Bevezetés

Napjainkban egyre népszerűbb kutatási terület az algebrai bonyolultságelmélet, amely az algebra témakörében felmerülő kérdések megoldására adható algoritmusok nehézségének mértékét vizsgálja. Leggyakoribb kérdés a szóprobléma. Ezt több különböző változatban is megfogalmazhatjuk. Egy algebra feletti termnek a típushoz tartozó (szabad) szóalgebra elemeit nevezzük. Ezek tehát változókból és az algebra műveleteiből felépített kifejezések. A term-ekvilalenciaprobléma (TERM-EQ) másszóval azonosságellenőrzés, a következő: Legyen adva egy véges algebra (például alapműveleteinek táblázataival, vagy bármilyen módon, mely egyértelműen meghatározza azokat). A feladat annak (algoritmikus) eldöntése, hogy két kifejezés mikor vesz fel minden behelyettesítés esetén azonos értéket, azaz, hogy a két kifejezés mikor határozza meg ugyanazt a függvényt. Ez tehát az univerzális algebra és a számítástudomány határterületén elhelyezkedő probléma, érdemes tehát röviden összefoglalni mindkét tudományág területéről a felhasznált fogalmakat, tételeket, jelöléseket. Az univerzális algebrának csupán alapelemeit fogjuk felhasználni, melyek nem haladják meg egy bevezető univerzális algeb-ra kurzus kereteit, úgy mind varietás, homomorfizmus, izomorfizmus, kongruencia, faktoralgebra, második izomorfizmus tétel. A számítástudomány területéről a legalapvetőbb bonyolultságelméleti problémaosztályokat érdemes ismerni. Egy algoritmust akkor nevezünk polinomiálisnak, ha a futási ideje a bemenő adatok méretének egy polinomjával korlátozható. Azon problémák osztályát melyekre adható polinomiális algoritmus P-vel jelöljük. Egy probléma NP-beli, ha a megoldására (amennyiben már ismert) van polinomidőben ellenőrizhető bizonyíték, illetve coNP-beli, ha a nemleges válasz bizonyítható polinom-időben. Egy probléma NP-teljes (coNP-teljes), ha minden NP-beli (coNP-beli) problémát vissza lehet rá vezetni. Egy véges algebra fölött a TERM-EQ probléma mindig véges sok lépésben eldönthető, legrosszabb esetben az összes behelyettesítés kiszámolásával, (ez azonban nem polinomiális algoritmus), és az is világos, hogy coNP-ben van, mert ha két kifejezés nem egyenlő, arra gyorsan ellenőrizhető bizonyíték egy olyan behelyettesítés amelynél különböznek.
A szóprobléma másik változata az egyenletmegoldás problémája (TERM-SAT), mely azt kérdezi, hogy van-e olyan behelyettesítés, amely mellett a két kifejezés megegyezik. Ez nyilván egy NP-beli probléma, hiszen ha már adva van egy behelyettesítés, akor könnyen kiszámolható, hogy a két kifejezés értéke tényleg megegyező-e.

A végső cél tehát, egy adott algebrára (algebraosztályra) annak eldöntése, hogy felette az azonosságellenőrzés (illetve az egyenletmegoldhatóság) polinomiális, vagy coNP-teljes (illetve NP-teljes). Természetesen elvileg lehetséges, hogy egyik sem igaz.

A legegyszerűbbnek látszó univerzális algebrai struktúrák talán a félcsoportok. Ezeken egyetlen kétváltozós asszociatív művelet van, tehát a félcsoportok nyelvén minden kifejezés $x_1x_2 \dots x_n$ alakú, a zárójeleket felesleges kiírni. Hogy egy adott félcsoportban két ilyen kifejezés milyen feltételek mellett lesz egyenlő, az azonban nem egyszerű kérdés. A dolgozat egyik fő témája ennek a vizsgálata. Abel-csoportok fölött ez szinte "ránézésre" eldönthető. Van azonban olyan félcsoport amelyre a probléma coNP-teljes, a legkisebb ilyen ismert példa hat elemű.

A Rees-mátrix félcsoportok ugyanolyan építőkövei a félcsoportoknak, mint a csoportoknak az egyszerű csoportok. Ezért reméljük, hogy a Rees-mátrix félcsoportok szóproblémáinak karakterizálása segíthet a félcsoportok szóproblémáiban az általános esetben is. Az első fejezetben ezeket vizsgáljuk, és néhány speciális esetre a probléma könnyen meg is oldható. A legáltalánosabb eset magában foglalja a véges csoportok szóproblémáját ezért egyelőre teljesen reménytelennek tűnik.

A szóprobléma nem egy-egy konkrét félcsoport önálló jellemzője, hanem egy teljes varietás közös tulajdonsága. A varietás algebrák olyan osztálya melyet azonosságok definiálnak. Így a szóproblémával szorosan összekapcsolódó kérdés a félcsoportvarietások vizsgálata. Ez képezi a második fejezet tárgyát. Érdekes összefüggések vannak egy félcsoportvarietásban teljesülő azonosságok típusai és a varietásban bizonyos speciális algebrák jelenléte között.

Egy algebraosztály vizsgálata kapcsán alapvető kérdés, hogy le tudjuk-e írni a varietások hálójának szerkezetét. Az Abel-csoportok esetén, például ez is nagyon egyszerű. A háló a természetes számok hálójával izomorf az osztthatósági relációval (illetve egyetlen "végtelen nagy", legnagyobb elem hozzávételével). Fécsoportokra lényegesen összetettebb a probléma, inkább negatív eredmények születnek. A félcsoportvarietások hálójának számossága kontinuum és semmiféle nemtriviális hálóazonosság nem teljesül benne. Az azonosságok általános vizsgálata lehetővé teszi annak viszonylag egyszerű bizonyítását, hogy ez a háló minden véges hálót tartalmaz ami igazolja is a fenti állítást.

Az utolsó két fejezetben igazolt tételek eddig csak oroszul jelentek meg (vagy egyáltalán nem), így bizonyításuk nem volt ismert. Az itt felhasznált alapvető univerzális algebrai tételeket, a bonyolultságelmélet teljes és precíz felépítését, valamint az első fejezetben Rees-mátrix félcsoportokról felhasznált, de itt nem bizonyított tételeket bőséggel tárgyalja a szakirodalom. Ezek bármiféle felsorolása szükségképpen hiányos lenne, ezért a teljesség igénye nélkül a következő néhány hivatkozás ajánlható:

[1] S. Burris, H. P. Sankappanavar: *Bevezetés az univerzális algebrába.* Tankönyvkiadó, Budapest, 1988.

[2] S. Burris, H. P. Sankappanavar: *A course in universal algebra.* Springer kiadó, 1981.

[3] M. R. Garey, D. S. Johnson: *"Computers and intractability"* W.H.Freeman and Co., San Francisco, 1979.

[4] J.M. Howie: *Fundamentals of semigroup theory*, Claredon, 1995

[5] S. Seif, Cs. Szabó: Computational complexity of checking identities in 0-simple semigroups and matrix semigroups over finite fields. *Semigroup Forum,* 2005.

Azonosságok és szóproblémák Rees-mátrix félcsoportokban

Legyen G egy véges csoport, M olyan mátrix, melynek elemei a $G \cup \{0\}$ halmazból valók, és minden sorban illetve oszlopban van 0-tól különböző elem. Jelölje Λ a mátrix sorainak I az oszlopainak indexhalmazát. Definiáljuk az $A := \{I \times G \times \Lambda\} \cup \{0\}$ halmazon a szorzást a következőképpen: $a0 = 0a = 0$ ha $a \in A$ illetve a 0-tól különböző elemeken:

$$(i, g, \lambda)(j, h, \mu) := \begin{cases} (i, gM(\lambda, j)h, \mu) & \text{ha } M(\lambda, j) \in G \\ 0 & \text{ha } M(\lambda, j) = 0 \end{cases}$$

Könnyen ellenőrizhető, hogy az így definiált szorzás asszociatív. A kapott félcsoport az M mátrixhoz tartozó Rees-mátrix félcsoport. A G csoportot struktúracsoportnak nevezzük. Ha a mátrixban egyáltalán nem szerepel 0 elem akkor ezt a félcsoportból is kihagyhatjuk.

Ha a struktúracsoport egy elemű, akkor kicsit egyszerűbben is meg lehet adni a Rees-mátrix félcsoportot:

Legyen M egy $|I| \times |\Lambda|$-as 0-1 mátrix és definiáljuk az $A := I \times \Lambda \cup \{0\}$ halmazon így a szorzást: $0a = a0 = 0$ illetve:

$$(i, \lambda)\,(j, \mu) := \begin{cases} (i, \mu) & \text{ha } (\lambda, j) = 1 \\ 0 & \text{ha } (\lambda, j) = 0 \end{cases}$$

Az ilyen félcsoportot kombinatorikus teljesen 0-egyszerű félcsoportnak hívjuk.

A következőkben foglaljunk össze néhány alapvető tételt:

1. Lemma: Legyen M az A Rees-mátrix félcsoport mátrixa. Ekkor:

1. A mátrix két sorát, illetve oszlopát felcserélve az eredetivel izomorf Rees-mátrix fél-csoportot kapunk.

2. A mátrix egy sorát, illetve oszlopát egy csoportelemmel megszorozva az eredetivel izomorf Rees-mátrix félcsoportot kapunk.

1. Tétel (Rees tétele): Legyen A olyan véges félcsoport melyben nincs nemtriviális ideál. Ekkor A izomorf egy Rees-mátrix félcsoporttal.

