Eötvös Lóránd Tudományegyetem
Természettudományi Kar, Matematikai Intézet

Csizmadia Gábor Béla
Matematika BSc
Matematikus szakirány

Csoportszavak és rövidítéseik

Szakdolgozat

Témavezető: Sziklai Péter, egyetemi docens
Számítógéptudományi Tanszék

Budapest, 2016

Tartalomjegyzék

Bevezetés

Jelen dolgozatomban áttekintést kívánok nyújtani a monoidok és csoportok szavainak néhány fontos algebrai és kombinatorikai tulajdonságáról, valamint a csoportok szavai közötti különböző rövidítésfogalmak bevezetését követően, célom ezek alapvető tulajdonságainak feltárása, és rájuk vonatkozólag több hasznos vagy érdekes állítás kimondása és bizonyítása.

Bizonyos helyeken lazán követni fogom a [1], [19], [12] könyvek egyes részeit, azonban mind a definíciók, mind a tételkimondások némileg eltérhetnek az ezekben szereplőktől, igyekezetem szerint ezek a különbségek azonban nem öncélúak, hanem arra voltam tekintettel, hogy ezek a lehető legjobban illeszkedjenek a dolgozat szerkezetébe.

A bizonyítások a legtöbb esetben saját ötlet alapján történnek, azt a néhány esetet, amikor valamelyik hivatkozott szakirodalomból származik a bizonyítás, külön jeleztem (ezeknél ugyanis többnyire létezik egy általánosan használt, sztenderd gondolatmenet, mint pl. az André-féle tükrözési elv a Ballot-számok meghatározására).

A 1. fejezet áttekinti a legfontosabb felhasznált algebrai alapfogalmakat, továbbá itt kerül bevezetésre a szó, monoidszó és csoportszó fogalma is. Megjegyzem, hogy már ez a fejezet is tartalmaz néhány újdonságot, felépítésében, szemléletében némileg eltér a hivatkozott szakirodalomtól. Többek közt bevezetésre kerül a *normális részmonoid* fogalma, mely a csoportok normálosztó-fogalmának egy analogonja, és ezen előbbi (egyik) természetes általánosításának bizonyul[1]. Megvizsgálom a normális részmonoidok alapvető tulajdonságait, és szabad monoidokra értelmezem a normális részmonoid szerinti hányadosmonoid fogalmát, majd ezeket felhasználom a szabad csoportok, valamint a monoidok prezentációinak a bevezetésénél is (ez által újfajta, a korábbiakkal természetesen ekvivalens definíciókat adva ezekre).

A 2. fejezetben a monoid- és csoportszavakkal kapcsolatos néhány kérdéskört vizsgálok meg. Ezen kérdések alapvetően három, logikailag egy-egy egységet alkotó csoportba sorolhatók: a 2.1. alfejezetben részmonoidok és részcsoportok szavaira kerülnek kimondásra hasznos és alapvető állítások, a 2.2. alfejezetben a csoportszavak körében többféle ún. rövidítésfogalmat vezetek be, és ezekkel kapcsolatban olyan jellegű problémák vizsgálatára kerül sor, mint pl., hogy mikor létezhet az adott típusú rövidítésre vonatkozóan minden szónak egyértelmű rövidített alakja. Végül a 2.3. alfejezetben szó*halmazokra* vonatkozó rövidítési feltételek és ezek néhány egyszerű következményei szerepelnek. Ezen alfejezet erősen felhasználja a [12] I. és V. fejezeit.

[1] Ld. pl. az 1.1.1. állítás 6. pontját.

A 3. fejezet jellegében némileg elüt az előző erősen algebrai színezetű 1. és 2. fejezetektől, és rácsutakkal, Catalan-számokkal valamint az ún. Ballot-számokkal, és ezek kombinatorikai tulajdonságaival foglalkozik, melyek alapozásként szolgálnak a következő, 4. fejezethez. Különbség a többi fejezethez képest még, hogy az itt szereplő definíciók és állítások lényegében mind megtalálhatók a hivatkozott szakirodalom valamelyikében[2] is.

A 4. fejezet lényegében egy, a szórövidítésekkel kapcsolatos, leginkább a leszámláló kombinatorika és a kombinatorikus csoportelmélet témaköreibe sorolható feladat megoldásáról szól: a csoportszó Dyck-útja fogalmának bevezetésével kiszámolásra kerül, hogy szabad csoportban hányféleképpen lehetséges, hogy egy n hosszú szó (szabadon) rövidített alakja k hosszú valamilyen n és k természetes számokra. Ezzel ekvivalens kérdés az, hogy a szabad csoport Cayley-gráfjában mennyi a valószínűsége, hogy a 1-nek megfelelő kezdőpontból n lépéses bolyongás után az 1-től k távolságra kerülünk. Feltehető ugyanez a kérdés más csoportok, illetve monoidok esetében is, és bizonyos esetekben hasonló módon meg is válaszolható, ezekre azonban terjedelmi okok miatt csak utalás szintjén tudok kitérni. Megjegyzem, hogy ennek a problémának a megoldása szabad csoportokra és $k = 0$ esetre, lényegében hasonló módszerrel, csak másféle rácsutakkal, és kevésbé részletesen megtalálható a [9] cikk 348. oldalán is.

Történetileg a csoport- és monoidszavak, valamint kombinatorikai tulajdonságaik vizsgálata a XX. század első felében (és részben már a XIX. század végén), többek között Thue, Dyck, Nielsen, Dehn és még sokan mások munkássága nyomán alakult ki[3]. A terület egyik első klasszikus összefoglaló műve, amelyet egyébként szakirodalomként jelen dolgozathoz is felhasználtam, Magnuss, Karrass és Solitar 'Combinatorial Group Theory' (ld. [19]) című könyve volt. Ezen vizsgálatok az algebrai és kombinatorikai eszköztár mellett viszonylag hamar az algebrai topológia területére vezettek, elsősorban Dehnnek köszönhetően, az ebbe való betekintés azonban már sajnos túlmutatna a szakdolgozat (terjedelmi) keretein.

Megjegyzem, hogy az itt ismertetett állításokon túlmenően néhány további saját eredmény is van ebben a témakörben, melyek közé tartoznak egyrészt a 4.2.6. tétel általánosításai néhány más monoid és csoport szavaira, másrészt csoportok normálosztóinak szavaira, csoportszavak általánosan rövidített alakjának egyértelműségére és ezeknek a kis kiejtési feltételekkel való kapcsolatára vonatkozó további állítások, melyek már szintén nem fértek bele jelen dolgozatba. További céljaim közé tartozik ezen eredmények továbbvitele.

[2] Elsősorban: [14], [15], [7], [2] [13] és [8]

[3] Részletesebben ld. még pl. a [16], [18], [17] weboldalakon vagy a [12] előszavában.

Köszönetnyilvánítás

Köszönetet szeretnék mondani Sziklai Péternek a témavezetés elvállalásáért, Homa Gábornak, aki a 4.2.6. tétel kérdését feltette, majd a kapott eredményemet ellenőrizte, továbbá a családomnak türelmükért és támogatásukért.

Jelölések

A következő jelöléseket fogjuk használni:

$\lfloor x \rfloor,\ \lceil x \rceil$	-	az $x \in \mathbb{R}$ szám alsó és felső egészrésze
$\mathbb{N}$	:=	$\{0, 1, 2, \dots\}$ - természetes (nemnegatív egész) számok halmaza
$\mathbb{N}^+$	:=	$\{1, 2, \dots\} = \mathbb{N} \setminus \{0\}$ - pozitív egész számok halmaza
$\mathbb{N}_n$	:=	$\{k \in \mathbb{N} \mid 1 \leq k \leq n\}$
$\mathbb{Z}^d$	-	d-dimenziós egész vektorok halmaza ($d \in \mathbb{N}$)
id_X	-	identitás-függvény[4]
1_G	-	csoport (monoid) egységeleme[4]
$G \cong H$	-	izomorf csoportok (félcsoportok, monoidok)
$\mathrm{Ker}(\phi),\ \mathrm{Im}(\phi)$	-	homomorfizmus magja és képe
$G \leq H$	-	részcsoport (rész-félcsoport, részmonoid)
$G \trianglelefteq H$	-	normálosztó (normális részcsoport), normális részmonoid[5]
$\langle A \rangle_G$	-	az A halmaz által generált részcsoport (részmonoid) G-ben[4]
$N_G(A)$	-	az A halmaz által generált normálosztó a G csoportban; az A halmaz által generált normális részmonoid a G monoidban [4,5]
$G/\sim$	-	a $\sim$ kongruencia-reláció szerinti hányadoscsoportja a G csoportnak, hányadosmonoidja a G monoidnak vagy hányadosalgebrája egyéb algebrai struktúrának[6,7]
G/H	-	normálosztó szerinti hányadoscsoport; normális részmonoid szerinti hányadosmonoid[5,7,8]
$F_A^{(M)},\ F_A = \langle A \rangle$	-	az A halmaz által generált szabad monoid ill. szabad csoport[9]
$\langle S \mid R \rangle_M,\ \langle S \mid R \rangle$	-	monoid ill. csoport prezentációja[10]

[4] Ha nem okoz félreértést, akkor az X-re, illetve G-re vonatkozó jelölés elhagyható.

[5] A normális részmonoid defícióját ld. 1.1.2. definíció.

[6] Ld. [1], Definition II/1.3., II/5.1., II/5.2.

[7] A hányadoscsoport, hányadosmonoid, hányadosstruktúra helyett használatos a faktorcsoport, faktormonoid, faktorstruktúra elnevezés is.

[8] A normális részmonoid szerinti hányadosmonoid definícióját ld. 1.2.4. definíció

[9] Ld. 1.1.3. definíció

[10] Ld. 1.2.5. és 1.2.6. definíciók

ε	-	az üres szó [11]
$\Sigma_0^*,\ \Sigma^*$	-	a Σ ábécé feletti szavak halmaza az üres szóval és anélkül [11]
$u \star v$	-	az u és v szavak összefűzése [11,12]
$\lvert u \rvert$	-	az u szó hossza [11]
u^n	-	az u szó n-edik hatványa [11]
$u \leq v$	-	szavak közötti részszó-reláció[13]
$u \trianglelefteq v$	-	szavak közötti konvex részszó-reláció[13]
$u(n)$	-	az u szó n-edik betűje[11]
$u^{(k)}$	-	az u szó első k betűjéből álló konvex részszava
$W(G)$	-	a G csoport adott prezentációhoz tartozó szavainak halmaza [14]
$W[G],\ W'[G]$	-	az F_S szabad csoport G részcsoportjának szavai és egyszerű szavai [15]
$\sim_G$	-	szavak G csoport szerinti ekvivalenciája [1,14]
$\leq_g,\ \leq_c,\ \leq_f$	-	csoportszavak közötti mohó, általános és szabad rövidítés [16]
$\lvert\cdot\rvert_g,\ \lvert\cdot\rvert_c,\ \lvert\cdot\rvert_f$	-	csoportszó mohón, általánosan és szabadon rövidített hossza [16]
C_n	-	az n-edik Catalan-szám [17]
$B(m,n),\ B^*(m,n)$	-	Ballot-számok [18]
$D(w),\ M(w)$	-	a w szó Dyck-útja ill. Motzkin-útja [19]

[11] Ld. 1.2.1. definíció

[12] Mivel nem fog félreértést okozni, így a 2. fejezettől kezdve a szavak összefűzését simán egymás mellé írással jelöljük.

[13] Ld. 1.2.3. definíció

[14] Ld. 1.2.8. definíció és az utána következő bekezdés

[15] Ld. 2.1.2. szakasz

[16] Ld. 2.2.1. és 2.2.2. definíciók

[17] Ld. 3.1. képlet

[18] Ld. 3.3.1. definíció

[19] Ld. 4.1.1. definíció

1. fejezet

Algebrai alapok és szavak

1.1. Félcsoportok és csoportok

A későbbiekben fel fogjuk használni a következő algebrai alapfogalmakat:

- *félcsoport*, *monoid* (egységelemes félcsoport), *csoport*;
- *egységelem*, *inverz*;
- *részfélcsoport*, *részcsoport*;
- az ezen algebrai struktúrák közötti *homomorfizmusok* és *izomorfizmusok*, *izomorf* struktúrák fogalma, homomorfizmus *magja* és *képe*;
- egy algebrai struktúra *generátorrendszere* és ennek *minimalitása*;
- egy csoportban egy nemüres halmaz által *generált részcsoport*, egy elem *konjugáltjai*, *normálosztók* (normális részcsoportok), nemüres halmaz által *generált normálosztó* és a normálosztó szerinti *hányadoscsoport*[1] fogalma;
- monoidban, csoportban (vagy egyéb algebrai struktúrában) a kongruencia-reláció és kongruencia-reláció szerinti hányadosmonoid, hányadoscsoport (általánosan: hányadosalgebra) fogalma[1,2];
- valamint ismertnek tételezzük fel ezek legfontosabb tulajdonságait is.

A fentiek közül a csoportokra vonatkozó fogalmak definíciói és ezek legfontosabb tulajdonságai megtalálhatók a [6] könyvben, a fogalmak és tulajdonságaik általános algebrai struktúrákra (így speciálisan csoportokra, félcsoportokra és monoidokra is) vonatkozó változatai pedig a [6] 8.2. és a [1] II. fejezeteiben.

[1] A hányadoscsoport, hányadosmonoid helyett használatos a faktorcsoport, faktormonoid elnevezés is.
[2] Ld. [1], Definition II/1.3., II/5.1., II/5.2.

A monoidokra vonatkozó néhány speciális definíciót és ezekre vonatkozó alapvető állításokat külön szerepeltetünk az 1.1.1., 1.1.2., 1.2.2., 1.2.3. és 1.2.4. pontokban, mivel a szakirodalomban ezek nem feltétlenül egységesen szerepelnek, és itt a szokásostól kicsit eltérő szemléletű felépítést adunk.

1.1.1. *Megjegyzés.* Homomorfizmus magjára a hivatkozott szakirodalomban kétféle definíció is használatos, csoportelméletben általában a $\phi : G \to H$ magján a $\mathrm{Ker}(\phi) = \{x \mid \phi(x) = 1_H\} \leq G$ részcsoportot értjük, míg univerzális algebrában a $\mathrm{Ker}(\phi) = \{(a, b) \in G^2 \mid \phi(a) = \phi(b)\}$ G-beli kongruencia-relációt. Ha külön nem jelezzük, akkor csoportokra és monoidokra homomorfizmus magján az előbbit fogjuk érteni.

1.1.1. Monoidok néhány tulajdonsága és normális részmonoidok

1.1.1. Definíció. Az M monoid egy H részhalmaza *részmonoidja* M-nek ($H \leq M$), ha részfélcsoportja (az M-beli műveletre nézve), és $1_M \in H$. Ha S és T két monoid, akkor a $\phi : S \to T$ leképezés *monoid-homomorfizmus*, ha félcsoport-homomorfizmus S és T között, valamint az S 1_S és a T 1_T egységelemére $\phi(1_S) = 1_T$.[3]

A normális részmonoidnak a szakirodalomban nincs egységes definíciója; egy lehetséges, néhány forrásban előforduló definíció pl. a csoportok analógiájára H M-beli részmonoidot normálisnak nevezni akkor, ha minden $x \in M$-re $Hx = xH$, ez viszont számunkra nem szerencsés, mivel azt a tulajdonságát szeretnénk a csoport normálosztójának felhasználni, hogy lehet vele faktorizálni, ezért más definíciót adunk:

1.1.2. Definíció. Azt mondjuk, hogy egy M monoid H részmonoidja *normális részmonoid* (jelben: $H \trianglelefteq M$), ha $\forall h \in H$-ra és $x, y \in M$-re:

$$xy \in H \iff xhy \in H$$

Vagyis, szemléletesen fogalmazva, H akkor normális részmonoid, ha H-beli elembe tetszőleges H-beli elemet „beszúrva”, vagy az elemből H-beli elemet „elhagyva” szintén H-beli elemet kapunk.

1.1.1. Állítás. 1. *Az M monoid egy H részmonoidja valóban monoid, és egységeleme megegyezik M-éval.* 2. *Részmonoidok metszete részmonoid.* 3. *Normális részmonoidok metszete is normális részmonoid.* 4. *Ha $a, b \in M$-re és $H \trianglelefteq M$-re $ab = 1$, akkor $a \in H \iff b \in H$ és $c \in H \implies acb \in H$, vagyis normális részmonoid zárt a tetszőleges inverzképzésre és konjugálásra.* 5. *Monoid-homomorfizmus magja normális részmonoid.* 6. *Egy csoport egy részhalmaza akkor és csak akkor normális részmonoid, ha normálosztó.* 7. *Ha az M monoid nem csoport, akkor egy H normális részmonoidjára nem feltétlenül igaz, hogy minden $x \in M$-re $Hx = xH$.*

[3]Megjegyzés: Csoportok esetében hasonló feltevésekre az egységelem (és az inverz) tekintetében nem volt szükség, ezek automatikusan következnek a szorzattartásból (vagyis, ha egy G csoport H részhalmaza csoport az eredeti művelet megszorítására nézve, akkor az egységelem és az elemek inverzei megegyeznek G-ben és H-ban; valamint egy csoport képe félcsoport-homomorfizmusnál szintén csoport).

Bizonyítás. Az 1. állítás triviális, figyelembe véve, hogy $1_M h = h 1_M = h \ \forall h \in M$-re, így speciálisan $\forall h \in H$-ra is, és egységelem egyértelmű.

A 2. állítás szintén azonnal adódik, ha figyelembe vesszük, hogy minden részmonoidban definíció szerint benne van az egységelem és két elemükkel együtt azok szorzata is.

3. Ha H_i-k normális részmonoidok M-ben, akkor mindenesetre $\bigcap H_i$ részmonoid, és ha minden i-re és minden $h \in H_i$-re $xy \in H_i \iff xhy \in H_i$, akkor tetszőleges $h \in \bigcap H_i$-re $xy \in \bigcap H_i \iff xhy \in \bigcap H_i$, így $\bigcap H_i$ valóban normális.

4. Ha $ab = 1$ és $a \in H$, akkor $1 = 1ab \in H \implies 1b = b \in H$, és hasonlóan adódik, hogy $b \in H$ esetén $a \in H$; $c \in H$ esetén pedig $1 = ab \in H \implies acb \in H$.

5. Legyenek most S és T monoidok, és $\phi : S \to T$ monoid-homomorfizmus. Mármost $xy \in \mathrm{Ker}(\phi)$ és $h \in \mathrm{Ker}(\phi)$ esetén

$$\phi(xhy) = \phi(x)\phi(h)\phi(y) = \phi(x)\phi(y) = \phi(xy) = 1_{G'} \implies xhy \in \mathrm{Ker}(\phi),$$

$xhy \in \mathrm{Ker}(\phi)$ és $h \in \mathrm{Ker}(\phi)$ esetén pedig

$$\phi(xy) = \phi(x)\phi(y) = \phi(x)\phi(h)\phi(y) = \phi(xhy) = 1_{G'} \implies xy \in \mathrm{Ker}(\phi),$$

amely bizonyítja az állítást.

6. Ha H a G csoport egy normális részmonoidja, akkor a 4. pont szerint H normálosztó, hiszen zárt az invertálásra és tetszőleges konjugálásra. Most legyen G csoportban $N \trianglelefteq G$ egy normálosztó. Tudjuk, hogy csoportban egy részhalmaz akkor és csak akkor normálosztó, ha valamely homomorfizmus magja, és két csoport között egy homomorfizmus akkor és csak akkor csoport-homomorfizmus, ha monoid-homomorfizmus, ezért az előző pontból következik, hogy N valóban normális részmonoid.

A 7-re ellenpéldát ad például az $\langle a, b \rangle_M$ szabad monoidban az $\{a\}$ által generált N normális részmonoid (a szabad monoid és ezen jelölés definícióját ld. az 1.1.3. és az 1.2.5. definíciókban), melynek, mint az 1.2.2. pontban definiciált kongruenciára vonatkozó 1.2.6. állítás 3. pontjából következni fog, az elemei a csupa a betűből álló szavak, így a bN halmaz elemeinek pontosan az első betűje b, az Nb halmaz elemeinek pedig pontosan az utolsó, tehát a kettő nem eshet egybe.

■

Az előbbi állítás második és harmadik pontja alapján beszélhetünk halmaz által *generált részmonoidról* és *generált normális részmonoidról*, amit $\langle X \rangle_M$-mel és $N_M(X)$-el (vagy simán $\langle X \rangle$-el és $N(X)$-el) jelölünk.

1.1.2. Szabad monoidok és csoportok

A szabad monoidok és a szabad csoportok definíciójára ezek ún. univerzális tulajdonságát fogjuk felhasználni. A szakirodalom egy részében ezt következményként említik, és egy ezzel ekvivalens meghatározást adnak meg, mi egy kicsit más felépítést követünk.

1.1.3. Definíció. Legyen S egy tetszőleges monoid, A egy nemüres halmaz, és legyen adott egy $\tau : A \to S$ injektív függvény (beágyazás). Ekkor azt mondjuk, hogy az A halmaz *szabadon generálja* S-t (a τ-n keresztül), ha egyrészt $\tau(A)$ generátorrendszere S-nek, másrészt tetszőleges T monoidra és $f : A \to T$ függvényre létezik egy $\phi : S \to T$ homomorfizmus, hogy $\phi \circ \tau = f$. Ha $A \subseteq S$, akkor megállapodás szerint τ-nak mindig az identikus beágyazást tekintjük. Az A által generált monoidot $F_A^{(M)}$-mel is jelöljük (ennek a jelölésnek az értelmességét illetően ld. a következő állítás 3. pontját). Azt mondjuk, hogy S monoid *szabad*, ha létezik olyan nemüres A halmaz, mely őt szabadon generálja ($S \cong F_A^{(M)}$ valamilyen A-ra).

Teljesen hasonlóan tudjuk definiálni egy A nemüres halmaz által *szabadon generált csoportot*, ha az előző bekezdésben monoid helyett mindenütt csoportot mondunk, ezt jelöljük F_A-val. Egy csoport *szabad*, ha létezik olyan nemüres halmaz, amely őt szabadon generálja.

Jegyezzük meg, hogy a fenti jelölésekkel, az A által generált szabad monoid/csoport helyett mondhatunk $\tau(A)$ által generált szabad monoidot/csoportot is (ennek érvényességét illetően ld. még a következő állítás 3. és 4. pontját, és vegyük figyelembe, hogy τ injektív).

1.1.2. Állítás.

1. *A fenti ϕ homomorfizmus egyértelmű.*
2. *A $\tau(A) \subseteq S$ halmaz minimális generátorrendszer S-ben.*
3. *Egy A által szabadon generált $F_A^{(M)}$ monoid valamint F_A csoport izomorfia erejéig egyértelmű (vagyis nem függ τ választásától sem).*
4. $(|A| = |B|) \iff (F_A^{(M)} \cong F_B^{(M)}) \iff (F_A \cong F_B)$
5. *Ha A szabadon generálja az $F_A^{(M)}$ monoidot (vagy F_A csoportot) a τ beágyazással, és $X \subseteq A$, akkor az $F_A^{(M)}$-ben (vagy F_A-ban) $\tau(X)$ által generált részmonoid (vagy részcsoport) X által szabadon generált.*

Bizonyítás. Szabad csoportok esetére adjuk meg a bizonyítást, a szabad monoidok esete teljesen hasonlóan működik.

1. Triviális, ha figyelembe vesszük, hogy ϕ egy generátorrendszeren elő van írva.
2. Először is jegyezzük meg, hogy, könnyen láthatóan, a triviális csoport nem szabad, tehát S-nek létezik az egységelemen kívül még legalább egy h eleme. Tegyük fel indirekt, hogy $\tau(A)$-nak létezik X valódi részhalmaza, amely generálja S-t. Adjuk meg

$f : A \to S$-et úgy, hogy $x \in \tau^{-1}(X)$ esetén $f(x) = \tau(x)$, és, ha $g \in \tau(A) \setminus X$ és $g \neq 1_S$, akkor legyen $f\left(\tau^{-1}(g)\right) = 1_S$, ha pedig $g \in \tau(A) \setminus X$ és $g = 1_S$, akkor legyen $f\left(\tau^{-1}(g)\right) = h$. A definíció alapján léteznie kell f-hez egy $\phi : S \to S$ homomorfizmusnak, amely X elemein identitás, viszont van olyan $g \in S$, hogy $\phi(g) \neq g$, ami ellentmondás, mivel X generátorrendszer, így a ϕ-nek az X-en felvett értékei meghatározzák ϕ-t, ami tehát csak az identikus izomorfizmus lehetne.

3. Legyen indirekt S és T két A által szabadon generált csoport, és $\tau_S : A \to S$, $\tau_T : A \to T$ a megfelelő beágyazások. Ekkor a definíciót S-re és $f = \tau_T$-re alkalmazva létezik egy $\phi : S \to T$ homomorfizmus, amely $\tau_S(A)$-t $\tau_T(A)$-ba viszi, T-re és $f = \tau_S$-re alkalmazva pedig létezik egy $\psi : T \to S$ homomorfizmus, amely $\tau_T(A)$-t $\tau_S(A)$-ba viszi. Ekkor $\psi \circ \phi$ egy olyan $S \to S$ homomorfizmus, amely a $\tau_S(A)$ generátorrendszert önmagába viszi, így ez csak az identikus izomorfizmus lehet, vagyis ϕ és ψ is izomorfizmus, tehát S és T izomorfak.

4. Nézzük először az oda irányt. Legyen tehát F_A egy A, F_B pedig egy B által generált szabad csoport, τ_A, τ_B a megfelelő beágyazások és $g : A \to B$ egy bijekció. Azt fogjuk belátni, hogy F_B-t A is szabadon generálja. Legyen $\tau := \tau_B \circ g$. Azt kellene belátni, hogy tetszőleges G csoportra és $f : A \to G$ függvényre létezik $\phi : F_B \to G$ homomorfizmus, melyre $\phi \circ \tau = f$. Mivel B az F_B-t szabadon generálja, így mindenesetre az $f \circ g^{-1} : B \to G$ függvényre létezik $\psi : F_B \to G$, hogy $\psi \circ \tau_B = f \circ g^{-1}$. Itt mindkét oldal kompozícióját véve jobbról g-vel látszódik, hogy $\phi = \psi$ megfelel. Vagyis $F_A \cong F_B$ érvényes.

   A másik irányt nem fogjuk használni, erre vonatkozóan ld. [12, p. 1] (Proposition 1.1.), amely szabad csoportokra bizonyítja az állítást, de a bizonyítás szabad monoidokra is változtatás nélkül érvényes.

5. Bármely T csoportra és $f : X \to T$ függvényre, ha az f-et tetszőlegesen kiterjesztjük A-ra egy $f' : A \to T$ függvénnyé, akkor az f'-höz az F_A szabad volta alapján tartozó ϕ'-nek a ϕ megszorítása a $\tau(X)$ által generált részcsoportra épp egy megfelelő homomorfizmus lesz, melyre $\phi \circ \tau|_X = f$.

   Jegyezzük meg, hogy általánosan is igaz, hogy egy szabad csoport részcsoportja szabad, de ennek bizonyítása jóval nehezebb (Nielsen-Schreier tétel, ld. [19, p. 95], Corrolary 2.9), ugyanez szabad monoidok részmonoidjaira nem feltétlenül igaz (ld. [10, p. 5], Example 1.2.2.).

■

Definiálhattuk volna a szabad félcsoport fogalmát is, ez azonban az egységelem hiánya miatt a későbbiekben nem lenne túl „kényelmes”, és nem igazán jelentene újdonságot, ugyanis meggondolható, hogy egyrészt egy szabad monoid egységelemét elhagyva szabad félcsoportot kapnánk,

másrészt bármely félcsoport egyértelműen beágyazható egy őt tartalmazó legszűkebb monoidba[4], amely szabad félcsoport esetén szabad monoid lenne. Szintén definiálható a szabad kommutatív monoid és a szabad Abel-csoport fogalma is (sőt, univerzális algebra segítségével algebrai struktúrák egy széles osztályára definiálható a „szabadság" fogalma[5]).

