens transzformációja. Hány idempotens transzformációja van egy 3 elemü halmaznak?

4. Egynél többelemü halmaz teljes transzformációfélcsoportja nem kommutativ.

15. Szabad félcsoport

Legyen X tetszőleges halmaz. Tekintsük az $F(X) = \bigcup_{n=0}^{\infty} X^n$ halmazt, más szóval az összes - tetszőleges hosszuságu - X feletti szavak halmazát. Megállapodunk abban, hogy X^0 egyetlen elemét e-vel jelöljük. Vezessünk be $F(X)$-en egy kétváltozós müveletet, amely az $a_1 \dots a_m$ és $b_1 \dots b_n$ $(a_i, b_j \in X)$ szavakhoz az $a_1 \dots a_m\, b_1 \dots b_n$ szót rendeli, bármely $p \in F(X)$ szóhoz és e-hez pedig (akármelyik sorrendben is tekintjük ezeket), magát a p szót. Nevezzük ezt a müveletet szorzásnak. Szavakat tehát ugy szorzunk, hogy egymás után irjuk őket (konkatenáció), az e tényezőt pedig egyszerüen elhagyjuk. Az igy értelmezett szorzás nyilvánvalóan asszociativ, igy $F(X)$ e szorzásra nézve félcsoport, amelynek

e egységeleme. Ezt az $F(X)$ félcsoportot (egységelemes) szabad félcsoportnak[1], X-et pedig $F(X)$ szabad generátorrendszerének vagy ábécéjének nevezzük. Ha $X = \langle x_1, \dots, x_n \rangle$, $F(\langle x_1, \dots, x_n \rangle)$ helyett rövidebben $F(x_1, \dots, x_n)$-t irunk. Az $F(X)$ szabad félcsoport akkor és csak akkor végesen generált, ha szabad generátorrendszere véges (ha ugyanis végesen generált, akkor bármely generátorrendszeréből, s igy szabad generátorrendszeréből is kiválasztható egy véges generáló részrendszer, amely azonban a szabad generátorrendszerrel szükségképpen megegyezik, hiszen abból egyetlen elem sem hagyható el).

Az X halmaz elemeit szokás betüknek nevezni. Ha a $p \in F(X)$ szó n betüből áll, azt mondjuk, hogy p hosszusága n, és ezt igy jelöljük: $\ell(p) = n$. Ennek megfelelően megállapodunk abban, hogy $\ell(e) = 0$. Észrevesszük, hogy szavak szorzásakor hosszuságaik összeadódnak.

Legyen $p \in F(X)$. Ha $q\,(\in F(X))$-hez létezik olyan $r\,(\in F(X))$, hogy $p = qr$ akkor q p prefixének nevezzük. Ha tehát $p = x_1 \dots x_n$ (ahol $x_1, \dots, x_n$ X-beli betük, melyek között megegyezők is lehetnek), akkor p prefixei a következők: $e, x_1, x_1x_2, \dots, x_1 \dots x_n = p$ (az utóbbi azért, mert $pe = p$). Ha $t\,(\in F(X))$-hez létezik olyan $s\,(\in F(X))$ hogy $p = st$, akkor t-t p szuffixének nevezzük. p szuffixei $e, x_n, x_{n-1}x_n, \dots, x_1 \dots x_n = p$.

Mivel az izomorf strukturákat nem különböztetjük meg, az olyan félcsoportot is szabad félcsoportnak nevezzük, amely izomorf valamely - az előzőkben definiált - szabad félcsoporttal. Ha az $F(X)$ szabad félcsoportnak S részfélcsoportja is szabad félcsoport, azaz van olyan Y halmaz, hogy $S \cong F(Y)$, akkor S minden eleme egyetlen módon áll elő az Y elemeinek az adott izomorfizmusnál megfelelő szavak szorzataként. Forditva, ha S-ben vannak olyan $p_1, \dots, p_n$ szavak, hogy bármely S-beli elem egyetlen módón áll elő e szavakból képezett szorzatként, akkor S izomorf az $\langle y_1, \dots, y_n \rangle$ szabad generátorrendszerü szabad félcsoporttal. Ilyenkor S azon elemeinek halmazát, melyek az $y_1, \dots, y_n$ szabad generátoroknak felelnek meg, S szabad generátorrendszerének nevezzük.

A következő tételre a későbbiekben szükségünk lesz.

---

[1] Használatos a szabad monoid elnevezés is (monoid egységelemes félcsoportot jelent), ami gyakran előnyös; pl. $F(X)$ olyan részfélcsoportját, amely tartalmazza az egységelemet, egyszerüen részmonoidnak fogjuk nevezni. Az $F(X) \setminus \langle e \rangle$ félcsoportot - amely nem tartalmaz egységelemet - szabad félcsoportnak nevezzük.

Tétel: Legyen X véges halmaz, L pedig $F(X)$ -nek végtelen részhalmaza, amely bármely elemével együtt tartalmazza annak minden prefixét. Akkor létezik X-beli elemeknek olyan $x_1, x_2, \ldots$ végtelen sorozata, hogy bármely n -re $x_1 x_2 \ldots x_n \in L$.