2. Tétel (Seif-Szabó): kombinatorikus teljesen 0-egyszerű félcsoportokra az azonosságellenőrzés mindig polinomiális.

Ez tehát azt jelenti például, hogy ha egy Rees-mátrix félcsoport mátrixában nincsenek 1-től különböző csoportelemek, akkor a szóproblémájának bonyolultságát a struktúracsoport határozza meg. Emiatt egy Rees-mátrix félcsoport szóproblémájának megoldása alighanem nehezebb feladat mint a struktúracsoportjáé. Éppen ezért érdemes a szóproblémát olyan Rees-mátrix félcsoportokra vizsgálni, amelyek struktúracsoportjára ez már ismert. Sajnos, csoportok szóproblémájáról nagyon keveset tudunk. Van azonban csoportoknak egy osztálya amelyekre ez rendkívül egyszerű: a kommutatív csoportok szóproblémája szinte triviális. A teljesség kedvéért ezt is foglaljuk össze:

3. Tétel (az Abel-csoportok szóproblémája): Legyen G tetszőleges véges Abel-csoport, és legyen G exponense m.
Ekkor: a csoportok nyelvén fölírt $u = v$ azonosság pontosan akkor teljesül G-ben ha minden x változó esetén x u-beli és v-beli előfordulásainak száma kongruens $mod\ m$.

(Egy változó előfordulásainak számán egyszerűen megfogalmazva a kitevőinek összgét értjük, beleértve a negatív kitevőket is, tehát x^{-1} előfordulásainak számát le kell vonni.)

Bizonyítás: a feltétel szükségességéhez elég olyan behelyettesítéseket tekinteni, ahol egy kivétellel minden változó értéke az egységelem, a fordított irány pedig triviális.

Ezek nyilván polinom időben ellenőrizhető feltételek, ezért az Abel-csoportok szóproblémája polinomiális. Most megvizsgáljuk, hogy mi öröklődik ebből Rees-mátrix félcsoportokra:

4. Tétel: Legyen A olyan Rees-mátrix félcsoport melynek struktúracsoportja kommutatív és mátrixa 2×2-es.

Ekkor A-ban az azonosság-ellenőrzés polinomiális.

A bizonyítás előtt vezessünk be néhány jelölést:

Legyen $u = x_1 x_2 \dots x_n$ tetszőleges szó. Definiáljuk u-hoz a következő gráfot: $G_u = G_u(U, V, E)$ legyen az a páros gráf melynek csúcshalmaza: az u-ban szereplő változók halmaza két példányban: $U = V = \{x_1, x_2 \dots x_n\}$ és élei: az $U \ni x_i$ csúcsot akkor kötjük össze az $x_j \in V$ ha az $x_i x_j$ részszóként szerepel u-ban (szigorúan ebben a sorrendben és közvetlenül egymás mellett).

Hasonlóan definiáljuk a $\widetilde{G}_u$ gráfot ugyanezen a csúcshalmazon csak itt az éleket multiplicitással számoljuk: az $U \ni x_i$ csúcsot annyi él köti össze az $x_j \in V$ csúccsal ahányszor $x_i x_j$ részszóként szerepel u-ban.

Bizonyítás: jelölje M az A mátrixát, ez 2×2-es, elemei: $a, b, c, d \in A \cup \{0\}$

$$M := \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Mivel a mátrix minden sorában illetve oszlopában van nemnulla elem, egy 2×2-es mátrixban vagy kettő, vagy egy 0 elem van, vagy egy sincs. Az 1. lemma szerint a mátrix sorait, oszlopait szabad cserélgetni és csoportelemekkel szorozni. Ezért, ha a mátrixban két 0 van akkor feltehető, hogy az b és c. Ekkor szorozzuk az első sort a^{-1}-el a másodikat d^{-1}-el. Ha csak egy 0 van feltehető, hogy ez b. Ekkor szorozzuk az első sort a^{-1}-el, a másodikat c^{-1}-el, majd a második oszlopot cd^{-1}-el. Mindenképpen olyan mátrixot kapunk amelyben csak 0-k és 1-esek vannak. Ilyen Rees-mátrix félcsoportokra pedig a szóprobléma a 2. és 3. tétel (utáni megjegyzés) szerint polinomiális.

Tehát az egyetlen nemtriviális eset az, amikor a mátrixban nincsenek 0-k. Ebben az esetben szorozzuk az első sort b^{-1}-el, a másodikat d^{-1}-el, majd az első oszlopot dc^{-1}-el. Ekkor minden elem 1 lesz, kivéve esetleg a bal felsőt. Tehát elég ilyen mátrixokra igazolni az állítást.

Legyen tehát G Abel-csoport, M a következő mátrix:

$$M = \begin{bmatrix} g & 1 \\ 1 & 1 \end{bmatrix} \quad \text{ahol } g \in G \quad o(g) = m$$

Legyen A a nekik megfelelő Rees-mátrix félcsoport és legyen $u = x_1 x_2 \dots x_n$ és $v = y_1 y_2 \dots y_k$ két tetszőleges szó.

Most két esetet különböztetünk meg aszerint, hogy A-ban van-e 0 elem vagy sem. Mivel a mátrixban nincsenek nullák mindkét eset lehetséges, és ez a szóproblémát valamelyest meg is változtatja.

1. eset: Ha $0 \notin A$ akkor: $A \models u = v$ akkor és csak akkor, ha a következő 4 feltétel teljesül:

1. $x_1 = y_1$
2. $x_n = y_k$
3. $G \models u = v$
4. $\widetilde{G}_u \equiv \widetilde{G}_v \; mod \; m$

2. eset: Ha $0 \in A$ akkor: $A \models u = v$ akkor és csak akkor, ha a következő 5 feltétel teljesül:

1. $x_1 = y_1$
2. $x_n = y_k$
3. $G \models u = v$
4. $\widetilde{G}_u \equiv \widetilde{G}_v \; mod \; m$
5. $c(u) = c(v)$

Tehát az azonosság teljesülésének feltételei, hogy a két szó első és utolsó betűje megegyezik, az azonosság teljesül G-ben, a gráfok kongruenciája azt jelenti, hogy a kettő husszu részszavak száma a két oldalon megegyezik mod m, és egy extra feltétel, ha a félcsoportban van 0 elem akkor a két szónak ugyanazon változókból kell állni: $c(u)$ jelöli a szó változóit.

Bizonyítás: először tegyük fel, tehát, hogy $u = v$ teljesül A-ban, és ellenőrizzük sorban a megadott féltételek teljesülését:

Tekintsük az $a := (2, 1, 2)$ és a $b := (1, 1, 2)$ elemeket. Ezekre a következő szorzási szabály áll fenn: $a^2 = a$, $b^2 = b$, $ab = a$, $ba = b$, azaz a szorzat értéke mindig a baloldali tényező. Most tekintsük azt az E értékelést amelynél

$$E(x_1) = a \;\; E(z) = b \;\; \forall z \neq x_1$$

Ekkor $E(u) = a$, $E(v) = E(y_1)$ ez pedig csak úgy lehet egyenlő a-val, ha $y_1 = x_1$. Ezzel be is láttuk az első feltételt.
Ugyanígy látható be, a második feltétel ehhez például a $(2, 1, 1)$ és $(2, 1, 2)$ elemeket kell nézni: ezeknek a szorzata mindig a jobboldali.

A 3. feltétel ellenőrzéséhez csak azt kell észrevenni, hogy az $\{(2, g, 2) : g \in G\}$ elemek G-vel izomorf részcsoportot alkotnak A-ban.

Végezetül nézzük a 4. feltételt: tegyük fel, hogy az xy él k-szoros $\widetilde{G}_u$-ban és l-szeres $\widetilde{G}_v$-ben másszóval az xy részszó k-szor szerepel u-ban és l-szer v-ben ($k, l \geq 0$ egész számok.) Most a következő behelyettesítést nézzük:

$$E(x) := (2, 1, 1) \quad E(y) := (1, 1, 2) \quad E(z) := (2, 1, 2) \quad \text{ha } z \neq x, y$$

Itt $E(u)$-ban a csoportelem éppen g^k, $E(v)$-ben pedig g^l, mert extra g-k csak x és y találkozásánál jöhetnek be. Ezek pedig akkor és csakis akkor egyenlőek, ha $k \equiv l \; mod \; m$

A 2. esetben még azt is be kell látni, hogy $c(u) = c(v)$. Ha ez nem teljesülne, legyen például $x \in c(u) \setminus c(v)$, azaz x olyan változó, mely szerepel u-ban, de nem szerepel v-ben. Tekintsük ekkor a következő értékelést:

$$E(x) = 0 \qquad E(y) = (2, 1, 2) \quad \text{ha } y \neq x$$

Itt $E(u) = 0 \neq (2, 1, 2) = E(v)$, tehát az azonosság nem teljesülne.

Nézzük a fordított irányt: az első esetben tegyük fel, hogy u-ra és v-re teljesül a négy feltétel, és legyen E a változók tetszőleges kiértékelése. Mivel u és v ugyanazon betűvel kezdődik és végződik $E(u)$ és $E(v)$ első és utolsó koordinátája megegyezik. (Rees-mátrix félcsoportban bármely szorzat értékének első illetve utolsó koordinátája csak a szorzat első illetve utolsó tényezőjétől függ). Tekintsük a csoportelemet: ez sok tényezős szorzat mely tetszőlegesen átrendezhető. Bontsuk a tényezőit két részre aszerint, hogy miért kerültek a szorzatba, azaz válasszuk le a behelyettesítésnél eleve szereplő elemekről a szorzás során keletkező extra g-ket. A 3. feltétel szerint a szorzat első része u-ban illetve v-ben ugyanaz, a 4. tulajdonság miatt pedig az extra g-k is ugyanannyiszor szerepelnek $mod \; m$, tehát ezek is egyenlőek.