Jegyezzük meg továbbá, hogy tetszőleges A nemüres halmazra létezik az A által szabadon generált $F_A^{(M)}$ monoid, valamint F_A csoport, ezek konstrukcióját ld. az 1.2.2. állításban és az 1.2.9. következményben.

1.2. Szavak

1.2.1. Szavak alaptulajdonságai

1.2.1. Definíció. [6] Legyen adott egy Σ nemüres halmaz (*ábécé*). A Σ elemeiből képezett véges hosszúságú sorozatok halmazát a Σ ábécé feletti (vagy: Σ által generált) *szavak* halmazának nevezzük. Az egyetlen, Σ elemeiből képzett 0 hosszúságú sorozatot *üres szónak* nevezzük, és ε-gal jelöljük (ez nyilván független Σ választásától). A Σ elemeiből képzett összes szó halmazát, az üres szó nélkül Σ^*-al, üres szóval együtt pedig Σ_0^*-al jelöljük. (Megállapodás szerint, amikor külön nem mondjuk, a Σ által generált szavak halmazán mindig a Σ_0^* halmazt értjük.)[7]

Formálisan:

$$\Sigma^* = \bigcup_{n\in\mathbb{N}^+} (\mathbb{N}_n \to \Sigma), \Sigma_0^* = \Sigma^* \bigcup \{\varepsilon\},$$

ahol egy $\mathbb{N}_n \to \Sigma$ elemet *n-hosszú* szónak nevezünk. Jelöljük egy tetszőleges $w \in \Sigma_0^*$ szó hosszát $|w|$-vel, megállapodás szerint $|\varepsilon| = 0$.

A tetszőleges $w \in \Sigma^*$-ra a körülményes $\{(1, w(1)), \ldots, (|w|, w(|w|))\}$ helyett a sorozatoknál szokásos $(w(1), \ldots, w(|w|))$, vagy, ha nem félreérthető, simán a $w(1) \ldots w(|w|)$ jelölést használjuk.

Két, $u, v \in \Sigma^*$ szó *összefüzésének* (vagy konkatenációjának) nevezzük a következő, $u \star v$-vel jelölt, $|u| + |v|$-hosszú szót:

$$(u \star v)(k) = u(k), \text{ ha } 1 \le k \le |u| \text{ és}$$

$$(u \star v)(k) = v(k - |u|), \text{ ha } |u| + 1 \le k \le |u| + |v|.$$

Definíció szerint tetszőleges $u \in \Sigma_0^*$-ra $u \star \varepsilon = \varepsilon \star u = u$, ezzel $\star$ a teljes Σ_0^* halmazon értelmezve van.

[4] ld. [3], Proposition 2.

[5] ld. [1], II/10.

[6] Megjegyzés: a szavakat általában a matematikai logikában vagy a számítástudományban szokták az itt leírtakhoz hasonló módon, formálisan definiálni.

[7] A kitevőben szereplő $*$ jelet, mint operátort, amely tetszőleges Σ ábécéhez a Σ^* halmazt rendeli, *Kleene-csillagnak* is szokták nevezni. Változó, hogy Σ^*-ba az üres szót beleértik-e vagy sem, mi ezért itt kétféle jelölést is bevezetünk a kétféle esetre.

Egy $u \in \Sigma_0^*$ szó nemnegatív egész kitevős hatványait a következőképpen értelmezzük: $u^0 = \varepsilon$ és $u^1 = u$ minden u-ra, és rekurzívan, ha $n \in \mathbb{N}$-re már értelmeztük u^n-t, akkor legyen $u^{n+1} = u^n \star u$.

Jegyezzük meg, hogy mivel általában nem okoz félreértést, így az 1-hosszú Σ^*-beli szavakat azonosítani fogjuk a Σ elemeivel.

A definíciókból közvetlenül látszódik a következő:

1.2.1. Állítás. *A $|\cdot| : \Sigma_0^* \to \mathbb{R}_0^+$ hosszúság „norma" a Σ_0^* halmazon, az alábbi értelemben:*

$$|u| \geq 0$$

$$|u| = 0 \Longleftrightarrow u = \varepsilon \text{ és}$$

$$|u \star v| = |u| + |v|$$

minden $u, v \in \Sigma_0^*$-ra.

1.2.2. Állítás. *Tetszőleges Σ véges, nemüres halmazra a $(\Sigma^*, \star)$ pár félcsoportot alkot, a $(\Sigma_0^*, \star)$ pedig monoidot a ε egységelemmel. A $(\Sigma_0^*, \star)$-t Σ szabadon generálja. Speciálisan, tetszőleges Σ nemüres halmazhoz létezik Σ által generált $F_\Sigma^{(M)}$ szabad monoid.*

Bizonyítás. Az üres szó definíció szerint egységeleme a $\star$ műveletnek, az asszociativitás következik abból, hogy $u, v, w \in \Sigma_0^*$ esetén mind $(u \star v) \star w$, mind $u \star (v \star w)$ megegyezik a következő $t \in \Sigma_0^*$, $|u| + |v| + |w|$-hosszú szóval:

$$t(k) = u(k), \text{ha } 1 \leq k \leq |u| \text{ és}$$

$$t(k) = v(k - |u|), \text{ha } |u| + 1 \leq k \leq |u| + |v| \text{ és}$$

$$t(k) = w(k - |u| - |v|), \text{ha } |u| + |v| + 1 \leq k \leq |u| + |v| + |w|.$$

Legyen M tetszőleges monoid és $f : \Sigma \to M$ tetszőleges függvény. A $\phi : \Sigma_0^* \to M$ függvényt a következőképpen definiáljuk: $\phi(\varepsilon) = 1_M$, és, ha $w \in (\mathbb{N}_n \to \Sigma)$, akkor $\phi(w) = \prod_{i=1}^n f(w(i))$, ahol a produktumban az M-beli szorzást tekintjük. A ϕ megadásából rögtön látszódik, hogy ez homomorfizmus lesz.

■

Az előző tétel szerint tehát minden Σ halmazra létezik az $F_\Sigma^{(M)}$ szabad monoid, és az 1.1.2. állítás szerint ez izomorfia erejéig csak Σ számosságától függ. Tehát általában nem okoz félreértést, ha tetszőleges S halmazra a továbbiakban az $F_S^{(M)}$ szabad monoidot azonosítjuk az S_0^* monoiddal, és a szabad monoid betűiről, szavairól stb. beszélünk. (Megjegyzés: Ez alól kivételt képez, amikor egy monoid szabad részmonoidjairól szeretnénk beszélni.)

1.2.3. Következmény. *Tetszőleges $n, m \in \mathbb{N}$ és $u \in \Sigma_0^*$ esetén $u^{n+m} = u^n \star u^m$.*

1.2.2. Definíció. Azt mondjuk, hogy egy $u \in \Sigma_0^*$ szónak $v \in \Sigma_0^*$ egy *ciklikus permutációja*, ha $u = w_1 \star w_2$ és $v = w_2 \star w_1$ valamilyen $w_1, w_2 \in \Sigma_0^*$ szavakra.

A definícióból közvetlenül adódik:

1.2.4. Állítás. *A ciklikus permutálás ekvivalencia-reláció és ciklikus permutáltak egyforma hosszúak.*

A szavak között többféle részbenrendezést szokás definiálni, ezek közül az egyik leggyakoribb, és amit mi is fogunk használni, az ún. részszó-reláció. Ezen kívül többször fel fog merülni az egymás melletti betűkből álló részszó fogalma, amire ezért külön elnevezést és jelölést vezetünk be.

1.2.3. Definíció. Azt mondjuk, hogy egy $u \in \Sigma_0^*$ szó *részszava* $v \in \Sigma_0^*$-nak (jelben: $u \leq v$), ha létezik v-nek olyan $v = v_1 \star \cdots \star v_k$ felbontása valamilyen $k \in \mathbb{N}^+$-ra, hogy $\mathbb{N}_k$-nak van olyan I részhalmaza, hogy $u = v_{i_1} \star \cdots \star v_{i_l}$, ahol $l \in \mathbb{N}^+$, $m < n \Longrightarrow i_m < i_n$, $l = |I|$ és $i_j \in I$ $(\forall\, j \in \mathbb{N}_l)$-re.

Egy $u \in \Sigma_0^*$ szó *konvex részszava* $v \in \Sigma_0^*$-nak (jelben: $u \trianglelefteq v$), ha $v = a \star u \star b$ valamilyen $a, b \in \Sigma_0^*$ szavakra.[8]

Használni fogjuk még a valódi részszó és a valódi konvex részszó fogalmát is, arra az esetre, ha még $u \neq v$ is teljesül.

1.2.5. Állítás. *Tetszőleges $u, v \in \Sigma_0^*$ szavakra $u \trianglelefteq v \Longrightarrow u \leq v$ és $u \leq v \Longrightarrow |u| \leq |v|$; a szavak közötti részszó és konvex részszó relációk részbenrendezést alkotnak (vagyis reflexívek, antiszimmetrikusak és tranzitívek); valamint mindkettő pontosan akkor teljes rendezés, ha $|\Sigma| = 1$.*

Bizonyítás. Az első állítás a definíciók közvetlen következménye.

A reflexivitáshoz a definícióban az első esetben legyen $I = \mathbb{N}_k$, a második esetben $a = b = \varepsilon$. Az antiszimmetria adódik abból, hogy $u \leq v$ és $v \leq u$ vagy $u \trianglelefteq v$ és $v \trianglelefteq u$ esetén $|u| = |v|$, tehát a megfelelő definíciókban csak $I = \mathbb{N}_k$, illetve $a = b = \varepsilon$ lehetséges. A $\leq$ tranzivitivitásához vegyük észre, hogy v akkor és csak akkor részszava u-nak, ha abból tetszőleges (esetlegesen üres halmazt alkotó) betűk elhagyásával keletkezik, és, ha egy u szóból elhagyunk betűket, majd a kapott v-ből szintén elhagyunk betűket, akkor azokat egyszerre is elhagyhattuk volna u-ból. Ha $u \trianglelefteq v$ és $v \trianglelefteq w$, akkor $w = a \star v \star b = a \star (c \star u \star d) \star b = (a \star c) \star u \star (d \star b)$ valamilyen $a, b, c, d \in \Sigma_0^*$ szavakra, vagyis $u \trianglelefteq w$.

Legyen most $\Sigma = \{a\}$, ekkor minden $k \in \mathbb{N}$-ra egyetlen k-hosszú (csupa a betűből álló) w_k szó létezik, és $k \leq l \iff w_k \leq w_l \iff w_k \trianglelefteq w_l$. Ha $a, b \in \Sigma$ $(a \neq b)$, akkor pedig $a \not\trianglelefteq b,\ b \not\trianglelefteq a$, tehát speciálisan $a \not| b,\ b \not| a$.

[8] Az elnevezés arra utal, hogy pontosan ugyanezt kapnánk, ha a részszó definíciójában azt követelnénk meg, hogy $\mathbb{N}_k$-nak egy konvex részhalmazát válasszuk.

■

Használni fogjuk még a következő jelölést: egy $w \in \Sigma_0^*$ szóra és $1 \leq k \leq |w|$ egész számra, $w^{(k)}$ jelölje a w első k darab betűjéből álló részszavát.

1.2.2. Normális részmonoid szerinti hányadosmonoid

Legyen M egy monoid, $H \leq M$ egy részmonoidja. Az M elemeire definiálunk egy $\sim_H$ relációt a következőképpen: $a \sim_H b$, ha léteznek olyan $h_0, h_1, \ldots, h_k \in H$, $g_0, g_1, \ldots g_l \in H$, $a_1, \ldots, a_k \in M$ és $b_1, \ldots, b_l \in M$ elemek, hogy

$$a_1 \ldots a_k = a,\ b_1 \ldots b_l = b, \text{ és}$$

$$h_0 a_1 h_1 a_2 h_2 \ldots h_{k-1} a_k h_k = g_0 b_1 g_1 \ldots g_{l-1} b_l g_l$$

1.2.6. Állítás. *Legyen M egy tetszőleges monoid. Ekkor:*

1. *Az előbb definiált $\sim_H$ reflexív és tranzitív, és, ha M szabad, akkor tranzitív is (vagyis ekvivalencia-reláció).*
2. *Ha $a \sim_H a'$ és $b \sim_H b'$, akkor $ab \sim_H a'b'$, vagyis, ha $\sim_H$ tranzitív, akkor $\sim_H$ kongruencia-reláció.*
3. *Ha $\sim_H$ tranzitív, akkor az M-ben 1 ekvivalencia-osztálya $\sim_H$ szerint normális részmonoid, tartalmazza H-t, és akkor és csak akkor egyezik meg H-val, ha H maga is normális részmonoid.*
4. *Tetszőleges M-beli $\sim$ kongruencia-relációra az 1 ekvivalencia-osztálya egy H' normális részmonoid, és ezzel a H'-vel $\sim_{H'} \subseteq \sim$.*
5. *Ha $M = T_0^*$ szabad monoid, akkor tetszőleges $H \trianglelefteq M$ normális részmonoidra, minden $w \in T_0^*$ szóra létezik egy $v \in T_0^*$, $w \sim_H v$ szó, hogy v-nek nincs nemüres H-beli konvex részszava.*

Bizonyítás.

1. A reflexivitás és a szimmetria triviális bármely M-re.

   Most legyen M szabad, vagyis $M \cong \Sigma_0^*$ valamilyen Σ-ra, belátjuk, hogy $\sim_H$ tranzitív.

   A bizonyításban a megszokottnál kevésbé leszünk precízek, mivel a teljesen precíz bizonyítás hosszadalmas volna, de nem lenne túl tanulságos (az alábbi szemléletes bizonyítás alapján egyértelműen megkonstruálható):

   Szabad monoidra tehát két szó akkor és csak akkor lehet egyenlő, ha betűről betűre megegyeznek. Ekkor az $a \sim_H b$ definíciója azt jelenti, hogy az a szóba először beszúrva néhány H-beli h_i szót, majd a kapott szóból elhagyva H-beli h_i' konvex részszavakat

b-hez jutunk. A $b \sim_H c$ pedig hasonlóan b-be g_i H-beli szavak beszúrását, majd g_i' H-beli szavak elhagyását jelenti. Ha most a-ba először beszúrjuk a h_i szavakat, majd a kapott szóba a g_i szavakat megfelelő helyekre (itt többféle választási lehetőségünk is adódhat, hogy hova szúrjunk, ezek közül szabadon választhatunk, csak arra figyeljünk, hogy a g_i'-ket ne vágjuk ketté), majd elhagyunk megfelelő helyeken lévő g_i', majd h_i' szavakat, akkor c-t kapjuk, vagyis $a \sim_H c$ is érvényes lesz.

2. Legyen $a \sim_H a'$ és $b \sim_H b'$, ekkor

$$a_1 \dots a_k = a,\ a_1' \dots a_l' = a',\ b_1 \dots b_m = b,\ b_1' \dots b_n' = b',$$
$$h_0 a_1 h_1 \dots h_{k-1} a_k h_k = h_0' a_1' \dots h_{l-1}' a_l' h_l'$$
$$g_0 b_1 g_1 \dots g_{m-1} b_m g_m = g_0' b_1' g_1' \dots g_{n-1}' b_n' g_m',$$

és ebből

$$h_0 a_1 h_1 \dots h_{k-1} a_k \left(h_k g_0\right) b_1 g_1 \dots g_{m-1} b_m g_m =$$
$$= h_0' a_1' \dots h_{l-1}' a_l' \left(h_l' g_0'\right) b_1' g_1' \dots g_{n-1}' b_n' g_m'$$
$$a_1 \dots a_k b_1 \dots b_m = ab,\ a_1' \dots a_l' b_1' \dots b_n' = a'b',$$

ami épp $ab \sim_H a'b'$-t jelenti, figyelembe véve, hogy $h_k g_0, h_l' g_0' \in H$, mivel H részmonoid.

3. Legyen most $\sim_H$ tranzitív (vagyis kongruencia-reláció) és H' az 1 ekvivalencia-osztálya $\sim_H$ szerint.

   A $\sim_H$ reflexivitása miatt $1 \in H'$, és $a \sim_H 1, b \sim_H 1$ esetén $ab \sim_H 1$ az előző pont szerint, tehát H' részmonoid.

   Tetszőleges $h \in H'$-re és $x, y \in M$-re $h \sim_H 1 \implies xh \sim_H x \implies xhy \sim_H xy$, így ebből $\sim_H$ tranzitivása miatt $xy \sim_H 1 \iff xhy \sim_H 1$ következik, vagyis H' valóban normális részmonoid.

   A $h \in H$ eseteben az $1h = h$ felbontás alapján $h \sim_H 1$, tehát $H \leq H'$.

   Most tegyük fel, hogy H normális részmonoid, és $1 \sim_H x$. Ekkor léteznek olyan $g_0, \dots, g_k \in H$, $e_1, \dots, e_k \in M$, $h_0, \dots, h_l \in H$ és $x_1, \dots, x_l \in M$ elemek, hogy

$$g_0 e_1 g_1 \dots g_{k-1} e_k g_k = h_0 x_1 h_1 \dots h_{l-1} x_l h_l,$$

$$e_1 \dots e_k = 1,\ x_1 \dots x_l = x.$$

   Mivel H normális, így a definíciót felhasználva, indukcióval belátható, hogy $1 = e_1 \dots e_k \in H \iff g_0 e_1 g_1 \dots g_{k-1} e_k g_k \in H$, és $h_0 x_1 h_1 \dots h_{l-1} x_l h_l \in H$ akkor és csak

akkor, ha $x_1 \dots x_l = x \in H$. Mivel $1 \in H$ triviális, így ebből $x \in H$ adódik, vagyis most valóban $H' \leq H$, így a fentieket figyelembe véve $H' = H$.

4. Legyen most $\sim$ tetszőleges M-beli kongruencia-reláció, és H' az 1 ekvivalencia-osztálya $\sim$ szerint. Először is, figyeljük meg, hogy az előző pontban annak bizonyításánál, hogy az 1 ekvivalencia-osztálya $\sim_H$ szerint normális részmonoid, kizárólag $\sim_H$ kongruencia-reláció voltát használtuk fel, így ez tetszőleges $\sim$ kongruencia-relációra érvényes.

   Most belátjuk, hogy $\sim_{H'} \subseteq \sim$.

   Legyen $a \sim_{H'} b$, tehát

   $$a_1 \dots a_k = a,\ b_1 \dots b_l = b, \text{ és}$$

   $$h_0 a_1 h_1 \dots h_{k-1} a_k h_k = g_0 b_1 g_1 \dots g_{l-1} b_l g_l$$

   alkalmas $a_1, \dots, a_k, b_1, \dots, b_l \in M,\ h_0, \dots, h_k, g_0, \dots, g_l \in H'$ elemekre. Mivel $\sim$ kongruencia-reláció, így tetszőleges $h \in H'$, $x \in M$ esetén $h \sim 1$ miatt $hx \sim xh \sim x$, és ebből indukcióval látszódik, hogy $a = a_1 \dots a_k \sim h_0 a_1 h_1 \dots h_{k-1} a_k h_k$ és $b = b_1 \dots b_l \sim g_0 b_1 g_1 \dots g_{l-1} b_l g_l$, vagyis $a \sim b$, így $\sim_{H'} \subseteq \sim$.

5. A $\sim_H$ kongruencia definíció alapján, ha $w \in T_0^*$ tartalmaz egy H-beli nemüres konvex részszót, akkor azt elhagyva w-ből egy olyan $w_1 \in T_0^*$ szót kapunk, melyre $w_1 \sim_H w$. Mivel így w hossza csökkent, így indukcióval előbb-utóbb egy olyan $v \in T_0^*$ szót kapunk, melynek nincs H-beli nemüres konvex részszava.

■

Az előző állítás 4. pontjában a tartalmazás lehet szigorú is, pl. a $\Sigma = \{a, b, c\}$ ábécé által generált Σ_0^* szabad monoidra a $\phi : M \to M$, $\phi(a) = 1, \phi(b) = \phi(c) = b$ és a $\psi : M \to M$, $\psi(a) = 1, \psi(b) = b, \psi(c) = c$ által meghatározott homomorfizmusoknak az 1.1.1. megjegyzés szerinti második értelemben vett $\mathrm{Ker}(\phi)$ és $\mathrm{Ker}(\psi)$ magjai (mint kongruenciák) mutatják, hogy az 1 ekvivalencia-osztálya nem feltétlenül határozza meg a teljes kongruencia-relációt. Csoportokra ismert, hogy ez nem fordulhat elő.

1.2.4. Definíció. Az M szabad monoid H *normális részmonoidja szerinti hányadosmonoidján* (vagy faktormonoidján) az M-nek a $\sim_H$ kongruencia szerinti hányadosmonoidját értjük és M/H-val jelöljük.[9]

1.2.7. Állítás. *Tetszőleges M szabad monoidra, és $H \trianglelefteq M$ normális részmonoidra létezik M' monoid és $\phi : M \to M'$ szürjektív homomorfizmus, hogy $Ker(\phi) = H$.*

Bizonyítás. Ez az ún. természetes leképezés az M szabad monoidról az $M' = M/\sim_H = M/H$ faktormonoidra, erre vonatkozóan ld., általános algebrai struktúrákra kimondva, az [1] 59. oldalán a 6.9. definíciót és a 6.10. tételt, továbbá, vegyük figyelembe, hogy ilyenkor, ha a

[9] Kongruencia szerinti hányadosstruktúrát illetően ld. [1], Definition II/5.2.

homomorfizmus magját kongruenciaként tekintve $\mathrm{Ker}(\phi) = \sim_H$, akkor az 1.2.6. állítás 3. pontja szerint a homomorfizmus magját részhalmazként tekintve $\mathrm{Ker}(\phi) = H$.

■

1.2.3. Monoidok és csoportok prezentációja

1.2.5. Definíció. Legyen S egy tetszőleges nemüres halmaz, $F_S^{(M)}$ az S által generált szabad monoid, és $R \subseteq F_S^{(M)}$ tetszőleges halmaz (ún. *definiáló relációk*), és $N(R)$ az R által az $F_S^{(M)}$-ben generált normális részmonoid. Ekkor az $M = F_S^{(M)}/N(R)$ halmazt az S generátorok és az R definiáló relációk által generált monoidnak nevezzük. Ilyenkor azt mondjuk, hogy az $M = \langle S \mid R \rangle_M$ felírás M-nek egy *prezentációja.*

1.2.8. Állítás. *Legyen S egy nemüres halmaz, és rögzítsünk egy S^{-1}, az S-től diszjunkt, azzal azonos számosságú halmazt és egy $\omega : S \to S^{-1}$ bijekciót, és legyen T_0^* a $T = S \cup S^{-1}$ halmaz által szabadon generált monoid, és álljon $R \subseteq T_0^*$ az összes $s \star \omega(s)$ és $\omega(s) \star s$ $(s \in S)$ alakú 2-hosszú szóból. Ekkor $G = \langle T \mid R \rangle_M$ csoport, amit S szabadon generál.*

Bizonyítás. Rögzítsük le a $\xi : T_0^* \to G$ természetes monoid-homomorfizmust, amelyre tehát $\mathrm{Ker}(\xi) = N(R)$.

Nyilván G definíció szerint monoid, így még azt kell belátni, hogy minden $g \in G$-nek van inverze. Terjesszük ki ω-t T-re a $\omega' = \omega \cup \omega^{-1}$ értelmezéssel. Legyen $w \in T_0^*$ $(|w| = n)$ tetszőleges, ekkor $w^{-1} \in T_0^*$-ot definiáljuk a következőképpen: $w^{-1} = \prod_{i=n}^{1} \omega'(w(i))$, ekkor könnyen ellenőrizhetően $\xi(w) \in G$ inverze éppen $\xi\left(w^{-1}\right)$ lesz.

Legyen most H tetszőleges csoport, $\tau : S \to G$ $(\tau = \xi|_S)$ beágyazás és $f : S \to H$ tetszőleges függvény. Ezt terjesszük ki T-re az $x \in S$ esetben $f'(x) = f(x)$, az $x \in S^{-1}$ esetben pedig az $f'(x) = f\left(\omega^{-1}(x)\right)^{-1}$ definícióval. Tetszőleges $w \in T_0^*$ $(|w| = n)$-re pedig legyen $\psi(w) = \prod_{i=1}^{n} f'(w(i))$. Ekkor ψ monoid-homomorfizmus T_0^* és H között. Mivel ψ az R elemeit a H egységelemébe képezi, így meghatároz egy $\phi : G \to H$ monoid-homomorfizmust, ugyanis egyrészt az 1.1.1. állítás 5. pontja szerint ψ magja normális részmonoid, vagyis $N(R) \subseteq \mathrm{Ker}(\psi)$, ezáltal az 1.2.2. pontbeli kongruencia definíciója szerint pedig, ha $u, v \in T_0^*$-ra $u \sim_{N(R)} v$, akkor tehát $u \sim_{\mathrm{Ker}(\psi)} v$, és ilyenkor könnyen látható-an $\psi(u) = \psi(v)$ is következik. Ekkor a homomorfizmus-tétel bizonyításához[10] hasonlóan a $\psi = \phi \circ \xi$ feltétel egyértelműen meghatároz egy $\phi : G \to H$-t, és épp ilyet kerestünk. Most a kapott ϕ csoport-homomorfizmus is lesz, mivel G és H csoport. Vagyis G valóban szabad, és az S szabadon generálja.

■

[10] Ld. [1, p. 46], Theorem 6.12.

1.2.9. Következmény. *Minden S nemüres halmazra létezik az S által szabadon generált F_S csoport.*

Mivel az 1.1.2. állítás szerint az S által generált F_S szabad csoport izomorfia erejéig egyértelmű, így megállapodhatunk, hogy amennyiben nem okoz zavart, a továbbiakban az 1.2.8. állításban meghatározott G-t azonosítjuk F_S-sel. (Ez akkor jelenthetne problémát, ha egy csoport különböző szabad részcsoportjait tekintenénk.)

A fentiek alapján a monoid prezentációjához hasonlóan definiálhatjuk a csoportok prezentációját:

1.2.6. Definíció. Legyen S egy tetszőleges nemüres halmaz, F_S az S által generált szabad csoport és $R \subseteq F_S$ egy tetszőleges halmaz (ún. *definiáló relációk*), és $N(R)$ az R által F_S-ben generált normálosztó. Ekkor a $G = F_S/N(R)$ halmazt az S generátorok és R definiáló relációk által generált csoportnak nevezzük. Ilyenkor azt mondjuk, hogy a $G = \langle S \mid R \rangle$ felírás a G-nek egy *prezentációja.*

Megjegyezzük, hogy tetszőleges G csoportnak létezik prezentációja, továbbá tetszőleges S nemüres halmazra és $R \subseteq F_S$ halmazra létezik (izomorfia erejéig egyértelmű) G' csoport, melynek $\langle S \mid R \rangle$ egy prezentációja. Ez utóbbi a hányadoscsoport létezése miatt triviális, az előbbi pedig abból következik, hogy ha G-nek X egy generátorrendszere, úgy az F_X szabad csoportra és $f : X \to X \subseteq G$ függvényre létezik egy egyértelmű $\phi : F_X \to G$ homomorfizmus, amely most szürjektív lesz, így az első izomorfizmus-tétel szerint $G \cong F_X/\mathrm{Ker}(\phi)$, vagyis $G = \langle X \mid R \rangle$, ahol $R \subseteq F_X$ tetszőleges olyan, hogy $N(R) = \mathrm{Ker}(\phi)$.