Bizonyitás: Valóban, létezik legalább egy olyan $x_1 \in X$ amely végtelen sok L-beli szónak kezdőszelete. Legyen $k>1$. Ha L_k L-nek az a végtelen részhalmaza, amely az $x_1 \ldots x_k$ szót kezdőszeletként tartalmazó L-beli szavakból áll, akkor van olyan $x_{k+1} \in X$, hogy $x_1 \ldots x_k x_{k+1}$ végtelen sok L_k-beli szónak kezdőszelete. Ez a meggondolás definiálja az $x_1 \ldots x_k x_{k+1} \ldots$ végtelen sorozatot. Most bármely n -re $x_1 \ldots x_n$ (végtelen sok) L -beli (sőt L_{n-1}-beli) szónak prefixe, tehát $x_1 \ldots x_n \in L$.

Szabad félcsoport részhalmazait az automaták elméletében eseményeknek nevezik. Ugyancsak használatos a nyelv megnevezés is (ami összhangban van a "betü" és "szó" elnevezésekkel).

Példák

1. A latin betükkel leirható összes szavak (mint pl. liba, subset, qwcsnystt stb.) szabad félcsoportot alkotnak, melynek az összes latin betük halmaza szabad generátorrendszere. Értelmes összetett szó esetén az előtag a szó prefixe, az utótag pedig szuffixe.

2. Az összes természetes számok tizes számrendszerbeli felirásai (a konkatenáció müveletével) egy D félcsoportot alkotnak, amely az $F(0,1,\ldots,9)$ szabad félcsoportnak részfélcsoportja. A 0 szó a D félcsoport egyetlen elemének sem prefixe; forditva, ha az α szónak 0 nem prefixe, akkor $\alpha \in D$.

3. Az egyelemü szabad generátorrendszerrel rendelkező szabad félcsoport izomorf a nemnegativ egész számok additiv félcsoportjával. Izomorfiától eltekintve ez az egyetlen kommutativ szabad félcsoport.

Gyakorlatok

1. Szabad félcsoportnak nem minden részfélcsoportja szabad félcsoport.

2. Minden félcsoport egy alkalmas szabad félcsoport homomorf képe.

3. Legyen $F(x_1,\ldots,x_n)$ tetszőleges szabad félcsoport. Ha $p_1,\ldots,p_n \in F(x_1,\ldots,x_n)$, létezik $F(x_1,\ldots,x_n)$ -nek egyetlen olyan φ endomorfizmusa, amelyre $x_1\varphi = p_1, \ldots, x_n\varphi = p_n$.

4. Ha $X \subseteq Y$ akkor $F(X)$ egyrészt részfélcsoportja $F(Y)$ -nak, másrészt homomorf képe $F(Y)$ -nak.

5. Bármely egynél több elemü szabad félcsoport izomorf egy valódi részfélcsoportjával.

6. A 2. példa D félcsoportja maga is szabad félcsoport, de végtelen szabad generátorrendszerrel.

16. Kódolás

Jelöljön F tetszőleges, végesen generált szabad monoidot. Legyen M F-nek részhalmaza. Ha M véges - és csak ekkor - létezik M-ben leghosszabb szó. Ennek hosszuságát M hosszuságának nevezzük és $\ell(M)$-mel jelöljük.

Az F félcsoport K részfélcsoportját véges defektusunak nevezzük, ha van hozzá olyan $M \subseteq F$ véges halmaz, hogy a KM komplexusszorzat éppen az F félcsoport. Ilyen véges halmaz több is van (bármelyikhez hozzávehetünk például egy további szót); tegyük fel, hogy M máris közülük a legkisebb hosszuságut jelöli. Ekkor M hosszuságát K defektusának nevezzük és igy jelöljük: $d(K)$. Speciálisan, F önmagának (egyetlen) 0 defektusu részfélcsoportja, mert $F = F\langle e \rangle$. F-nek B részhalmazát prefixmentesnek nevezzük, ha egy eleme sem prefixe egyetlen más elemének sem.

Ha $K(\subseteq F)$ félcsoportnak létezik prefixmentes generátorrendszere, akkor prefixmentesen generáltnak nevezzük. Pl. F maga prefixmentesen generált: szabad generátorrendszere prefixmentes.

Megmutatjuk, hogy F bármely K részmonoidjának egyetlen minimális generátorrendszere van. Legyen K nak generátorrendszere az A halmaz. Minden n természetes számra hagyjuk el A-ból azokat az n hosszuságu szavakat, amelyek előállnak n -nél rövidebb A-beli szavak szorzataként. A megmaradó szavak alkotta A' halmaz minimális generá-

torrendszere K-nak. Legyen mostmár $K=\{B\}=\{C\}$, ahol B és C minimálisak. Jelölje B_i B i hosszuságu szavainak halmazát; megfelelően értelmezzük a C_i halmazokat. Ha igazoljuk, hogy minden i természetes számra $B_i = C_i$, készen leszünk a bizonyitással. Legyen $x \in B_1$, akkor $x \in K$, ezért szükségképpen $x \in C$, tehát $x \in C_1$; igy $B_1 \subseteq C_1$. A másik irányu tartalmazás hasonlóan igazolható. Tegyük fel, hogy minden n-nél kisebb j-re $B_j = C_j$. Legyen $p \in B_n$. Mint minimális generátorrendszer eleme, p nem áll elő nála rövidebb B-beli elemek szorzataként, de mivel ezek éppen a p-nél rövidebb C-beli elemek, p nem áll elő nála rövidebb C-beli elemek szorzataként sem. Mivel $p \in K$, p-nek szerepelnei kell C-ben, s mivel $\ell(p)=n$, C_n-ben is. Tehát $B_n \subseteq C_n$ s ugyanugy igazolható $C_n \subseteq B_n$ is. Megjegyezzük, hogy ha a K részfélcsoportnak létezik prefixmentes generátorrendszere, akkor az minimális, tehát az a minimális.

