Azonosságok 0-egyszerű félcsoportokban

Vértesi Vera

2005. június 6.

Előszó

Jelen diplomamunka az azonos című OTDK I. díjas pályamunka [19] bővített és átdolgozott változata. A dolgozat fő eredménye M. Volkovval és S. Pleschevával készülő közös cikkben fog megjelenni.

Elsősorban köszönetet szeretnék mondani témavezetőmnek, Szabó Csabának, aki úgy a problémák felvetésében, mint a megoldásukban komoly segítséget nyújtott. Köszönet illeti továbbá Friedl Katalint, a Budapesti Műszaki Egyetem oktatóját, aki a Bonyolultságelméleti rész megírását tanácsaival és értékes megjegyzéseivel segítette. Végül ezúton is szeretném megköszönni Győri Sándor és Vértesi Róbert segítségét a dolgozat jelen formájának kialakításában.

Tartalomjegyzék

1. fejezet

Bevezetés

A számítógépek egyre nagyobb térhódítása tapasztalható az algebrai kérdések bonyolultságának elemzésében. Azt gondolhatnánk, hogy egy adott algebrai struktúrára vonatkozó állítás ellenőrzése mindössze egy alkalmas program megírásának kérdése. Egy ilyen programnak azonban nemcsak a számítógépek képességei, hanem a matematikai logika is határt szab. Az egyik legtöbbet vizsgált kérdés a szóprobléma: a feladat annak eldöntése, hogy két adott kifejezés megegyezik-e tetszőleges behelyettesítés mellett.

2002-ig nem volt ismert olyan félcsoport, amelyre a szóprobléma coNP-teljes lenne. Végül Volkov (2002) mutatott egy körülbelül 2^{1700} elemszámú félcsoportot, amelyre a feladat coNP-teljes. Nem sokkal később Kisielewicz (2002) konstruált egy néhány ezer elemű példát. Szabó Csabával (2003) megadtunk egy 13 elemű félcsoportot, amelyre a probléma coNP-teljes. A legkisebb elemszámú példa Klima (2003) eredménye: az úgynevezett Brandt-monoid, amely hatelemű. A 0-egyszerű félcsoportok olyan építőkövei a félcsoportoknak, mint a csoportok körében az egyszerű csoportok. Mindkét esetben a struktúra fő faktorairól van szó. Így remélhető, hogy azon 0-egyszerű félcsoportok karakterizálása, amelyekre a szóprobléma polinomiális, segíthet a félcsoportok általános karakterizálásában is.

Az eddigiekben a 0-egyszerű félcsoportok közül csak olyanokra voltak eredmények, amelyek struktúracsoportjára a szóprobléma coNP-teljes, s ebből automatikusan adódott az eredeti félcsoportra is a coNP-teljesség; illetve a kombinatorikus 0-egyszerű félcsoportokra, amelyekre a probléma polinomiális (Seife, Szabó 2000). A dolgozatban belátom Volkov (2001) sejtését, mely szerint egy konkrét 19 elemű 0-egyszerű félcsoportra a szóprobléma coNP-teljes. Ez a legkisebb olyan példa, amelynek struktúracsoportjára polinomiális a szóprobléma, de magára a félcsoportra mégis coNP-teljes.

2. fejezet

Előzmények, alapfogalmak

Mivel a szóprobléma bonyolultságelméleti vizsgálata a számítástudomány és az algebra határterületén van, ezért mindkét témakörben le kell rögzíteni a jelöléseket, definiálni kell az alapfogalmakat. Ennek a fejezetnek ez az egyik fő célja. Ugyanakkor betekintést szeretnénk adni a szóproblémával kapcsolatos eddigi eredményekről is.