Ha tehát adott egy tetszőleges G csoport és egy $X \subseteq G$ generátorrendszer, akkor olyan szempontból egyértelműen tudunk G-hez hozzárendelni egy X szerinti prezentációt, hogy, ha $G = \langle X \mid R_1 \rangle$ és $G = \langle X \mid R_2 \rangle$ is G-nek két ilyen, az előző bekezdés szerinti prezentációja, akkor $N(R_1) = N(R_2)$. Ezt az F_X-beli generált normálosztó erejéig egyértelmű prezentációt nevezzük a G-nek az X *generátorrendszere szerinti prezentációjának.*

Azt mondjuk, hogy a G csoportnak a $G = \langle S \mid R \rangle$ prezentációja *rendes*, ha $1_G \notin R$ és $S \cap N(R) = \varnothing$.

Megjegyezzük, hogy tetszőleges G csoportnak létezik rendes prezentációja. Ugyanis, ha $G = \langle S \mid R \rangle$ egy prezentáció, akkor $G = \langle S \setminus N(R) \mid R \setminus 1_G \rangle$ könnyen ellenőrizhetően egy rendes prezentáció.

Ugyanezek a definíciók és állítások érvényesek, hasonló gondolatmenettel, monoidokra is.

Jelölés. Ha $S = \{s_1, \ldots, s_k\}$ és $R = \{r_1, \ldots, r_n\}$ véges, akkor a kapcsos zárójeleket elhagyva használni fogjuk az $\langle S \mid R \rangle = \langle s_1, \ldots, s_k \mid r_1, \ldots, r_n \rangle$ jelöléseket is, és, ha R még üres is, akkor simán $\langle S \mid R \rangle = \langle S \rangle = \langle s_1, \ldots, s_k \rangle$-t írunk, amely mellesleg megegyezik F_S-sel, hiszen az üres halmaz által generált normálosztó a triviális egyelemű részcsoport. Hasonló egyszerűsítés használható természetesen a monoidok prezentációi esetén is.

1.2.1. *Megjegyzés.* A monoidok prezentációt definiálhattuk volna egy kicsit általánosabban is, mégpedig olyan módon, hogy R az $r_1 = q_1$, $r_2 = q_2$ stb. $(r_i, q_i \in F_S^{(M)})$ típusú egyenlőségek halmaza, és ilyenkor $\langle S \mid R\rangle_M$ az $F_S^{(M)}$ azon „legnagyobb" homomorf képe, melyben az R-beli egyenlőségek teljesülnek, abban az értelemben, hogy, ha N egy másik monoid, amely $F_S^{(M)}$-nek homomorf képe és teljesíti az R-beli egyenlőségeket, akkor N az $\langle S \mid R\rangle_M$-nek is homomorf képe. Be lehet látni, hogy ez a definíció is mindig egyértelmű monoidot definiál. A mi definíciónk annak a speciális esetnek felel meg, amikor minden egyenlőség $r_1 = 1, r_2 = 1$ stb. alakú. Másféle monoid-prezentációra azonban nem lesz szükségünk, így maradunk ennél a speciális alaknál. Csoportok prezentációi esetén a kétféle megközelítés egyenértékű, mivel egy csoportban $r = q$ ekvivalens $rq^{-1} = 1$-gyel.

1.2.4. Monoidszavak

Az 1.2.2. állítás bizonyítása után megemlítettük, hogy az $F_S^{(M)}$ szabad monoidot azonosíthatjuk a vele izomorf S_0^* monoiddal, melynek elemeit a szabad monoid szavainak is nevezhetjük, melyek tehát kölcsönösen egyértelmű megfeleltetésben állnak az $F_S^{(M)}$ elemeivel. Ez azonban nem szabad monoidok illetve csoportok szavai esetében nem érvényes.

1.2.7. Definíció. Legyen M tetszőleges monoid, melynek adott egy $\langle S \mid R\rangle_M$ prezentációja. Ekkor tudjuk, hogy $M \cong S_0^*/N(R)$, ahol $N(R)$ az R által M-ben generált normális részmonoid. Legyen $\theta : \ S_0^* \to M$ az S_0^* és M közötti természetes homomorfizmus[11].

Jelen esetben az S_0^* halmazt az M monoid *szavainak* is nevezzük, és tetszőleges $x \in S_0^*$-ra $\theta(x)$ az x monoidszóhoz tartozó monoidelem. Egy monoidelemhez több szó is tartozhat, az $m \in M$ elemhez tartozó szavak halmaza $\theta^{-1}(m)$ (amely sosem üres, mivel tudjuk, hogy θ szürjektív).

1.2.5. Csoportszavak

Először tekintsük a szabad csoportok szavait:

1.2.8. Definíció. Legyen S egy nemüres halmaz, és F_S az S által generált szabad csoport, $\tau : \ S \to F_S$ beágyazás. Ezen kívül rögzítsünk egy S^{-1}, az S-től diszjunkt, és azzal azonos számosságú halmazt, és egy $\omega : S \to S^{-1}$ bijekciót. Ekkor a $T = S \cup S^{-1}$ halmaz, mint ábécé által generált szavak $W(F_S) := T_0^*$ monoidját az F_S szabad csoport szavainak nevezzük.

Állapodjunk meg, hogy tetszőleges $x \in T$ elemre $\left(\omega \cup \omega^{-1}\right)(x)$-et x^{-1}-el is fogjuk jelölni.

Az $f : T \to F_S$ függvényt definiáljuk a következőképpen:

$$f(x) = \tau(x) \text{ , ha } x \in S \text{ és}$$

$$f(x) = \left(\tau\left(\omega^{-1}(x)\right)\right)^{-1} \text{ , ha } x \in S^{-1}.$$

[11] Ld. [1, p. 59]

Ekkor a szabad monoid definíciója szerint ez egyértelműen kiterjeszthető egy $\phi : W(F_S) \to F_S$ monoid-homomorfizmussá, amely szürjektív lesz, hiszen F_S-t, mint monoidot generálja az $f(T)$ halmaz.

Tetszőleges $w \in W(F_S)$ csoportszónak megfelelő csoportelem legyen $\phi(w)$, egy $g \in F_S$ csoportelemhez tartozó szavak (nemüres) halmaza pedig $\phi^{-1}(g)$.

Jegyezzük meg, hogy egy csoportelemhez több szó is tartozhat. Két $u, v \in W(F_S)$ szót *ekvivalensnek* nevezünk (jelben: $u \sim v$), ha $\phi(u) = \phi(v)$. Egy $u \in W(F_S)$ szót *egységértékűnek* nevezünk, ha $u \sim \varepsilon$.

Végül a fenti definíció könnyen kiterjeszthető szabad csoportokról tetszőleges, prezentációval megadott csoportra:

Legyen G tetszőleges csoport, melynek adott egy $\langle S \mid R\rangle$ prezentációja. Ekkor tudjuk, hogy $G \cong F_S/N(R)$, ahol $N(R)$ az R által G-ben generált normálosztó. Legyen $\theta : F_S \to G$ az F_S-ből G-be menő természetes homomorfizmus. A $\phi : W(F_S) \to F_S$ függvényt definiáljuk ugyanúgy, mint az előző definícióban. Ekkor a $\rho = \theta \circ \phi$ ($\rho : W(F_S) \to G$) függvény megadja tetszőleges $w \in W(F_S)$ csoportszóhoz a hozzátartozó $\rho(w)$ G-beli csoportelemet. Ha G-beli csoportszavakról beszélünk, akkor a $W(F_S)$ jelölés helyett használjuk a $W(G)$ jelölést is (feltéve, hogy egyértelműen rögzítve van G-nek az $\langle S \mid R\rangle$ prezentációja). Ha az $u, v \in W(F_S)$ szavakra az előbbi ρ-val $\rho(u) = \rho(v)$, akkor u és v ekvivalens G-ben (jelben: $u \sim_G v$; ahol, ha nem okoz félreértést, a G-re vonatkozó jelölés elhagyható), ha pedig $u \sim_G \varepsilon$, akkor u-t egységértékűnek mondjuk G-re nézve.

Használni fogjuk egy csoportszó inverzének a fogalmát is, egy $w \in W(G)$ ($|w| = n > 0$) inverzét a $w^{-1}(i) := (w(n-i))^{-1}$ ($i \in \mathbb{N}_n$), $w = \varepsilon$ esetén pedig a $w^{-1} := w = \varepsilon$ definíció adja meg. Egy szó inverze definíció szerint mindig ugyanolyan hosszú, mint w. Könnyű látni, hogy tetszőleges $n \in \mathbb{N}$-re $\left(w^{-1}\right)^n = (w^n)^{-1}$, és legyen w^{-n} definíció szerint ez a közös érték.

Azt mondjuk, hogy csoportszavak egy $H \subseteq W(G)$ részhalmaza generálja a G csoportot, ha $\phi(H)$ generátorrendszere G-nek. Továbbá, nyilván nem okoz félreértést, ha a generált részcsoportra és generált normálosztóra vonatkozó $\langle R\rangle$ és $N(R)$ jelöléseket használjuk akkor is, ha R szavaknak egy halmaza (ezen operációk eredménye viszont ez esetben is részcsoport lesz).

Általában a csoportok prezentációi esetében a definiáló relációkat szeretjük a csoport egy generátorrendszere, mint betűk által alkotott szavaknak tekinteni, így tudunk beszélni például a definiáló relációk hosszáról, és egyéb, szavakra definiált tulajdonságairól is:

1.2.9. Definíció. Legyen G adva a $G = \langle S \mid R\rangle$ prezentációval, ahol $X \subseteq G$ a G egy generátorrendszere, és legyen $R' \subseteq W(F_S)$ olyan szóhalmaz, hogy minden R-beli elemnek pontosan egy R'-beli szó felel meg, és megfordítva. Ekkor azt is mondjuk, hogy G a $G = \langle S \mid R'\rangle$ *szóprezentációval* adott. Egy szóprezentáció rendes, ha a hozzá tartozó prezentáció rendes.

2. fejezet

Monoid- és csoportszavak és rövidítéseik

Mostantól a szavak összefűzésére vonatkozó $\star$ jelölést a nagyobb áttekinthetőség érdekében elhagyjuk, és azt simán egymás mellé írással jelöljük (ez nem okoz félreértést, mivel másféle szorzás nem fog szerepelni, és monoidoknak és csoportoknak csak szavairól lesz szó, nem pedig az elemeiről).

2.1. Részmonoidok és részcsoportok szavai

2.1.1. Részmonoidok szavai

Az alábbiakban először szabad monoidok részmonoidjainak és normális részmonoidjainak a szavaira adunk néhány hasznos állítást, melyek segítségünkre lesznek majd csoportszavak és rövidítéseik szerkezetének feltárásában. Az 1.2.2. pontban szereplő kongruencia az 1.2.6. állítás alapján megadta, hogy általában hogy kaphatjuk meg egy X halmaz által generált $N(X)$ normális részmonoid elemeit. Bizonyos speciális halmazok esetén azonban $N(X)$ elemei egyszerűbben is jellemezhetők.

2.1.1. Lemma. *Tetszőleges nemüres $X \subseteq T_0^*$-ra jelöljük X'-vel azon T_0^*-beli szavak halmazát, melyekből X-beli konvex részszavak egymás utáni elhagyásával valamilyen módon az üres szóhoz tudunk jutni.*

1. *$X \subseteq X' \leq N(X)$*
2. *Ha minden $x \in X'$-re a rövidítést mohó módon is megtehetjük, vagyis X-beli konvex részszavakat tetszőleges módon elhagyva x-ből, előbb-utóbb az üres szóhoz jutunk, akkor $N(X) = X'$.*
3. *Az előző feltétel akkor és csak akkor teljesülhet, ha $v \in X$ esetén $avb \in X' \Longrightarrow ab \in X'$ tetszőleges $a, b \in T_0^*$ szavakra.*

4. Ha $X \subseteq T_0^*$ egy olyan halmaz, hogy $\forall x \in X$-re $|x| = 2$, $ab \in X$ ($|a| = |b| = 1$) esetén $ba \in X$, továbbá $ab \in X$, $bc \in X$ ($|a| = |b| = |c| = 1$) esetén $a = c$, akkor X-re teljesül a 2. pontban megfogalmazott feltétel, vagyis $N(X) = X'$.

Bizonyítás.

1. Tetszőleges $x \in X$-ből önmagát elhagyva egyből az üres szóhoz jutunk, így $X \subseteq X'$.

   Most belátjuk, hogy minden X'-beli szó része kell, hogy legyen $N(X)$-nek, ugyanis, egyrészt az üres szó mindig része $N(X)$-nek, másrészt az 1.2.2. pontban definiált kongruencia szerint, ha egy nemüres $x \in X'$-beli szóból elhagyunk egy X-beli (így speciálisan $N(X)$-beli) szót, akkor a kapott x'-re $x \sim_{N(X)} x'$, és mivel a végén ε-hoz jutunk, így a tranzitivitás miatt $x \sim_{N(X)} \varepsilon \Longrightarrow x \in N(X)$, tehát $X' \subseteq N(X)$.

   Ha x és $y \in X'$, akkor xy-ra is igaz, hogy belőle X-beli konvex részszavakat elhagyva üres szóhoz tudunk jutni, ha előbb az x-nek, majd az y-nak megfelelő részét „tüntetjük" el xy-nak, így xy is $\in X'$, továbbá $\varepsilon \in X'$ triviális, vagyis X' részmonoid.

2. Most tegyük fel, hogy valamely nemüres X halmazra X' olyan, hogy abból mohó módon elhagyva X-beli elemeket is mindig ε-ba tudunk jutni.

   Ha xy és $h \in X'$, akkor xhy-ból előbb a középen lévő h-nak megfelelő konvex részszót kiejtve xy-t kapunk, amit tovább tudunk vinni ε-ba, így $xhy \in X'$.

   Ha xhy és $h \in X'$, akkor xhy-t valamilyen módon az üres szóba tudjuk vinni, és most feltettük, hogy ebből következik az, hogy bármilyen módon az üres szóba vihetjük, vagyis, ha először a középen lévő h-t ejtjük ki, akkor a kapott xy-t is tovább kell tudnunk vinni az üres szóba, vagyis xy is $\in X'$, vagyis X' normális részmonoid.

   Ezekből és az előző állításból következik, hogy X' egy X-et tartalmazó normális részmonoid, így $N(X) \subseteq X'$, és mivel $X' \subseteq N(X)$-et már láttuk, így $X' = N(X)$ következik.

3. Ez tulajdonképpen nem más, mint az előző állítás feltételének egy precízebb átfogalmazása.

4. Az X-re tett feltevés következtében tetszőleges $a \in T_0^*$ ($|a| = 1$) betűre legfeljebb egy $b \in T_0^*$ ($|b| = 1$) betű létezhet, melyre $ab \in X$, ugyanis $ab_1 \in X$, $ab_2 \in X$ esetén $b_2a \in X$, és ebből $b_1 = b_2$ következne, másrészt, ha $ab \in X$, akkor $ba \in X$, és b az egyetlen olyan betű is, amellyel a-t balról szorozva X-beli elemet kaphatunk. Ha a egy olyan betű, amely tehát bármelyik X-beli szóban szerepel, akkor hozzá pontosan egy olyan b betű tartozik, amellyel balról, és így jobbról szorozva is X-beli elemet kapunk; nevezzük ezt most a kiejtő betűpárjának.

   Egy $x \in X'$ nemüres szó esetén az $\{1, \ldots, |x|\}$ halmaz két különböző i,j elemét nevezzük kiejtőnek, ha x-ből ki lehet hagyni egymás után X-beli konvex részszavakat úgy, hogy az x i-edik és j-edik betűi egymás mellé kerüljenek, és X-beli szót alkossanak.

A kiejtő helyzet nyilván szimmetrikus, így vegyük az x szóhoz azt az (irányítatlan) gráfot, melyben minden $\{1, \ldots, |x|\}$-beli számnak megfeleltetünk egy-egy csúcsot, és két csúcsot akkor kötünk össze éllel, ha a nekik megfelelő elemek kiejtők.

Legyen az x i-edik helyén álló betűje a, amelynek kiejtő betűpárja b, és nézzük az előző gráf azon összefüggőségi komponensét, mely tartalmazza az i-edik csúcsot. Az ezen komponenshez tartozó betűk az x bármilyen mohó rövidítésénél csak egymást ejthetik ki, tehát elegendő egy ilyen komponensre belátni, hogy, ha azt valamilyen módon el lehet tüntetni, akkor mohó módon is el lehet.

Nézzük az összefüggőségi komponens csúcsainak megfelelő helyeken álló betűk által meghatározott t részszavát x-nek. Mivel a és b csak egymást ejthetik ki, így más betű nyilván nem szerepelhet t-ben, és mivel valamilyen módon t-t az üres szóba lehet vinni, így t-ben ugyanannyi a és b betű kell, hogy legyen. Másrészt, ha ab és ba konvex részszavakat egymás után mohón elhagyogatva elakadnánk, az csak úgy lehetne, ha a kapott szóban egyáltalán nem találnánk egymás melletti a és b betűket, ami viszont csak úgy lenne lehetséges, ha eredetileg az a és b betűk száma mégsem egyezne meg, amit épp az előbb zártunk ki.

■

Jegyezzük meg, hogy az előző állításban lényeges megkövetelni, hogy, ha egy (nemüres) $x \in X'$-ből valahogy üres szót tudunk csinálni, akkor azt mohó módon is meg kell tudnunk tenni. Például a $T = \{a, b, c, d, e\}$ betűkből álló T_0^* monoid $X = \{abcde, abc\}$ részhalmazára az $x = abcde \in X$ szót egy lépésben ε-ba tudjuk vinni, de, ha előbb az $abcde \to de$ rövidítést hajtjuk végre, akkor elakadunk. Még akkor sem igaz a mohó rövidíthetőség, ha X elemeire megköveteljük, hogy ilyesmi ne fordulhasson elő, ugyanis az előbbi T_0^*-ra az $X = \{abc, da\}$ halmaz elemei nyilván mohón ε-ba vihetők, viszont az $x = dabca \in X'$ szó olyan, hogy két lépésben ε-ba tudjuk vinni ($dabca \to da \to \varepsilon$), de ha előbb a $dabca \to bca$ rövidítést végeznénk el, akkor szintén elakadnánk.

2.1.2. Állítás.

1. *Legyen T_0^* szabad monoid, $M \leq T_0^*$ és X az M egy generátorrendszere. Ekkor $w \in T_0^*$-ra akkor és csak akkor $w \in M$, ha w előáll X elemeinek összefűzéseként.*

2. *Szabad monoid minden részmonoidjának van (egyértelmű) minimális generátorrendszere.*

3. *Legyen T_0^* szabad monoidban az $X \subseteq T_0^*$ olyan, hogy teljesül rá az előző lemma 4. pontjának feltétele, és az általa generált normális részmonoid legyen $N(X)$. Ekkor minden $\varepsilon \neq x \in N(X)$-re x-nek van X-beli konvex részszava.*

Bizonyítás.

1. Ez azonnal adódik a monoid generátorrendszerének definíciójából, és abból, hogy szabad monoid esetén különböző szavak különbözőek.

2. Tegyük fel, hogy T_0^* szabad monoid M részmonoidjának X generátorrendszere nem minimális. Legyen $X'' \subset X$ az a halmaz, melyre $x \in X''$ esetén $x \notin \langle X \setminus \{x\}\rangle$. Tetszőleges $x \in X \setminus X''$ szóra indukcióval látható, hogy felbontható X''-beli szavak összefűzésére, tehát X'' is generátorrendszere M-nek és nyilván minimális.

   Legyen X és X'' két minimális generátorrendszere T_0^*-nak, és tegyük fel indirekt, hogy létezik $x \in X$, melyre $x \notin X''$. Ekkor x előáll X''-beli elemek legalább kéttagú összefűzéseként: $x = x'_1 \dots x'_n$ (ahol $|x'_i| < |x|$), itt pedig minden x'_i előáll X-beli elemek összefűzéseként, melyek együtt x-nek egy felbontását adják nála rövidebb X-beli szavak összefűzésére, ami ellentmond X minimalitásának, tehát $X \subseteq X''$, és hasonlóan $X'' \subseteq X$, amiből $X'' = X$.

3. Ez nyilvánvaló a 2.1.1 2. és 4. pontjai alapján.

■

2.1.2. Részcsoportok szavai

Legyen S tetszőleges nemüres halmaz, és $G \leq F_S$. Ilyenkor jelöljük $W[G]$-vel a $W(F_S)$ azon szavaiból álló részhalmazát, melyeknek G-beli elemek felelnek meg. Nevezzünk egy $w \in W[G]\setminus\{\varepsilon\}$ szót *egyszerűnek*, ha w tetszőleges $w = w_1w_2$ nemtriviális ($|w_1|, |w_2| > 0$) felbontására $w_1 \in W[G]$ vagy $w_2 \in W[G] \Longrightarrow w_2 = \varepsilon$ vagy $w_1 = \varepsilon$. Jelöljük a $W[G]$-beli egyszerű szavak halmazát $W'[G]$-vel. Lényeges az alábbi egyszerű állítás, amely szerint tetszőleges $w \in W[G]$ szó egyértelműen bontható fel egyszerű szavak összefűzésére:

2.1.3. Állítás. *Legyen $\varepsilon \neq w \in W[G]$ tetszőleges. Ekkor léteznek olyan egyértelmű $u_1, \dots, u_n \in W'[G]$ szavak valamilyen $n \in \mathbb{N}_+$-ra, hogy $w = u_1 \dots u_n$. Nevezzük ezt a felbontást w (G szerint)* maximálisan finom felbontásának.

Bizonyítás. Először is jegyezzük meg, hogy tetszőleges $v, v_1, v_2 \in W(F_S)$ szavakra, ha $v = v_1v_2$, akkor könnyen látható módon, amennyiben v, v_1 és v_2 közül bármelyik kettő eleme $W[G]$-nek, akkor a harmadik is.

Először azt látjuk be, hogy ilyen felbontás létezik minden $w \in W[G]$-re. Legyen k_1 a legkisebb olyan pozitív egész, melyre a w első k_1 darab betűjéből álló u_1 szóra $u_1 \in W[G]$. Ekkor $w = u_1w_1$, és a bevezető megjegyzés alapján $w_1 \in W[G]$ is teljesül. Legyen most k_2 a legkisebb olyan pozitív egész, hogy a w_1 első k_2 betűjéből álló u_2 szóra $u_2 \in W[G]$. Ilyen k_2 biztosan létezik, hiszen legfeljebb $|w_1|$-nek meg kell felelnie. Erre szintén $w_1 = u_2w_2$, és $u_2, w_2 \in W[G]$, ami w-nek a $w = u_1u_2w_2$ felbontását adja. Az eljárást folytatva, mivel $|w|$ véges, egy $w = u_1u_2 \dots u_n$ felbontáshoz jutunk. A konstrukció alapján tetszőleges $1 \leq i \leq n$-re és $1 \leq j < |u_i|$-re u_i-nek az első j betűjéből álló részszava nem $W[G]$-beli, de így a bevezető megjegyzés alapján az utolsó $|u_i| - j$ betűjéből álló részszó sem $W[G]$-beli, és mivel ez minden $1 \leq j < |u_i|$-re igaz, ez épp azt jelenti, hogy $u_i \in W'[G]$.

Most tegyük fel indirekt, hogy $w = u_1 \dots u_k$ és $w = v_1 \dots v_l$ a w-nek két különböző maximálisan finom felbontása. Legyen $1 \leq i \leq \min(k, l)$ a legkisebb olyan index, melyre $|u_i| \neq |v_i|$. Ilyen létezik, különben a kétféle felbontás mégis megegyezne. Ekkor $u_1 \dots u_{i-1} = v_1 \dots v_{i-1}$, tehát u_i és v_i közül az egyik a másiknak a részszava. Az általánosság megszorítása nélkül feltehető, hogy $u_i = v_i x$ valamilyen $x \in W(F_S)$-re. Ekkor azonban a bevezető megjegyzés alapján $x \in W[G]$ is teljesül, vagyis $u_i \notin W'[G]$, tehát w-nek valóban nem lehet két különböző maximálisan finom felbontása.

■

2.1.4. Következmény. *A $W'[G]$ szavak generálják G-t.*

Megjegyezzük, hogy monoidok részmonoidjainak szavaira hasonlóan definiálható az egyszerű szavak és a maximálisan finom felbontás fogalma, és normális részmonoidok esetén ennek egyértelműsége is teljesen hasonlóan bizonyítható, mivel ilyenkor is érvényes, hogy $v = v_1 v_2$ esetén, ha v, v_1 és v_2 közül kettő eleme egy normális részmonoidnak, akkor a harmadik is.

2.2. Csoportszavak rövidítései

2.2.1. Rövidítések típusai

2.2.1. Definíció. Legyen G egy tetszőleges csoport. Azt mondjuk, hogy egy $v \in W(G)$ szónak $u \in W(G)$ egy *mohó rövidítése* G szerint, ha $v = v_1 \dots v_n$ és $I \subseteq \mathbb{N}_n$ olyan, hogy $u = v_{i_1} \dots v_{i_k}$, ahol (i_k) növekvő sorrendben felsorolja I elemeit és $i \in \mathbb{N}_n \setminus I$ esetén $v_i \sim \varepsilon$ (vagyis u olyan részszava v-nek, amely G-ben egységértékű konvex részszavak egymás utáni elhagyásával keletkezik v-ből; jelben: $u \leq_g v$). A v-nek u *általános rövidítése* G szerint, ha $|u| \leq |v|$ és $u \sim v$ (jelben: $u \leq_c v$). Egy $u \in W(G)$ szó *mohón redukált* (vagy rövidített), ha $v \leq_g u \Longrightarrow v = u$, és u *általánosan redukált* (vagy általánosan rövidített), ha $|v| \leq |u|,\ v \sim u \Longrightarrow |v| = |u|$. Egy $v \in W(G)$ szó *mohón redukált hossza* (jelben: $|v|_g$) megegyezik a(z egyik) legrövidebb olyan mohón redukált $u \in W(G)$ szó hosszával, melyre u mohó rövidítése v-nek, v *általánosan redukált hossza* (jelben: $|v|_c$) megegyezik a(z egyik) legrövidebb olyan általánosan redukált u szó hosszával, melyre u általános rövidítése v-nek.

2.2.2. Definíció. Legyen $G = \langle S \mid R \rangle$ egy tetszőleges csoport. Tetszőleges $u, v \in W(G)$ szavak tekinthetők úgy is, mint az $F(S)$ szabad csoport szavai. Ha u szó mohó rövidítése a v szónak $F(S)$ szerint, akkor azt mondjuk, hogy u *szabad rövidítése* v-nek G szerint (jelben: $u \leq_f v$). Ha u mohón redukált szó $F(S)$ szerint, akkor azt mondjuk, hogy u *szabadon redukált* G szerint, továbbá egy v szó *szabadon redukált hossza* alatt v $F(S)$ szerinti mohón redukált hosszát értjük (jelben: $|v|_f$).

2.2.3. Definíció. Két $W(G)$-beli u és v szó *konjugált*, ha a nekik megfelelő G-beli elemek konjugáltak. Egy $w \in W(G)$ szó rövidítetlen konjugáltjain az $u^{-1}wu$ alakú szavakat értjük tetszőleges $u \in W(G)$-re, ezek szabadon redukált szabad rövidítései pedig w *rövidített konjugáltjai.*

Azt mondjuk, hogy egy $w \in W(G)$ csoportszó *ciklikusan rövidített*, ha egyrészt szabadon rövidített, másrészt nem léteznek olyan $u, v \in W(G)$ ($|u| \geq 1$) szavak, hogy $w = u^{-1}vu$. Egy szó ciklikus rövidítése alatt egy tetszőleges olyan rövidített konjugáltját értjük, amely ciklikusan rövidített. (Jegyezzük meg, hogy az előző három rövidítésfogalommal ellentétben egy ciklikus rövidítés általában nem lesz ekvivalens az eredeti szóval.)