E bevezető fogalmak és összefüggések után megadhatjuk a kódolás defincióját. Kódolásnak nevezzük F egy prefixmentesen végesen generált, véges defektusu K részmonoidjának az $F(0,1)$ szabad monoidba való izomorf leképezését. K defektusát a szóban forgó kódolás defektusának nevezzük. Speciálisan F-nek $F(0,1)$-be való bármely izomorfizmusa 0 defektusu kódolás.

Szemléletesen egy n defektusu φ kódolás olyan leképezést jelent, amely a következő tulajdonsággal rendelkezik: F bármely p eleméből egy legfeljebb n hosszuságu szuffix elhagyásával olyan p' szót kaphatunk, amelyre $p'\varphi$ létezik; továbbá $p'\varphi$ p'-t egyértelmüen meghatározza.

Mivel a kódolás értelmezési tartománya F-nek végesen generált részmonoidja, azért (egyetlen) minimális generátorrendszere véges. Álljon ez a $p_1,\dots,p_k$ szavakból; akkor ezeket a szavakat az adott kódolás blokkjainak, a $p_1\varphi,\dots,p_k\varphi (\in F(0,1))$ szavakat pedig megfelelően e blokkok kódjainak nevezzük. Ha tehát a φ kódolás értelmezési tartománya a K monoid, K minden eleme előáll - mégpedig a blokkok halmazának prefixmentessége miatt egyetlen módon - blokkok szorzataként (K tehát F-nek mindig szabad részmonoidja). Mivel φ izomorfizmus, a szorzással felcserélhető, s igy K bármely q elemének $q\varphi$ képe nem más, mint a q blokk-szorzatként való előállításában szereplő blokkok kódjainak (azaz φ melletti képeinek) szorzata. Magát $q\varphi$-t szokás q kódjának nevezni, ami összhangban van a kód előbbi értelmezésével.

Tétel: Szavak egy $B(\subseteq F)$ halmaza akkor és csak akkor alkotja egy kódolás összes blokkjainak halmazát, ha B $\langle e\rangle$-től különböző véges maximális prefixmentes halmaz.

A tételt ugy is megfogalmazhatjuk, hogy prefixmentesen végesen generált, véges defektusu monoidok minimális generátorrendszerei éppen az $\langle e\rangle$-től különböző véges maximális prefixmentes halmazok.

Bizonyitás: Tegyük fel először, hogy B egy K értelmezési tartományu φ kódolás blokkjainak halmaza. Ekkor B prefixmentes, továbbá lehetetlen $B=\langle e\rangle$, mert ekkor $K=\langle e\rangle$ is igaz lenne, márpedig $\langle e\rangle$ nem véges defektusu félcsoport. Elég tehát azt bizonyitanunk, hogy B bármely további szó hozzávételével elveszíti prefixmentességét. Legyen $r\ (\notin B)$ tetszőleges e-től különböző, F-beli szó. Legyen továbbá a φ kódolás defektusa d. Tekintsük az rs szót, ahol $s(\in F)$ tetszőleges d hosszuságu szó. Akkor $\ell(rs)>d$, $\ell(r)=\ell(rs)-d$, ezért az előbbi meggondoláshoz hasonlóan rs-nek van olyan legalább $\ell(r)$ hosszuságu - tehát r-t prefixként tartalmazó - t prefixe, amelyre $t \in K$. Legyen $t=q_1\cdots q_j$, ahol $q_1,\dots,q_j \in B$. Ha most $\ell(q_1)<\ell(q_1)$, akkor q_1 prefixe r-nek, ha pedig $\ell(r)<\ell(q_1)$, akkor r prefixe q_1-nek ($\ell(q_1)=\ell(r)$ lehetetlen, mivel ebből következne $q_1=r$, ellentmondásban az $r\notin B$ feltevéssel). Mindkét esetben a $B\cup\langle r\rangle$ halmaz nem prefixmentes.

Forditva, tegyük fel, hogy B $\langle e\rangle$-től különböző véges maximális prefixmentes halmaz F-ben, és legyen $K=\{B\}$. Ekkor K prefixmentesen generált; emellett B a K részfélcsoportnak (prefixmentes, tehát) minimális generátorrendszere. Elég tehát azt bizonyitanunk, hogy K véges defektusu. Jelölje M a B-beli szavak összes prefixeinek halmazát. Mivel B véges, M is véges. Megmutatjuk, hogy $F=KM$. Legyen p tetszőleges eleme F-nek; $\ell(p)$ szerinti indukcióval megmutatjuk, hogy $p \in KM$. Ha $p=e$, $p \in KM$. Tegyük fel, hogy $\ell(p)\geq 1$. Mivel B maximális prefixmentes halmaz, van olyan $q \in B\ (q\neq e)$, hogy p valódi prefixe q-nak, vagy q prefixe p-nek. Az első esetben $p=ep$ és $e \in K$, $p \in M$, tehát $p \in KM$. A második esetben legyen $p=qp'$. Itt $\ell(p')<\ell(p)$ ezért feltehetjük, hogy $p'=st$ $(s \in K,\ t \in M)$. Nyerjük, hogy $p=(qs)t \in KM$. A bizonyitás kész.