2.1. Számítási bonyolultság

A dolgozatban nem célunk a bonyolultságelmélet egzakt felépítése, inkább csak a szükséges fogalmak felelevenítése. A témát kimerítően tárgyalja a szakirodalom [12, 14]. A számítási bonyolultság a számítástudomány azon területe, mely annak okát kutatja, hogy egyes problémákat miért olyan nehéz számítógéppel megoldani. Ezen nehézség mértéke alapján az eldöntési problémák, vagy más néven nyelvek, bonyolultsági osztályokba sorolhatóak. Most csak azon bonyolultsági osztályokat fogjuk áttekinteni, melyekre a későbbiekben szükségünk lesz, ilyen a P, NP, coNP nyelvosztályok és az NP-teljes, coNP-teljes nyelvek. Azt mondjuk, hogy egy algoritmus polinomiális, ha futásideje az input méretének egy polinomjával becsülhető[1]. Eldöntendő kérdések egy halmaza P-ben van, ha van egy minden inputra polinomidőben válaszoló algoritmus. Ilyen például az OSZTÓ nyelv, mely az a és b inputokról azt kérdezi, hogy a osztója-e b-nek. A kérdésekre pl. az Euklideszi algoritmus polinomidőben választ ad. Eldöntendő kérdésekből álló halmazt NP-belinek nevezünk, ha az igen válasz egy polinomidőben ellenőrízhető tanúval bizonyítható (ez az osztály épp abban különbözik a P-től, hogy ebben az esetben a tanút nem az algoritmus szolgáltatja, hanem pl. egy orákulum súgja).

[1] Nem térünk ki rá, hogy pontosan mit is nevezünk algoritmusnak, és milyen egységekben mérjük a tárat, illetve az időt.

Az ÖSSZETETT nyelv, amely során egy bemenetként kapott a számról kell eldönteni, hogy összetett-e, például NP-beli, hiszen ha a válasz igen, akkor tanúként megadhatjuk egy osztóját, amelyről az előbbiek szerint polinomiidőben ellenőrízhető, hogy valóban osztó. Hasonlóan, egy nyelv coNP-ben van, ha a nem válasz bizonyítható polinomiális tanúval. Például a PRÍM [2] nyelv, melynél egy bemenetként kapott a számról azt kell eldönteni, hogy prím-e. Általában véve, ha egy A nyelv NP-beli, akkor az A^C nyelv, amely azt kérdezi egy bementről, hogy nem teljesül-e A, coNP-beli. Azt mondjuk, hogy egy A nyelv polinomiálisan redukálható B nyelvre ($A \preceq_P B$), ha A minden bemenetéhez polinom időben adható B-nek egy olyan bemenete, amelyre B pontosan akkor igaz, ha A igaz volt az eredeti problémára. A és B polinomiálisan ekvivalens ($A \equiv_P B$), ha $B \preceq_P A$ és $A \preceq_P B$. Egy nyelv NP-teljes, ha minden NP-beli nyelv redukálható rá polinomiálisan. Tehát valamilyen értelemben az NP-teljes nyelvek a legnehezebbek az NP-beli nyelvek közül. A coNP-teljes nyelvosztály hasonlóan definiálható. Jól ismert NP-teljes problémák: a SAT, mely egy bemenetként kapott konjunktív normálformában adott Boole-formuláról kérdezi, hogy kielégíthető-e, a 3SAT, mely a SAT megszorítása az olyan konjunktív normálformában adott Boole-formulákra, melyekben minden klóz pontosan három literált tartalmaz, és az r-COLOR ($r \geq 3$), melynél egy bemenetként kapott gráfról kell eldönteni, hogy színezhető-e r színnel.

A bonyolultságelmélet egyik legtöbbet vizsgált problémája az úgynevezett *relációhomomorfizmus-probléma* (Constraint Satisfaction Problem, CSP). Egy $B = (S, \varrho)$ relációs struktúra az S alaphalmazból, és egy az S-en adott r-változós, $\varrho \subseteq S^r$, relációból áll. CSP(B) egy adott $B = (S, \varrho)$, relációsstruktúrára a következő: minden bemenetként kapott $A = (T, \nu)$ ugyanolyan típusú relációs struktúráról el kell dönteni, hogy van-e relációtartó $T \rightarrow S$ leképezés, azaz igaz-e, hogy B homomorf képe A-nak? A probléma nyilvánvalóan NP-beli. A CSP két legismertebb esete a SAT, a gráfhomomorfizmus-probléma és a színezettgráf-homomorfizmus probléma. Ugyanakkor, mint azt Feder és Vardi [4] belátta minden CSP redukálható színezettgráf-homomorfizmus problémára, sőt már a páros gráfok színezettgráf-homomorfizmus problémájára is. A kutatások mai fő célja dichotómia tételek bizonyítása általános esetben. Sokan azt gondolják, hogy ha van bonyolultsági osztály P és NP között, akkor van ilyen bonyolultságú CSP probléma is.

[2] A közelmúltban a PRÍM nyelvről megmutatták, hogy valójában P-beli is.