2.2.1. *Megjegyzés.* Példák a bevezetett rövidítésfogalmakra: az $\langle a, b, c, d \mid abc, cc\rangle$ csoportban az $abcca^{-1}adab$ szónak szabad rövidítése $abccdab$, mohó rövidítése mind $cdab$ mind $abdab$, általános rövidítése pedig például a cdc vagy a cdc^{-1} szó, ez utóbbinak pedig egy ciklikus rövidítése d (amely már nem lesz ekvivalens az eredeti szóval).

Egy szó általános rövidítései közül a legrövidebbek nem feltétlenül egyértelműek, és ugyanígy a legrövidebb mohó rövidítések sem, pl. az $\langle a, b \mid a^{-1}b^{-1}ab\rangle$ csoportban $baa^{-1}b^{-1}ab$ szónak ab és ba is legrövidebb mohó (és általános) rövidítései. Egy szó mohón redukált mohó rövidítései nem is feltétlenül egyforma hosszúak, pl. a $\mathbf{Z_3} = \langle a \mid a^3\rangle$ ciklikus csoportban az $aaaa^{-1}$ szónak aa és a^{-1} is mohón redukált mohó rövidítései.

Ha egy csoportban a fentiekkel ellentétben mégis minden szónak van egyértelmű legrövidebb általános rövidítése, azt nevezzük a szó általánosan redukált alakjának, ha pedig minden szónak van egyértelmű legrövidebb mohó rövidítése, akkor az legyen a szó mohón redukált alakja. Majd később látni fogjuk, hogy ez lesz a helyzet például szabad csoportok esetében.

2.2.2. Rövidítések alaptulajdonságai

Az alábbiakban összefoglaljuk az előbbi definíciók néhány egyszerűbb következményét:

2.2.1. Állítás.

1. *Az $u, v \in W(G)$ szavakra $u \leq_f v \Longrightarrow u \leq_g v$ és $u \leq_g v \Longrightarrow u \leq_c v$.*
2. *Szabad csoport $u, v \in W(F_S)$ szavaira $u \leq_g v \Longleftrightarrow u \leq_f v$.*
3. *A $\leq_g$, $\leq_f$ és $\leq_c$ relációk reflexívek és tranzitívak, $\leq_g$ és $\leq_f$ antiszimmetrikus. ($\leq_c$-nél $u \leq_c v$ és $v \leq_c u$ esetén csak $|u| = |v|$-re következtethetünk.)*
4. *Mohón, általánosan, szabadon vagy ciklikusan rövidített szó inverze is ugyanilyen.*
5. *Az $u, v \in W(G)$ szavakra $u \leq_g v$ vagy $u \leq_f v$ esetén $u \leq v$ és $u \sim v$.*
6. *Ha $u \leq v$, $u \sim v$ esetén $u = v$, akkor v mohón (és így szabadon) rövidített.*
7. *Ha egy $u \in W(G)$ szó mohón (vagy általánosan vagy szabadon) rövidített, akkor u-nak minden u' konvex részszava is mohón (vagy általánosan vagy szabadon) rövidített.*
8. *Ha $u \in W(G)$-re $u \sim_G \varepsilon$, akkor $v \trianglelefteq u$, $|v| > \frac{1}{2}|u|$, akkor v nem általánosan rövidített.*

9. *Ha $u, v \in W(G)$, $v \leq_c u$ és v általánosan redukált, akkor $|v| = |u|_c$. Mohó rövidítés esetén hasonló állítás nem feltétlenül érvényes.*

Bizonyítás.

1. Az első állítás következik abból, hogy szabad rövidítés speciális mohó rövidítés, a második pedig abból, hogy mohó rövidítéssel az eredeti szónál nem hosszabb, vele ekvivalens szóhoz jutunk (ami épp az általános rövidítés definíciója).
2. A definícióból közvetlenül adódik.
3. A reflexivitás evidens, ha figyelembe vesszük, hogy az üres szó is egységértékű, $|u| \leq |u|$ és $u \sim u$.

   Ha u és v egymás mohó rövidítései, akkor speciálisan $u \leq v$ és $v \leq u$ is érvényes, amiből $u = v$ adódik, a $\leq_f$ antiszimmetriája pedig az előző pontból adódik. Ha u és v egymás általános rövidítései, akkor $|u| = |v|$ mindenesetre világos, a $\langle a, b \mid ab^{-1} \rangle$ csoportban az a és b szavak mutatják, hogy $u = v$ nem feltétlenül igaz.

   Az általános rövidítés tranzitivitása azonnal adódik, a mohó és szabad rövidítésnél annyit kell meggondolni, hogy, ha $w = abc$ az u-nak egy konvex részszava, és u-ból először a $b \sim \varepsilon$-t, majd a kapott szóból $ac \sim \varepsilon$-t hagyjuk el, akkor ezt a két lépést egyszerre is megtehetjük, vagyis, hogy $w \sim \varepsilon$ is érvényes, ami világos abból, hogy ilyenkor $abc \sim ac \sim \varepsilon$.
4. A definíció alapján evidens, hogy egy szó akkor és csak akkor lehet ciklikusan rövidített, ha első és utolsó betűje nem egymás inverzei, ezen tulajdonság megléte vagy hiánya viszont megőrződik a szó invertálásakor is.

   Az $u \leq_c v \Longrightarrow u^{-1} \leq_c v^{-1}$ következtetés evidens, és mivel egységértékű konvex részszó inverze is ugyanilyen, így $u \leq_g v$ vagy $u \leq_f v$ esetén $u^{-1} \leq_g v^{-1}$ valamint $u^{-1} \leq_f v^{-1}$ is következik. Ha most az u szó (bármelyik értelemben) rövidített, és indirekt, u^{-1}-nek létezne egy (ugyanilyen értelemben vett) valódi v rövidítése (vagyis $|v| < \left|u^{-1}\right|$), akkor v^{-1} az u-nak lenne valódi rövidítése, amit kizártunk.
5. Mind mohó, mind szabad rövidítés során egységértékű konvex részszavakat hagyunk el v-ből, így u valóban ekvivalens részszava lesz v-nek.
6. A definíció közvetlen következménye, figyelembe véve az előző pontot.
7. Ha $u = u_1u_2u_3$, és u_2 kicserélhető lenne egy nála rövidebb és vele ekvivalens u_2' mohó (vagy általános vagy szabad) rövidítésére, akkor u is kicserélhető volna a nála rövidebb és vele ekvivalens $u_1u_2'u_3$ mohó (vagy általános vagy szabad) rövidítésére.
8. Legyen $u = u_1vu_2 \sim_G \varepsilon$, ekkor ennek u_2u_1v konjugáltja is egységértékű, és ebből $v \sim (u_2u_1)^{-1}$ következik, és az állítás adódik, figyelembe véve, hogy $\left|(u_2u_1)^{-1}\right| = |u_2u_1| < \frac{1}{2}|u| < |v|$.

9. A 2.2.1. megjegyzésben példát adtunk arra, hogy mohón redukált mohó rövidítések lehetnek különböző hosszúak is, így ilyenkor nem mindegyik hossza egyezhet meg a szó mohón redukált hosszával.

   Általánosan redukált esetben ilyen nem fordulhat elő, hiszen, ha $v, w \leq_c u$, és mondjuk $|v| < |w|$, akkor mivel $v \sim u \sim w$, így $v \leq_c w$ is igaz, vagyis w nem lehet általánosan redukált. Ezt úgy is fogalmazhatjuk, hogy az általánosan redukált általános rövidítés hossza egyértelmű.

■

2.2.2. *Megjegyzés.*

1. Jegyezzük meg, hogy $u \leq v$, $u \sim v$ esetén még akkor sem következtethetünk $u \leq_g v$-re, ha u mohón redukált. Például a $\langle a, b \mid aba^{-1}b^{-1} \rangle$ csoportban $b \sim a^{-1}ba$ és $b \leq a^{-1}ba$, de nem lehet b-t egységértékű konvex részszavak elhagyásával $a^{-1}ba$-ból előállítani.

2. Szabad csoportban az általános rövidítés nem feltétlenül egyezik meg a szabad (és így mohó) rövidítéssel, pl. $\langle a, b, c, d \rangle$-ben $a^{-1}bb^{-1}acaa^{-1}$-nek $cdd^{-1}aa^{-1}$ egy általános rövidítése, de nyilván nem szabad rövidítése, viszont, mint mindjárt látni fogjuk, egy szó pontosan akkor szabadon redukált, ha általánosan redukált.

3. A mohó és az általános rövidítés fogalma monoidok szavaira is teljesen hasonlóan értelmezhető, és a 2.2.1. állítás összes olyan pontja érvényes lesz, amely monoidokra is kimondható, kivéve a 8. pontot, amelynek bizonyításában kihasználtuk az inverz létezését.

A következő állítás a definíciók közvetlen következménye:

2.2.2. Állítás. *A $|\cdot|_g$, $|\cdot|_f$ és $|\cdot|_c : W(G) \to \mathbb{N}$ függvények „félnormák" a következő értelemben:*

$$|u|_g \geq 0,\ |u|_f \geq 0,\ |u|_c \geq 0,$$

$$|\varepsilon|_g = |\varepsilon|_f = |\varepsilon|_c = 0,$$

$$|uv|_g \leq |u|_g + |v|_g,\ |uv|_f \leq |u|_f + |v|_f,\ |uv|_c \leq |u|_c + |v|_c$$

minden $u, v \in W(G)$-re. Ha G nem a triviális csoport, akkor a három közül egyik sem „valódi norma", vagyis létezik $w \in W(G)$, $|w|_g = |w|_f = |w|_c = 0$, hogy $w \neq \varepsilon$.

2.2.3. Ciklikus rövidítés alaptulajdonságai

A következő állítás a ciklikus rövidítés legfontosabb tulajdonságait adja meg:

2.2.3. Állítás. *Minden $w \in W(G)$ szónak van olyan rövidített konjugáltja, amely ciklikusan rövidített. Ha $w \in W(G)$-nek u ciklikusan rövidített konjugáltja, akkor a következő állítások ekvivalensek: (i) v szintén ciklikusan rövidített konjugáltja w-nek; (ii) u és v egymás ciklikus*

permutációi; (iii) v rövidített konjugáltjai w-nek és $|u| = |v|$. A w konjugáltjai közül ezek a legrövidebbek.

Bizonyítás. Ha w nem szabadon rövidített, akkor először vegyük egy w' szabadon redukált szabad rövidítését. Ha most w' nem ciklikusan rövidített, akkor $w' = u^{-1}vu$ valamilyen u, v ($|u| \geq 1$) szavakra, és ekkor v egy rövidebb konjugáltja w'-nek. Ha ez még mindig nem ciklikusan rövidített, akkor az eljárást folytathatjuk, és ez véget ér, mivel $|w|$ véges.

Legyen u ciklikusan rövidített konjugáltja w-nek. (ii) $\Longrightarrow$ (i): Ha u és v egymás ciklikus permutációi, akkor $u = ab$, $v = ba$ valamilyen a, b szavakra, és $v = ba \sim a^{-1}aba = a^{-1}ua$ mutatja, hogy u és v konjugáltak, és sem b első és a utolsó betűje, sem pedig b utolsó és a első betűje nem lehetnek egymás inverzei, mivel ez ellentmondana u ciklikusan (és így szabadon is) rövidített voltának, vagyis v is ciklikusan rövidített.

(i) $\Longrightarrow$ (iii): Ha u és v is ciklikusan rövidített konjugáltjai w-nek, akkor speciálisan egymásnak is konjugáltjai, vagyis $v \sim a^{-1}ua$ (ahol válasszuk a-t is szabadon rövidítettnek), és ennek szabad rövidítése v. Mivel u első és utolsó betűje nem egymás inverzei, így a^{-1} utolsó betűje és u első betűje, valamint u utolsó betűje és a első betűje közül csak legfeljebb az egyik pár olthatja ki egymást, tehát $|v| \geq |u|$. És mivel v első és utolsó betűje sem egymás inverzei, így $a^{-1}ua$-ban az a^{-1} első és a utolsó betűje közül legalább az egyiknek ki kell esnie szabad rövidítéskor, ami csak úgy lehet, ha vagy a^{-1} vagy a teljesen kiesik, tehát $|v| \leq |u|$, amiből végül $|v| = |u|$-t kapjuk (és nyilván v rövidített konjugáltja w-nek).

(iii) $\Longrightarrow$ (ii): Legyen végül u ciklikusan rövidített, v rövidített konjugáltja w-nek és $|v| \leq |u|$. Ekkor az előbbihez hasonlóan u és v egymásnak is konjugáltjai és v az $a^{-1}ua$-nak szabad rövidítése, amiből legalább $2|a|$ betűnek kell kiesnie, viszont az előbbiekhez hasonlóan a^{-1} utolsó és u első, valamint u utolsó és a első betűi közül legfeljebb csak az egyik pár olthatja ki egymást, és ez csak úgy lehet, ha vagy a^{-1} vagy a teljesen eltűnik, és ekkor $|v| = |u|$ is adódik (vagyis w-nek valóban nem lehet u-nál rövidebb konjugáltja). Az első esetben $u = ab$, és ekkor csak $v = ba$, a második esetben pedig $u = ca^{-1}$, és ilyenkor csak $v = a^{-1}c$ lehetséges valamilyen b, c betűkre, ami épp azt jelenti, hogy u és v egymás ciklikus permutációi.

■

2.2.4. Szabad rövidítés további tulajdonságai

Most nézzük a szabad rövidítések néhány további fontosabb tulajdonságát:

2.2.4. Állítás.

1. *Ha $u \in W(G)$ nem szabadon redukált, akkor vannak egymás melletti betűi, melyek egymás inverzei, és tetszőleges $v \leq_f u$ szó előáll u-ból egymás melletti inverz betűpárok egymás utáni elhagyásával is.*

2. *Ha $u, v \in W(F_S)$-re $u \sim v$, és u is és v is szabadon rövidített, akkor $u = v$.*

3. *Egyetlen egy olyan $u \in W(G)$ szó létezik, amely szabad rövidítése v-nek, és hossza megegyezik v szabadon rövidített hosszával. Ezt az egyértelmű u-t v* szabadon redukált alakjának *nevezzük. Ha $u, v \in W(G)$, $v \leq_f u$ és v szabadon redukált, akkor $|v| = |u|_f$. Szabad csoportban minden szónak létezik egyértelmű mohón és általánosan redukált alakja is, és ezek megegyeznek a szabadon redukált alakkal.*

4. *Az $u, v \in W(F_S)$ szavakra $u \sim v$ pontosan akkor, ha létezik $w \in W(F_S)$, hogy $u \leq_f w, v \leq_f w$, és $u \leq_c v$ pontosan akkor, ha az előbbiek mellett még $|u| \leq |v|$ is teljesül.*

   Ha $u \sim v$, és u szabadon rövidített, akkor pedig ebből $u \leq_f v$ is következik.

Bizonyítás.

1. Mivel egy nem szabadon redukált szó mindig tartalmaz nemüres $W(F_S)$-beli egységértékű konvex részszót, így elég belátni, hogy $W(F_S)$-ben egy egységértékű nemüres szónak mindig vannak egymás melletti inverz betűpárjai. Az 1.2.8. definíció szerint az egységértékű szavak épp az xx^{-1}, $x^{-1}x$ $(x \in S)$ alakú inverz betűpárok X halmaza által generált normális részmonoid elemei $W(F_S) = T_0^*$ $(T = S \cup S^{-1})$-ban.

   Mivel X-re teljesül a 2.1.1. lemma 4. pontjának feltétele (figyelembe véve, hogy S és S^{-1} diszjunkt), így a 2.1.2. állítás 3. pontja szerint valóban $N(X)$ minden nemüres eleme tartalmaz X-beli konvex részszót.

   Ha $v \leq_f u$, akkor v előáll u-ból $N(X)$-beli konvex részszavak elhagyásával, és a 2.1.1. lemma 2. és 4. pontjai alapján $N(X)$ elemei pontosan azon szavak, melyeket (mohó módon) X-beli konvex részszavak elhagyásával el lehet tüntetni, így az állítás második fele a konvex részszó tranzitivitásából adódik (ld. 1.2.5. állítás).

2. Tegyük fel indirekt, hogy $u \sim v$, $u \neq v$, és u is és v is szabadon rövidített. Ekkor $uv^{-1} \sim \varepsilon$, és ha x maximális hosszú olyan szó, hogy $u = u_1 x$, $v^{-1} = x^{-1} v_1^{-1}$, akkor mivel, $u \neq v$ miatt u és v^{-1}, mint szavak, nem egymás inverzei, így vagy $|x| < |u|$, vagy $|x| < |v|$ teljesül. Tehát uv^{-1}-ben kihúzva az egymás mellé került inverz betűpárokat, az $u_1 v_1^{-1}$ nemüres szót kapjuk, amelyben már nincsenek egymás melletti inverz betűpárok, ekkor viszont az előző pont szerint $u_1 v_1^{-1} \sim uv^{-1}$ mégsem lehet egységértékű, ami ellentmondás.

3. Az első állítás az előző pont közvetlen következménye, figyelembe véve, hogy $u_1 \leq_f v$, $u_2 \leq_f v$ esetén $u_1 \sim u_2$. A második állítás ennek közvetlen folyománya. Szabad csoportban a mohó és a szabad redukálás, így a mohón és a szabadon redukált alak fogalma is egybeesik. Ha $W(F_S)$-ben v-nek u_1 a szabadon redukált alakja, u_2 pedig egy tetszőleges általánosan redukált általános rövidítése, akkor $u_1 \sim u_2$ és u_2 speciálisan szabadon is redukált, így alkalmazható az előző pont, ami szerint $u_1 = u_2$.

4. Az 1.2.8. állításban láttuk, hogy $F_S \cong T_0^*/N(R)$, ahol $T = S \cup S^{-1}$, és $N(R)$ éppen az egységértékű szavakat tartalmazza, és $T_0^*/N(R) = T_0^*/\sim_{N(R)}$, ahol $\sim_{N(R)}$ az 1.2.2. pont elején definiált kongruencia. Ennek definíciója szerint két u és w $T_0^* = W(F_S)$-beli elem éppen akkor kongruens (vagyis akkor felel meg nekik azonos F_S-beli csoportelem), ha u-ba $N(R)$-beli szavakat beleírva, majd a kapott w szóból $N(R)$-beli konvex részszavakat elhagyva v-hez jutunk, ami épp az állítás első fele, másképp megfogalmazva. Az állítás második fele ezek után közvetlenül adódik az általános rövidítés definíciójából.

   Ha $u \sim v$ és u szabadon rövidített, akkor a v-nek a v' szabadon redukált alakjával u-ra és v'-re teljesülnek a 2. pont feltételei, így $u = v'$, ami épp azt jelenti, hogy $u \leq_f v$ (sőt, u a v-nek a szabadon redukált alakja).

■

A fentiek szerint tehát szabad csoportban egy szó mindhárom értelemben véve ugyanakkor redukált, ugyanannyi a redukált hossza, és létezik a mindhárom értelemben vett redukált alakja, melyek megegyeznek, ezért ilyenkor a jelzőket elhagyva simán redukált szóról, redukált hosszról és az egyértelműen létező redukált alakról beszélhetünk, félreértés lehetősége nélkül. Az általános rövidítés fogalma a 2.2.2. megjegyzés 2. pontja szerint viszont ilyenkor sem feltétlenül egyezik meg a mohó rövidítéssel, a mohó és szabad rövidítés viszont igen. Állapodjunk meg, hogy szabad csoportban simán rövidítés alatt ez utóbbit fogjuk érteni (az általános rövidítést külön jelezzük).

Az előző állítás alapján egy egyszerű karakterizációt is kaphatunk szabad csoportok részcsoportjainak szavaira is:

2.2.5. Következmény. *Legyen F_S szabad csoport, $G \leq F_S$ és $X \subseteq W[G]$ szavak generálják G-t. Ekkor egy $w \in W(F_S)$ szóra akkor és csak akkor teljesül, hogy $w \in W[G]$, ha léteznek az $u, v \in W(F_S)$ szavak, hogy $w \leq_f u, v \leq_f u$ és v előáll X elemei és azok inverzeinek összefűzéseként.*

Ha w szabadon rövidített, akkor pedig ebből $w \leq_f v$ is következik.

Bizonyítás. Az „akkor” irány következik abból, hogy, ha egy részcsoport szavait összefűzzük, vagy, ha egy részcsoportszóhoz hozzáírunk vagy belőle elveszünk F_S-ben egységértékű szavakat, akkor szintén a részcsoporthoz tartozó szót kapunk.

Most nézzük a „csak akkor” irányt, és legyen $w \in W[G]$. Az egyszerűség kedvéért felhasználjuk az 1.2.8. definícióban szereplő ϕ homomorfizmust. Mivel $\phi(w) \in G$, és $\phi(X)$ egy generátorrendszere G-nek, így $\phi(w) = \phi(x_1) \cdot \dots \cdot \phi(x_k)$ valamilyen $x_i \in X \cup X^{-1}$-ekre, és ebből $\phi(w) = \phi(x_1 \dots x_k)$, így $w \sim v := x_1 \dots x_k$ az F_S szerint. Az előző állítás 4. pontja szerint ilyenkor valóban létezik a tétel állításában szereplő $u \in W(F_S)$ szó is, és, ha w szabadon rövidített, akkor a $W(F_S)$-beli $w \sim v$ miatt $w \leq_f v$, szintén az előző állítás 4. pontja miatt.

■

2.2.5. Redukált alakok néhány további tulajdonsága

Az alábbiakban belátunk még néhány hasznos állítást a csoportszavak redukált alakjaival és redukált hosszaival kapcsolatban:

2.2.6. Állítás. *Legyen G tetszőleges, $G = \langle S \mid R \rangle$ rendes prezentációval adott csoport, és $u \in W(G)$ csoportszó, ekkor:*

$$(|u| = 1) \Longrightarrow ((|u|_g = 1) \Longleftrightarrow (|u|_c = 1) \Longleftrightarrow (|u|_f = 1))$$

Ha a prezentáció nem feltétlenül rendes, akkor is érvényes, hogy, ha $u \sim_{F_S} v$, akkor $|u|$ és $|v|$ azonos paritású, és ezért páratlan $|u|$ esetén $|u|_f \neq 0$, így speciálisan $(|u| = 1) \Longrightarrow (|u|_f = 1)$ ilyenkor is következik minden csoportra.

Bizonyítás. Az első állítás abból következik, hogy feltettük, hogy a csoportprezentáció rendes, vagyis S egyetlen eleme sem lehet $N(R)$-beli, így egybetűs szavak nem lehetnek egységértékűek.

A 2.2.4. állítás 1. és 4. pontja alapján $W(F_S)$-ben csak azonos paritású szavak lehetnek ekvivalensek, hiszen inverz betűpárok beírása és elhagyása a szó paritását nem változtatja meg, továbbá vegyük figyelembe, hogy a szabad rövidítés független a prezentációtól.

■

2.2.7. Állítás.

1. *Ha egy csoportban, adott prezentációra nézve, minden szónak létezik egyértelmű mohón redukált alakja (vagy: a legrövidebb mohó rövidítése egyértelmű), akkor minden szónak létezik egyértelmű általánosan redukált alakja is.*

2. *Legyen adva G a $G = \langle S \mid R \rangle$ szóprezentációval, és legyen $u \in W[N(R)]$ (i) az egyik legrövidebb $W[N(R)]$-beli F_S-ben nem egységértékű szó; (ii) az egyik legrövidebb páratlan hosszú $W[N(R)]$-beli szó. Ekkor $x \trianglelefteq u$ esetén x akkor és csak akkor mohón rövidített G szerint, ha $|x| < |u|$, és akkor és csak akkor általánosan rövidített G szerint, ha $|x| \leq \frac{1}{2}|u|$.*

   Ha $u \in W[N(R)]$ (iii) az egyik legrövidebb páros hosszú F_S-ben nem egységértékű $W[N(R)]$-beli szó, akkor $x \trianglelefteq u$, $x \neq \varepsilon$, $x \neq u$ esetén csak akkor lehet x egységértékű G szerint, ha $|u| = 4n + 2$ alakú valamilyen $n \in \mathbb{N}$-re, és $|x| = \frac{1}{2}|u|$; csak akkor lehet x nem mohón rövidített G szerint, ha szintén $|u| = 4n + 2$ alakú és $|x| \geq \frac{1}{2}|u|$; és csak akkor lehet x nem általánosan rövidített G szerint, ha $|x| > \frac{1}{4}|u|$.

3. *Legyen adva G a $G = \langle S \mid R \rangle$ rendes szóprezentációval. Akkor és csak akkor létezik a G csoportban minden szónak egyértelmű mohón redukált alakja, ha G szabad.*

4. *Legyen adva G a $G = \langle S \mid R \rangle$ rendes szóprezentációval. Ha R nemüres, és minden $r \in R$-re $|r|$ páros, akkor nem létezhet minden szónak egyértelmű általánosan redukált alakja.*

5. *Legyen adva G a $G = \langle S \mid R \rangle$ rendes szóprezentációval.*

   Ha minden $r \in R$-re $|r|_f \leq 2$, akkor minden $u \in W(G)$-re $|u|_c = |u|_g$ és egy szó akkor és csak akkor mohón redukált, ha általánosan redukált.

   Ha létezik olyan $r \in R$, hogy $|r|$ páratlan, akkor van olyan $u \in W(G)$ szó is, melyre $|u|_c < |u|_g$.

6. *Pontosan akkor létezik olyan $u \in W(G)$ szó, melyre*

$$|u|_g < |u|_f < |u|,$$

   ha G nem szabad. Szabad csoportra mindig $|u|_c = |u|_g = |u|_f$.

Bizonyítás.

1. Indirekt, ha a G-beli w szónak u_1 és u_2 is két különböző általánosan redukált általános rövidítése, akkor az $u_1 (u_1)^{-1} u_2$ szónak u_1 és u_2 is általánosan redukált mohó rövidítése, amelyeknél így nyilván nincs rövidebb mohó rövidítés, vagyis ilyenkor valóban nem mindig van egyértelmű mohón redukált alak, és egyértelmű legrövidebb mohón redukált alak sem létezhet, mivel $|u_1| = |u_2|$.

2. Először is, jegyezzük meg, hogy mivel u az egyik legrövidebb (vagy az egyik legrövidebb adott paritású) $W[N(R)]$-beli, F_S-ben nem egységértékű szó, és, mivel F_S szerint ekvivalens szavak azonos paritásúak, így u-nak és ez által minden konvex részszavának is mindenképpen szabadon rövidítettnek kell lennie.

   Először a mohó redukálásra vonatkozó (i) és (ii) állításokat látjuk be. Ha $|x| = |u|$, akkor $x \sim_G u \sim_G \varepsilon$, tehát nem lehet mohón rövidített. Most legyen $|x| < |u|$, és nézzük előbb az (i) esetet. Mivel u az egyik legrövidebb $W[N(R)]$-beli szó volt, így egyetlen valódi nemüres konvex részszava sem lehet $W[N(R)]$-beli, vagyis nem lehet G szerint egységértékű, így pedig x-nek sem lehet G szerint egységértékű konvex részszava, ami épp azt jelenti, hogy G szerint mohón rövidített.

   Most nézzük a (ii) esetet. Először is, megjegyezzük, hogy a 2.2.6. állítás szerint páratlan hosszú szó nem lehet F_S szerint egységértékű. Ha $y \trianglelefteq u$, $y \neq \varepsilon$ és $y \neq u$, akkor $u = ayb$ valamilyen $a, b \in W(G)$ $(0 < |ab| < |u|)$ szavakkal, és ilyenkor u-nak a bay konjugáltja is $\in W[N(R)]$, és így G szerint $y \sim a^{-1}b^{-1}$. Most mivel $|y| + \left|a^{-1}b^{-1}\right| = |y| + |ba| = |u|$, és $|u|$ páratlan, így $|y|$ és $\left|a^{-1}b^{-1}\right|$ közül is az egyik páratlan, és mivel mindkét szó szigorúan rövidebb u-nál, így a kettő közül a páratlan nem lehet G-re nézve egységértékű, de mivel ezek ekvivalensek, így egyik sem lehet

egységértékű. Vagyis u-nak egyetlen valódi konvex részszava sem egységértékű, és az előzőhöz hasonlóan ilyenkor minden valódi konvex részszava mohón rövidített.