A látottak szerint bármely kódolás megadható a következő módon: veszünk F-ben egy $\langle e\rangle$-től különböző maximális prefixmentes $\langle p_1,\dots,p_n\rangle$ halmazt (a kódolás blokkjainak halmazát), s e halmaz minden egyes p_i eleméhez hozzárendelünk egy $q_i \in F(0,1)$ szót (azaz minden blokkhoz hozzárendeljük a kódját). Ezután tehát a kódolásokat a következő alakban fogjuk felirni:

$$(1)\qquad \frac{p_1 \to q_1}{\cdots\cdots\cdots}\qquad p_n \to q_n$$

Természetesen a $q_1, \dots, q_n$ szavak nem akármilyen választása mellett kapunk kódolást; pl. e szavak között nem lehetnek egyenlők, mert ez ellentmondana a kódolás kölcsönösen egyértelmű voltának. Ahhoz, hogy (1) kódolást határozzon meg, szükséges és elegendő, hogy bármely, a $q_1, \dots, q_n$ szavakból véges számú szorzással előálló szó egyetlen ilyen szorzatelőállítással rendelkezzék, tehát, hogy $\{q_1, \dots, q_n\}$ $F(0,1)$-nek szabad részmonoidja legyen a $q_1, \dots, q_n$ szabad generátorrendszerrel. Speciálisan, elegendő az is, hogy $\langle q_1, \dots, q_n \rangle$ prefixmentes halmaz legyen; ugyanis, nyilvánvaló, hogy ebből következik az általa generált részmonoidbeli szavak szorzatelőállításának egyértelműsége.

Ha (1) jobb oldalán prefixmentes $\langle q_1, \dots, q_n \rangle$ halmaz áll, akkor az (1) által megadott kódolást prefixmentes kódolásnak nevezzük. Prefixmentes a kódolás, ha a blokkok kódjai mind egyenlő hosszúságuak. Ilyenkor egyenletes kódolásról beszélünk. Ugyancsak prefixmentes a kódolás, ha létezik olyan $v \in F(0,1)$ $(\ell(v) > 0)$, amely minden blokk kódjának szuffixe, de egyetlen blokk kódja sem $u_1 v u_2$ $(u_1, u_2 \in F(0,1),\ \ell(u_2) > 0)$ alaku, vagyis a közös szuffix egyetlen blokk kódjának belsejében, vagy elején sem fordul elő. Az ilyen kódolást vesszős kódolásnak nevezzük, mivel tetszőleges szó kódjában v jelzi - elválasztó "vessző" gyanánt - az egyes blokkok kódjainak végét.

Mivel egy kódolás definiciója szerint kölcsönösen egyértelmű leképezés, létezik az inverz leképezése. Ezt az adott kódoláshoz tartozó dekódolásnak nevezzük. A dekódolás, mint izomorfizmus inverze, maga is izomorfizmus, ezért pl. az (1) megfeleltetéssel megadott φ kódolás esetén a $(q_i \dots q_k)\varphi^{-1} = (q_i\varphi^{-1}) \dots (q_k\varphi^{-1}) = p_i \dots p_k$ összefüggés mutatja a dekódolás elvégzésének szabályát.

Példák

1. A latin betűknek feleltessük meg kölcsönösen egyértelmű módon $F(0,1)$ egy-egy 5 hosszuságu szavát. Ez egyenletes kódolás, amely az előző fejezet első példájában szereplő szabad félcsoportnak $F(0,1)$ -be való izomorfizmusa.

2. A
$$\begin{aligned} 00 &\to 0 \\ 01 &\to 10 \\ 10 &\to 110 \\ 11 &\to 111 \end{aligned}$$

megfeleltetés $F(0,1)$ -nek önmagába való prefixmentes kódolását határozza meg.

3. $F(0,1)$-nek $\{00, 01, 10, 11\}$ 1 defektusu részfélcsoportja, mig $F(0)$ nem véges defektusu részfélcsoportja. $\langle 0, 10, 11 \rangle$ maximális prefixmentes részhalmaz $F(0,1)$ -ben.

Gyakorlatok

1. Az $F(0,1)$ szabad félcsoport bármely n természetes számra tartalmaz n elemü szabad generátorrendszerrel rendelkező szabad részfélcsoportot.

2. Az $F(0,1)$ szabad félcsoportnak van olyan véges defektusu részfélcsoportja, amelynek

   a) nincs véges generátorrendszere,
   b) van véges generátorrendszere, de nincs prefixmentes generátorrendszere.

3. Az ismert Morse-jelrendszer nem kódolás a most bevezetett értelemben. Általánositsuk a kódolás fogalmát: definiciójában az $F(0,1)$ szabad félcsoportot helyettesitsük tetszőleges végesen generált szabad félcsoporttal. Ebben az általáhosabb értelemben az a megfeleltetés, mely minden latin betünek a (végén szünettel kiegészitett) Morse-jelét feleltetti meg, vesszős kódolásnak bizonyul, amelynek értékkészlete az F(ti, tá, szünet) szabad félcsoportnak részhalmaza.