Most nézzük a második esetet: csak azt kell még észrevenni, hogy a 0-tól különböző elemek halmaza zárt a szorzásra, ezért tetszőleges E értékelés mellett, minden w szó esetén: $E(w) = 0 \iff \exists x \in c(w) : E(x) = 0$. Emiatt $E(u) = 0 \implies \exists x \in c(u) = c(v) : E(x) = 0 \implies E(v) = 0$ és viszont, tehát a két szó minden értékelés esetén egyszerre válik A-ban 0-vá. Ugyanakkor az 1. eset bizonyításánál láttuk, hogy ha egyik szó sem 0, akkor egyenlőek. Ezzel mindkét eset bizonyítva van.

Mindebből már nyilván következik a 4. tétel, mert a megadott feltételek polinom-időben ellenőrizhetőek. Mégis megvizsgálva a bizonyítást többet is mondhatunk.

Az $u = v$ azonosság pontosan akkor teljesül A-ban (minden értékelés mellett), ha teljesülnek rá a triviális ($x_1 = y_1$ és $x_n = y_k$) feltételek és teljesül minden olyan értékelés mellett, ahol legfeljebb 2 kivétellel minden változó helyére a $(2, 1, 2)$ elemet helyettesítjük. (A feltételek szükségességének igazolásakor csak ilyen behelyettesítéseket használtunk.) A szóprobléma tehát polinomsok behelyettesítés leelenőrzésével is eldönthető, ez pedig megtehető $O(N^2)$ időben, ha N az azonosság hossza azaz $n + k$.

Nézzük most meg, mi lesz, ha elengedünk valamit a tétel feltételeiből. Próbáljuk megtalálni a legegyszerűbb olyan példát, amivel még nem foglalkoztunk. A legkisebb szóbajövő csoport a két elemű, a legkisebb szóbajövő mátrix 3×3-as. Könnyű meggondolni, hogy ha egy 3×3-as mátrixban legalább 4 db 0 van, akkor a sorok és oszlpok szorozgatásával elérhető, hogy minden csoportelem az egységelem legyen. Ezekre pedig a szóprobléma polinomiális. Legyen tehát a mátrixban pontosan 3 db 0. Vegyük azt a szép szimmetrikus esetet, amikor mindhárom 0 külön sorban és oszlopban van, azaz feltehető, hogy a mellékátlóban helyezkednek el. Ismét sorok és oszlopok szorozgatásával elérhető, hogy a mátrixban minden nemnulla elem egyetlen kivétellel 1 legyen. Ez az egy kimaradó elem tehát a két elemű csoport generátoreleme:

$$M = \begin{bmatrix} a & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad \text{ahol } a \in Z_2 \quad a^2 = 1$$

A kapott félcsoport 19 elemű és M_{19}-nek nevezik. M_{19} szóproblémája mára már ismert eredmény, ez valóban "nehéz":

5. Tétel (Vértesi Vera, Svetlana Plescheva): M_{19}-ben az azonosság-ellenőrzés coNP-teljes.

Nem ismert, hogy mi a helyzet abban az esetben, ha a nem a kettő, hanem például a három elemű (vagy valami más) csoport (generátor)eleme. Ne vonjuk le azonban ebből azt a következtetést, hogy a 3×3-as (vagy nagyobb) mátrixok esete reménytelen. M_{19}-el valószínűleg sikerült megtalálnunk az egyetlen igazán bonyolult példát. Nézzünk meg még néhány mátrixot:

Változtassuk M_{19} mátrixában a középső 0-t 1-re, és nézzük mi változik:

$$M := \begin{bmatrix} a & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad \text{ahol } a \in Z_2 = \langle a \rangle$$

A kapott félcsoport látszólg "majdnem ugyanolyan" mint M_{19}, ez azonban valóban csak a látszat. Jelöljük ezt a félcsoportot mondjuk N_{19}-el. Könnyű meggondolni, hogy N_{19} szóproblémája polinomiális, sőt a következő feltételek karakterizálják:

Legyen $u = x_1 \dots x_n$, $v = y_1 \dots y_k$ két tetszőleges szó. $N_{19} \models u = v \iff$

1. $x_1 = y_1$
2. $x_n = y_k$
3. $Z_2 \models u = v$
4. $\widetilde{G}_u \equiv \widetilde{G}_v \ mod\ 2$
5. $G_u = G_v$

A bizonyításhoz csak azt kell észrevenni, hogy a bal felső 2×2-es részmátrix miatt az $\{(i, g, \lambda) : i, \lambda \in \{1, 2\}, g \in Z_2\}$ elemek olyan részfélcsoportot alkotnak, amiről a 4. tétel szólt, az első 4 feltétel az ottaniaknak speciális esete. Az 5. feltétellel kapcsolatos jelenséget érdemes általánosan bizonyítani, mert később is felhasználjuk majd.

2. Lemma: Tegyük fel, hogy az A Rees-mátrix félcsoport mátrixában van az alábbi mátrixal szimmetria (tükrözés, elforgatás) erejéig megegyező alakú részmátrix:

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \quad a,\ b,\ d \neq 0$$

Ekkor: Tetszőleges u és v szavak esetén a következő ekvivalencia teljesül:

$$\forall\ E \text{ értékelésre } E(u) = 0 \Leftrightarrow E(v) = 0 \iff G_u = G_v$$

Bizonyítás: Az egyszerűbb jelölés kedvéért tegyük fel, hogy a fenti részmátrix a mátrix bal felső sarkában van. (Ez nem jelenti az általánosság megszorítását.) Tegyük fel először, hogy a két gráf különbözik. Ez kétféleképpen fordulhat elő: vagy csúcshalmazuk különbözik, vagy élhalmazuk.
A csúcshalmazok különbözősége éppen azt jelenti, hogy $c(u) \neq c(v)$ azaz van olyan x változó mely szerepel u-ban de v-ben nem (vagy fordítva). Ekkor azonban vehetjük azt az E értékelést amelyre:

$$E(x) = 0,\ E(y) = (2, 1, 2) \text{ ha } y \neq x.$$

Ekkor $E(u) = 0 \neq (2, d^{|v|-1,2}) = E(v)$ lenne, ez tehát nem fordulhat elő.

Ha két gráf élhalmaza különbözik az pedig azt jelenti, hogy például az xy részszó szerepel u-ban de v-ben nem, (vagy fordítva). Ekkor tekintsük azt az E értékelést amelynél:

$$E(x) = (1, 1, 2),\ E(y) = (1, 1, 1,),\ E(z) = (2, 1, 1) \text{ ha } z \neq x, y$$

Ekkor is $E(x) = 0 \neq E(y)$ tehát ez sem fordulhat elő.

A megfordításhoz csak azt kell észrevenni, hogy Rees-mátrix félcsoportban bármely $n \geq 2$ elemre: $a_1 a_2 \dots a_n = 0$ pontosan akkor teljesül, ha van olyan i index, melyre $a_i a_{i+1} = 0$. Ezért, ha a gráfok megegyeznek, akkor: $\forall$ E értékelésre $E(u) = 0$ esetén $\exists$ xy részszó, hogy $E(xy) = 0$ de xy részszó v-ben is, így $E(v) = 0$.

Ebből valóban következik, az 5. feltétel szükségessége. Megfordítva pedig az 5. feltétel szerint a két szó egyszerre 0, az első négy feltétel pedig azt biztosítja, hogy ha egyik szó sem nulla, akkor egyenlőek (a 4. tétel bizonyításának gondolatmenete szerint).

Felmerül a kérdés mi okozza az M_{19} és N_{19} közti drasztikus különbséget. Úgy tűnik a szóprobléma nagyon érzékeny a mátrixban levő nullák számára, de éppen fordítva, mint ahogy várható. Rossz koncepció azt gondolni, hogy a Rees-mátrix félcsoport annál egyszerűbb, minél több 0-t tartalmaz a mátrixa. Éppen ellenkezőleg. Ezt támasztja alá, a következő állítás, mely könnyen következik már eddigi okoskodásainkból:

6. Tétel: Legyen az A Abel-csoport fölötti Rees-mátrix félcsoport mátrixa 3×3-as, melyben legfeljebb két 0 van. Ekkor: A szóproblémája P-beli.

Bizonyítás: Két 0 esetén két lényegesen különböző eset van: ha a két 0 két különböző sorban és oszlopban van, feltehető, hogy ezek a bal alsó és jobb felső elem. Szorozzuk mindhárom sort a középső elem inverzével, majd az első és harmadik sort is a középső elem inverzével. Ha mindkét 0 ugyanabban az oszlopban van, akkor legyenek a jobb felső és alsó elem. Ugyanúgy mint az előző estben, most is eltüntethető a középső sor és oszlop. Ha a mátrixban egyetlen egy 0 elem van, legyen ez a középső. Most például a harmadik sor és oszlop tüntethető el.

Tehát a következő alakú mátrixok léphetnek fel:

$$M_1 = \begin{bmatrix} a & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & b \end{bmatrix} \quad M_2 = \begin{bmatrix} a & 1 & 0 \\ 1 & 1 & 1 \\ b & 1 & 0 \end{bmatrix} \quad M_3 = \begin{bmatrix} a & b & 1 \\ c & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

A szóproblémát mindhárom esetben az alábbi feltételek oldják meg:

1. $x_1 = y_1$
2. $x_n = y_k$
3. $G \models u = v$
4. $\widetilde{G}_u \equiv \widetilde{G}_v \; mod \; m$
5. $G_u = G_v$

Ahol m a mátrixban lévő elemek rendjeinek legkisebb közös többszöröse.