2.2. Gráfok

A klasszikus gráfelméleti fogalmakon kívül, mint a *gráf*, *páros gráf*, *csúcs* (*pont*), *él*, *többszörös él*, *hurokél*, *egyszerű gráf*, *pont foka*, *részgráf*, *út*, *séta*, *ciklus*, *kör*, *összefüggő gráf*, *összefüggőségi komponens*, *színezés*, szükségünk lesz néhány kevésbé ismert gráfelméleti fogalomra is. A $G(A, B, E)$ páros gráf *szomszédsági mátrixa*, egy olyan $|A| \times |B|$-es 0-1 mátrix, melynek az $M(a, b)$ eleme 1, ha a megfelelő $a \in A$ és $b \in B$ csúcsok között él fut G-ben. Két azonos csúcshalmazú, $G(V, E)$ és $H(V, F)$, esetleg többszörös éleket tartalmazó gráf uniója: $(G \uplus H)(V, E \uplus F)$, tehát csúcshalmaza megegyezik G illetve H csúcshalmazával, az élhalmaz az élhalmazok uniója, és egy adott $e \in E \uplus F$ él multiplicitása a két gráfbeli multiplicitásának összege. A $G(V, E)$ és $H(U, F)$ gráfok közötti *(gráf-)homomorfizmus* a csúcshalmazok olyan $\varphi : V \to U$ leképezése, mely élet élbe visz, azaz $(v, w) \in E$-ből következik $(\varphi(v), \varphi(w)) \in F$. Ha H részgráfja G-nek, és a $\varphi : G \to H$ gráfhomomorfizmus fixálja H-t ($\varphi|_H \equiv id$), akkor φ G-nek H-ra való *retrakiciója*.

Rögzítsünk egy $H(U, F)$ gráfot. A H-ra vonatkozó *gráfhomomorfizmus-probléma*, $\textsc{hom}(H)$, melynek során egy bemenetként kapott $G(V, E)$ gráfról azt kell eldönteni, hogy van-e G-nek H-ba menő homomorfizmusa. Természetesen ez a probléma NP-beli. Ha H tartalmaz hurokélet, akkor mindig létezik ilyen homomorfizmus. Ugyanakkor általában a kérdés nehezen megválaszolható, hiszen például ha $H = K_r$ az r csúcsú teljes gráf, akkor ez épp G r-színezhetőségének kérdése, ami NP-teljes ($r \geq 3$). Hurokélet nem tartalmazó gráfokra Hell és Nešetřil [7] bebizonyította, hogy ha a gráf páros, akkor $\textsc{hom}$ P-beli, nem párosokra pedig NP-teljes. A H-ra vonatkozó *retrakciós probléma*, $\textsc{ret}(H)$, ebben az esetben az a kérdés, hogy egy bemenetként kapott G, H-val izomorf H' részgráfot tartalmazó gráfnak létezik-e retrakciója H'-re. Büki és Szabó [1] által bizonyítottak szerint, ha J_n az $n \times n$-es csupa 1-esből álló mátrix, I_n pedig $n \times n$-es egységmátrix, akkor, ha H szomszédsági mátrixa $J_n - I_n$, akkor $\textsc{ret}(H)$ NP-teljes. Tehát például a hatszögre NP-teljes a probléma. A *színezettgráf-homomorfizmus probléma*, $\textsc{oal}(H)$ annak eldöntése, hogy egy bemenetként kapott $G(V, E)$ gráfhoz és $f : V \to U$ részleges leképezéshez található-e olyan $\varphi : G \to H$ homomorfizmus, mely f-nek kiterjesztése, azaz $\varphi|_H \equiv f$. Azon G-beli csúcsokat, amelyekre f meg van adva, nevezzük színezettnek. Ez a kérdéskör magában foglalja a $\textsc{hom}(H)$ és $\textsc{ret}(H)$ problémákat is, így legalább olyan bonyolult. Feder, Hell és Huang belátták [5], hogy minden hurokélet nem tartalmazó nem páros gráfra $\textsc{oal}$ NP-teljes. Páros gráfok esetében csak a legalább 6 hosszú páros hosszú körökre, azaz például a hatszögre sikerült NP-teljességet bizonyítaniuk.

A dolgozat folyamán szükségünk lesz még egy H-ra vonatkozó eldöntendő kérdésre, ehhez definiáljuk a *páros homomorfizmus* fogalmát: egy $G \to H$ homomorfizmus páros, ha az összes $f \in F$ él inverzképének elmeszáma páros, azaz $\varphi^{-1}(f) \equiv 0 \pmod 2$. Az úgynevezett *pároshomomorfizmus-probléma*, $2\textsc{hom}(H)$, során egy bementként kapott G gráfról kell eldönteni, hogy minden $\varphi : G \to H$ homomorfizmusra páros-e. Mint azt majd a 31. tételben belátjuk ez a probléma coNP-teljes a hatszögre.