4. Tekintsünk egy olyan φ kódolást, melynek értelmezési tartománya $F(0,1)$ -nek részhalmaza. Kódolás-e mindig a φ^{-1} dekódolás?

5. Az
$$\begin{aligned} 1 &\to 1 \\ 00 &\to 00 \\ 01 &\to 10 \end{aligned}$$
megfeleltetés (nem prefixmentes) kódolást határoz meg.

17. Optimális kódolás

Tekintsünk egy jelforrást, amely az $x_1, \dots, x_m$ jeleket képes kibocsátani ugy, hogy az x_i jelet (bármely jelkibocsátás alkalmával) $P(x_i)$ $(0 \le P(x_i) \le 1)$ valószinüséggel adja ki. Jelölje a $(P(x_1), \dots, P(x_n))$ sorozatot P. Ekkor annak valószinüsége, hogy jelforrásunk, miközben egymásután ℓ számu jelet bocsát ki, éppen az ℓ hosszuságu $p_i \in F(x_1, \dots, x_m)$ szót adja ki, egyenlő $(P(x_1))^{k_1} \dots (P(x_m))^{k_m}$ -mel, ahol k_i $(i = 1, \dots, m)$ a p_j szóban előforduló x_i jelek száma. Jelölje ezt a valószinüséget $P(p_j)$.

Legyen most φ tetszőleges kódolás, mely a

$$(1) \qquad \begin{matrix} p_1 \to q_{r_1} \\ \hline p_n \to q_{r_n} \end{matrix}$$

megfeleltetés által van megadva ($p_1, \dots, p_n \in F$; lehetséges pl. $\langle p_1, \dots, p_n \rangle = \langle x_1, \dots, x_m \rangle$). Elemi valószinüségszámitási meggondolásokkal megmutatható, hogy ha jelforrásunk a $p (\in F)$ kódolható szót bocsájtja ki, akkor az $\ell(p\varphi) / \ell(p)$ hányados (azaz p -nek a φ kódoláskor bekövetkező "rövidülése") várható értéke

$$\sum_{i=1}^{n} \ell(q_i) P(p_i) \Big/ \sum_{j=1}^{n} \ell(p_j) P(p_j) \ .$$

Ezért az utóbbi hányadost a φ kódolás gazdaságossági együtthatójának nevezzük, és $e_\varphi(P)$ -vel jelöljük. A gazdaságossági együttható tehát a lehetséges P sorozatok (másképpen: eloszlások) halmazán értelmezett nemnegativ értékü valós függvény. (Az elnevezést az indokolja, hogy amennyiben F -beli szavakat valamilyen berendezés segitségével tárolni, vagy továbbitani akarunk, s az egy betüre eső ezzel kapcsolatos költséget állandónak tekintjük, akkor a $p\varphi$ -re eső költség a p -re eső költségnek átlagosan $e_\varphi(P)$ -szerese; a kódolt szavak tárolása vagy továbbitása tehát annál gazdaságosabb, minél kisebb $e_\varphi(P)$.)

Tekintsünk tetszőleges kódolást a $p_1, \dots, p_n$ $(\in F)$ blokkokkal. Megmutatjuk, hogy ha e blokkok kódjainak célszerü megválasztásával arra törekszünk, hogy kódolásunk gazdaságossági együtthatója minél kisebb legyen, elegendő prefixmentes kód-halmazokra szoritkoznunk.

Tétel: Bármely olyan φ kódoláshoz, melynek blokkjai $p_1, \dots, p_n$ létezik olyan Ψ prefixmentes kódolás, ugyanezekkel a blokkokkal, hogy $e_\Psi = e_\varphi$ (azaz $e_\Psi(P) = e_\varphi(P)$ minden lehetséges P -re).

Bizonyitás: Legyen φ az (1) megfeleltetéssel megadva. A gazdaságossági együttható definiciójából látszik, hogy elegendő olyan $\langle r_1, \dots, r_n \rangle \subseteq F(0,1)$ prefixmentes szóhalmazt találnunk, hogy $\ell(r_1) = \ell(q_{r_1}), \dots, \ell(r_n) = \ell(q_{r_n})$ legyen, ekkor ugyanis a

$$\begin{matrix} p_1 \to r_1 \\ \hline p_n \to r_n \end{matrix}$$

megfeleltetés által meghatározott Ψ kódolásra teljesül $e_\Psi = e_\varphi$.