Foglaljuk össze az általános bizonyítási sémát: az első három feltétel szükségessége triviális; az öt feltétel együttes elégségessége szintén; az 5. feltétel mindig $G_u = G_v$ vagy $c(u) = c(v)$ (ha a mátrixban nincs 0 de a félcsoportban van) vagy semmi: ez biztosítja hogy a két szó egyszerre legyen 0; a másik négy biztosítja, hogy ha egyik szó értéke sem 0, akkor egyenlőek. A kritikus lépés mindig az, hogy tudjuk-e (speciális behelyettesítésekkel) igazolni a 4. és 5. feltétel szükségességét. Nézzük: az 5.-hez a 2. lemmában megadott részmátrixot elegendő találni, ilyen pedig mindhárom mátrixban van, például a jobb felső sarokban. A 4. feltétel azt jelenti, $\widetilde{G}_u \equiv \widetilde{G}_v \; mod \; o(g)$ $\forall$ g a mátrixban szereplő csoportelemre. Ehhez pedig a 4. tétel miatt elég

$$\begin{bmatrix} g & 1 \\ 1 & 1 \end{bmatrix} \quad g \in M$$

alakú részmátrixokat találni, mert a feltétel már az ehhez tartozó részfélcsoportban is szükséges. A fenti mátrixokban ilyenek is vannak, úgyhogy ezzel az esettel is készen vagyunk.

Mindebből már nyilvánvaló, hogy hogyan kell igazolni azt az esetet, ha egyáltalán nincs a mátrixban 0. Ekkor a középső oszlop és sor tüntethető el, a mátrix alakja ilyen lesz:

$$\begin{bmatrix} a & 1 & b \\ 1 & 1 & 1 \\ c & 1 & d \end{bmatrix}$$

Világos, hogy mik a szóprobléma feltételei: $m := lkkt(o(a), o(b), o(c), o(d))$

1. $x_1 = y_1$
2. $x_n = y_k$
3. $G \models u = v$
4. $\widetilde{G}_u \equiv \widetilde{G}_v \ mod \ m$
5. $c(u) = c(v)$

Meg vannak a megfelelő részmátrixok, úgyhogy a hozzá tartozó A félcsoportban az $A \models u = v$ szóprobléma ekvivalens az első 4 feltétel teljesülésével, ha $0 \notin A$ és mind az 5 feltétel teljesülésével, ha $0 \in A$.

Ezek alapján azt gondolhatnánk, hogy a szóproblémánál a döntő feltétel a mátrixban lévő 0-k száma. De ez sem igaz. Nézzük meg a kihagyott eseteket: három db 0 esetén három lehetőség van: a három 0 elfoglalhat három künönböző sort és oszlopot, két oszlopot és három sort, vagy két oszlopot és két sort. 1 kivétellel minden csoportelem eltüntethető a mátrixból, sorok, oszlopok cseréje után az alábbi lehetőségek maradnak meg:

$$\begin{bmatrix} a & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} b & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & c & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

A bal oldali mátrix éppen M_{19}, ha $\langle a \rangle = \mathbb{Z}_2$ és ebben az esetben a szóprobléma coNP-teljes. Más csoportokra ez ugyan még nincs bizonyítva, de valószínűleg igaz. A másik két mátrixban azonban megvannak a megfelelő részmátrixok, a szóproblémát éppen a 6. tétel első felében leírt feltételek oldják meg. Ezzel az összes 3×3-as mátrixot letárgyaltuk

Foglaljuk össze az eddigieket: Legyen A Abel-csoport fölötti Rees-mátrix félcsoport. Ha A mátrixa 2×2-es akkor szóproblémája polinomiális, ha 3×3-as akkor a szóproblémát a mátrixban lévő 0-k elhelyezkedése dönti el, és mindig polinomiális, kivéve azt az egyetlen esetet amikor a 0-k az átló mentén helyezkednek el, akkor pedig legalábbis $\mathbb{Z}_2$ fölött coNP-teljes. Ezek szerint Rees-mátrix félcsoport szóproblémáját a mátrixában lévő 0-k konfigurációja dönti el, az egyes csoportelemeknek nincs akkara jelentőségük. Az eddigi trükkök felhasználásával igazolható még egy egyszerű állítás.

7. Tétel: Legyen az A Abel-csoport fölötti Rees-mátrix félcsoport M mátrixa (tetszőleges $n \times k$ -as, de) olyan, melyben van olyan sor és oszlop is melyben nincs 0. Ekkor: A szóproblémája polinomiális.

Bizonyítás: Feltehető, hogy az utolsó sor és oszlop csupa 1 (mert minden sort és oszlopot végigszorozhatunk utolsó elemének inverzével). Ha m a mátrixban lévő elemek rendjeinek legkisebb közös többszöröse, a szóproblémának megoldása : $A \models u = v \Leftrightarrow x_1 = y_1,\ x_n = y_k,\ G \models u = v$ és

$$\begin{array}{l} \widetilde{G}_u \equiv \widetilde{G}_v\ (m) \\ \mathrm{G}_u = G_v \end{array} \quad \text{vagy} \quad \begin{array}{l} \widetilde{G}_u \equiv \widetilde{G}_v\ (m) \\ c(u) = c(v) \end{array} \quad \text{vagy} \quad \widetilde{G}_u \equiv \widetilde{G}_v\ (m)$$

attól függően, hogy $0 \in M$ vagy $0 \notin M$ de $0 \in A$ vagy $0 \notin A$.

A gráfokra vonatkozó feltételek igazolásához csak azt kell látni, hogy ha $M(\lambda, i) = g \neq 0$ vagy, ha $M(\lambda, i) = 0$ akkor is, az $M(\lambda, i)$, $M(\lambda, k)$, $M(n, i)$ és $M(n, k)$ elemek olyan részmátrixot alkotnak amire szükségünk van.

Mivel minden mátrixhoz hozzávehetünk egy csupa 1 oszlopot és sort ezzel azt is bebizonyítottuk, hogy sajnos Rees-mátrix félcsoportok esetén a szóprobléma NP-teljessége nem következik abból, hogy ezt esetleg egy kisebbre már tudjuk. Pontosabban:

Következmény: Minden Rees-mátrix félcsoport beágyazható egy olyanba, melynek szóproblémája polinomiális.

Vizsgáljuk meg most azt a kérdést, hogy mi a helyzet a Rees-mátrix félcsoporttal, ha a mátrixára nem teljesül a 2. lemma feltétele. Először is fogalmazzuk meg egyszerűbben ezt az esetet. A 2. lemma feltételének nem teljesülése azt jelenti, hogy minden 2×2-es részmátrixban, ha 3 elem nem nulla, akkor a negyedik sem, vagy másszóval, ha van benne nulla, akkor legalább kettő van. Ezek éppen azok a mátrixok, melyek sorok és oszlopok cseréjével (diagonális) blokkmátrixá alakíthatóak (a blokkokon kívül minden elem nulla, a blokkokon belül azonban nincsenek nullák). Ezek a mátrixok kimaradtak eddigi részletesebb vizsgálatainkból, most azonban rátérünk erre is. Első célunk a 2. lemmához hasonló feltételt találni arra, hogy az ilyen félcsoportokban mikor válik két szó mindig egyszerre nullává. Ezt a problémát most külön is megfogalmazzuk.

Legyen A egy olyan félcsoport, melyben van 0 elem. TERM-0-SET(A) az a probléma, mely két kifejezésről azt kérdezi, hogy A-ban mindig egyszerre válnak-e nullává. Az előző esetekben ennek a problémának mindig nagyon egyszerű megoldása adódott. Blokkmátrixokra a dolog kicsit nehezebb. Megkönnyíti azonban a dolgunkat az az észrevétel, hogy ezt a kérdést elég teljesen kombinatorikus 0-egyszerű félcsoportok fölött vizsgálni.
Legyen ugyanis A tetszőleges Rees-mátrix félcsoport G struktúracsoporttal és M mátrixal. Az A kombinatorikus redukáltjának nevezzük azt az A' teljesen kombinatorikus 0-egyszerű félcsoportot, melynek mátrixát úgy kapjuk M ből, hogy minden csoportelemet 1-el helyettesítünk, a nullákat pedig természetesen változatlanul hagyjuk. Ezzel olyan félcsoportot kapunk, amely A-nak homomorf képe a "középső koordináta eltörlése" függvénynél, azonban megőriz A-ról néhány lényeges információt, többek között egy kifejezés nemnulla-ságát. Ezért a TERM-0-SET problémát elég A'-ben megoldani, azaz ha u és v két kifejezés, akkor A-ban u és v pontosan akkor lesz mindig egyszerre nulla, ha A'-ben mindig egyszerre nulla.

3. Lemma (Seif-Szabó): Legyen M egy 0-1-es blokkmátrix, mely tényleg tartalmaz 0-t azaz legalább két blokkból áll. Legyen A az M-hez tartozó Rees-mátrix félcsoport.
Ekkor a TERM-0-SET(A) probléma polinomiális, és pontosan a következő feltétel határozza meg: minden u és v kifejezés esetén u és v mindig egyszerre válik A-ban 0-vá, pontosan akkor, ha G_u-ban és G_v-ben ugyanazok az összefüggőségi komponensek (beleértve természetesen, hogy a két gráf egyazon csúcshalmazon van adva, azaz u és v ugyanazon változókból áll.)