2.3. A szóprobléma

Az algebra napjainkban egyre szélesebb körben vizsgált területe az algebrai bonyolultságelmélet, amely az algebra tárgykörében felmerülő kérdések megoldására adható algoritmusok nehézségének mértékével foglalkozik. Ide tartozik a *szóprobléma* is, amely egy effektív módon (pl. a Cayley-táblájával) adott A algebra fölött azt a kérdést vizsgálja, hogy teljesül-e két tetszőleges kifejezésre (u és v), hogy minden behelyettesítésre egyenlő értéket vesznek fel, azaz, hogy $u \equiv v$ azonosság-e A-ban. A szóproblémának több változata fogalmazható meg aszerint, hogy milyen fajta kifejezéseket engedünk meg bemenetként (mi lehet u és v). Egy adott algebra felett egy kifejezést *term*nek nevezünk, ha az adott algebra feletti alapműveletkből, és változókból áll, formálisan a típushoz tartozó kifejezésalgebra elemeiről van szó. Például félcsoportok esetében egy term $x_1 x_2 \cdots x_m$ alakú. Egy kifejezés *polinom*, ha algebrabeli konstansok is szerepelhetnek benne. Így a két — univerzális algebrai szempontból — legfontosabb változat a term ekvivalencia probléma (TERM-EQ) és a polinom ekvivalencia probléma (POL-EQ), amikor tehát a bemenetként kapott kifejezések termek illetve polinomok. Amennyiben a 0 benne van az algebrában, értelmezhetőek a TERM $\equiv 0$ és a POL $\equiv 0$ problémakörök is, amelyek során egy bemenetként kapott t termről, illetve p polinomról kell eldönteni, hogy azonosan 0-e? A POL $\equiv 0$ a POL-EQ egy megszorítása, és ha a 0 konstans A-ban, akkor a TERM $\equiv 0$ a TERM-EQ megszorítása. Az *egyenletmegoldhatósági probléma*, POL-SAT, TERM-SAT pedig az előzőekhez hasonlóan azt kérdezi, hogy az $u = v$ egyenletnek van-e megoldása. Véges struktúrákra mindkét problématípus behelyettesítéssel eldönthető, ezért ilyenkor a feladat bonyolultsága a kérdés. Mivel minden term egyben polinom is, ezért a TERM-EQ (TERM-SAT) mindig legfeljebb olyan nehezen eldönthető, mint a POL-EQ (POL-SAT). A szóprobléma változatai, természetesen, coNP-ben vannak, hiszen ha a két kifejezés nem egyenlő, akkor ennek egy gyorsan ellenőrizhető bizonyítéka az a behelyettesítés, amelyre a kifejezések különböző értékeket vesznek fel. Hasonlóan látható, hogy az egyenletmegoldhatósági probléma NP-beli. Az eddigieket összfoglalva:

1. állítás. *Tetszőleges A algebrára*

1. TERM-EQ$(A) \preceq_P$ POL-EQ(A);
2. TERM-SAT$(A) \preceq_P$ POL-SAT(A);
3. *Ha* $0 \in A$, *akkor* POL $\equiv 0(A) \preceq_P$ POL-EQ(A);
4. *Ha pedig* 0 *konstans is* A*-ban, akkor* TERM $\equiv 0(A) \preceq_P$ TERM-EQ(A).

Adott struktúratípusoknál általában a dichotómia bizonyítása a cél, azaz, hogy a szóprobléma (egyenletmegoldhatósági probléma) a struktúrák egy részére P-beli, a többire coNP-teljes (NP-teljes). A továbbiakban a szóproblémával kapcsolatos eddigi eredményeket foglaljuk össze. Minden a továbbiakban szerplő struktúra végesnek tekintendő.