Előkészületül bebizonyitjuk az un. Szilárd-Kraft-egyenlőtlenséget: Ha $\{q_1, \dots, q_n\}$ $F(0,1)$ -nek szabad részmonoidja a $q_1, \dots, q_n$ szabad generátorrendszerrel, akkor

$$(2) \qquad \sum_{i=1}^{n} \frac{1}{2^{\ell(q_i)}} \le 1 \ .$$

Legyen r tetszőleges természetes szám és jelölje $s_1, \dots, s_{n^r}$ a $q_1, \dots, q_n$ szavakból képezhető összes r -tényezős szorzatokat. Mivel $\{q_1, \dots, q_n\}$ szabad, ezek mind különböző szavak. Legyen s_k szorzatelőállitása $q_{k_1} \cdots q_{k_r}$. Érvényes

$$\sum_{k=1}^{n^r} \frac{1}{2^{\ell(s_k)}} = \sum_{k=1}^{n^r} \frac{1}{2^{\ell(q_{k_1} \cdots q_{k_r})}} = \sum_{k=1}^{n^r} \frac{1}{2^{\ell(q_{k_1})}} \cdots \frac{1}{2^{\ell(q_{k_r})}} = \left(\sum_{i=1}^{n} \frac{1}{2^{\ell(q_i)}} \right)^r .$$

Ha $\max_{1 \le i \le n} \ell(q_i) = M$, akkor $\max_{1 \le k \le n^r} \ell(s_k) = rM$ és $\min_{1 \le k \le n^r} \ell(s_k) \ge r$. Legyen továbbá a $s_1, \dots, s_{n^r}$ szavak közül az ℓ hosszuságuak száma t_ℓ. Minden ℓ -re $(r \le \ell \le rM)$ érvényes $t_\ell \le 2^\ell$, ezért

$$\sum_{k=1}^{n^r} \frac{1}{2^{\ell(s_k)}} = \sum_{\ell=r}^{rM} \frac{t_\ell}{2^\ell} \le \sum_{\ell=r}^{rM} \frac{2^\ell}{2^\ell} \le \sum_{\ell=1}^{rM} 1 = rM \ .$$

Összevetve ezt az előző egyenlőséggel, nyerjük:

$$\left(\sum_{i=1}^{n} \frac{1}{2^{\ell(q_i)}}\right)^r \leq r M .$$

Ha $\sum_{i=1}^{n} \frac{1}{2^{\ell(q_i)}} > 1$ lenne, ez az egyenlőtlenség nem teljesülhetne minden r természetes számra. Ezért a bizonyitandó egyenlőtlenség valóban igaz.

Mivel az (1) kódolásban szereplő $q_{i_1}, \ldots, q_{i_n}$ szavak F-nak szabad részfélcsoportját generálják, teljesül rájuk és minden részhalmazukra (2). Az általánosság megszoritása nélkül feltehetjük, hogy $\ell(q_{i_1}) \leq \ldots \leq \ell(q_{i_n})$. Legyen $k = 1, \ldots, n$-re r_k a $\sum_{i=1}^{k-1} \frac{1}{2^{\ell(q_i)}}$ összeg kettes számrendszerbeli felirásában a vessző ("kettedes-vessző") utáni első $\ell(q_{i_k})$ számu számjegyből álló szó, (ha a felirásban nincs ennyi számjegy, akkor zérusokkal egészitjük ki). Megmutatjuk, hogy az $\langle r_{i_1}, \ldots, r_{i_n} \rangle$ halmaz prefixmentes. Ez elegendő is a bizonyitáshoz, hiszen definició szerint $\ell(r_k) = \ell(q_{i_k})$ $(k = 1, \ldots, n)$.

A Szilárd-Kraft-egyenlőtlenség szerint $k = 1, \ldots, n$ -re $\sum_{i=1}^{k-1} \frac{1}{2^{\ell(q_i)}}$ egynél kisebb nemnegativ szám. Ezek a számok k növekedésével ugyancsak növekednek. Ha $j < k$ -ra r_j prefixe r_k -nak, akkor $\sum_{i=1}^{j-1} \frac{1}{2^{\ell(q_i)}}$ és $\sum_{i=1}^{k-1} \frac{1}{2^{\ell(q_i)}}$ vessző utáni első $\ell(q_{i_j})$ számu számjegye megegyezik, igy különbségük kisebb, mint $1/2^{\ell(q_{i_j})}$ (itt használjuk fel, hogy mindkét összeg kisebb egynél). Ez azonban lehetetlen, mert a második összeg ugy keletkezik az elsőből, hogy $1/2^{\ell(q_{i_j})} + \ldots + 1/2^{\ell(q_{k-1})}$-et (amelynek $j < k$ miatt legalább egy tagja van) hozzáadjuk. A bizonyitás kész.

Tekintsük az F végesen generált szabad félcsoport egy $\langle p_1, \ldots, p_n \rangle$ maximális prefixmentes részhalmazát, valamint az F szabad generátoraihoz rendelt valószinüségek P rendszerét. Az (1) megfeleltetéssel megadott olyan φ kódolást, melyre $e_\varphi(P)$ nem nagyobb, mint a $p_1, \ldots, p_n$ blokkokkal rendelkező bármely Ψ kódolás $e_\Psi(P)$ gazdaságossági együtthatója, optimális kódolásnak (pontosabban: $\langle p_1, \ldots, p_n \rangle$ -re és P -re

vonatkozóan optimális kódolásnak) nevezzük. Az optimális kódolás megtalálásának feladata tehát alkalmas $q_{i_1}, \ldots, q_{i_n}$ $(\in F(0,1))$ kódszavak meghatározását jelenti.