Most nézzük az általános redukálásra vonatkozó (i) és (ii) állításokat. A 2.2.1. állítás 8. pontja szerint $x \trianglelefteq u$, $|x| > \frac{1}{2}|u|$ esetén valóban nem lehet x általánosan rövidített.

Most legyen $x \trianglelefteq u$, $|x| \leq \frac{1}{2}|u|$, és először vegyük az (i) esetet. Tegyük fel indirekt, hogy x nem általánosan rövidített, és legyen y az x egy általánosan redukált általános rövidítése, amelyre tehát $|y| < |x|$. Mivel $x \sim y$, így $xy^{-1} \sim \varepsilon \Longrightarrow xy^{-1} \in W\,[N(R)]$, ami lehetetlen, hiszen egyrészt $\left|xy^{-1}\right| < 2|x| \leq |u|$, másrészt x és y^{-1} összefűzésekor, ezek szabadon rövidítettsége legfeljebb $2\left|y^{-1}\right| < |x| + \left|y^{-1}\right|$ betű eshet ki, így $xy^{-1} \not\sim_{F_S} \varepsilon$.

Vegyük az általános redukálásra vonatkozó (ii) eset „akkor” részét, és most is tegyük fel indirekt, hogy x nem általánosan rövidített, és y egy általánosan redukált általános rövidítése. Legyen $u = axb$. Ha most $|x|$ és $|y|$ azonos paritású, akkor $u = axb \sim_G u' = ayb$, és $|u'| < |u|$, és szintén páratlan, valamint az (i) esethez hasonló megfontolással $|y| < |x| \leq |ab|$ miatt u' nem lehet egységértékű F_S-ben, ami ellentmondás.

Most legyen $|x|$ és $|y|$ különböző paritású. Ekkor az (i) esethez hasonlóan $xy^{-1} \sim \varepsilon$ egy páratlan hosszú hosszú u-nál rövidebb, F_S-ben nem egységértékű, de G-ben egységértékű szó lenne, ami szintén lehetetlen.

Most tekintsük a (iii) esetet. Ha $|u|$ páros és $|x| \neq \frac{1}{2}|u|$, és $u = axb$, akkor u-nak az $u' = bax$ konjugáltja is egységértékű G-ben, és vagy $|ba| < \frac{1}{2}|u|$, vagy $|x| < \frac{1}{2}|u|$, és G szerint, ha x és ba közül az egyik egységértékű, akkor a másik is, de a kettő közül az $\frac{1}{2}|u|$-nál rövidebből kettőt egymás mellé írva ismét egy u-nál rövidebb páros hosszú, G-ben egységértékű, de F_S-ben nem egységértékű szót kapnánk (mivel könnyen végiggondolhatóan F_S-ben egy nem egységértékű szó nem lehet önmagának az inverze), ami ellentmondás.

Ha most $|u| = 4n$ valamilyen $n \geq 1$-re, akkor viszont amennyiben $|x| = \frac{1}{2}|u|$, akkor x maga egy u-nál rövidebb páros szó, tehát nem lehet G-ben egységértékű. Tehát, összefoglalva, az $|u| = 4n$ esetben u egyetlen valódi konvex részszava sem lehet G-ben egységértékű, és így mindegyik G szerint mohón rövidített.

Az egyetlen lehetőség, hogy u egy valódi konvex részszava egységértékű lehet G szerint, az az, ha $|u| = 4n+2$ alakú valamilyen $n \in \mathbb{N}$-re, és $|x| = \frac{1}{2}|u|$, és így csak akkor lehet nem mohón rövidített, ha szintén $|u| = 4n + 2$ alakú és $|x| \geq \frac{1}{2}|u|$.

Ha most $x \trianglelefteq u$ és $|x| \leq \frac{1}{4}|u|$, és indirekt, x nem általánosan rövidített, és y az egyik általánosan redukált általános rövidítése, akkor $|xy^{-1}xy^{-1}| < 4|x| \leq |u|$, szintén páros és G-ben egységértékű lenne, továbbá az előző esetek gondolatmenete alapján sem xy^{-1}, ez által sem $xy^{-1}xy^{-1}$ nem lehet F_S-ben egységértékű, ami lehetetlen.

3. Tegyük fel, hogy G nem szabad, vagyis $N(R)$ nem csak F_S-ben egységértékű szavakból áll, és vegyünk egy legrövidebb $W\,[N(R)]$-beli, F_S-ben nem egységértékű r szót, amire

tehát $|r| \geq 2$. Legyen r-nek az első $|r|-1$ betűjéből álló konvex részszava q, az utolsó betűje x. Ekkor egyrészt q és x nemüresek, másrészt az előző pont szerint mind q, mind x mohón redukáltak, és ekkor x^{-1} is mohón redukált, valamint $r \sim_G \varepsilon$ miatt $q \sim_G x^{-1}$. Mármost $q = x^{-1}$ nem lehetséges, mivel ekkor $r = x^{-1}x$ lenne, és akkor r F_S-ben egységértékű volna, tehát találtunk két különböző, ekvivalens, mohón redukált szót, és ilyenkor például a qxx^{-1} szónak x^{-1} és q is mohón redukált mohó rövidítése. Szabad csoportban pedig már láttuk a 2.2.4. állítás 3. pontjában, hogy minden szónak van egyértelmű mohón redukált alakja.

4. Legyen tehát adva $G = \langle S \mid R \rangle$ rendes szóprezentációval, és tegyük fel, hogy R nemüres.

   Mivel egy páros hosszú $r \in W(F_S)$ szó inverze, összes konjugáltja, összes szabad rövidítése, és $r \leq_f w$ esetén w is páros hosszú, továbbá páros hosszú szavak összefűzése is ugyanilyen, így egyrészt a 2.2.5. következmény, valamint amiatt, hogy $N(R)$-t generálják az R elemei és ezek konjugáltjai, következik, hogy, ha minden $r \in R$-re $|r|$ páros, akkor minden $W[N(R)]$-beli szó is páros hosszú.

   Legyen $r \in W[N(R)]$ olyan F_S-ben nem egységértékű szó, amelyre $|r|$ minimális. Jelen állítás 2. pontja alapján $x \trianglelefteq r$, $|x| \leq \frac{1}{2}|r|$ esetén x általánosan rövidített. Most mivel tehát $|r|$ páros, így legyen r_1 az első $\frac{1}{2}|r|$ darab betűjéből álló konvex részszava, és r_2 pedig az utolsó $\frac{1}{2}|r|$ darab betűjéből álló konvex részszava.

   Az r_1 és r_2 szavak tehát általánosan rövidítettek, és így $(r_2)^{-1}$ is az, továbbá ezek egyforma hosszúak, valamint $x \sim_G \varepsilon$ miatt $r_1 \sim (r_2)^{-1}$. Ez azt jelenti, hogy r_1 és $(r_2)^{-1}$ egymás általánosan redukált általános rövidítései, és nem lehetnek azonosak, mivel akkor r F_S-ben egységértékű lenne, tehát ilyenkor valóban nem létezhet egyértelmű általánosan rövidített alak.

5. Végig feltehetjük, hogy minden $r \in R$ szabadon rövidített, különben vegyük minden elemnek a szabadon redukált alakját.

   Először tegyük fel, hogy minden $r \in R$-re $|r| = 2$ ($|r| = 0$ és $|r| = 1$ nem lehetséges, mivel a szóprezentáció rendes). Induljunk ki egy tetszőleges $v \in W(G)$ szóból.

   Ha valamilyen $r \in R$ $x^{-1}x^{-1}$ alakú, akkor ebből $x^{-1} \sim x$ és így $x^{-1}x^{-1} \sim xx$ következik, így $x^{-1}x^{-1}$-et R-ben kicserélhetjük xx-re. Ez minden csupa 2-hosszú szavakból álló definiáló reláció-halmazra igaz, vagyis, végig feltehetjük, hogy egyetlen csupa 2-hosszú szavakból álló definiáló reláció-halmazban sem fordulnak elő az előbb említett relációtípusok. (Továbbá azt is végig feltesszük, hogy minden prezentáció rendes, így xx^{-1} és $x^{-1}x$ alakú relációk sem fordulnak elő.)

   Ilyenkor minden $r \in R$-re $r = xy$ valamilyen $x, y \in W(G)$ ($|x| = |y| = 1$) betűkre, vagyis $y \sim x^{-1}$. Nézzük először azt az esetet, amikor $y \neq x$. Ha most v-ben az y betű minden előfordulását x^{-1}-re, y^{-1} minden előfordulását pedig x-re cseréljük, akkor egy az eredetivel ekvivalens v_1 szót kapunk. Viszont a v_1-ben y vagy y^{-1} nem szerepel ,

vagyis $v_1 \in W(\langle S \setminus \{y\} \mid R_1 \rangle)$, ahol R_1-et úgy kapjuk R-ből, hogy abban szintén minden y-t x^{-1}-re, és minden y^{-1}-et x-re cserélünk, és, ha szükséges, elvégezzük az említett átalakításokat is.

Most válasszunk egy tetszőleges $r_1 \in R_1$-t, melyre $r_1 = zt$, és $z \neq t$, és v_1-ben most z minden előfordulását cseréljük ki t^{-1}-re, z^{-1} előfordulásait pedig t-re. Ezt a rekurziót tovább folytatva, végül egy olyan v' szót kapunk, amely v-vel G szerint ekvivalens, de amelyre $v' \in W(\langle S' \mid R' \rangle)$ valamilyen $S' \subseteq S$-re, és minden $r \in R'$-re $r = xx$ alakú valamilyen $x \in S'$-re. Az ilyen r-ekre $x \sim x^{-1}$, így cseréljük ki v'-ben minden $r = xx \in R'$ esetén az x^{-1} összes előfordulását x-re, így végül egy olyan mohón redukált v'' szót kapunk, melyben $r \in R'$, $r = xx$ esetén v''-ben nem szerepel az x^{-1} betű.

Legyen $T \subseteq S' \cup (S')^{-1}$ az a betűhalmaz, melyre $r \in R'$, $r = xx$ esetén $x \in T$, $x^{-1} \notin T$, és $x \in S'$, $\nexists r \in R'$, hogy $r = xx$ esetén $x, x^{-1} \in T$. Álljon most $\mathring{S}$ az összes olyan xx^{-1} és $x^{-1}x$ ($x \in S'$) alakú szóból, melyre nem létezik $r \in R'$, hogy $r = xx$, és nézzük az $\mathring{R} = \mathring{S} \cup R'$ halmazt.

A T-t úgy konstruáltuk, hogy $v'' \in T_0^*$ legyen, és a fentiek alapján tehát minden $t \in W(G)$ szóval van olyan ekvivalens t'' szó, hogy $t'' \in T_0^*$, és, mivel a feltevések szerint R' minden eleme is T_0^*-beli, így $t_1, t_2 \in T_0^*$ esetén $t_1 \sim t_2$ $\langle S' \mid R' \rangle$ szerint akkor és csak akkor, ha $t_1 \sim t_2$ $\langle T \mid \mathring{R} \rangle_M$ szerint, figyelembe véve még, hogyha $r \in R'$, $r = xx$, akkor x-nek a $\langle T \mid \mathring{R} \rangle_M$ monoidban is önmaga az inverze, így egyrészt $\langle T \mid \mathring{R} \rangle_M$ is csoportot alkot, másrészt egy új x^{-1} betű és a megfelelő xx^{-1}, $x^{-1}x$ definiáló relációk hozzávétele $\mathring{R}$-hoz redundáns, és nem változtatja meg a szavak ekvivalenciáját.

Mármost az $\mathring{R}$ szóhalmazra, mint T_0^* részhalmazára könnyen láthatóan teljesül a 2.1.1. lemma 4. állításának feltétele, mivel egy betű legfeljebb két $\mathring{R}$-beli szóban szerepelhet, és ebben az esetben a két szó közül az egyik ab ($|a| = |b| = 1$), a másik pedig ba alakú; és ezért teljesül $N\left(\mathring{R}\right)$-re a 2.1.2. állítás 3. pontja, így $\langle T \mid \mathring{R} \rangle_M$ szavaira a 2.2.4. állítás első 3 pontja is analóg módon érvényes, csak arra figyeljünk, hogy $r \in R'$, $r = xx$ esetén az ottani bizonyításokban x^{-1} helyett x-et írjunk. Ebből következik, hogy $\langle T \mid \mathring{R} \rangle_M$-ben is igaz, hogy egy szó akkor és csak akkor mohón redukált, ha általánosan is redukált, tehát speciálisan minden szó mohón redukált hossza is megegyezik az általánosan redukált hosszával.

Ha most feltesszük, hogy létezik olyan $r \in R$, hogy $|r|$ páratlan, akkor $W[N(R)]$-ben is van páratlan hosszú szó, és ekkor vegyük a legrövidebb $W[N(R)]$-beli, F_S-ben nem egységértékű, páratlan hosszú u szót, és legyen v az u első $|u| - 1$ betűjéből álló részszava, x pedig az u utolsó betűje.

Ekkor jelen állítás 2. pontja alapján v mohón rövidített, x, és így x^{-1} pedig általánosan rövidített, ugyanakkor $u \sim_G \varepsilon$ miatt $v \sim x^{-1}$, és $\left|x^{-1}\right| < |v|$, tehát a mohón rövidített v-nek a nála rövidebb x^{-1} egy általános rövidítése, így valóban $|v|_c < |v|_g$.

6. A szabad csoportra vonatkozó állítást már beláttuk a 2.2.4. állítás 3. pontjában.
   Legyen most G nem szabad, $G = \langle S \mid R \rangle$ egy rendes szóprezentációja, ahol tehát R nem üres, és legyen $r \in R$ tetszőleges. Tudjuk, hogy $r \not\sim_{F_S} \varepsilon$. Ennek szabadon redukált alakja legyen r'. Ekkor tetszőleges $x \in W(G)$-re, amelynek első betűje nem az r' utolsó betűjének inverze, az $u = r'xx^{-1}$ szónak a nála rövidebb $u' = r'$ a szabad rövidítése, és az ennél rövidebb $u'' = \varepsilon$ a mohó rövidítése.

■

2.2.3. *Megjegyzés.* Megjegyezzük, hogy az egyértelmű mohón redukált alakkal ellentétben egyértelmű általánosan redukált alak nem csak szabad csoportban létezhet. Ha például G az olyan $G = \langle S \mid R \rangle$ rendes szóprezentációval van megadva, ahol R véges, és $\sum_{r \in R} |r|$ minimális, továbbá minden $s \in S$ betű valamint az inverze együtt összesen legfeljebb egyszer fordul elő az R-beli szavakban, és minden $r \in R$-re $|r|$ páratlan, akkor meg lehet mutatni, hogy szintén létezik minden szónak egyértelmű általánosan redukált alakja, ehhez azonban a normálosztók szavaira vonatkozó bonyolultabb állítások szükségesek, melyek nem férnek bele jelen dolgozat kereteibe. A szerző sejtése, hogy az ilyen tulajdonságú szóprezentációval adott csoportokra akkor és csak akkor létezik egyértelmű általánosan redukált alak, ha az említett feltételek teljesülnek.

2.3. Kiejtési és rövidítési feltételek

A kombinatorikus csoportelméletben fontos szerepet játszanak az ún. kis kiejtési feltételek ('small cancellation conditions'[1]), ez azonban messzire vezet, itt csak az ún. metrikus kiejtési feltételeket említjük:

2.3.1. Definíció. Legyen $H \subseteq W(F_S)$ olyan nemüres halmaz, melynek minden eleme szabadon rövidített, $\varepsilon \notin H$ és $h \in H$ esetén $h^{-1} \in H$. Azt mondjuk, hogy valamilyen $0 < \lambda < 1$ ($\lambda \in \mathbb{R}$)-ra H *λ-kiejtő*, ha $h_1, h_2 \in H$, $h_1 \neq h_2$, $h_1 = bc_1$, $h_2 = bc_2$ esetén $|b| \leq \min(\lambda |h_1|, \lambda |h_2|)$, és *szigorúan λ-kiejtő* (vagy másképpen: teljesíti a $C'(\lambda)$ metrikus kis kiejtési feltételt), ha $\leq$ helyett itt $<$ szerepel.

Tetszőleges $H \subseteq W(F_S)$ nemüres, $\varepsilon \notin H$ halmazra teljesül az *első Nielsen-rövidítési feltétel*, ha $h_1, h_2 \in H$, $h_1 h_2 \not\sim \varepsilon$ esetén $|h_1 h_2|_f \geq \max\left(|h_1|_f, |h_2|_f\right)$, és teljesül H-ra a *második Nielsen-rövidítési feltétel*, ha $h_1, h_2, h_3 \in H$, $h_1 h_2 \neq \varepsilon$, $h_2 h_3 \neq \varepsilon$ esetén $|h_1 h_2 h_3|_f > |h_1|_f + |h_3|_f - |h_2|_f$[2].

2.3.1. Állítás.

1. *Ha $H \subseteq W(F_S)$ nemüres halmaz, melynek minden eleme szabadon rövidített, $\varepsilon \notin H$ és $h \in H$ esetén $h^{-1} \in H$, akkor H akkor és csak akkor $\frac{1}{2}$-kiejtő, ha teljesül rá az első Nielsen-rövidítési feltétel.*

[1] Ezek elméletének alapjait ld. pl. [12], V. fejezetében, de hasznos összefoglalást nyújt a wikipedia [17] cikke is.

[2] Részletesebben ld. [12, p. 6]

2. *Ha $H \subseteq W(F_S)$-re teljesülnek az előbbi feltételek, és H még szigorúan is $\frac{1}{2}$-kiejtő, akkor H-ra teljesül mindkét Nielsen-rövidítési feltétel.*

3. *Ha $H \subseteq W(F_S)$ nemüres, $\varepsilon \notin H$ halmazra teljesülnek a Nielsen-rövidítési feltételek, akkor $h = h_1 \dots h_k$ $(h_1, \dots, h_k \in H)$ esetén, ahol egymás melletti h_i-k nem ejtik ki egymást, teljesül, hogy $|h|_f \geq \max\left(|h_1|_f, \dots, |h_k|_f\right)$.*[3]

   Ha H nemüres, $\varepsilon \notin H$, $h \in H \Longrightarrow h^{-1} \in H$, és H szigorúan $\frac{1}{2}$-kiejtő, akkor az előbbi állításban $k > 1$ esetén $|h|_f > \max\left(|h_1|_f, \dots, |h_k|_f\right)$ írható.

4. *Ha $H \subseteq W(F_S)$ nemüres, $\varepsilon \notin H$ halmazra $h \in H \Longrightarrow h^{-1} \notin H$, és H-ra teljesülnek a Nielsen-rövidítési feltételek, akkor H a $\langle H \rangle \leq F_S$-t szabadon generálja.*

5. *Ha $\varepsilon \neq h \in W(F_S)$ ciklikusan rövidített, akkor $n \in \mathbb{N}$ esetén $|h^n|_f = |h^n| = n|h|$, és, ha $\varepsilon \neq h$ szabadon rövidített, akkor $n \in \mathbb{N}$ esetén $|h^n|_f < \left|h^{n+1}\right|_f$, így minden szabadon rövidített $\varepsilon \neq h \in W(F_S)$ esetén $H = \{h, h^{-1}\}$-re teljesülnek a Nielsen-rövidítési feltételek, speciálisan ilyenkor minden $\varepsilon \neq w \in W\,[\langle h \rangle]$-ra $|w| \geq |h|$.*

Bizonyítás.

1. Legyen $H \subseteq W(F_S)$ a megadott feltételeknek megfelelő halmaz, és tegyük fel először, hogy $\frac{1}{2}$-kiejtő, és legyen $h_1, h_2 \in H$ olyan, hogy $h_1 h_2 \not\sim \varepsilon$. Legyen k a maximális olyan természetes szám, melyre igaz, hogy h_1 utolsó k betűjéből álló b részszava inverze a h_2 első k betűjéből álló (b^{-1}) részszavának. Mivel H $\frac{1}{2}$-kiejtő volt, és $(h_1)^{-1}$ is $\in H$, így $k \leq \min\left(\frac{1}{2}|h_1|, \frac{1}{2}|h_2|\right)$, figyelembe véve, hogy most h_1 és h_2 szabadon rövidítettek. Így most $|h_1 h_2|_f = |h_1| + |h_2| - 2k \geq \max\left(|h_1|, |h_2|\right)$, és épp ezt kellett megmutatni.
   Ha H a feltételeknek megfelelő, akkor mivel $h_1, h_2 \in H$, $h_1 \neq h_2$, $h_1 = bc_1$, $h_2 = bc_2$ esetén $\left|(h_1)^{-1} h_2\right|_f = |h_1| + |h_2| - 2|b|$, így ez akkor és csak akkor $\geq \max\left(|h_1|, |h_2|\right)$, ha $|b| \leq \min\left(\frac{1}{2}|c_1|, \frac{1}{2}|c_2|\right)$, így, ha H nem $\frac{1}{2}$-kiejtő, akkor nem teljesülhet minden $(h_1)^{-1}$ és h_2 párra az első Nielsen-rövidítési feltétel sem.

2. Azt kell még belátni, hogy, ha a feltételeket teljesítő H szigorúan $\frac{1}{2}$-kiejtő, akkor teljesül rá a második Nielsen-rövidítési feltétel is.
   Ha H szigorúan $\frac{1}{2}$-kiejtő, és $h_1, h_2 \in H$, $h_1 h_2 \neq \varepsilon$, akkor $h_1 h_2$-ben mind h_1-ből, mind h_2-ből csak kevesebb, mint a betűinek a fele eshet ki, így $h_3 \in H$, $h_2 h_3 \neq \varepsilon$ esetén a $h_1 h_2 h_3$ összefűzésben az inverz betűpárok kiejtése során h_2-nek legalább egy középső betűjének meg kell maradnia, és így a h_1 és h_3 betűi nem ejthetik ki egymást. Legyen tehát x és y maximális olyan, hogy $h_1 = g_1 x^{-1}$, $h_2 = x g_2 y^{-1}$, $h_3 = y g_3$, ekkor $|x|, \left|y^{-1}\right| < \frac{|h_2|}{2}$ miatt $|h_1 h_2 h_3| = |h_1| + |h_2| + |h_3| - 2|x| - 2|y| > |h_1| - |h_2| + |h_3|$.

[3] Ld. még [12, p. 9], Proposition 2.13.

3. Feltehetjük, hogy H minden eleme szabadon is rövidített, és így az egyszerűség kedvéért a tételben $|\cdot|_f$ helyett $|\cdot|$ is írható, ellenkező esetben H minden elemét helyettesíthetjük egy szabadon redukált szabad rövidítésével. Legyen $h = h_1 \dots h_k$ $(k \geq 2)$ olyan, hogy egymás melletti h_i-k nem oltják ki egymást ($k = 1$-re az állítás triviális), és legyenek x_i-k $(1 \leq i \leq k-1)$ maximális hosszú olyan szavak, hogy $h_1 = g_1 x_1$, $1 < i < k$ esetén $h_i = (x_{i-1})^{-1} g_i x_i$ és $h_k = (x_{k-1})^{-1} g_k$. Az előző pont bizonyításában látottakhoz hasonlóan, a második Nielsen-rövidítési feltétel miatt $|g_i| > 0$, és csak egymás melletti h_i-k között történhet kiejtés. Most legyen $1 \leq l \leq k$ tetszőleges. Mivel H az első pont szerint $\frac{1}{2}$-kiejtő, így tudjuk, hogy $1 \leq i < l$ esetén

$$|x_i| \leq \frac{1}{2} |h_i| , \tag{2.1}$$

és $l \leq i \leq k-1$ esetén

$$|x_i| \leq \frac{1}{2} |h_{i+1}| , \tag{2.2}$$

így

$$|h_1 \dots h_l \dots h_k|_f =$$

$$= |h_1| + \dots + |h_l| + \dots + |h_k| - 2|x_1| - \dots - 2|x_{i-1}| - 2|x_i| - \dots - 2|x_{k-1}| \geq |h_l| , \tag{2.3}$$

és mivel ez minden $1 \leq l \leq k$-ra igaz, így ez adja az állítást.

Ha H nemüres, $\varepsilon \notin H$, $h \in H \implies h^{-1} \in H$, és H szigorúan is $\frac{1}{2}$-kiejtő, akkor H-ra az előző pont szerint teljesülnek a Nielsen-kiejtési feltételek, és az iménti bizonyítást elmondva rá, a $k \geq 2$ esetben, (2.1)-ben, (2.2)-ben és (2.3)-ban $\leq$ és $\geq$ helyett mindenütt $<$ és $>$ írható.

4. Legyen $\overline{H}$ a H elemeiből és azok inverzeiből álló halmaz. Könnyen láthatóan H-ra és $\overline{H}$-ra pontosan ugyanakkor teljesülnek a Nielsen-rövidítési feltételek. Mivel H generálja a $\langle H \rangle$ halmazt, így tekinthetjük a $\langle H \rangle$ halmaz H szerinti $W_H(\langle H \rangle)$ szavainak a halmazát. Az előző pont szerint most tetszőleges $h = h_1 \dots h_k$, $h_i \in \overline{H}$ szóra, ha egymás melletti h_i-k nem oltják ki egymást (vagyis nem egymás inverzei), akkor $W(F_S)$-ben tekintve $|h|_f \geq \max\left(|h_1|_f, \dots, |h_k|_f\right) \geq 1$, tehát speciálisan $h \not\sim \varepsilon$, márpedig minden $h \in W_H(\langle H \rangle)$ előáll ilyen alakban, kivéve esetleg az egységértékű szavakat. Ez azt jelenti, hogy egy $h \in W_H(\langle H \rangle)$ szó csak akkor lehet egységértékű, ha vannak benne egymás melletti inverz H-betűpárok, így minden egységértékű szó vagy az üres szó, vagy pedig szabadon rövidíthető $W_H(\langle H \rangle)$-ban, vagyis egy szó pontosan akkor egységértékű, ha szabadon redukált szabad rövidítése az üres szó, amiből pedig az adódik, hogy $u, v \in W_H(\langle H \rangle)$ esetén $u \sim v$ $\langle H \rangle$ szerint akkor és csak akkor, ha $u \sim v$ F_H szerint, így a $\phi : W(F_H) \to W_H(\langle H \rangle)$ (identikus) izomorfizmus egyértelműen kiterjeszthető

az $F_H \cong W(F_H)/\sim_{F_H}$ csoportra $\phi' : F_H \cong W(F_H)/\sim_{F_H} \to W_H(\langle H\rangle)/\sim_{\langle H\rangle} \cong \langle H\rangle$ izomorfizmusként, speciálisan tehát $\langle H\rangle$ izomorf az F_H szabad csoporttal, vagyis szabad.

5. Ha $h \neq \varepsilon$ ciklikusan rövidített, akkor első és utolsó betűi nem lehetnek egymás inverzei, tehát minden $n \in \mathbb{N}$-ra h^n szintén ciklikusan rövidített.

   Most legyen $h \neq \varepsilon$ szabadon rövidített, és legyen $x \trianglelefteq h$ a leghosszabb olyan, melyre $h = x^{-1}cx$. Ekkor $c \neq \varepsilon$ és első és utolsó betűje nem olthatja ki egymást, így c ciklikusan rövidített, vagyis $|c^n|_f = n|c|$, és ebből

$$|h^n|_f = \left|\left(x^{-1}cx\right)^n\right|_f = \left|x^{-1}c^nx\right|_f = \left|x^{-1}c^nx\right| =$$
$$= 2|x| + n|c|,$$

   és ebből az is adódik, hogy $\left|c^{n+1}\right| > |c^n|$. Mivel $H = \left\{h, h^{-1}\right\} = \left\{x^{-1}cx, x^{-1}c^{-1}x\right\}$ és $c \neq \varepsilon$, így $\left|x^{-1}\right| < \frac{|h|}{2}$, vagyis H egy a feltételeknek megfelelő szigorúan $\frac{1}{2}$-kiejtő halmaz, így teljesülnek rá a Nielsen-rövidítési feltételek.