A jelenlegi kérdés szempontjából teljesen lényegtelen, hogy pontosan milyen feltételek oldják meg a TERM-0-SET problémát. A fontos az az egyszerű észrevétel, hogy egy Rees-mátrix félcsoport fölött az a kérdés mindig polinomiális, hogy két kifejezés egyszerre lesz-e mindig nulla vagy sem. Ez részét képezi a szóprobléma megoldásának. Ezt felhasználva beláthatjuk, hogy a teljesen kombinatorikus 0-egyszerű félcsoportok szóproblémájának polinomialitása tetszőleges Rees-mátrix félcsoportra érvényben marad blokkmátrixok esetén.

8. Tétel: Legyen A olyan Rees-mátrix félcsoport melynek G struktúracsoportja kommutatív és M mátrixa blokkmátrix. Ekkor A-ban az azonosságellenőrzés polinomiális.

Bizonyítás: Nézzük csak a nemtriviális eseteket: feltehető, hogy a mátrixnak van legalább két sora és oszlopa, és tartalmaz legalább egy db. legalább 2×2-es blokkot (sor- vagy oszlop- illetve diagonális mátrix esetén feltehető, hogy nincs benne 1-től különböző csoportelem, erre az esetre pedig igaz a tétel). Most szorozzunk meg minden sort és oszlopot utolsó nemnulla elemének inverzével. Ekkor külön-külön minden blokk utolsó sora és oszlopa csupa 1 lesz. Jelölje m a mátrixban levő csoportelemek rendjeinek legkisebb közös többszörösét. Ekkor a szóproblémát meghatározó feltételek a következőképpen foglalhatóak össze: $A \models u = v \Leftrightarrow$ ha:

1. $x_1 = y_1$
2. $x_n = y_k$
3. $G \models u = v$
4. $\widetilde{G}_u \equiv \widetilde{G}_v \ mod\ m$
5. $E(u) = 0$ és $E(v) = 0$ minden E értékelés esetén egyszerre teljesül

Mindez nem szorul bizonyításra. Az első két feltétel szükségességének biztosítása érdekében zártuk ki a triviális eseteket. A harmadik és ötödik feltétel szükségessége triviális, ahogyan az öt feltétel együttes elégségessége is. A 4. feltétel szükségességét a csupa 1 sorok és oszlopok miatt létező részmátrixok biztosítják. A 3. lemma szerint az 5. feltétel is polinom-időben tesztelhető, sőt részletesen megfogalmazhatjuk mit jelent: G_u-ban és G_v-ben ugyanazok az összefüggőségi kompononsek, ha M legalább két blokkból áll, $c(u) = c(v)$ ha egyetlen blokk van, azaz a mátrixban nincs nemnulla elem, de A-ban van, és nem létező feltétel, ha A-ban nincs 0 elem.

Összefoglalva az eddigieket: Abel-csoport fölötti Rees-mátrix félcsoportok szóproblémájának vizsgálata során kiderül, hogy egy azonosság teljesülésének 4 triviális szükséges és egy 5. elégséges feltétele van, mely teljesülése esetén a szóprobléma P-beli. Blokkmátrixokra mind az öt feltétel igyazolható, ezért ezekre a szóprobléma polinomiális. Nem blokkmátrixok esetés a szóprobléma kapcsán egy gráfokra vonatkozó kongruenciafeltétel bizonyult vízválasztónak. Amennyiben ez speciális behelyettesítésekkel igazolható, abban az esetben a szóprobléma P-beli. Könnyen elképzelhető, hogy ez megfordítva is igaz. Az eddig bizonyított tételek ennek legalábbis nem mondanak ellent.

Normális azonosságok

Definíció: Az $u = v$ félcsoportazonosságot normálisnak nevezzü, ha mindkét oldalon ugyanazok a változók szerepelnek, azaz $c(u) = c(v)$.

Rees-mátrix félcsoportoknál azt tapasztaltuk, hogy ez a feltétel mindig akkor jelentkezik a szóprobléma kapcsán, ha a félcsoportban van 0 elem. Most bebizonyítjuk, hogy ez tényleg mindig így van.

1. Tétel: Legyen A egy Rees-mátrix félcsoport. Ekkor a következő két állítás ekvivalens:

1. Minden A-ban teljesülő azonosság normális
2. $0 \in A$

Bizonyítás : felhasználjuk a következő egyszerű észrevételt: Minden Rees-mátrix félcsoportban van (nullától különböző) idempotens elem. Ugyanis legyenek λ és i olyan indexek, amelyre A mátrixában $M(\lambda, i) = g \neq 0$ Ekkor (i, g^{-1}, λ) idempotens.

Most tegyük fel először, hogy $0 \in A$, és legyen $A \ni a \neq 0$ idempotens elem. Ha most u és v olyan szavak, amelyekre például $x \in c(u) \setminus c(v)$ akkor tekintsük azt az E értékelést melyre:

$$E(x) = 0 \quad E(y) = a \quad \forall y \neq x$$

Ezen értékelésnél: $E(u) = 0 \neq a = E(v)$.

A fordított irányhoz tegyük fel, hogy $0 \notin A$. Megmutatjuk, hogy ekkor A-ban teljesül az $(xyx)^n = (xzx)^n$ nem normális azonosság, ahol n a stuktúracsoport exponense. Legyen ehhez E tetszőleges értékelés és jelöljük az egyes változók értékeit a következőképpen:

$$E(x) = (i, g, \lambda) \quad E(y) = (j, h, \mu)$$

Valamint vezessük be a mátrix egyes elemeire is a következő jelöléseket:

$$M(\lambda, j) = g_1 \quad M(\mu, i) = g_2 \quad M(\lambda, i) = g_3$$

Számoljuk most ki, mi lesz az $E((xyx)^n) \in A$ középső koordinátája, azaz a csoportelem: az xyx-hez tartozó (gg_1hg_2g) elemből n db melyet $n-1$ db g_3 választ el egymástól, ez lesz:

$$(gg_1hg_2g)g_3(gg_1hg_2g)g_3 \dots g_3(gg_1hg_2g) = [(gg_1hg_2g)g_3]^n g_3^{-1} = g_3^{-1}$$

g_3 azonban nem függ $E(y)$-tól, csak $E(x)$-től. Ha y-t lecseréljük egy másik változóra, ez az elem nem változik, azaz $E((xzx)^n)$-ben ugyanezt kapjuk. Tehát: $E((xyx)^n) = (i, g_3^{-1}, \lambda) = E((xzx)^n)$ minden E értékelés mellett.
Azaz $A \models (xyx)^n = (xzx)^n$ ahogy állítottuk.

A bizonyítás során a következőt használtuk ki: van $\{a, b\} \subseteq A$ két elemű részfélcsoport a következő szorzási szabályokkal:

$$a^2 = a \quad b^2 = b \quad ab = ba = a$$

Definíció: A fenti félcsoportot két elemű félhálónak nevezzük.

Az tétel bizonyításában éppen azt használtuk, hogy (a 0 és egy idempotens elem kételemű félhálót alkot és) a kételemű félhálóban csak normális azonosságok teljesülnek. Az tételt tehát átfogalmazhatjuk a következőképpen:

1. Következmény: minden A Rees-mátrix félcsoportra ekvivalensek:

1. A-ban minden azonosság normális
2. a kételemű félháló részfélcsoport A-ban

A továbbiakban az lesz a cél, hogy a fentihez hasonló szükséges és elégséges feltételt adjunk arra, hogy egy félcsoportban minden azonosság normális legyen. Az 1. következmény természetesen nem igaz minden félcsoportra, ahogyan azt a természetes számok példája is mutatja.

Azonosságok vizsgálatakor azonban nem egy-egy félcsoportot célszerű megnézni, hiszen egy azonosság teljesülése (illetve nem teljesülése) egy egész varietásra jellemző tulajdonság. Érdemes ezért néhány varietásról eldönteni, hogy minden azonossága normális-e.

Tétel (Birkhoff): félcsoportok egy V osztályára ekvivalensek a következők:

1. V zárt a részalgebra (S), homomorf kép (H) és direkt szorzat (P) operációkra
2. V azonosságokkal definiálható, azaz $\exists\ \Sigma$ azonosságokból álló halmaz, amivel: $\forall\ A$ félcsoportra $A \in V \iff A \models \Sigma$

Ebben az esetben V-t varietásnak nevezzük.
A V varietás normális, ha minden V-ben teljesülő azonosság normális, ellenkező esetben V nem normális.

2. Tétel: A minimális félcsoportvariátások a következők:

1. Balzéró félcsoportok: BZ
2. Jobbzéró félcsoportok: JZ
3. Zéró félcsoportok: Z
4. Félhálók: FH
5. valamely prímrendű ciklikus csoport által generált varietás: Z_p

Nézzük sorban mik ezek:

balzéró: definiáljuk tetszőleges alaphalmazon a szorzást az $ab := a$ képlettel; világos, hogy így egy félcsoportot kapunk, és az összes ilyen félcsoport egy varietást alkot melyet az $xy = xz$ azonosság definiál

jobbzéró: az előző duálisa, a szorzási szabály: $ab = b$

zéró: legyen tetszőleges $H \neq \emptyset$ alaphalmazon bármely két elem szorzata ugyanaz a $0 \in H$ elem; az összes ilyen félcsoportból álló varietás bázisa nyilván $xy = zv$;

félhálók: idempotens és kommutatív félcsoportok; mivel ez minimális varietás ez ugyanaz mint a kételemű félháló által generált varietás;

Z_p: a p-edrendű ciklikus csoport által generált félcsoportvarietás; ez ugyanaz mintha a generált csoportvarietást néznénk: éppen a p expononsű kommutatív csoportokból áll;

1. Lemma: Legyen G tetszőleges csoport. Ekkor a G által generált félcsoportvarietásban, $V(G)$-ben pontosan akkor találhatóak valódi félcsoportok (amelyek nem csoportok) ha G exponense végtelen.