A továbbiakban az általánosság korlátozása nélkül feltesszük, hogy $P(p_1) \geq \ldots \geq P(p_n)$. A következő tétel megmutatja, milyen tulajdonságokkal rendelkezik egy optimális kódolás kódjainak halmaza. Megjegyezzük, hogy az optimális kódolás nem egyértelmüen meghatározott: ha (1) optimális kódolást ad meg és $\ell(r_i) = \ell(q_{i_i})$ $(r_i \in F(0,1);\ i = 1, \ldots, n)$, akkor a gazdaságossági együttható definiciójából látjuk, hogy a

$$\frac{p_1 \to r_1}{p_n \to r_n}$$

megfeleltetés ugyancsak optimális kódolást ad meg. Megjegyezzük továbbá, hogy az előző tétel alapján optimális kódolás keresésénél elegendő a prefixmentes kódolásokat figyelembe venni.

Huffman tétele: Ha $n \geq 2$ és az (1) megfeleltetés prefixmentes optimális φ kódolást ad meg, akkor

a) $\ell(q_{i_1}) \leq \ldots \leq \ell(q_{i_{n-1}}) = \ell(q_{i_n})$,

b) vannak olyan maximális hosszuságu kódszavak, amelyek csak utolsó betüjükben különböznek,

c) $\langle q_{i_1}, \ldots, q_{i_n} \rangle$ maximális prefixmentes halmaz.

Bizonyitás: a) Bármely $a \leq b$, $c \leq d$ valós számokra $ac + bd \geq bc + ad$. Ezért a gazdaságossági együttható számlálója - amennyiben a kódok hosszának rendszere rögzitett - akkor minimális, ha $\ell(q_{i_1}) \leq \ldots \leq \ell(q_{i_{n-1}}) \leq \ell(q_{i_n})$. A nevezője viszont nem függ a kódok megválasztásától.

Ha továbbá $\ell(q_{i_{n-1}}) < \ell(q_{i_n})$, akkor q_{i_n} -t helyettesitve saját $\ell(q_{i_{n-1}})$ hosszuságu prefixével, a kódok igy módositott halmaza továbbra is prefixmentes; a gazdaságossági együttható viszont csökken, ellentétben φ optimális voltával. Ezért

$$\ell(q_{i_{n-1}}) = \ell(q_{i_n}) .$$

b) Jelölje q'_{i_i} azt a szót, amely q_{i_i} -ből utolsó betüje elhagyásával keletkezik. Mivel az utolsó betü csak 0 vagy 1 lehet, elegendő belátnunk, hogy ha a maximális hosszuságu kódszavak $q_{i_j}, \ldots, q_{i_n}$, akkor a $q'_{i_j}, \ldots, q'_{i_n}$ szavak nem mind különbözők. Ez valóban igy van; ellenkező

esetben ugyanis a $q_{j_1},\dots,q_{j_n}$ kódszavakat helyettesithetnénk a $q'_{j_1},\dots,q'_{j_n}$ szavakkal, s a kódok igy módositott halmaza továbbra is prefixmentes maradna; a gazdaságossági együttható viszont csökkenne, ellentében φ optimális voltával.

c) Legyen $q_{n+1} \in F(0,1)$ minimális hosszuságu olyan szó, hogy $\langle q_1,\dots,q_n,q_{n+1}\rangle$ prefixmentes halmaz. Ekkor $\ell(q_{n+1}) \leq \ell(q_n)$. Ha ez nem teljesülne, akkor $\langle q_1,\dots,q_n,q'_{n+1}\rangle$ is prefixmentes lenne, ellentétben q_{n+1} minimális választásával. Az is nyilvánvaló, hogy $\ell(q_{n+1}) = \ell(q_n)$. Ugyanis az $\ell(q_{n+1}) < \ell(q_n)$ esetben q_n-et helyettesithetnénk q_{n+1}-gyel, és igy javithatnánk a kód gazdaságosságát. Továbbá, q'_{n+1} prefixe valamelyik q_i-nek. (Ellenkező esetben szintén javithatnánk a kód gazdaságosságát azáltal, hogy q_n-et kicseréljük q'_{n+1}-re.) Ekkor $\ell(q_i) = \ell(q_n)$, különben q_i prefixe lenne q_{n+1}-nek. Az is világos, hogy q_{n+1} egyetlen más q_j-nek sem prefixe, mert q'_{n+1} egyetlen betü hozzáadásával csak kétféleképpen folytatható; ez a két folytatás q_{n+1} és q_i. Tehát, ha q_i-t kicseréljük q'_{n+1}-re, a kód gazdaságossága javul, ez pedig ellentmondás.

A bizonyitás kész.

Huffman tétele lehetőséget nyujt optimális kódolás gyakorlati megkeresésére. Az $n=2$ esetben a

$$p_1 \to 0$$
$$p_2 \to 1$$

megfeleltetéssel megadott kódolás nyilvánvalóan mindig optimális. Tegyük fel, hogy $n-1$ számu blokkhoz és valószinüségeik bármely sorozatához már meg tudunk adni egy optimális kódolást. Tekintsük most a $p_1,\dots,p_n \in F$ blokkokat és valószinüségeik $P = (P(p_1),\dots,P(p_n))$ sorozatát (feltehetjük, hogy $P(p_1) \geq \dots \geq P(p_n)$). Meg fogunk adni olyan $q_1,\dots,q_n \in F(0,1)$ szavakat, amelyekre az (1) megfeleltetés által meghatározott kódolás optimális.