■

2.3.1. *Megjegyzés.*

1. Be lehet látni, hogy egy szabad csoport minden végesen generált részcsoportjának van olyan generátorrendszere, amelyre az előző állítás 4. pontjának a feltételei teljesülnek (bármely véges generátorrendszer átvihető ilyenbe az ún. Nielsen-transzformációk segítségével), vagyis szabad csoport minden végesen generált részcsoportja is szabad,[4] és ezt felhasználva be lehet látni, hogy mint már említettük, ez tetszőleges részcsoportra is igaz.[5]

2. Jegyezzük meg, hogy generált normálosztó szavai általában még az előbbieknél némileg szigorúbb feltételek esetén sem viselkednek olyan „szépen", mint egy generált részcsoport szavai.

   Például az $\langle a, b, c, d, e, f, g, h, i\rangle$ szabad csoportban a

$$H = \{abcde, c^{-1}b^{-1}fgh, e^{-1}d^{-1}h^{-1}g^{-1}i\}$$

   halmaz esetén H minden eleme ciklikusan rövidített, a H elemeinek és ezek inverzeinek összes ciklikus permutációiból álló halmaz szigorúan $\frac{1}{2}$-kiejtő, ugyanakkor az előző állítás 3. pontjának az a megfelelője, hogy H-beli szavak és ezek konjugáltjainak összefűzéséből álló szó szabad rövidítése legalább olyan hosszú lenne, mint valamelyik H-beli szó, nem marad igaz, például:

[4] Ld. [12, p. 7], Proposition 2.6..
[5] Nielsen-Schreier tétel, ld. [12, p. 8], Proposition 2.11..

$$(abcde)\left(e^{-1}d^{-1}\left(c^{-1}b^{-1}fgh\right)de\right)\left(e^{-1}d^{-1}h^{-1}g^{-1}i\right) = afi.$$

Sőt, az sem feltétlen igaz, hogy, ha h_1 és h_2 egymás ciklikusan rövidített konjugáltjai, akkor $|h_1h_2|_f \geq \min(|h_1|, |h_2|)$, például $\left(t^{-1}a^{-1}a^{-1}a^{-1}a^{-1}\right)(aaaata) = t^{-1}a^{-1}ta$, így a 2.3.1. állítás 5. pontjának analogonja (vagyis, hogy tetszőleges ciklikusan rövidített $\varepsilon \neq h \in W(F_S)$ esetén a h és h^{-1} összes ciklikus permutációiból álló halmazra teljesülnének a Nielsen-rövidítési feltételek, és így $N(\{h\})$ minden nemüres eleme legalább $|h|$ hosszú lenne) sem mindig igaz.

Némileg bonyolultabb feltételek teljesülése esetén azonban már ezekről is kimondhatóak bizonyos gyengébb állítások, például, ha $\varepsilon \notin H \subseteq F_S$, H minden eleme ciklikusan rövidített, és a H halmaz elemeinek és ezek inverzeinek összes ciklikus permutációiból álló $\widetilde{H}$ halmaz szigorúan $\frac{1}{6}$-kiejtő, akkor minden $N(H)$-beli nemüres szónak valamilyen $h \in H$-val van egy olyan közös u konvex részszava, hogy $|u| > \frac{1}{2}|h|$. Ez alapján, ilyen esetben a $G = \langle S \mid H \rangle$ csoportban az ún. szóprobléma megoldására egy egyszerű algoritmus is adható (Dehn algoritmusa).[6]

[6]Ld. Greendlinger lemma: [12, p. 250], Theorem 4.5., és Dehn algoritmusa: [12, p. 246], V./4.

3. fejezet

Rácsutak és Ballot-számok

3.1. Rácsutak típusai

A rácsutak egy fontos bizonyítási segédeszközt fognak nyújtani a 4.2.6. problémánk megoldása során, különösen annak speciális esetei, a Dyck-utak. Jegyezzük meg, hogy a szakirodalomban az elnevezések, többek közt például a Dyck-út definíciói nem egységesek. Ebben a munkában az általunk itt megadott definíciókhoz fogjuk konzekvensen tartani magunkat, függetlenül attól, hogy egyes felhasznált, hivatkozott szakirodalomban ez nem feltétlenül lesz azonos a miénkkel.

A rácsutak teljesen általános definíciója a következő:[1]

3.1.1. Definíció. Egy d-dimenziós $n \geq 1$-lépéses L **rácsút** S-beli megengedett lépésekkel egy $v_0, v_1, \ldots, v_n \in \mathbb{Z}^d$ pontsorozat, hogy minden $i \in \mathbb{N}_n$-re $v_i - v_{i-1} \in S$. A lépésszámra használhatjuk az $|L| = n$ jelölést is.

A v_i pontokat a rácsút csúcsainak, a $v_i - v_{i-1}$ vektorokat pedig a rácsút lépéseinek vagy éleinek is nevezzük. Két rácsutat megállapodás szerint azonosnak tekintünk, ha azonos a dimenziójuk és a lépésszámuk, továbbá lépéseik páronként megegyeznek (vagyis a kezdőpont szabadon eltolható). Ilyen értelemben beszélhetünk az (egyértelmű) 0-lépéses rácsútról, mely egyetlen (tetszőleges) pontból áll, és minden S-re S-megengedett, jelöljük ezt ε-nal.

Jegyezzük meg, hogy amennyiben mást nem mondunk, akkor alapértelmezés szerint rácsúton síkbeli rácsutat értünk (vagyis $d = 2$), továbbá kezdőpontnak az origót tekintjük ($v_0 = (0, 0)$).

Ha $L_1 = (u_0, \ldots, u_n)$ és $L_2 = (v_0, \ldots, v_m)$ két d-dimenziós rácsút, akkor ezek összefűzésén vagy kompozícióján azt az $L_1 \star L_2$-vel jelölt d-dimenziós $(w_0, \ldots, w_{n+m})$ rácsutat értjük, melyre $0 \leq i \leq n$ esetén $w_i = u_i$ és $n \leq i \leq (n+m)$ esetén $w_i = v_{i-n} + (u_n - v_0)$. (Megjegyzés: Könnyen látható, hogy tetszőleges L-re $\varepsilon \star L = L \star \varepsilon = L$.)

A rácsutak közül különösen fontosak azok, melyek az origóból indulnak és amelyeknél két lépést, egy jobbra és egy felfelé történő egységnyi lépést engedélyezünk, vagyis melyre

[1] Ld. [14, p. 28].

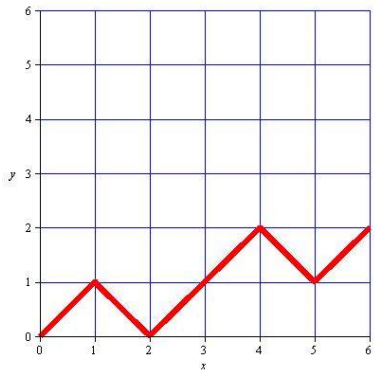
$$S = \{(1,0),(0,1)\},$$

ezeket a továbbiaknak **JF-rácsutaknak** hívjuk (Ld. 3.3 ábra)

A **Dyck-utak** olyan speciális síkbeli rácsutak, melyeknél a kezdőpont az origó, a megengedett lépések a következők:

$$S = \{(1,1),(1,-1)\},$$

továbbá nem lehet pontja a nyílt alsó félsíkban (szigorúan a zárt felső félsíkban fekszik; ld. 3.1 ábra). További feltételként általában fel szokás tenni, hogy a végpont az x-tengelyen fekszik, minket viszont érdekelni fognak az olyan Dyck-utak is, melyekre ez nem feltétlenül igaz. Állapodjunk meg, hogy amennyiben ezt *nem* tesszük fel, akkor nevezzük ezen utak halmazát *általános* Dyck-utaknak, ha pedig feltesszük, akkor *egyszerű* Dyck-utaknak. Ha külön nem kötjük ki, akkor a továbbiakban Dyck-úton alapból mindig általános Dyck-utat értünk.



3.1. ábra. Példa Dyck-útra

Még egy fontos rácsút típust érdemes megemlíteni:

3.1.2. Definíció. Az olyan $\mathbb{Z}^2$-beli rácsutakat, melyek a $v_0 = (0,0)$ kezdőpontból indulnak, és a megengedett lépések halmaza:

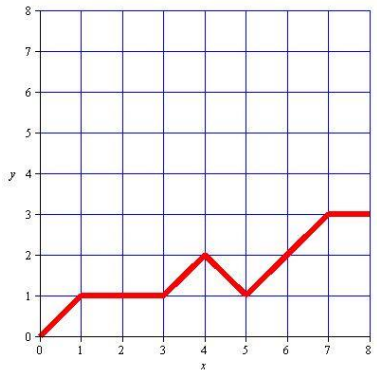
$$S = \{(1,0),(1,1),(1,-1)\},$$

Motzkin-utaknak nevezzük (ld. 3.2 ábra). Ha a v_n végpont y-koordinátája 0, akkor *egyszerű*, különben *általános* Motzkin-utakról beszélünk. Ha külön nem említjük, akkor Motzkin-úton mindig egyszerű Motzkin-utat értünk.

3.1.1. *Megjegyzés.* A Dyck-utak speciális Motzkin-utak, ahol az $(1,0)$ lépést nem használjuk fel.

3.1.1. Rácsutakra vonatkozó alapvető kombinatorikai tulajdonságok

3.1.1. Állítás. *Egy n-hosszú egyszerű Dyck-út a $(2n,0)$ pontban végződik.*



3.2. ábra. Példa Motzkin-útra

Bizonyítás. Evidens, ha észrevesszük, hogy a megengedett S-beli mindkét lépés első koordinátája $= 1$.

■

Jegyezzük meg, hogy bijekció van a Dyck-utak és azon JF-utak között, melyek sosem haladnak az átló egyenese ($y = x$) felett (de érinthetik azt). Ezt adja meg a következő:

3.1.2. Állítás. *Az*

$$F = (n, m) \mapsto \left(\frac{n+m}{2}, \frac{n-m}{2} \right)$$

függvény bijekciót ad a Dyck-utak halmazából azon JF-utak halmazába, melyeknek nincs pontja az $y = x$ (átló) egyenese felett. Ez a függvény az $(1, 1)$ utakat $(1, 0)$ utakba, az $(1, -1)$ utakat $(0, 1)$ utakba, az $y = 0$ egyenest (x-tengelyt) pedig az $y = x$ egyenesbe (átlóba) viszi. Ha a T Dyck-út az (N, M) pontban végződik, akkor az $F(T)$ JF-út az $\left(\frac{N+M}{2}, \frac{N-M}{2}\right)$ pontban, speciálisan a $(2N, 0)$ pontban végződő L egyszerű Dyck-út $F(L)$ képe pedig az (N, N) pontban fog.

Ezen függvény inverze az

$$F^{-1} = (n, m) \mapsto (n + m, n - m)$$

függvény.

Bizonyítás. Mivel

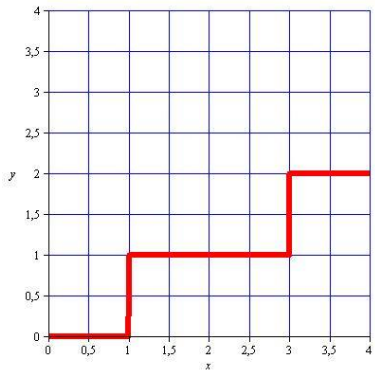
$$\frac{n+m}{2} + \frac{n-m}{2} = n, \qquad \frac{n+m}{2} - \frac{n-m}{2} = m$$

$$\frac{(n+m)+(n-m)}{2} = n, \qquad \frac{(n+m)-(n-m)}{2} = m,$$

így $F \circ F^{-1} = F^{-1} \circ F = \mathrm{id}$, tehát F és F^{-1} bijektívek, és egymás inverzei. Ha v_k és v_{k+1} egy Dyck-út két egymást követő pontja, akkor $v_{k+1} - v_k = (1,1)$ esetén $F(v_{k+1} - v_k) = F(1,1) = (1,0)$, $v_{k+1} - v_k = (1,-1)$ esetén pedig $F(v_{k+1} - v_k) = F(1,-1) = (0,1)$, ez az $F(0,0) = (0,0)$-al együtt azt jelenti, hogy F Dyck-utakat valóban a JF-utak halmazába képez. Az $F(n,0) = \left(\frac{n}{2}, \frac{n}{2}\right)$, $F(n,n) = (n,0)$, $F^{-1}(n,0) = (n,n)$ és a $F^{-1}(n,n) = (2n,0)$ összefüggésekből látszik, hogy az $y = 0$ és az $y = x$ egyenesek valóban egymásra képződnek F-nél és F^{-1}-nél. Mivel F folytonos, így elég egyetlen, a két egyenes által határolt, első síknegyedbe eső pontra ellenőrizni, hogy a képe ugyanitt van (pl. $F(2,1) = \left(\frac{3}{2}, \frac{1}{2}\right)$), ez már adja az állítást. $F(2N,0) = (N,N)$ triviális.

■

Egy a fenti bijekció szerint egymásnak megfelelő Dyck-utat és JF-utat mutatnak a 3.1 és 3.3 ábrák.



3.3. ábra. A 3.1 Dyck-útnak megfelelő JF-rácsút

3.1.3. Következmény. *Tetszőleges, az (m,n) pontban végződő Dyck-útra az $\frac{m+n}{2}$ és $\frac{m-n}{2}$ értékek mindig egészek, így m és n paritása megegyezik. Ha m és n azonos paritású, akkor mindig létezik egy a $(0,0)$-ból (m,n)-be menő Dyck-út.*

Egy a $(0,0)$-ból az (m,n) pontba menő Dyck-út összesen $\frac{m+n}{2}$ felfelé és $\frac{m-n}{2}$ lefelé lépésből áll.

Bizonyítás. A 3.1.2. állításban definiált F bijekció alapján világos, hogy, ha létezik egy (m,n) pontban végződik Dyck-út, akkor $\frac{m+n}{2}$ és $\frac{m-n}{2}$ csak egészek, így pedig m és n csak azonos paritásúak lehetnek.

Ha m és n azonos paritású, akkor a $(0,0)$ pontból $\left(\frac{m+n}{2}, \frac{m-n}{2}\right)$ pontba menő JF-út képe F^{-1}-nél egy (m,n) pontban végződő Dyck-út lesz.

Szintén az előző állításban lévő bijekció szerint, mivel a $(0,0)$-ból az (m,n) pontba menő Dyck-utak kölcsönösen megfeleltetésben állnak a $(0,0)$-ból az $\left(\frac{m+n}{2}, \frac{m-n}{2}\right)$ pontba menő JF-utakkal, és felfelé útból jobbra út, lefelé útból felfelé út lesz, így a megfelelő koordináták leolvasásából adódik az állítás.

■

3.1.4. Állítás. *A $(0,0)$ pontból az (n,m) pontba vezető JF-rácsutak száma $\binom{n+m}{m}$.*

Bizonyítás. A $(0,0)$-ból az (n,m)-be menő JF-rácsutak minden esetben n db jobbra ($(1,0)$) és m db felfelé ($(0,1)$) útból tevődnek össze, továbbá minden ilyen JF-rácsút (n,m)-ben végződik. Ebből látszik, hogy a $J=(1,0)$ és $F=(0,1)$ kódolás felhasználásával, bijekció van az n db J és m db F betűből álló, $n+m$ hosszú szavak és a kérdéses rácsutak között. Ezen szavak száma pedig épp $\binom{n+m}{m}$.

■

Speciálisan a $(0,0)$ pontból az (n,n) pontba $\binom{2n}{n}$ darab JF-rácsút létezik.

3.2. Catalan-számok

Tekintsük a következő kombinatorikai problémákat:

1. Hányféleképpen lehet egy $(n+2)$ oldalú konvex síkbeli sokszöget az átlóival háromszögekre bontani, ha az egymással forgásszimmetrikus, de nem egybeeső megoldások különbözőnek számítanak?

2. Álljon egy ábécé két betűből, X-ből és Y-ból. Vegyük azokat a $2n$ hosszú szavakat, melyekre igaz, hogy az első k betűből álló részszó legalább annyi X betűt tartalmaz, mint Y-t, bármely $1 \leq k \leq 2n$-re.

3. Hányféleképpen lehet n darab '(' nyitó és n darab ')' csukó zárójelből helyesen zárójelezett kifejezést alkotni?

4. Tekintsük azokat a JF-rácsutakat $\mathbb{Z}^2$-en, melyek $(0,0)$-ból (n,n)-be mennek (a megengedett lépések tehát: jobbra ($(1,0)$) és a felfelé ($(0,1)$)), továbbá sosem mennek az átló fölé (de érinthetik azt). Az 3.1.2. állításban láttuk, hogy ez ekvivalens a $(0,0)$-ból $(2n,0)$-ba menő Dyck-utak számával.

A fenti feladatokban az a közös, hogy mind az ún. Catalan-számokra vezetnek. Ugyanis mindegyik esetben a megoldás kielégíti a következő rekurziót (Segner-rekurzió[2]), melynek (természetesen) egyértelmű megoldása van:

$$C_0 = 1 \quad \textbf{és} \quad C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i}, \ \textbf{ha } n \geq 0. \tag{3.1}$$

Az ezt kielégítő C_i számokat hívjuk **Catalan-számoknak**.

[2]Pontosabban az indexek 2-vel el vannak tolva a Segner-rekurzióhoz képest, ld. [21] vagy [14, p. 49]

Itt csak azt mutatjuk meg, hogy a $(0,0)$ és $(2n,0)$ közötti Dyck-utak számát megadó D_n számok kielégítik a rekurziót, mivel nekünk csak erre lesz szükségünk, és a többi esetben is teljesen hasonlóan működik a dolog[3]. Az egyszerűség kedvéért alkalmazzuk az $U = (1,1)$ és $D = (1,-1)$ jelöléseket. Először is, jegyezzük meg, hogy 0-hosszú Dyck-útból egyetlen darab van, tehát D_0 választható 1-nek. Egy tetszőleges $2n$ $(n > 0)$ hosszú T Dyck-utat bontsunk fel 4 részútra:

1. Az első részút álljon egyetlen U felfelé lépésből (ezt megtehetjük, mivel minden Dyck-út egy felfelé lépéssel kezdődik), amely tehát $(0,0)$ pontból $(1,1)$ pontba mutat.

2. Ha a második lépés szintén U, akkor a második részút álljon a T Dyck-út origó és az x-tengelyre való első visszatérése közé eső szakaszának lépéseiből, kivéve az első U és az utolsó D lépést. (Mivel a feltétel szerint a Dyck-út a $(2n,0)$ pontban végződik, így ilyen biztosan van.) Ha a második lépés D, akkor a második részút üres út.

3. A harmadik részút legyen az T Dyck-út x-tengelyre való első visszatérésének utolsó (D) lépése.

4. A negyedik részút legyen az T x-tengelyre való első visszatérését követő része, továbbá üres út, amennyiben az első visszatérés megegyezik T végpontjával.

Ezáltal T-t egyértelműen felbontottuk 4 részútra, ahol könnyű látni, hogy az első mindig U, a második egy (esetleg üres) T_1 egyszerű Dyck-út, a harmadik mindig D, a negyedik pedig szintén egy (esetleg üres) T_2 egyszerű Dyck-út, és T_1 valamint T_2 hosszának összege $(2n-2)$, és mind az T_1, mind az T_2 hossza 0 és $(2n-2)$ között változhat.

Megfordítva, egy U lépés, egy $2k$ $(0 \le 2k \le 2n-2)$ hosszú T_1 egyszerű Dyck-út, egy D lépés, továbbá egy $(2n-2-2k)$ hosszú T_2 egyszerű Dyck-út egymás után fűzése mindig egy $2n$ hosszú egyszerű Dyck-utat eredményez, és ha ezt vesszük $k = 0, \ldots, n-1$ számok mindegyikére, akkor az összes $2n$ hosszú egyszerű Dyck-utak megkapjuk.

Ez azt jelenti, hogy bijekció van a $2n$ hosszú egyszerű Dyck-utak, és az $U \star T_1 \star D \star T_2$ alakú utak között, ahol T_1 egy $2k$ $(0 \le k \le n-1)$ hosszú, T_2 pedig egy $(2n-2-2k)$ hosszú egyszerű Dyck-út. Ezt számszerűsítve:

$$D_n = \sum_{k=0}^{n-1} D_k D_{n-1-k} \quad (n > 0),$$

vagyis valóban fennáll a kérdéses rekurzió.

A Catalan-számok explicit alakját a következő pont 3.3.1. tételének speciális eseteként fogjuk megkapni.

[3]Ld. pl. [15, p. 173].

3.3. Ballot-számok

Tekintsük a következő feladatot (Bertrand szavazási problémája):

1. Az eredeti probléma a következő: Egy választás során egy A jelölt p szavazatot kap és B jelölt q szavazatot kap ($p > q$), mennyi a valószínűsége, hogy A a választás során végig szigorúan előnyben volt B-hez képest?

2. Egy kicsit módosítva a kérdést, feltehetjük azt is, hogy mennyi a valószínűsége, hogy a választás során B sosem vezetett A-hoz képest, de a szavazatok száma lehetett azonos.

A kérdésre a választ az ún. Ballot-számok segítségével fogjuk megadni:

3.3.1. Tétel. *Azon JF-utak számát, melyek a $(0,0)$ pontból az (m,n) pontba mennek, és sosem haladnak az $y = x$ átló fölött (de azt érinthetik), a következő képlet adja meg:*

$$B^*(m,n) := \frac{m-n+1}{m+1}\binom{m+n}{n}.$$

Ez megegyezik azon Dyck-utak számával, melyek a $(0,0)$ pontból az $(m+n, m-n)$ pontba mennek.

Azon JF-utak számát pedig, melyek szintén a $(0,0)$ pontból az (m,n) pontba mennek, de (az origót kivéve) szigorúan az $y = x$ átló alatt futnak, az ún. Ballot-számok[4] *adják meg:*

$$B(m,n) := B^*(m-1,n) = \frac{m-n}{m+n}\binom{m+n}{n}$$

Ez azon Dyck-utak számával egyezik, melyek a $(0,0)$ pontból az $(m+n, m-n)$ pontba futnak, és az origón kívül nem érintik az x-tengelyt.

Speciálisan, $m = n$ esetén az első képlet a C_n Catalan-számokat adja vissza:

$$C_n = B^*(n,n) = B(n+1,n) = \frac{1}{n+1}\binom{2n}{n},$$

ez tehát a $(0,0)$ pontból az (n,n) pontba tartó átló alatt haladó, azt esetleg érintő JF-utak, valamint a $(0,0)$ pontból a $(2n,0)$ pontba tartó Dyck-utak száma.

Bizonyítás. A megoldáshoz az ún. André-féle tükrözési módszert fogjuk használni.[5]

Nevezzük *rossz* útnak azokat az utakat, melyek a $(0,0)$ pontból az (m,n) pontba úgy jutnak el, hogy közben keresztezik az átlót is. Ezen utak mindenképpen érintik az $y = x+1$ egyenest. Minden rossz útra van egy első olyan P pont, amely tehát az $y = x+1$ egyenesen

[4]Megjegyzés: Valójában nem igazán helyes magyarul a Ballot-szám elnevezés, hiszen Ballot nem egy vezetéknév, hanem azt jelenti, hogy 'szavazás', 'szavazócédula', így pl. a „szavazási szám" elnevezés helyesebb volna, de a szakirodalommal való egyezőség és az elfogadott magyar elnevezés hiánya miatt mégis meghagytuk az eredetit.

[5]Ld. pl. [8, p. 1] vagy [7, p. 2]

fekszik. Az André-féle tükrözési módszer lényege, hogy a rácsút P pont utáni szakaszát tükrözzük az $y = x+1$ egyenesre. Mivel, ha P pont x-koordinátája k, akkor y-koordinátája $k+1$, így eredetileg P-t megelőzően épp eggyel több felfelé utat tettünk meg, mint jobbra vezető utat, tehát, mivel összesen n felfelé és m jobbra vezető út van, így a P után következő szakaszban $n-k-1$ darab felfelé út, és $m-k$ jobbra vezető út található. Tükrözést követően a felfelé vezető utak jobbra vezető útba mennek át és fordítva, tehát, ha a P utáni szakaszt tükrözzük, akkor az eredeti utunk végpontja (m, n) helyett $(n-1, m+1)$ lesz. Mármost ezek alapján vegyük észre, hogy az eredeti (m, n)-be vezető rossz utak és az összes $(0, 0)$-ból $(n-1, m+1)$-vezető utak között bijekció van, melyet az $y = x+1$ egyenesre való tükrözés ad meg. Valóban, valamennyi $(n-1, m+1)$-be vezető út szükségképpen érinti az $y = x+1$ tengelyt, tehát tükrözve az $y = x + 1$-re egy rossz (m, n)-be vezető utat kapunk! A rossz utak száma tehát (ld. 3.1.4. állítás):

$$\binom{(n-1)+(m+1)}{m+1} = \binom{m+n}{m+1} = \binom{m+n}{n-1}$$

A jó utakat végül a rossz utaknak az összes útból való kivonása adja meg:

$$\binom{m+n}{n} - \binom{m+n}{n-1} = \binom{m+n}{n} - \frac{n}{m+1}\binom{m+n}{n} =$$

$$= \binom{m+n}{n}\left(1 - \frac{n}{m+1}\right) = \frac{m-n+1}{m+1}\binom{m+n}{n},$$

ami épp az első bizonyítandó összefüggés.

Most vegyük azokat az utakat, melyek a $(0, 0)$ pontból az (m, n) pontba úgy jutnak el, hogy az origót követően nem érintik az $y = x$ egyenest, végig alatta futnak. Vegyük észre, hogy minden ilyen utat fel lehet bontani két részútra: az első részút egy darab jobbra útból áll, a második részút pedig az $(1, 0)$ pontból az (m, n) pontba megy úgy, hogy végig az $y = x - 1$ egyenes alatt halad és érintheti azt. Vagyis:

$$B(m, n) = B^*(m-1, n) = \frac{m-n}{m}\binom{m+n-1}{n} =$$

$$= \frac{m-n}{m} \cdot \frac{m}{m+n}\binom{m+n}{n} = \frac{m-n}{m+n}\binom{m+n}{n}$$

A Dyck-utakra vonatkozó állítások a 3.1.2-ban szereplő bijekció, a Catalan-számok képlete pedig egyszerű behelyettesítés alapján következnek. Mivel a $(0, 0)$ és a $(2n, 0)$ közötti Dyck-utak számát így kétféleképpen is meghatároztuk, így speciálisan a (3.1) rekurzió explicit megoldását is megkaptuk.

■

3.3.2. Állítás. *Bertrand eredeti szavazási problémájának a megoldása, ha a szavazategyenlőség nem megengedett:*

$$\frac{p-q}{p+q},$$

ha pedig megengedett:

$$\frac{p-q+1}{p+1}.$$

Bizonyítás. Ábrázoljuk a választás alakulását egy JF-rácsút formájában: induljunk ki a $(0,0)$ pontból, és valahányszor az A jelöltre érkezik szavazat, haladjunk az $(1,0)$ irányba, ha pedig a B jelöltre, akkor a $(0,1)$ irányba. Így a végén nyilván a (p,q) pontba fogunk eljutni. Az, hogy A végig szigorúan vezet B-hez képest, éppen azt jelenti, hogy végig szigorúan az $y=x$ átló alatt haladunk. Ezen rácsutak számát az előző tétel szerint éppen a $B(p,q)$ Ballot-szám adja meg. Az összes olyan lehetőséget, ahol A p darab, B pedig q darab szavazatot szerez, a $\binom{p+q}{p}$ érték adja meg, így a valószínűség:

$$\frac{B(p,q)}{\binom{p+q}{p}} = \frac{p-q}{p+q},$$

ami épp az állítás szövege szerinti érték.