Bizonyítás: Az egységelem és inverz létezése nyilván öröklődik a direkt szorzatra és a homomorf képre és ha x benne van egy csoport részfélcsoportjában és x véges rendű elem, akkor hatványai előbb utóbb kiadják az inverzét és az egységelemet is, így minden részfélcsoport csoport.

Ha viszont G exponense végtelen akkor $\forall n\ \exists x_n$ legalább n-edrendű elem, de akkor a generált részcsoportok $\prod \langle x_n \rangle$ direkt szorzatában van végtelen rendű elem, melynek hatványai a természetes számokkal izomorf részfélcsoportot alkotnak.

Jelölje most H a félcsoportvarietások hálóját és vizsgáljuk meg néhány elemi tulajdonságát, melyet később fel fogunk használni. Minimális elemeit már ismerjük, ezt foglalja össze a 2. tétel: BZ, JZ, Z, FH és Z_p. Mindegyikben van nem normális azonosság kivéve persze a félhálókat amiben nem is lehet. Ezek közül véges sok FH-tól különbözőnek az uniójában szintén, hiszen ha r jelöli azon véges sok prím szorzatát amely Z_p-k az egyesítésben szerepelnek, akkor az $xy^r x = xz^r x$ teljesül mindegyikben. Annál meglepőbb, hogy hogyan viselkedik végtelen sok minimális félcsoportvarietás egyesítése.

3. Tétel: Végtelen sok minimális félcsoportvarietás egyesítése mindig tartalmaz kételemű félhálót (és így minden azonossága normális).

Ennél is erősebb tételt érdemes igazolni, éspedig a következőt:

4. Tétel: Legyen P tetszőleges végtelen prímhalmaz.
Ekkor: a $V := \bigvee Z_p$ varietás minden kommutatív félcsoportot tartalmaz.

A bizonyítás előtt tegyünk néhány egyszerű észrevételt. Jelölje G a szóbajövő prímekre a p-edrendű ciklikus csoportok direkt szorzatát. Ebben van végtelen rendű elem mely, $\mathbb{N}$-el izomorf félcsoportot generál. Megfordítva minden ciklikus csoport homomorf képe $\mathbb{N}$-nek ezért ezek benne vannak a $V(\mathbb{N})$ varietásban. Továbbá G-ben egységelem is van, mely egy végtelen rendű elemmel együtt $\mathbb{N} \cup \{0\}$-val izomorf félcsoportot generál. Azaz mind $\mathbb{N}$, mind $\mathbb{N} \cup \{0\}$ V-ben van, és generálja is V-t.

3. Tétel bizonyítása: Tekintsük az $\mathbb{N} \cup \{0\}$ félcsoportot. Ebben $\mathbb{N}$ egy ideál, húzzuk ezt össze egyetlen pontba. A keletkező félcsoport ekkor $\mathbb{N} \cup \{0\}$-nak homomorf képe, és a két elemű félhálóval izomorf.

Hasonlóan láthatjuk be, hogy a varietás tartalmaz zéró félcsoportot: ehhez az $\mathbb{N}$ félcsoportban húzzuk össze egyetlen ∞-el jelölt pontba az $\{2, 3, \ldots\}$ halmazt. A keletkező félcsoportban a most additívan írt művelet így működik:

$$1 + 1 = \infty + \infty = 1 + \infty = \infty + 1 = \infty$$

Másszóval ez egy két elemű zéró félcsoport, ahogy állítottuk.

4. Tétel bizonyítása: Tekintsük most az $\mathbb{N} \cup \{0\}$ félcsoport n-edik direkt hatványát, és hagyjuk el ebből a csopa 0 vektort. Világos, hogy ez a félcsoport is benne van V-ben. Ha belátjuk, hogy ez az n elem által generált szabad kommutatív félcsoport, akkor készen leszünk, mert a végesen generált szabad algebrák együtt már mindig generálják a varietást. Ez pedig teljesen triviális: ha φ tetszőlegesen előírt függvény a $(0, 0, \ldots, 1, 0, \ldots 0)$ elemeken, valamely kommutatív félcsoportba, akkor világos, hogy ezt hogyan kell kiterjeszteni tetszőleges $\vec{a} = (a_1, \ldots a_n) \in \mathbb{N} \cup \{0\}$ pontba:

$$\varphi(a_1, \ldots a_n) := \sum a_i \varphi(0, 0 \ldots, 1, 0, \ldots 0)$$

a műveletet most is aditívan írva. A kommutativitás biztosítja, hogy ez homomorfizmus. Ezzel a bizonyítást befejeztük.

Megjegyzés: a bizonyítás gondolatmeletéből világos, hogy a

$$Z_2 \leq Z_4 \leq \ldots Z_{2^i} \leq Z_{2^{i+1}} \leq \ldots$$

varietások láncának egyesítése is kiadja a teljes $V_{xy=yx}$ varietást. Speciálisan ez $\aleph_0$ sok nem normális varietás láncának egyesítése, amely már normális, tehát a nem normális varietások nem teljes részhálót alkotnak H-ban.

Térjünk vissza most ahhoz a kérdéshez, hogy mitől lesz egy varietás normális. A legtriviálisabb oka ennek, ha tartalmaz kételemű félhálót. Megmutatjuk, hogy ez megfordítva is igaz. Ez lesz a Rees-mátrix félcsoportokra bizonyított 1. következmény általánosítása: egy félcsoportban akkor és csakis akkor lesz minden azonosság normális, ha az általa generált varietásban van kételemű félháló.

5. Tétel: Ha V normális varietás akkor van benne kételemű félháló.

A bizonyításhoz szükség lesz néhány előkészítő és egyszerűsítő lépésre:

2. Lemma: Egy V varietás pontosan akkor minimális ha minden $A \in V$ $|A| \geq 2$ (nemtriviális) algebrája generálja.

Bizonyítás: triviális

Tekintsük most a félhálók FH varietását. Ez a kommutatív és idempotens félcsoportokból áll. A 2. lemma szerint bármely nem egy elemű félháló ugyanezt a varietást generálja (nem kisebbet). Ezért minden legalább kételemű félhálóban pontosan ugyanazok az azonosságok teljesülnek. És persze csak normális azonosságok. Megmutatjuk, hogy a normális azonosságok mind teljesülnek is:

3. Lemma : Kommutatív és idempotens félcsoportban (azaz félhálóban) minden normális azonosság teljesül.

Bizonyítás: Legyenek $u = x_1 x_2 \dots x_n \quad v = y_1 y_2 \dots y_k$ olyan szavak melyek ugyanazon változókból épülnek fel. És legyen A egy félháló. Megmutatjuk, hogy $A \models u = v$.

Először is a kommutativitás miatt a szavak változói szabadon permutálhatóak azaz u olyan u' szóvá alakítható, amelyben a változók növekvő indexek szerint rendezve állnak egymás után, azaz $u' = x_1^{a_1} x_2^{a_2} \dots x_l^{a_l}$ alakú ahol $a_i \geq 1$ és az x_i $(i = 1 \dots l)$ változók az u-ban előforduló összes különböző változó. Ekkor $A \models u = u'$. Mivel v ugyanezen változókból épül fel, v is átalakítható olyan $v' = x_1^{b_1} x_2^{b_2} \dots x_l^{b_l}$ szóvá melyben ugyanezek a változók ugyanebben a sorrendben csak esetleg más kitevővel szerepelnek, és persze $A \models v = v'$.

Végül, mivel A idempotens a kitevőket el szabad hagyni, azaz: A-ban: $u' = x_1^{a_1} x_2^{a_2} \dots x_l^{a_l} = x_1 x_2 \dots x_l$ és ugyanígy $v' = x_1^{b_1} x_2^{b_2} \dots x_l^{b_l} = x_1 x_2 \dots x_l$.

Az így kapott szavak már betűről betűre megegyeznek, tehát minden félcsoportban egyenlőek.

2. Következmény: Tetszőleges A félcsoportra ekvivalensek a következők

1. A legalább két elemű félháló, azaz $V(A) = FH$
2. $A \models u = v \iff u = v$ normális azonosság

Ezzel két dogot értünk el az 5. tétel bizonyításával kapcsolatban. Egyrészt, ha meg akarjuk mutatni, hogy egy varietásban van két elemű félháló, ez azzal ekvivalens, hogy van benne akármilyen (nem egy elemű) félháló. Másrészt most már tudjuk, hogy miről lehet egy félhálót felismerni: ezek azok a félcsoportok amelyekben pontosan a normális azonosságok teljesülnek. Ez látszólag bonyolultabb jellemzés mint az, hogy "kommutatív és idempotens", mégis így érdemes leírni őket. Most már mindent előkészítettünk. Az 5. tételre két bizonyítást is adhatunk.