Tartozzanak az $x_1,\dots,x_{n-2},x_{n-1} (\in F(x_1,\dots,x_{n-1}))$

blokkokhoz rendre a $P(p_1),\dots,P(p_{n-2}),\ P(p_{n-1})+P(p_n)$ valószinüségek; utóbbiak sorozatát jelölje P'. Ha

$$\begin{array}{l} x_1 \to q_1 \\ \hline \\ x_{n-1} \to q_{n-1} \end{array}$$

$\langle x_1,\dots,x_{n-1}\rangle$ -re és P'-re vonatkozóan egy φ' prefixmentes optimális kódolást ad meg, akkor

$$\begin{array}{l} p_1 \to q_1 \\ \hline \\ p_{n-2} \to q_{n-2} \\ p_{n-1} \to q_{n-1}0 \\ p_n \to q_{n-1}1 \end{array}$$

$\langle p_1,\dots,p_n\rangle$ -re és P-re vonatkozóan ugyancsak egy prefixmentes optimális φ kódolást határoz meg. Tegyük fel ugyanis, hogy $p_1,\dots,p_n$-hez rendre az $r_1,\dots,r_n$ kódokat rendelve prefixmentes optimális Ψ kódolást kapnánk, melyre $e_\Psi(P) < e_\varphi(P)$. Huffman tétele szerint ekkor $\ell(r_{n-1}) = \ell(r_n)$ és r_{n-1} r_n-től csak utolsó betüjében különbözik. Legyen $r_{n-1} = r'_n 0$ és $r_n = r'_n 1$. Tekintsük azt a Ψ' kódolást, melyet az

$$\begin{array}{l} x_1 \to r_1 \\ \hline \\ x_{n-2} \to r_{n-2} \\ x_{n-1} \to r'_n \end{array}$$

megfeleltetés határoz meg. Itt a kódok $\langle r_1,\dots,r_{n-2},r'_n\rangle$ halmaza prefixmentes; másrészt a gazdaságossági együtthatókat kiszámitva nyerjük, hogy

(3) $$e_\varphi(P) - e_\Psi(P) \leq e'_\varphi(P') - e_{\Psi'}(P'),$$

ahonnan $e_{\Psi'}(P') < e_{\varphi'}(P')$, ellentmondásban φ' optimális voltával.

(A (3) egyenlőséget igy bizonyithatjuk:

Vezessük be a $\sum_{i=1}^{n} \ell(p_i) P(p_i) = a$, $\sum_{i=1}^{n} P(p_i) = b$, $\sum_{i=1}^{n-1} \ell(q_i) P(p_i) +$

$+ \ell(q_{n-1}) P(p_n) = c$, $\sum_{i=1}^{n} \ell(r_i) P(p_i) = d$, $P(p_{n-1}) + P(p_n) = e$

jelöléseket. Akkor $a,b,c,d,e > 0$, továbbá $e_\varphi(P) = \frac{c+e}{a}$, $e_\Psi(P) = \frac{d}{a}$,

$e_{\varphi'}(P') = \frac{c}{b}$; $e_{\Psi'}(P') = \frac{d-e}{b}$. Az $e_\Psi(P) < e_\varphi(P)$ feltevés miatt $d < c+e$, másrészt definiciójuk szerint $b \leq a$. Ezért

$$e_\varphi(P) - e_\Psi(P) = \frac{c+e-d}{a} \leq \frac{c-(d-e)}{b} = e_{\varphi'}(P') - e_{\Psi'}(P') ,$$

Példák

1. Az előző fejezet 2. példájában szereplő φ kódolás gazdaságossági együtthatója $P = (P(0) = 0,9, \quad P(1) = 0,1)$ esetén

$$e_\varphi(P) = \frac{1 \cdot 0,81 + 2 \cdot 0,09 + 3 \cdot 0,09 + 3 \cdot 0,01}{2} = 0,645 .$$

2. Az előző fejezet 5. gyakorlatában szereplő kódolás gazdaságossági együtthatója tetszőleges P esetén 1.

3. Az $F(x_1, x_2, x_3)$ szabad félcsoport x_1, x_2, x_3 blokkokkal rendelkező kódolása $P = (0,7;\ 0,21;\ 0,09)$ esetén optimális, ha a kódok megfelelően: $0, 10, 11$.

4. Az $F(0,1)$ szabad félcsoport $1, 00, 01$ blokkokkal rendelkező kódolása $P = (0,3;\ 0,7)$ esetén optimális, ha a kódok ugyanazok, mint a 3. példában. Ugyancsak optimális (de nem prefixmentes) az előző fejezet 5. gyakorlatában szereplő kódolás.

Gyakorlatok

1. Általánositsuk a Szilárd-Kraft - egyenlőtlenséget végesen generált szabad félcsoportokra!

2. Tekintsük $F(0,1)$ -nek azon kódolásait, melyeknél a blokkokat az összes 3 hosszuságu szavak alkotják. Határozzuk meg az optimális

kódolást $P(0)$ minden $0,5$ és 1 közti értékére ($P(1) = 1 - P(0)$) és számitsuk ki az optimális kódolás gazdaságossági együtthatóját!

3. $F(0,1)$ részfélcsoportján értelmezett optimális kódoláshoz tartozó dekódolás is kódolás. Milyen összefüggés van gazdaságossági együtthatóik között?