Ha a szavazategyenlőség is megengedett, akkor ugyanezzel a gondolatmenettel a választ a

$$\frac{B^*(p,q)}{\binom{p+q}{p}} = \frac{p-q+q}{q+1}$$

érték adja meg, ami szintén megegyezik a keresett értékkel.

■

3.3.3. Állítás. *A $B(m,n)$ Ballot-számok eleget tesznek a következő rekurziónak:*

$$B(m,n) = B(m-1,n) + B(m,n-1), \text{ ha } 0 \le n < m,$$

ahol a $B(0,0)=1$ kezdeti feltételt és a $B(m,-1)=0$, $B(m,m)=0$ $(0<m)$ határfeltételeket tesszük.

Bizonyítás. A $B(m,n)$ értékek azon JF-utak számát adják meg, melyek a $(0,0)$ pontból az (m,n) pontba mennek, és az origót kivéve szigorúan az átló alatt futnak, ezek $n=m=0$ és $0 \le n < m$ esetekben vannak értelmezve. A $B(m,n)$ számok értelmezését a többi egész

számpárra is kiterjeszthetjük, $B(m,n) = 0$-ként, hiszen ezen (m,n) pontokba egyáltalán nem lehet eljutni a megadott módon.

Mivel JF-út esetében egy (m,n) pontba csak az $(m-1,n)$ és $(m,n-1)$ pontból vezethet él, így $B(m,n) = B(m-1,n)+B(m,n-1)$ következik minden (m,n) számpárra, az előbbi kiterjesztést figyelembe véve.

Ha a $B(m,n)$ értékeket megadjuk minden $(m,-1)$ $(0 < m)$ és minden (m,m) $(0 \leq m)$ esetén, akkor könnyen láthatóan, a rekurzió alapján minden (m,n) $(0 \leq n < m)$ pontpárra is egyértelműen meg van határozva. A $B(0,0) = 1$ triviális.

■

3.3.4. Állítás. *A Catalan-számok generátorfüggvénye:*

$$C(x) = \sum_{n=0}^{\infty} C_n x^n = \frac{1-\sqrt{1-4x}}{2x},$$

ahol C_n az n-edik Catalan-szám.

Bizonyítás. Ld. pl. [2, p. 535] (3.4).

■

3.4. Dyck-utak visszatéréseinek száma

3.4.1. Definíció. Legyen T egy Dyck-út, amelynek pontjai $v_0 = (0,0), \ldots, v_n$. Azt mondjuk, hogy T *primitív*, ha pontosan a v_0 és a v_n csúcsok második koordinátája 0.

A T Dyck-út k-szorosan visszatérő ($k \in \mathbb{N}^+$), ha pontosan $k+1$ olyan csúcsa van, amelynek második koordinátája 0.

A 4.2.6. kérdésének megválaszolásában fontos szerepet játszik a következő lemma, melynek bizonyításánál a [13] 5. pontjában szereplő gondolatmenetet követjük:

3.4.1. Lemma. *A $(0,0)$ pontból az (n,m) pontba tartó, k-szorosan visszatérő Dyck-utak száma különböző paritású n és m esetén 0, azonos paritású n és m esetén pedig megegyezik a $(0,0)$ pontból az $(n-k, m+k)$ pontba menő primitív Dyck-utak számával.*

Ezen közös értéket a

$$B\left(\frac{n+m}{2}, \frac{n-m}{2} - k\right)$$

Ballot-szám adja meg. Speciálisan, $m = 0$ esetén ez a

$$B\left(\frac{n}{2}, \frac{n}{2} - k\right)$$

-ba megy át.

Bizonyítás. Azt mindenesetre láttuk a 3.1.3. állításban, hogy pontosan azonos paritású n és m esetén létezhet Dyck-út $(0,0)$-ból (n,m)-be. Tegyük most fel tehát, hogy n és m azonos paritású. Először is, jegyezzük meg, hogy egy (n,m) pontban végződő Q Dyck-út pontosan akkor k-szorosan visszatérő, ha felbontható k db nemtriviális primitív Dyck-út és egy az $y=m$ egyenesen végződő origóra nem visszatérő $\overline{Q}$ Dyck-út kompozíciójára ($Q = Q_1 \star \cdots \star Q_k \star \overline{Q}$, $k \in \mathbb{N}$). Minden ilyen primitív Q_i ($i \in \mathbb{N}_k$) Dyck-út kölcsönösen egyértelmű módon megfeleltethető egy-egy olyan Q_i' Dyck-útnak, amely az origón kívül nem érinti az x-tengelyt, és a végpontja az $y=1$ egyenesen található (egyszerűen az utolsó lefelé menő éleket elhagyjuk). Mármost a $Q' = Q_1' \star \cdots \star Q_k' \star \overline{Q}$ Dyck-út az $y = m+k$ egyenesen végződik, és hossza k-val kevesebb, mint Q hossza, vagyis $n-k$. Megfordítva, tetszőleges, az $y=m+k$ egyenesen végződő, x-tengelyre nem visszatérő T Dyck-út egyértelműen felbontható k db, 1 magasságban végződő, az x-tengelyt az origón kívül nem érintő T_i ($i \in \mathbb{N}_k$) és 1 db, az x-tengelyt az origón kívül nem érintő, k magasságban végződő $\overline{T}$ Dyck-út kompozíciójára, legyen ugyanis T_i a T-nek azon részútja, amelynek kezdőpontja az a pont, ahol T utoljára érinti az $y = i-1$ egyenest, a végpontja pedig az, ahol T utoljára érinti az $y=i$ egyenest, a $\overline{T}$ pedig a T-nek az $y=k$ egyenest utoljára érintő pontját követő szakasz. A kétféle Dyck-utak halmazai tehát azonos számosságúak.

A 3.1.2. állításbeli bijekció szerint a $(n-k, m+k)$ pontban végződő primitív Dyck-utak száma megegyezik a $\left(\frac{n+m}{2}, \frac{n-m}{2} - k\right)$ pontban végződő, szigorúan az átló alatt haladó JF-utak számával, ezek számát pedig a 3.3.1. tétel szerint épp a $B\left(\frac{n+m}{2}, \frac{n-m}{2} - k\right)$ érték adja meg.

■

4. fejezet

Szórövidítések kombinatorikai tulajdonságai

4.1. Csoportszavak Dyck- és Motzkin-útjai

Az alábbiakban definiálni fogunk minden $w \in W(F_S)$ csoportszóhoz egy hozzá tartozó $D(w)$ Dyck-utat, mely a későbbiekben fontos lesz számunkra. Azonban nem csak szabad csoportok szavaihoz tudunk hozzárendelni rácsutakat, ezért a definíciót általánosabban fogjuk megadni. Ekkor viszont nem biztos, hogy minden w szóhoz létezik megfelelő Dyck-út a szabad csoportokéval egyező értelemben, Motzkin-út viszont minden csoport szavaira létezni fog. (Pontosabban, egy szóhoz kétféle utat definiálunk, melyek közül az egyik mindig Dyck-út, a másik pedig általában Motzkin-út lesz.)

Ehhez szükségünk lesz a következő egyszerű lemmára:

4.1.1. Lemma. *Legyen G tetszőleges csoport, és $w, a \in W(G)$ csoportszavak, hogy $|a| = 1$.*

1. *Tetszőleges G csoportra:*

$$||wa|_c - |w|_c| \leq 1.$$

2. *Ha a $G = \langle S \mid R \rangle$ rendes szóprezentációra, minden $r \in R$-re $|r|$ érték páros, akkor*

$$||wa|_c - |w|_c| = 1.$$

Ha ez a feltétel nem teljesül, vagyis létezik $r \in R$, hogy $|r|$ páratlan, akkor léteznek $w, a \in W(G)$ ($|a| = 1$) szavak, hogy

$$||wa|_c - |w|_c| = 0.$$

3. Tetszőleges G csoportra:

$$||wa|_f - |w|_f| = 1$$

4. Ha $G = \langle S \mid R \rangle$ rendes szóprezentációra, létezik olyan $r \in R$, hogy $|r|$ páratlan, akkor léteznek olyan $w, a \in W(G)$ szavak, hogy $|a| = 1$, és

$$||wa|_g - |w|_g| > 1.$$

Bizonyítás.

1. Legyen $w' = wa$. Tegyük fel először indirekt, hogy $|w'|_c \geq |w|_c + 2$. Legyen u egy a w-vel ekvivalens, u' pedig egy a w'-vel ekvivalens általánosan redukált szó, ekkor a feltevés szerint tehát $|u'| \geq |u| + 2$. Viszont $w' = wa$ miatt $u' \sim ua$, és $|ua| = |u| + 1 < |u'|$, ami ellentmond annak, hogy u' általánosan redukált, tehát $|u'| \leq |u| + 1$.

   Most azt tegyük fel, hogy $|w|_c \geq |w'|_c + 2$, és szintén legyen u egy w-vel, u' pedig w'-vel ekvivalens általánosan redukált szó, ilyenkor tehát $|u| \geq |u'| + 2$. A $w' = wa$ miatt $w = w'a^{-1}$, így $u \sim u'a^{-1}$ is teljesül, így viszont egy u-nál rövidebb, vele ekvivalens szót kaptunk, ami szintén lehetetlen, tehát valóban $|u| \leq |u'| + 1$. A kettőt összefoglalva, adódik az állítás.

2. Az előző bekezdésből következik, hogy

$$||wa|_c - |w|_c| \leq 1,$$

   csak azt kell belátni, hogy ez nem lehet 0. Tegyük fel indirekt, hogy a $w' = wa$ jelöléssel, $|w'|_c = |w|_c$. Ha u egy a w-vel ekvivalens, u' pedig egy a w'-vel ekvivalens általánosan redukált szó, akkor tehát $|u| = |u'|$. A $w' = wa$-ból következik, hogy $u' \sim ua$, így $(u')^{-1}ua$ egy $2|u| + 1$, vagyis páratlan hosszú szó, amely az egységgel lenne ekvivalens, ami nem lehetséges akkor, ha R minden eleme páros hosszú, mivel a 2.2.7. állítás 4. pontjának bizonyításában láttuk, hogy minden $W[N(R)]$-beli szó páros.

   Most tegyük fel, hogy létezik $r \in R$, hogy $|r|$ páratlan, ekkor $W[N(R)]$-ben is létezik tehát páratlan hosszú szó, és vegyük a legrövidebb páratlan hosszú $w \in W[N(R)]$ szót. Mivel a szóprezentáció rendes volt, így $|r| \geq 3$. A 2.2.7. állítás 2. pontjában láttuk, hogy $x \trianglelefteq w$, $|x| \leq \frac{1}{2}|w|$ esetén x általánosan redukált.

   Ha $|r| = 2n+1$ valamilyen $n \in \mathbb{N}$, $n \geq 1$-re, akkor legyen r első n betűjéből álló konvex részszava p, az $(n+1)$. betűje a, az utolsó n betűjéből álló konvex részszava pedig q. Ekkor tehát a p, a q és ebből következően a q^{-1} szavak is általánosan rövidítettek, és mivel $r \sim_G \varepsilon$ miatt $pa \sim_G q^{-1}$, így $|p|_c = |pa|_c = n$, és épp ilyet akartunk mutatni.

3. A $G = \langle S \mid R \rangle$ csoport szavainak szabad rövidítései úgy tekinthetők, mintha ezek $W(F_S)$-beli szavak lennének, és ott bármelyik rövidítést vennénk (mivel mint láttuk, ilyenkor mindhárom rövidítésfogalom megegyezik), tehát az állítást elegendő szabad csoportokra, és szabad rövidítés helyett általánosan rövidített hosszra belátni, ami azonnal következik abból, hogy a 2. pont feltétele szabad csoportokra triviálisan teljesül.

4. Ha létezik olyan $r \in R$, hogy $|r|$ páratlan, akkor vegyük a legrövidebb páratlan hosszú $v \in W\left[N(R)\right]$ szót, és, mivel a szóprezentáció rendes, így $|v| \geq 3$.

   Ha w a v-ből az utolsó betűje elhagyásával keletkező szó, és a a w utolsó betűje, akkor a 2.2.7. állítás 2. pontja alapján w mohón rövidített, ugyanakkor $|wa|_g = |v|_g = 0$, és $|w|_g = |w| = |v| - 1 > 1$. Ebből már adódik az állítás.

■

4.1.1. Definíció. Legyen G tetszőleges csoport és $w \in W(G)$ egy csoportszó. Azt mondjuk, hogy $M(w)$ a w szóhoz tartozó *általánosan redukáló Motzkin-út*, ha tetszőleges $1 \leq k \leq |w|$-re az $M(w)$ Motzkin-út v_k csúcsának y-koordinátája megegyezik a w szó első k betűjéből álló $w^{(k)}$ részszavának általánosan redukált hosszával.

A w-hez tartozó $D(w)$ *szabadon redukáló Dyck-út* pedig olyan, hogy $1 \leq k \leq |w|$-re $D(w)$ v_k csúcsának y-koordinátája a $w^{(k)}$ szabadon redukált hosszával egyezik meg.

Jegyezzük meg, hogy az előző definíció értelmes, mivel az előző lemma alapján egy szóhoz egy betű hozzáírása a szó általánosan rövidített hosszát legfeljebb 1-gyel, míg szabadon rövidített hosszát pontosan 1-gyel változatja meg, tehát $M(w)$ valóban Motzkin-út, $D(w)$ pedig Dyck-út, és ezek rekurzívan előállíthatók. Szintén az előző lemmából látszik, hogy $M(w)$ definíciójában általánosan redukált hossz helyett mohón redukált hosszt írva, általában nem kapunk Motzkin-utat, ezért ezt nem definiáljuk.

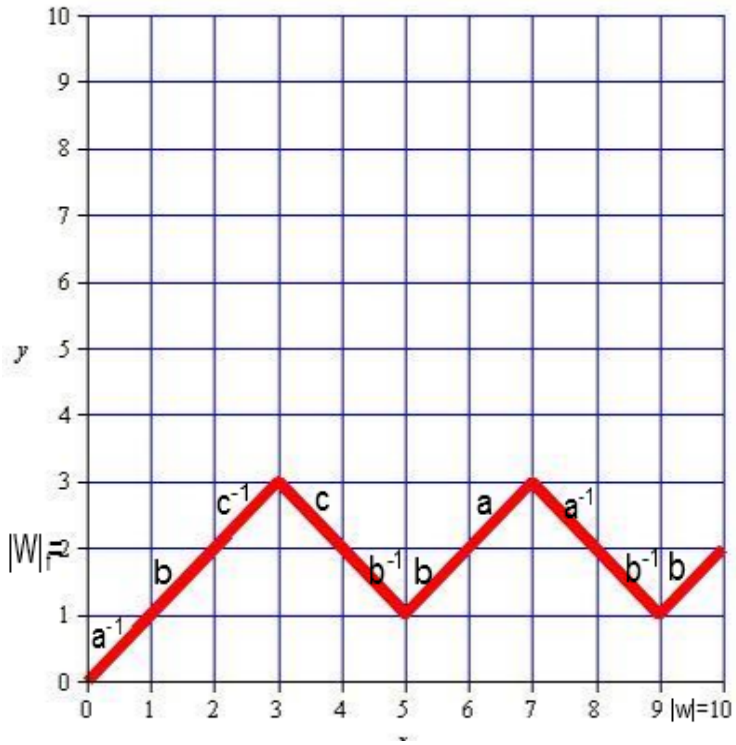
A 4.1. ábrán az $\langle a, b, c \rangle$ szabad csoportbeli $w = a^{-1}bc^{-1}cb^{-1}baa^{-1}b^{-1}b$ szó Dyck-útját láthatjuk, melynek szabadon redukált alakja $a^{-1}b$.

Érdemes lehet még tudni, hogy a kétféle rácsút mikor eshet egybe, és mikor lesz $M(w)$ speciálisan Dyck-út is, ezt adja meg a következő:

4.1.2. Lemma.

1. *Ha egy G csoport nem szabad, akkor létezik olyan $w \in W(G)$ szó, melynek általánosan redukáló Motzkin-útja és szabadon redukáló Dyck-útja különböző rácsút. Szabad csoportra minden szó általánosan redukáló Motzkin-útja egyben Dyck-út is lesz és megegyezik a szó szabadon redukáló Dyck-útjával.*

2. *Legyen G a $G = \langle S \mid R \rangle$ rendes szóprezentációval adott. Akkor és csak akkor lesz G minden általánosan redukáló Motzkin-útja Dyck út, ha minden $r \in R$-re $|r|$ páros.*



4.1. ábra. Az $\langle a, b, c\rangle$ szabad csoportbeli $w = a^{-1}bc^{-1}cb^{-1}baa^{-1}b^{-1}b$ szó Dyck-útja

Bizonyítás.

1. Ha a G csoport nem szabad, akkor a $G = \langle S \mid R\rangle$ rendes szóprezentációra R nem üres, legyen $r \in R$ tetszőleges. Mivel a prezentáció rendes, így $|r|_f \neq 0$. Ez viszont épp azt jelenti, hogy r általánosan redukáló Motzkin-útjának a végpontja az x-tengelyre esik, míg a szabadon redukáló Dyck-útjának nem, tehát a kettő nem egyezhet meg. Ha G szabad, akkor az állítás abból következik, hogy minden szóra a háromféle rövidítésfogalom megegyezik.

2. A 4.1.1. lemma 2. pontjában láttuk, hogy, ha a feltétel teljesül, akkor $w, a \in W(G)$ ($|a| = 1$)-re:

$$||wa|_c - |w|_c| = 1$$

lesz. Ez épp azt jelenti, hogy egy betű hozzáírása egy szó általánosan redukált hosszát csak 1-gyel vagy (-1)-gyel változtathatja meg, vagyis $M(w)$ valóban Dyck-út lesz. A 4.1.1. lemma 2. pontjában azt is láttuk, hogy ha viszont létezik $r \in R$, amelyre $|r|_c$ páratlan, akkor van olyan $w, a \in W(G)$ ($|a| = 1$), hogy

$$||wa|_c - |w|_c| = 0,$$

ami épp azt jelenti, hogy a általánosan redukáló Motzkin-út két szomszédos csúcsának magassága megegyezik, vagyis nem lehet Dyck-út.

■

Jegyezzük meg, hogy ha G szabad, akkor minden $w \in W(G)$ szó általánosan redukáló Motzkin-útja és szabadon redukáló Dyck-útja egybeesik, és ezt az egyértelmű $D(w)$ Dyck-utat ilyenkor egyszerűen a w Dyck-útjának is nevezzük.

Használni fogjuk még az $M(w)$ Motzkin-út és $D(w)$ Dyck-út esetében az élek súlyozásának fogalmát. Egy a v_{i-1} csúcsból a v_i csúcsba vezető él súlyán a w szó i-edik betűjét értjük. A kérdést azonban fordítva is feltehetjük: adott egy tetszőleges M Motzkin út (illetve D Dyck-út), és hány olyan $W(G)$-beli w szó létezik, melynek M a általánosan redukáló Motzkin-útja (illetve D a szabadon redukáló Dyck-útja)? Ilyenkor azt kell megválaszolnunk, hogy az M Motzkin-út (illetve D Dyck-út) éleit hányféleképpen tudjuk megsúlyozni a $W(G)$ betűivel úgy, hogy az így előálló szónak éppen M legyen az általánosan redukáló Motzkin-útja (illetve D a szabadon redukáló Dyck-útja). Ezt a kérdést a következő pontban vizsgáljuk, de mivel általános esetben ez rendkívül nehéz, így szabad csoportokra fogunk szorítkozni.

4.2. Rövidítések száma szabad csoportban

A következő kombinatorikai problémát szeretnénk megoldani: Legyen adott egy F_S szabad csoport, ahol $|S| = g \in \mathbb{N}^+$. Adott n és k számokra ($0 \leq k \leq n,\ k \in \mathbb{N}, n \in \mathbb{N}$) hány olyan $w \in W(F_S)$ szó létezik, melyre $|w| = n$ és $|w|_c = k$?

Mivel minden $g \in \mathbb{N}^+$-ra izomorfia erejéig egyetlen g darab elem által generált szabad csoport létezik, így ez az érték csak a g, n és k természetes számoktól függ, jelöljük ezt $S(g, n, k)$-val, feladat tehát ennek meghatározása.

Az előző pontban láttuk, hogy egy $w \in W(F_S)$ szabad csoportszónak egyféle $D(w)$ rácsút feleltethető meg a fenti módokon, amit w Dyck-útjának nevezünk. Az előző pont utolsó bekezdése alapján arra a kérdésre fogjuk keresni a választ, hogy egy adott, tetszőleges D Dyck-úthoz hányféle olyan $W(F_S)$-beli betűkkel történő súlyozás létezik, hogy az így létrejövő w szóra D éppen annak $D(w)$ Dyck-útjával egyezik meg.

Mielőtt továbbmennénk, tekintsük a következő lemmát: (ezt most kimondjuk általános csoportokra)

4.2.1. Lemma. *Legyen G tetszőleges csoport, $w \in W(G)$, és $D(w)$ w szabadon redukáló Dyck-útja, melynek csúcsai $v_0, \ldots, v_n$.*

Ha v_{i-1}, v_i, v_{j-1}, v_j $(0 < i < j \leq n)$ a $D(w)$ négy olyan csúcsa, hogy $v_i - v_{i-1} = (1, 1)$, $v_j - v_{j-1} = (1, -1)$ és v_{i-1} valamint v_j második koordinátái (magasságai) megegyeznek (legyen ez m), továbbá nincs olyan $i - 1 < k < j$ egész szám, hogy v_k magassága szintén m, akkor $w(j) = w(i)^{-1}$, vagyis w i-edik és j-edik betűi egymás inverzei.

Bizonyítás. Az, hogy v_{i-1} és v_j magassága azonos, azt jelenti, hogy w-nek az első $i-1$ betűjéből álló $w^{(i-1)}$ részszavának és az első j betűjéből álló $w^{(j)}$ részszavának a szabadon rövidített hossza megegyezik ($= m$). Mivel v_i magassága $(m+1)$ eggyel nagyobb, mint v_{i-1} magassága, így a $w(i)$ betű biztosan nem eshet ki a $w^{(i)}$ részszóból, viszont $w^{(j)}$ magassága már csak m, tehát abból biztosan ki kell esnie. Ez azt jelenti, hogy a $w^{(j)} = w^{(i-1)}w'$ jelölést használva, $w'(1)$ és $w'(l)$ kiejtik egymást valamilyen $2 \leq l \leq (j-i+1)$-re, mivel szabad rövidítésnél csak egymás melletti inverz betűk eshetnek ki, és speciálisan $w'(1)^{-1} = w'(l)$. Ekkor viszont minden $1 < h < l$ indexre is $w'(h)$ betűnek ki kell esnie (máskülönben $w'(1)$ és $w'(l)$ nem kerülhetnének egymás mellé), tehát a $w'^{(l)}$ részszó egységértékű. Ebből az is következik, hogy $m = |w^{(i-1)}|_f = |w^{(i-1)}w'^{(l)}|_f = |w^{(i-1+l)}|_f$. Mivel azonban feltevés volt, hogy nincs olyan $i-1 < k < j$, amelyre szintén $|w^{(k)}|_f = m$ lenne, és az i-edik él felfelé, a j-edik él pedig lefelé mutat, így tetszőleges $i-1 < k < j$-re $|w^{(k)}|_f > m$. Ez azt jelenti, hogy $(i-1+l) \geq j$, ami az $l \leq (j-i+1)$ feltétellel együtt $l = (j-i+1)$-t és épp a bizonyítandó $w(i)^{-1} = w'(1)^{-1} = w'(j-i+1) = w(j)$ állítást vonja maga után.

■

Jegyezzük meg, hogy (adott G-re, $w \in W(G)$-re és $D(w)$-re) tetszőleges, az $m+1$ ($m \geq 0$) magasságú v_{j-1} csúcsból az m magasságú v_j csúcsba tartó lefelé menő élre érvényes, hogy létezik $i < j$, amelyre a $D(w)$ i. éle az m magasságú v_{i-1} csúcsból az $(m+1)$ magasságú v_i csúcsba tartó felfelé menő él. Ez abból adódik, hogy a v_0 csúcs magassága 0, v_{j-1}-é $m+1$, és szomszédos csúcsok magasságai pontosan 1-gyel térnek el, így az első olyan v_i ($0 \leq i < j$) csúcsra, melynek magassága $m+1$, a v_{i-1} csúcs magassága m lesz (hiszen $m+2$ esetén léteznie kellene az i-nél kisebb indexnek is, amelyhez m magasságú csúcs tartozik). Legyen j' az utolsó olyan $j' < j$ index, melyre ez érvényes. Ekkor az előző lemma szerint $w(j) = w(j')^{-1}$ érvényes lesz, és nevezzük a $D(w)$ j-edik és j'-edik élét, valamint a $w(j)$ és $w(j')$ betűket egymást kioltó éleknek illetve betűknek. Egy lefelé menő élre tehát mindig van egy őt kioltó, kisebb indexű, felfelé menő él.

A Dyck-utak súlyozásaira a következő lemma ad feltételt:

4.2.2. Lemma. *Legyen F_S az S által generált szabad csoport ($|S| = g > 0$), és $w \in W(F_S)$ nemüres szó, $D(w)$ a Dyck-útja, melynek csúcsai $v_0, \ldots, v_k$. Legyen $u = w(c)$ a w egy betűje valamilyen c ($1 \leq c \leq |w|$) indexre, $w = w_1uw_2$, és $N(w,c)$ azon $w' \in W(F_S)$ szavak száma, melyekre w' első $c-1$ betűje megegyezik w első $c-1$ betűjével, $w'(c) = v$ valamilyen $v \in W(F_S)$ ($|v| = 1$) betűre, továbbá, ha az u-ra létezik őt kioltó $w(d)$ betű valamilyen $1 \leq d \leq k$ ($d \neq c$) indexre, akkor $w'(d) = v^{-1}$, és minden más $c < i \leq k$ ($i \neq d$) indexre $w'(i) = w(i)$ (ilyenkor $w' = w_1vw_2'$ valamilyen $w_2' \in W(F_S)$-re), továbbá $D(w') = D(w)$. Ekkor*

1. *$N(w,c) = (2g)$, ha $|w_1|_c = 0$,*
2. *$N(w,c) = (2g-1)$, ha $|w_1|_c \neq 0$ és $v_{c+1} - v_c = (1,1)$, valamint*
3. *$N(w,c) = 1$, ha $v_{c+1} - v_c = (1,-1)$.*

Bizonyítás. Legyen először $|w_1|_c = 0$. Ez azt jelenti, hogy a w_1 rövidített hossza 0, vagyis a v_c csúcs az x-tengelyen található. Mivel Dyck-út nem mehet az x-tengely egyenese alá, így mindenképpen $v_{c+1} - v_c = (1, 1)$ lesz, függetlenül a v betű választásától. Ha létezik a v-t kioltó $w'(d)$ betű, akkor mindenképpen $d > c$ lesz, és $w'(d) = v^{-1}$, tehát v megválasztása esetén $w'(d)$ egyféleképpen választható, más betű nem változik, így mivel összesen $(2g)$ darab betű van $W(F_S)$-ben, ez adja az 1. pontot.

Ha $v_{c+1} - v_c = (1, -1)$, akkor mindenképpen $|w_1|_c \neq 0$, hiszen az x-tengelyről nem indulhatna lefelé él. A 4.2.1. lemma és az utána fűzött megjegyzés szerint mindenképpen létezik $1 \leq d < c$ index, hogy $w(d)$ és v egymást kioltó betűk. Viszont a feltétel szerint w' és w első $c - 1$ betűje megegyezik, ez azonban csak akkor lehetséges, ha $u = w(c) = w'(c) = v$ is érvényes lesz, ez adja a 3. pontot.