5. Tétel első bizonyítása: Legyen V normális varietás, és jelölje

$$F_\infty^V := F^V \langle x_1, x_2, \dots x_n \dots \rangle \in V \quad \text{illetve} \quad F_\infty := F \langle y_1, y_2, \dots y_n \dots \rangle$$

a megszámlálhatóan végtelen sok elemmel generált V-beli relatív szabad félcsoportot illetve a megszámlálhatóan végtelen sok elemmel generált szabad félcsoportot. Ekkor persze F_∞^V homomorf képe F_∞-nek. Jelölje

$$\varphi : F_\infty \longrightarrow F_\infty^V$$

azt a homomorfizmust ahol a genereátorok egymásnak felelnek meg azaz az $y_i \longmapsto x_i$ generátorokon adott leképezés F_∞-re való egyértelmű kiterjesztését. Jelölje

$$\Phi := Ker\varphi$$

a φ által F_∞-en meghatározott kongruenciát. Emellett jelölje Θ a következő kongruenciát:

$$\forall\ u, v \in F_\infty\ \ u \equiv v\ mod\ \Theta \Longleftrightarrow c(u) = c(v)$$

azaz Θ az a kongruencia, ahol az u és v szó pontosan akkor van egy osztályban ha az $u = v$ azonosság normális. (Könnyű ellenőrizni, hogy Θ kongruencia.) Jelölje A a Θ szerinti faktort: $A := F_\infty/\Theta$

Most két dogot kell még észrevenni: először is mivel F_∞^V a varietás szabad algebrája ezért tetszőleges $u = v$ azonosságra $V \models u = v \Longleftrightarrow \varphi(u) = \varphi(v)$ azaz ha $u \equiv v\ mod\ \Phi$. Erre az állításra úgy szokás hivatkozni, hogy egy varietásban egy azonosságot elég a szabad algebra szabad generátorain ellenőrizni. Mivel V-ben csak normális azonosságok teljesülnek ez azt jelenti, hogy

$$u \equiv v\ mod\ \Phi \implies c(u) = c(v) \iff u \equiv v\ mod\ \Theta$$

Tehát ha két szó Φ szerint egy osztályban van, akkor Θ szerint is, azaz röviden $\Phi \leq \Theta$. A második izomorfizmus tétel szerint ilyenkor F_∞^V tovább faktorizálható Θ-val, azaz A homomorf képe F_∞^V-nek is ezért $A \in V$.

Másrészről, mivel Θ teljesen invariáns kongruencia, a szerinte vett faktorban pontosan azok az azonasságok teljesülnek amikkel faktorizáltunk, azaz definíció szerint A-ban pontosan a normális azonosságok teljesülnek. Ez pedig a 2. következmény szerint éppen azt jelenti, hogy találtunk V-ben egy félhálót. Persze nem két elemű, hanem mindig végtelen, mert az F_∞ -beli generátorok képei mind künönbözőek, de az általa generált varietásban két elemű félháló is van, és ezzel a bizonyítást be is fejeztük.

Második bizonyítás: Minden varietást azonosságok definiálnak. Jelölje tetszőleges V vaietás esetén Σ_V a V-ben teljesülő összes azonosságok halmazát. Ekkor világos, hogy a következő összefüggések állnak fenn:

$$V = W \Longleftrightarrow \Sigma_V = \Sigma_W \quad V \leq W \Longleftrightarrow \Sigma_W \subseteq \Sigma_V \quad V \geq W \Longleftrightarrow \Sigma_W \supseteq \Sigma_V$$

Másszóval a $V \leftrightarrow \Sigma_V$ megfeleleltetés duális hálóizomorfizmus a varietások és az azonosságok zárt részhalmazai között. Mármost a bizonyítandó állítás a következő: ha V normális varietás, akkor $FH \leq V$. A fentiek szerint ez ekvivalens a következővel:

$$\Sigma_V \subseteq \Sigma_{FH}$$

A 3. lemma szerint itt a jobboldalon az összes normális azonosság áll, a fenti tartalmazás tehát csupán a normális varietás definíciója. Ezzel a bizonyítást befejeztük.

Azonosságok és részhálók

A továbbiakban az lesz a cél, hogy a normális varietások karakterizálására adott tételt általánosítsuk. Legyen Ψ félcsoportazonosságok egy részhalmaza. Egy V varietásra azt mondjuk, hogy Ψ-varietás ha minden V-ben teljesülő azonosság benne van Ψ-ben.
A kérdés az jellemezhető-e a Ψ-varietások osztálya oly módon, mint az 5. tételben, azaz van-e olyan A félcsoport, amelyre: V Ψ-varietás $\Leftrightarrow A \in V$, azaz van-e olyan W varietás amelyre: V Ψ-varietás $\Leftrightarrow W \leq V$, azaz van-e a Ψ-varietások között legkisebb. Megint másképpen fogalmazva ez azzal ekvivalens, hogy a félcsoportvarietások H hálójában a Ψ-varietások teljes részhálót ($\Leftrightarrow$ metszetzárt részhalmazt) alkotnak. Mivel a H hálóról nem sokat tudunk, érdekes lehet, ha legalább egyes (megengedett azonosságokkal adott) részhálóit jellemezni tudjuk.

A válasz a kérdésre bizonyos esetekben triviális. Ha Ψ azonosságok (következményre) zárt halmaza, akkor nyilván vehetjük az általa definiált varietást, ez a legkisebb. Az 5. tétel második bizonyítása éppen arra épült, hogy az összes normális azonosságok által definiált varietás is normális. Először foglaljuk össze, milyen tulajdonságok jellemzik az ilyen azonossághalmazokat.

1. Lemma: Legyen Σ azonosságok egy halmaza. Σ pontosan akkor zárt halmaz, ha a következő 5 tulajdonság igaz rá:

1. $\forall\ x$ változóra $x = x \in \Sigma$
2. $u = v \in \Sigma \Rightarrow v = u \in \Sigma$
3. $u = v \in \Sigma$ és $v = w \in \Sigma \Rightarrow u = w \in \Sigma$
4. $\forall\ x$ változóra $u = v \in \Sigma \Rightarrow ux = vx \in \Sigma$ és $xu = xv \in \Sigma$
5. $u = v \in \Sigma \Rightarrow u|_{x=w} = v|_{x=w} \in \Sigma$

ahol $u|_{x=w}$ jelöli azt a szót amelyet úgy kapunk, hogy az x változó helyére minden u-beli előfordulásában a w szót írjuk;

A zárt azonosságok ezen egyszerű jellemzését később fel fogjuk használni, hogy olyan azonossághalmazokról igazoljuk a zártságot, amelyekről az egyáltalán nem triviális.

Bizonyítás: Erősebb állítást érdemes igazolni: Legyen Σ azonosságok tetszőleges halmaza. Jelölje $\overline{\Sigma}$ a Σ-t tartalmazó legszűkebb zárt halmazt, azaz Σ következményeinek halmazát, és $\widetilde{\Sigma}$ azon legszűkebb Σ-t tartalmazó halmazt, amely zárt a lemmában megadott tulajdonságokra, azaz álljon $\widetilde{\Sigma}$ azon φ azonosságokból, melyek elérhetőek Σ-ból a lemmában megadott lépések véges sorozatával. Állítjuk, hogy $\overline{\Sigma} = \widetilde{\Sigma}$. Ebből a $\widetilde{\Sigma} \subseteq \overline{\Sigma}$ tartalmazás triviális: minden azonosság ami Σ-ból ily módon levezethető, az természetesen következmény. A fordított irányhoz azt kell izazolni, hogy $\widetilde{\Sigma}$ zárt halmaz. Ehhez legyen F_∞ a megszámlálhatóan végtelen sok elemmel generált szabad félcsoportot. Mármost tekintsük a $u \equiv v \Leftrightarrow u = v \in \widetilde{\Sigma}$ F_∞-beli relációt. A lemmában megfogalmazott 5 feltétel épp azt jelenti, hogy $\equiv$ teljesen invariáns kongruencia, ezért a szerinte vett $F_\infty/_\equiv$ faktorban éppen a $\widetilde{\Sigma}$-beli azonosságok teljesülnek, ezért $\widetilde{\Sigma}$ zárt halmaz.

Mármost az eredeti kérdésre visszatérve az 5. tétel két bizonyítását megvizsgálva két állitást fogalmazhatunk meg:

1. Állítás: Tegyük fel, hogy a Ψ azonossághalmazra teljesül az 1. lemmában megadott 5. db feltétel. Ekkor van legkisebb Ψ-varietás (melyben az összes Ψ-beli azonosság teljesül).

2. Állítás: Tegyük fel hogy, a Ψ azonossághalmazra teljesül az 1. lemmában megfogalmazott 5 feltételből az első négy. Ekkor: van legkisebb Ψ-varietás (melyben pontosan akkor teljesül minden Ψ-beli azonosság, ha az 5. feltétel is igaz rá).

Bizonyítás: az első állítás triviális, vehetjük a Ψ által definiált varietást. A másodikhoz, az 5. tétel első bizonyítását kell követni. Legyen V egy Ψ-varietás, és jelölje mint eddig $F_\infty = F\langle y_1, y_2 \ldots\rangle$ illetve $F_\infty^V = F^V\langle x_1, x_2 \ldots\rangle$ a $\aleph_0$ sok elemmel generált szabad, illetve a V-beli relatív szabad félcsoportot, valamint $\varphi : F_\infty \to F_\infty^V$ az $y_i \mapsto x_i$ megfeleltetés által meghatározott homomorfizmust, és legyen $\Phi = Ker\varphi$. Definiáljuk a $\equiv_\Psi$ relációt a következőképpen: $u \equiv_\Psi v \Leftrightarrow u = v \in \Psi$. A feltevéseink azt mondják, hogy $\equiv_\Psi$ kongruencia F_∞-en. Jelölje A az $F_\infty/\equiv_\Psi$ faktort. Ugyanúgy, mint az 5. tétel bizonyításában $A \in V$ azaz az A által generált W varietásra $W \leq V$. Mivel ez minden V-re igaz, és W nem függ V-től, csak Ψ-től, W a legkisebb Ψ-varietás Csak azt kell megmutatni, hogy tényleg csak Ψ-beli azonosságok teljesülnek benne. Ez az egyetlen eltérés az 5. tétel bizonyításához képest: W nem feltétlenül tud minden Ψ-beli azonosságot. Azonban, ha $u = v$ azonosság W-ben akkor speciálisn a $\psi : F_\infty \to A$ természetes homomorfizmusnál is ugyanaz a képük, de ekkor valóban $u = v \in \Psi$.