Most nézzük a második esetet, vagyis $|w_1|_c \neq 0$ és $v_{c+1} - v_c = (1, 1)$. Az első esethez hasonlóan, ha létezik v-re őt kioltó $w'(d)$ betű, akkor $d > c$ és $w'(d) = v^{-1}$ érvényes lesz, tehát w' és w csak $w'(c)$-ben és $w'(d)$-ben térhet el, és $w'(d)$ pontosan egyféleképpen választható. A feltételből következik, hogy w_1-nek legalább egy betűje nem esik ki rövidítéskor, legyen ezek közül az utolsó $w(l)$ $(1 \leq l < c)$, továbbá, ha létezik is v-nek őt kioltó $w'(d)$ élpárja, $d > c$ miatt a $w_1 w(c)$ részszóból $w(c)$ semmiképp sem eshet ki. Ekkor tehát $w_1 w(c)$ redukált alakja $w_1' w(l) v$ lesz valamilyen w_1'-gyel. Egy szó pedig akkor és csak akkor redukált szabad csoportban, ha egymás melletti betűk nem egymás inverzei, így a $v = w(l)^{-1}$ kivételével minden eset előfordulhat, vagyis összesen $(2g - 1)$, ez adja a 2. pontot.

■

Jegyezzük meg, hogy, ha megváltoztatjuk w szó $w(c)$ betűjét u-ról v-re, akkor, ha létezik a $w(c)$-nek $w(d)$ kioltó betűpárja, akkor legalább még $w(d)$-t is meg kell változtatni u^{-1}-ről v^{-1}-re, hogy a régi w és az új w' szóra $D(w) = D(w')$ legyen. Ugyanis, ha a Dyck-út nem változik meg, akkor az egymást kioltó élpárok indexei sem változhatnak meg, mivel azok a 4.2.1. lemma alapján kizárólag a Dyck-út szerkezetétől függnek, vagyis minden, a Dyck-úthoz tartozó szóra a c-edik és a d-edik betűnek egymás inverzének kell lennie.

4.2.3. Lemma. *Legyen F_S az S által generált szabad csoport ($|S| = g > 0$), és $w \in W(F_S)$ nemüres szó, melynek Dyck-útja $D(w)$. Ekkor azon $w' \in W(F_S)$ szavak számát, melyre $D(w') = D(w)$, a következő összefüggés adja meg:*

$$\prod_{i=1}^{|w|} N(w, i).$$

Bizonyítás. Azt bizonyítjuk, hogy tetszőleges $1 \leq k \leq |w|$-re

$$\prod_{i=1}^{k} N(w, i)$$

azon $w' \in W(F_S)$ szavak számát adja meg, melyek legfeljebb w első k betűjében, és azok esetleges kioltó betűpárjaiban különböznek egymástól, és $D(w') = D(w)$. Az i-re vonatkozó indukciót használunk. Az $i = 1$ esetben $N(w, 1)$ a definíció szerint azt adja meg, hogy hányféleképpen lehet w első betűjét kicserélni úgy, hogy az esetleges kioltó élpárjához tartozó betűt is kicseréljük, minden mást viszont változatlanul hagyunk. Tegyük fel, hogy $k = m - 1$-re igaz az állítás, vagyis, hogy

$$\prod_{i=1}^{m-1} N(w, i)$$

azon $w' \in W(F_S)$ szavak számát adja meg, melyek legfeljebb w első $(m-1)$ betűjében és azok esetleges kioltó betűpárjaiban különböznek egymástól (és $D(w') = D(w)$). Ha $w(m)$ betű olyan, hogy annak kioltó párja szerepel az első $(m-1)$ betű között, akkor egyrészt azt nem tudjuk megváltoztatni úgy, hogy az első $(m-1)$ betű valamelyikét ne változtatnánk meg, és továbbra is $D(w') = D(w)$ lenne, viszont a $w(m)$ összes lehetséges, a Dyck-utat megtartó megváltoztatása előáll az első $(m-1)$ betű és azok kioltó betűpárjainak megfelelő megváltoztatása által, így a

$$\prod_{i=1}^{m-1} N(w, i)$$

érték egyben a w első m betűjének és azok esetleges kioltó betűpárjainak Dyck-út-tartó megváltoztatásainak számát is megadja. Mivel a $D(w)$ m-edik éle ilyenkor lefelé menő él (egy kioltó élpár második tagja), így $N(w, m) = 1$, tehát

$$\prod_{i=1}^{m} N(w, i) = \prod_{i=1}^{m-1} N(w, i) \cdot N(w, m) = \prod_{i=1}^{m-1} N(w, i).$$

Ha $w(m)$-nek nem szerepel kioltó betűpárja az első $(m-1)$ betű között, akkor az első $(m-1)$ betű és azok esetleges kioltó párjainak megváltoztatása a $w(m)$-et nem változtatja meg, valamint $w(m)$ és esetleges kioltó párjának változtatása is változatlanul hagyja az első $(m-1)$ betűt, vagyis az első m betű és azok esetleges kioltó párjainak változtatásai lehetőségeinek számát a két érték szorzata adja meg, amely szintén:

$$\prod_{i=1}^{m} N(w, i) = \prod_{i=1}^{m-1} N(w, i) \cdot N(w, m).$$

A $k = |w|$ esetre alkalmazva az észrevételt, és megjegyezve, hogy természetesen ilyenkor az első k betű esetleges kioltó párjai is az első k betű között vannak, adódik a lemma.

■

4.2.4. Lemma. *Legyen F_S az S által generált szabad csoport, és legyen adott egy $D(w)$ Dyck-út valamilyen $w \in W(F_S)$ szóra, amely az (m,n) pontban végződik, és k-szorosan visszatérő. Ekkor*

1. *azon $0 \leq i < m$ értékek száma, melyre $|w^{(i)}|_c = 0$, $n = 0$ esetén megegyezik k-val, $n \neq 0$ esetén megegyezik $(k+1)$-gyel,*
2. *azon $0 \leq i < m$ értékek száma, melyre $|w^{(i)}|_c \neq 0$ és $v_i - v_{i-1} = (1,1)$, $n = 0$ esetén megegyezik $\frac{n+m}{2} - k$-val, $n \neq 0$ esetén megegyezik $\frac{n+m}{2} - k - 1$-gyel,*
3. *azon $0 \leq i < m$ értékek száma, melyre $v_i - v_{i-1} = (1,-1)$, megegyezik $\frac{m-n}{2}$-vel.*

Bizonyítás. Akkor és csak akkor igaz, hogy az első i darab betűből álló $w^{(i)}$ szó redukált hossza 0, ha a v_i csúcs az x-tengelyen van. Mivel $D(w)$ k-szorosan visszatérő, így összesen $k+1$ darab ilyen csúcs van. Ha viszont $n = 0$, akkor az egyik ilyen csúcs v_m, minket viszont csak a $0 \leq i < m$ indexek érdekelnek, tehát ekkor valóban csak k darab megfelelő csúcs van.

Egy (m,n) pontban végződő Dyck-útnak a 3.1.3. állítás alapján összesen $\frac{m+n}{2}$ felfelé lépése van. Ezekből az $|w_i|_c = 0$-nak megfelelő eseteket az előbb számoltuk. A 4.2.2. lemma bizonyítása során megjegyeztük, hogy $|w_i|_c = 0$ esetén mindig $v_i - v_{i-1} = (1,1)$ lesz, tehát a maradék $n = 0$ esetén valóban $\frac{n+m}{2} - k$, és $n \neq 0$ esetén $\frac{n+m}{2} - k - 1$.

A harmadik állítás abból következik, hogy a 3.1.3. állítás alapján a $D(w)$ Dyck-útnak összesen $\frac{m-n}{2}$ lefelé útja van.

■

4.2.5. Lemma. *Legyen F_S a nemüres S által generált szabad csoport. Ekkor minden $l \in \mathbb{N}$ hosszú D Dyck-útra létezik $w \in W(F_S)$, hogy $|w| = l$ és $D(w) = D$.*

Bizonyítás. Legyenek a D csúcsai $v_0, \ldots, v_l$, $a \in S$ tetszőleges, és $w \in W(F_S)$ olyan, hogy

$$w(k) = a \iff v_k - v_{k-1} = (1,1) \text{ és}$$
$$w(k) = a^{-1} \iff v_k - v_{k-1} = (1,-1)$$

tetszőleges $1 \leq k \leq l$-re. Ekkor, ha a w első k betűjéből álló $w^{(k)}$ részszava h db a és $k-h$ db a^{-1} betűt tartalmaz ($1 \leq h \leq k$, és a Dyck-út tulajdonságai alapján $h \geq k-h$), akkor $\left|w^{(k)}\right|_c = k - 2(k-h) = 2h - k$, valamint ilyenkor, a fenti definíció miatt a D első k éléből álló rész-Dyck-út végpontjának a magassága is $h-(k-h) = 2h-k$ lesz, ami épp azt jelenti, hogy $D(w) = D$.

■

Most már megadhatjuk a $S(g,n,k)$ értékét megadó képletet:

4.2.6. Tétel. *Legyen S tetszőleges nemüres halmaz, $|S| = g > 0$, F_S az S által generált szabad csoport, ekkor a*

$$\{(w, w_R) \mid |w| = n,\ |w_R| = k,\ w_R \text{ a } w \text{ redukált alakja és } w, w_R \in W(F_S)\}$$

halmaz számosságát megadó $S(n,k,g)$ függvényre, különböző paritású n és k esetén

$$S(n,k,g) = 0,$$

$k = 0$ és páros n esetén:

$$S(n,0,g) = \sum_{i=1}^{\frac{n}{2}} \frac{i}{n-i} \binom{n-i}{\frac{n}{2}-i} (2g)^i (2g-1)^{\frac{n}{2}-i},$$

$k \neq 0$, és azonos paritású n és k esetén pedig:

$$S(n,k,g) = \sum_{i=0}^{\frac{n-k}{2}} \frac{k+i}{n-i} \binom{n-i}{\frac{n-k}{2}-i} (2g)^{i+1} (2g-1)^{\frac{n+k}{2}-i-1}.$$

Bizonyítás. Különböző paritású szavak a 2.2.6. állítás szerint nem lehetnek F_S-ben ekvivalensek, ugyanis inverz betűpárok elhagyása és beírása a szóba nem változtatja meg a szó paritását. Tegyük most fel, hogy n és k azonos paritásúak.

Vegyünk egy tetszőleges D Dyck-utat, mely az (a,b) pontban végződik, és c-szeresen visszatérő. Emlékeztetünk rá, hogy ilyen utakból a 3.4.1. lemma alapján összesen

$$B\left(\frac{a+b}{2}, \frac{a-b}{2} - c\right)$$

létezik.

Tetszőleges $|w| = n$ szóra $D(w)$ is n hosszú lesz, vagyis végpontjának x-koordinátája n, és megfordítva, az előző lemma alapján, tetszőleges olyan D Dyck-útra, amely végpontjának x-koordinátája n, létezik egy $|w| = n$ szó, hogy $D(w) = D$. Rögzítsünk egy tetszőleges n hosszú D Dyck-utat, amely az (n,k) pontban végződik, és c-szeresen vissszatérő, és egy olyan w szót, melyre $D(w) = D$.

Nézzük először a $k = 0$ esetet. A 4.2.4. lemma alapján azon $0 \leq i < n$ indexek száma, melyre

1. $|w_i|_c = 0$, összesen c darab lesz. Ezekre az i indexekre a 4.2.2. lemma 1. pontja alapján $N(w,i) = 2g$ lesz.
2. $|w_i|_c \neq 0$ és $v_i - v_{i-1} = (1,1)$, összesen $\frac{n}{2} - c$ lesz. Ezekre az i indexekre a 4.2.2. lemma 2. pontja alapján $N(w,i) = 2g - 1$ lesz.

3. $v_i - v_{i-1} = (1, -1)$, összesen $\frac{n}{2}$ lesz. Ezekre az i indexekre a 4.2.2. lemma 3. alapján $N(w, i) = 1$ lesz.

Az összes olyan w' szavak számát, melyekre $D(w') = D(w)$ lesz, a 4.2.3. lemma alapján a

$$\prod_{i=1}^{n} N(w, i)$$

érték adja meg, a fentiek alapján ennek értéke:

$$\prod_{i=1}^{n} N(w, i) = (2g)^c (2g-1)^{\frac{n}{2}-c}$$

Mivel összesen

$$B\left(\frac{n}{2}, \frac{n}{2} - c\right) = \frac{c}{n-c}\binom{n-c}{\frac{n}{2}-c}$$

olyan Dyck-út van, mely szintén az $(n, 0)$ pontban végződik, és c-szeresen visszatérő, így az összes olyan w' szavak száma, melyre $D(w')$ az $(n, 0)$ pontban végződik, és c-szeresen visszatérő:

$$\frac{c}{n-c}\binom{n-c}{\frac{n}{2}-c}(2g)^c(2g-1)^{\frac{n}{2}-c}.$$

Jegyezzük meg, hogy egy n hosszú, az $(n, 0)$ pontban végződő Dyck-út legalább 1-szeresen és legfeljebb $\frac{n}{2}$-szeresen visszatérő (és ezek el is érhetők), így ezt felösszegezve $c = 1$-től $c = \frac{n}{2}$-ig megkapjuk az összes olyan w' szavak $T(n, 0, g)$ számát, melyek az $(n, 0)$ pontban végződnek

$$T(n, 0, g) = \sum_{c=1}^{n} \frac{c}{n-c}\binom{n-c}{\frac{n}{2}-c}(2g)^c(2g-1)^{\frac{n}{2}-c}.$$

Mivel egy $w \in W(F_S)$ szónak akkor és csak akkor végződik a $D(w)$ Dyck-útja az $(n, 0)$ pontban, ha $|w| = n$ és $|w|_c = 0$, így

$$S(n, 0, g) = T(n, 0, g),$$

amivel a $k = 0$ esettel kész vagyunk.

Nézzük most a $k \neq 0$ esetet. A 4.2.4. lemma alapján azon $0 \leq i < n$ indexek száma, melyre

1. $|w_i|_c = 0$, összesen $c+1$ darab lesz. Ezekre az i indexekre a 4.2.2. lemma 1. pontja alapján $N(w,i) = 2g$ lesz.
2. $|w_i|_c \neq 0$ és $v_i - v_{i-1} = (1,1)$, összesen $\frac{n+k}{2} - c - 1$ lesz. Ezekre az i indexekre a 4.2.2. lemma 2. pontja alapján $N(w,i) = 2g-1$ lesz.
3. $v_i - v_{i-1} = (1,-1)$, összesen $\frac{n-k}{2}$ lesz. Ezekre az i indexekre a 4.2.2. lemma 3. alapján $N(w,i) = 1$ lesz.

Az összes olyan w' szavak számát, melyekre $D(w') = D(w)$ lesz, a 4.2.3. lemma alapján most is a

$$\prod_{i=1}^{n} N(w,i)$$

érték adja meg, a fentiek alapján ennek értéke jelen esetben:

$$\prod_{i=1}^{n} N(w,i) = (2g)^{c+1}(2g-1)^{\frac{n+k}{2}-c-1}$$

Mivel összesen

$$B\left(\frac{n+k}{2}, \frac{n-k}{2} - c\right) = \frac{k+c}{n-c}\binom{n-c}{\frac{n-k}{2}-c}$$

olyan Dyck-út van, mely szintén az (n,k) pontban végződik, és c-szeresen visszatérő, így az összes olyan w' szavak száma, melyre $D(w')$ az (n,k) pontban végződik, és c-szeresen visszatérő:

$$\frac{k+c}{n-c}\binom{n-c}{\frac{n-k}{2}-c}(2g)^{c+1}(2g-1)^{\frac{n+k}{2}-c-1}.$$

Egy n hosszú, az (n,k) pontban végződő Dyck-út legalább 0-szorosan és legfeljebb $\frac{n-k}{2}$-szörösen visszatérő (és ezek el is érhetők), így ezt felösszegezve $c =$ 0-től $c = \frac{n-k}{2}$-ig megkapjuk az összes olyan w' szavak $T(n,k,g)$ számát, melyek az (n,k) pontban végződnek:

$$T(n,k,g) = \sum_{c=0}^{\frac{n-k}{2}} \frac{k+c}{n-c}\binom{n-c}{\frac{n-k}{2}-c}(2g)^{c+1}(2g-1)^{\frac{n+k}{2}-c-1}.$$

Mivel egy $w \in W(F_S)$ szónak akkor és csak akkor végződik a $D(w)$ Dyck-útja az (n,k) pontban, ha $|w| = n$ és $|w|_c = k$, így

$$S(n,k,g) = T(n,k,g),$$

minden $k \neq 0$-ra, amivel az állítást beláttuk.

■

4.2.1. *Megjegyzés.*

1. Minimális módosítással a fentiek alapján meg lehet adni a $(\mathbf{Z})^m * (\mathbf{Z_2})^l$ alakú csoportokra is a megfelelő $S(n,k;m,l)$ értékeket, ahol $\mathbf{Z}$ az egygenerátoros szabad csoportot, $\mathbf{Z_2}$ a másodrendű ciklikus csoportot, $*$ csoportok szabad szorzatát, G^i pedig csoportok szabad hatványát jelöli. Néhány egyszerűbb monoidra, valamint a kommutatív szabad monoidra és csoportra szintén viszonylag egyszerűen megadható explicit képlet. Csoportok direkt szorzataira elméleti jellegű rekurzív képletek adhatók, de a gyakorlatban ezek már nem igazán használhatóak. A harmad- és negyedrendű ciklikus csoportok szabad hatványaira a feladat már jóval bonyolultabb, itt csak részeredmények ismertek, ennél általánosabb csoportok esetén pedig egyelőre egyáltalán nem ismert a feladat megoldása (a szerző számára).

2. A fenti eredmények kifejezhetők ún. hipergeometrikus függvények[1] segítségével is. Például, páros n esetén:

$$S(n,0,g) = \frac{1}{n-1} 2g\,(2g-1)^{\frac{n}{2}-1} \binom{n-1}{\frac{n}{2}-1} {}_2F_1\left(2, 1-\frac{n}{2}; 2-n; \frac{2g}{2g-1}\right),$$

   és a többi érték is hasonlóan kifejezhető.

4.3. Bolyongások Cayley-gráfban

Az előző tételt Cayley-gráfok nyelvén is megfogalmazhatjuk. Legyen adott egy G csoport és egy $X \subseteq G$ generátorrendszere, melyre $1_G \notin X$, $x \in X \Longrightarrow x^{-1} \notin X$. Ekkor a G csoport X-re vonatkozó $\Gamma(V,E)$ irányított, élszínezett Cayley-gráfját a következőképpen konstruáljuk meg:

- Minden $g \in G$ csoportelemhez tartozzon pontosan egy $v(g) \in V$ csúcs.
- Minden $x \in X \cup X^{-1}$ generátorhoz vagy inverzéhez tartozzon egy c_x szín.
- Minden $g \in G$ és $x \in X \cup X^{-1}$ esetén $v(g)$-ből $v(gx)$-be menjen egy c_x színű irányított él, és minden $e \in E$ ilyen alakban áll elő.

A Cayley-gráfon természetes módon lehet metrikát definiálni, $v_1, v_2 \in V$ esetén $d(v_1,v_2)$ a legrövidebb v_1-ből v_2-be menő út hossza, ez pedig megad a G elemei között is egy X generátorrendszertől függő távolságot, $g_1, g_2 \in G$ esetén $d(g_1,g_2) := d\,(v(g_1), v(g_2))$. Ha $w_1, w_2 \in W(G)$ két csoportszó, és $g_1, g_2 \in G$ rendre a nekik megfelelő csoportelemek, akkor pedig definíció szerint legyen $d(w_1,w_2) := d(g_1,g_2)$. A szavak közötti távolság már nem lesz metrika, hanem csak

[1] Ld. [5]

pszeudometrika, ugyanis $d(w_1, w_2) = 0$ $w_1 \neq w_2$ esetén is lehetséges, ha ezen szavaknak ugyanaz a csoportelem felel meg.

4.3.1. Állítás. *Ha X a G egy generátorrendszere, melyre $1_G \notin X$, $x \in X \implies x^{-1} \notin X$, és $G = \langle X \mid R \rangle$ a G egy prezentációja, akkor az előbb definiált pszeudometrikával tetszőleges $w_1, w_2 \in W(G)$-re*

$$d(w_1, w_2) = \left| (w_1)^{-1} w_2 \right|_c .$$

Bizonyítás. A Cayley-gráfon minden sétának természetes módon megfelel egy $w \in W(G)$ szó, melynek k. betűje a séta k. élének a színe, és $|w|$ éppen a séta hossza. Ha az S_1 és S_2 séták végpontjai megegyeznek (mindketten $g_1 \in G$-ből $g_2 \in G$-be mennek), akkor a nekik megfelelő w_1 és w_2 szavakhoz ugyanaz a $g \in G$ csoportelem kell, hogy tartozzon, ugyanis indukcióval látható, először a $g_1 = 1$ esetén, hogy mind w_1-nek, mind w_2-nek a g_2 csoportelem felel meg, majd általános esetben, azt felhasználva, hogy, ha u_1 és u_2 egy-egy g_1-nek illetve g_2-nek megfelelő szó, akkor $u_1 w_1 \sim_G u_2$ és $u_1 w_2 \sim_G u_2$, és ebből $w_1 \sim_G w_2$.

Tetszőleges $u_1, u_2 \in W(G)$ esetén, ha nekik rendre a $g_1, g_2 \in G$ elemek felelnek meg, akkor $v(g_1)$-ből mindig el tudunk úgy jutni a Cayley-gráfon $v(g_2)$-be, hogy előbb w_1-ből, a betűit a végétől kezdve „lefejtve" a betűk inverzeivel színezett éleken 1-be megyünk, majd onnan w_2-be a megfelelő betűivel színezett éleken, és ennek a sétának a $(w_1)^{-1} w_2$ szó felel meg. Az egyik legrövidebb $v(g_1)$-ből $v(g_2)$-be menő sétának pedig az egyik legrövidebb olyan $w \in W(G)$ szó, melyre $w \sim_G (w_1)^{-1} w_2$, ilyenkor pedig definíció szerint $d(w_1, w_2) = d(g_1, g_2) = |w| = \left| (w_1)^{-1} w_2 \right|_c$.

■

4.3.2. Tétel. [2]

Legyen az F_S ($|S| = g \geq 1$) szabad csoport S-hez tartozó Cayley gráfja $\Gamma(V, E)$, ekkor annak $P(n, 0, g)$ valószínűsége, hogy egy $v(1)$-ből kiinduló n-hosszú séta körséta lesz, páratlan n esetén 0, páros n esetén:

$$P(n, 0, g) = \sum_{i=1}^{\frac{n}{2}} \frac{i}{n-i} \binom{n-i}{\frac{n}{2}-i} (2g)^{i-n} (2g-1)^{\frac{n}{2}-i}.$$

Annak $P(n, k, g)$ valószínűsége pedig, hogy egy $v(1)$-ből kiinduló n-hosszú séta v végpontjára $d(v(1), v) = k \geq 1$, különböző paritású n és k esetén 0, azonos paritású n és k esetén pedig:

$$P(n, k, g) = \sum_{i=0}^{\frac{n-k}{2}} \frac{k+i}{n-i} \binom{n-i}{\frac{n-k}{2}-i} (2g)^{i-n+1} (2g-1)^{\frac{n+k}{2}-i-1}.$$

[2] Megjegyezzük, hogy ennek bizonyítása a $k = 0$ esetben, a 4.2.6. tételre adott bizonyításunkhoz hasonló módszerrel, csak Dyck-utak helyett JF-rácsutakat használva és kevésbé részletesen megtalálható a [9] cikk 348. oldalán is.

Bizonyítás. A 4.3.1. állítás és a 4.2.6. tételünk alapján ez azonnal adódik, figyelembe véve még, hogy az n-hosszú szavak száma $W(F_S)$-ben $(2g)^n$.

■

Tárgymutató

Irodalomjegyzék

[1] S. Burris and H.P. Sankappanavar. A course in universal algebra. https://www.math.uwaterloo.ca/~snburris/htdocs/UALG/univ-algebra2012.pdf, 2012. Elérve: 2016-04-30.

[2] L. Carlitz. Sequences, paths, ballot numbers. http://www.mathstat.dal.ca/FQ/Scanned/10-5/carlitz7.pdf. Elérve: 2016-04-30.

[3] Pete L. Clark. Introduction to semigroups and monoids. http://math.uga.edu/~pete/semigroup.pdf. Elérve: 2016-04-30.

[4] D.J. Collins and H. Zieschang. Encyclopaedia of mathematical sciences. In A.N. Parshin and I.R. Shafarevich, editors, *Volume 58: Algebra VII - Combinatorial Group Theory*. Springer-Verlag, 1993.

[5] A. B. Olde Daalhuis. Chapter 15, hypergeometric function, Â§ 15.2 definitions and analytical properties. http://dlmf.nist.gov/15.2, 2015. Elérve: 2016-05-25.

[6] Kiss Emil. *Bevezetés az algebrába*. Typotex Kiadó, 2007.

[7] Ira M. Gessel. An introduction to lattice path enumeration. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.121.5047&rep=rep1&type=pdf. Elérve: 2016-05-25.

[8] I. P. Goulden and Luis G. Serrano. Maintaining the spirit of the reflection principle when the boundary has arbitrary integer slope. https://www.math.uwaterloo.ca/~ipgoulde/revpathsju1903.pdf. Elérve: 2016-05-01.

[9] Harry Kesten. Symmetric random walks on groups. *Trans. Amer. Math. Soc.*, 92(2):336–354, 1959. http://www.ams.org/journals/tran/1959-092-02/S0002-9947-1959-0109367-6/S0002-9947-1959-0109367-6.pdf, Elérve: 2016-05-24.

[10] M. Lothaire, editor. *Combinatorics on Words*. Cambridge University Press, 1997.

[11] M. Lothaire, editor. *Algebraic Combinatorics on Words*. Cambridge University Press, 2002. http://www-igm.univ-mlv.fr/~berstel/Lothaire/AlgCWContents.html, Elérve: 2016-05-06.

[12] Paul E. Schupp Roger C. Lyndon. *Combinatorial Group Theory.* Springer, 2001.

[13] Oleg Sofrygin. Counting the number of dyck paths according to different types of parameters. `http://people.brandeis.edu/~gessel/47a/sofrygin.pdf`. Elérve: 2016-04-30.

[14] Richard P. Stanley. Enumerative combinatorics - volume 1, second edition (version of 15 july 2011). http://math.mit.edu/ rstan/ec/ec1.pdf. Elérve: 2016-05-28.

[15] Richard P. Stanley. *Enumerative Combinatorics - Volume 2.* Cambridge University Press, 1999.

[16] Combinatorics on words. `https://en.wikipedia.org/wiki/Combinatorics_on_words`. El'erve: 2016-05-28.

[17] Small cancellation theory. `https://en.wikipedia.org/wiki/Small_cancellation_theory`. El'erve: 2016-05-28.

[18] Word problem for groups. `https://en.wikipedia.org/wiki/Word_problem_for_groups`. El'erve: 2016-05-28.

[19] Abraham Karrass Wilhelm Magnus and Donald Solitar. *Combinatorial Group Theory - Presentations of Groups in Terms of Generators and Relations.* Dover Publications, Inc., 1976.

[20] Wolfgang Woess. *Random Walks on Infinite Graphs and Groups (Cambridge Tracts in Mathematics 138).* Cambridge University Press, 2000.

[21] Catalan number. `http://mathworld.wolfram.com/CatalanNumber.html`. Elérve: 2016-04-30.