Nézzünk egy példát arra, hogy a 2. állítás olyan azonossághalmazokra is működik amire az 1. nem. Álljon Ψ azon $u = v$ azonosságokból, melyekre: $|u| = |v|$ azaz u és v ugyanolyan hosszú szó. Ekkor Ψ-re igaz az első 4 tulajdonság, de nem igaz az ötödik. A 2. állítás szerint ezen Ψ-varietások egy [W,1] intervallumot alkotnak H-ban. Kérdés, mi lesz W. A bizonyításból ez is kiderül: ha F_∞-ben két szót akkor tekintünk ekvivalensnek, ha ugyanolyan hosszúak, akkor ezen kongruencia szerinti faktor, a természetes számok halmaza. Ez generálja tehát a legkisebb Ψ-varietást. Azonban $\mathbb{N}$-ben nem teljesül az összes ilyen azonosság. Mint már láttuk az $\mathbb{N}$ által generált félcsoportvarietás az összes kommutatív félcsoportból áll. Hogy ebben milyen azonosságok teljesülnek, azt könnyű meggondolni:

Definíció az $u = v$ azonosság permutációs, ha u-ban és v-ben ugyanazok a változók szerepelnek, és minden változó ugyanannyiszor jelenik meg u-ban és v-ben, azaz a két szó egymástól csak a változók sorrendjében különbözik.

A V varietás permutációs, ha csak ilyen azonosságok teljesülnek benne.

Világos, hogy minden permutációs azonosság a kommutativitás következménye. Mivel $\mathbb{N}$-ben minden permutációs azonosság teljesül és csakis ezek, ezen azonosságok halmaza zárt. Az eddigi tételek fényében világos a következő:

2. Lemma: A V varietás pontosan akkor permutációs, ha tartalmaz minden kommutatív félcsoportot, azaz: $V(\mathbb{N}) = V_{xy=yx} \leq V$.

Ez ugyanolyan karakterizációja a permutációs varietásoknak, mint a félhálók a normális varietásoknak voltak. Az eddigi egyszerű észrevételeket most arra fogjuk felhasználni, hogy a félcsoportvarietások hálójának szerkezetéről mondjunk valamit. Először foglaljuk össze az eddigi eredmények egy részét. Jelölje H a kérdéses hálót. Ennek számossága kontinuum és nem tesz eleget nemtriviális hálóazonosságnak. A kommutatív félcsoportvarietások hálójában valamivel jobb a helyzet, ugyanis minden kommutatív félcsoportvarietásnak van véges azonosságbázisa, így ez a háló megszámlálható és nincs benne végtelen leszálló lánc. Továbbra is igaz azonban, hogy ebben sem teljesül nemtriviális hálóazonosság. Most egy ennél gyengébb állítást igazolunk.

1. Tétel: A félcsoportvarietások H hálójába minden véges háló beágyazható.

A beágyazásnál kapott részháló nem kommutatív varietásokból fog állni, hanem éppen hogy a $[V_{xy=yx}, 1]$ intervallumba esik, ezért erről a részhálóról állíthatjuk, hogy nem tesz eleget nemtriviális hálóazonosságnak.

Bizonyítás: felhasználjuk a következő két hálóelméleti állítást:

Pudlak-Tuma tétel (1979)
Minden véges háló beágyazható egy véges halmaz partícióhálójába.

3. Lemma: Minden (véges) X halmaz partícióhálója beágyazható az S_X szimmetrikus csoport részcsoporthálójába.

Bizonyítás: A Pudlak-Tuma tétel rendkívül nehéz hálóelméleti eredmény, ezt természetesen nem bizonyítjuk. Az 5. lemma igazolásához a beágyazás a következőképpen adható meg: tekintsük minden partícióhoz azokat a permutációkat, amelyek invariánsan hagynak minden osztályt. Világos, hogy ez beágyazás S_X-be, abban az esetben, ha az X halmaz véges. Mivel az állítást csak erre az esetre használjuk, nem foglalkozunk azzal, hogy végtelen X esetén ezt hogyan lehet igazolni.

A tétel tehát igazolva lesz, ha megmutatjuk a következőt: legyen n egy tetszőleges természetes szám; ekkor van H-ban olyan részháló mely duálisan izomort S_n részcsoporthálójával. Ebből a bizonyítás könnyen összerakható: minden véges háló (duálisa) beágyazható egy véges halmaz partícióhálójába, ez beágyazható a szimmetrikus csoport részcsoporthálójába, mely viszont duálisan izomorf H egy részhálójával.

Legyen tehát n egy természetes szám ($n \leq 3$-ra a dolog nem túl látványos, de elvileg ezt sem kell kizárni), és legyen $G \leq S_n$ tetszőleges. Tekintsük most azt a V_G félcsoportvarietást, melynek azonosságbázisa a következő:

$\Gamma_G := \{x_1 x_2 \dots x_m = y_1 y_2 \dots y_k\}$ melyekre $m = k$ és
ha $m \leq n-1$ akkor $x_i = y_i$ azaz a két szó megegyezik
ha $m \geq n+1$ akkor $\forall\ x_i$ ugyanannyiszor szerepel mindkét oldalon
ha $m = n$ akkor $\exists\ \pi \in G : y_i = x_{\pi(i)}$

A V_G varietás bázisa tehát tartalmaz minden n-nél hosszabb permutációs azonosságot, n-nél rövidebbet nem, a pontosan n hosszúak közül pedig azokat melyeket G-beli permutációk írnak le. Érdemes megyjegezni, hogy ha egy azonosságban egy változó többször is szerepel, akkor az a permutáció amely azt leírja, nem lesz egyértelmű. Ez azonban nem jelent bajt, a feltétel egy konkrét azonosság esetén, hogy van-e (legalább 1db) G-beli permutáció amely azt leírja, egyértelműen eldönthető. Ahhoz, hogy a $G \to V_G$ hozzárendelés beágyazás legyen, azt a legnehezebb megmutatni, hogy injektív, ehhez az kell, hogy Γ_G azonosságok zárt halmaza.

4. Lemma: Mindegyik Γ_G azonossághalmaz zárt.

Bizonyítás: Egy azonossághalmaz zártságának bizonyítására két lehetőség kínálkozik: a könnyebbik út, hogy megadunk egyetlen konkrét félcsoportot (varietást), melyben mindegyik teljesül, de semmi más. Ez működött a normális azonosságok esetében, ott jó péda volt a kételemű félháló. A másik módszer, hogy leellenőrizzük az 1. lemma feltételeit. Most csak ez az út járható. Tegyük fel tehát, hogy a korábbi jelölésekkel $u = v \in \widetilde{\Gamma_G}$ azaz olyan azonosság, mely az 1. lemmában adott 5 lépés véges sokszori alkal-mazásával levezethető Γ_G-ből. Megmutatjuk, hogy ekkor már $u = v \in \Gamma_G$.
Ehhez először a következő egyszerű észrevételre lesz szükségünk: Legyen Σ permutációs azonosságok halmaza. Speciálisan Σ csak olyan azonosságokat tartalmaz ahol mindkét oldalon azonos hosszúságú szavak lépnek fel. Jelölje m a legkisebb ilyen fellépő szóhosszt. Ekkor tetszőleges $u = v \in \widetilde{\Sigma}$ nemtriviális azonosság szintén permutációs és $|u| = |v| \geq m$. Ennek igazolásához csak azt kell látni, hogy az 1. lemmában megadott lépések során nem tudjuk csökkenteni az azonosságban fellépő szavak hosszát. Ezt mind az 5 lépésre könnyű meggondolni.
Mármost ez alapján legyen $u = v \in \widetilde{\Gamma}_G$ nemtriviális azonosság. Természetesen ez is permutációs azonosság, és mivel Γ_G-ben minden azonosság hossza legalább n, ezért $|u| = |v| \geq n$. Ha most itt $|u| = |v| \geq n + 1$, akkor készen vagyunk mert Γ_G minden n-nél hosszabb permutációs azonosságot tartalmaz. Ha pedig $|u| = |v| = n$, akkor ezt az azonosságot Γ_G-ból csupán a tranzitivitás és szimmetria használatával kaptuk. Ezekre azonban Γ_G zárt. Ugyanis, ha $u' = v' \in \Gamma_G$, akkor ez azért van, mert $\exists\ \pi \in \Gamma_G$ permutáció úgy, hogy u-ból v-t π alkalmazásával kapjuk. Ekkor azonban $\pi^{-1} \in \Gamma_G$, és ez a permutáció ami a $v = u$ azonosságot adja meg, ezért $v = u$ is benne van Γ_G-ben. Hasonlóan ha az $u' = v'$ és $v' = w'$ Γ_G-beli azonosságokat a π_1 és π_2 permutációk írják le, akkor az $u' = w'$ azonosságot ezek szorzata. Ezzel be is láttuk a lemmát.

Ebből már világos, hogy a $G \to V_G$ hozzárendelés injektív S_n részcsoporthálójából H-ba, és megfordítja a rendezést és a műveleteket, tehát duális hálóizomorfizmus. Ezzel bebizonyítottuk a tételt.