2.3.1. Gyűrűk

Régóta ismert [9], hogy kommutatív gyűrűkre a szóprobléma P-beli, ha a gyűrű nilpotens, és coNP-teljes egyébként. Burris és Lawrence [2] belátta, hogy ugyanez igaz a gyűrűkre általában is: a TERM-EQ P-beli, ha a gyűrű nilpotens, és coNP-teljes egyébként. Így persze nem nilpotens gyűrűkre a POL-EQ is coNP-teljes, nilpotens gyűrűk esetében pedig a [2]-beli algoritmus még a POL-EQ-ra is polinomiális lefutású. Azaz gyűrűk esetében a két szóprobléma azonos bonyolultságú. Ez az összefüggés nem minden algebrai struktúrára igaz: kombinatorikus teljesen 0-egyszerű félcsoportokra a TERM-EQ probléma mindig P-beli, azonban van olyan kombinatorikus 0-egyszerű félcsoport, amelyre a POL-EQ coNP-teljes, erre konstruálunk példát a 3.1.1. illetve a 3.2.2. fejezetekben.

A 2-elemű gyűrűre, $\mathbb{Z}_2$-re a TERM-EQ coNP-teljessége a 3SAT NP-teljességének egyszerű következménye. Azonban a visszavezetés során összegek magas hatványait használják, melyeket monomok összegeként kifejtve már nem polinomiális visszavezetést kapnánk. Ezért Willard definiálta a szóproblémának egy másik változatát, az úgynevezett $_\Sigma$-verziót (TERM$_\Sigma$-EQ, POL$_\Sigma$-EQ) amikor a két megadott szó csak monomok összege lehet. Ez a mód természetesebb, hiszen például — a klasszikus algebrában — a polinomokat is ilyen formában szoktuk megadni. A kérdés ebben az esetben is a szokásos, csak bizonyos szavak kifejtve lényegesen hosszabbak lehetnek, így a bemenő adatok mérete változik. Ha egy gyűrűre az eredeti szóprobléma P-beli, akkor nyilván polinomiális a $_\Sigma$-verziója is. Willard és Lawrence [11] igazolták, hogy ha a Jacobson-radikál szerinti faktor kommutatív, akkor a TERM$_\Sigma$-EQ P-beli; azon $M_n(\mathbb{F}_q)$ mátrixgyűrűkre pedig coNP-teljes, amelyekre az invertálható elemek csoportja nem feloldható. Ezzel megoldották az $n \geq 3$ illetve $q \geq 4$ eseteket. Az eddig még megoldatlan esetekre, az $M_2(\mathbb{Z}_2)$ és az $M_2(\mathbb{Z}_3)$ mátrixgyűrűkre a [18] és a [17] cikkekben témavezetőmmel beláttuk, hogy a probléma ekkor is coNP-teljes, tehát TERM$_\Sigma$-EQ coNP-teljes a nemkommutatív teljes mátrixgyűrűkre, és persze polinomiális a kommutatívokra. Valójában ennél erősebb állítást sikerült igazolni; azt, hogy a fenti mátrixgyűrűk multiplikatív félcsoportjában is coNP-teljes a szóprobléma. Ez az addig ismerteknél nagyságrendileg kisebb példát adott olyan félcsoportra, amelyben a szóprobléma coNP-teljes. Egy TDK dolgozatomban [20] belátom, hogy a nemkommutatív mátrixgyűrűknek már a multiplikatív félcsoportjában is coNP-teljes a probléma. Ezen eredmény felhasználásával bizonyítható véges gyűrűkre a dichotómia: a TERM$_\Sigma$-EQ bonyolultsága is csak a Jacobson-radikál szerinti faktortól függ: P-beli, ha a faktor kommutatív, és coNP-teljes egyébként.

2.3.2. Csoportok

Csoportokra a kérdés koránt sincs megoldva. Tudjuk, hogy nemfeloldható csoportra a TERM-EQ coNP-teljes és hogy nilpotens csoportokra P-beli [6]. Itt ugyanis, ha van „ellenpélda”, akkor van korlátos elemszámú is. A nem nilpotens, de feloldható csoportokra nincsenek általános eredmények, a kérdés még S_4-re sincs megoldva. Horváth Gábor [8] egy TDK dolgozatában megmutatta, hogy bizonyos metaciklikus csoportokra a TERM-EQ coNP-teljes.

2.3.3. Félcsoportok

2001-ben Szabó Csaba és Steve Seif [15] megmutatták, hogy minden CSP-hez van egy olyan 0-egyszerű S félcsoport hogy az adott CSP polinomiálisan ekvivalens POL-SAT(S)-sel. Ettől kezdve mindkét szóprobléma gyors karriert futott be. Először Popov és Volkov [13] mutattak egy olyan (2^{1700} elemű) félcsoportot, amelyre a TERM-EQ coNP teljes, majd ugyanebben az évben Kisieliewicz mutatott egy párezer elemszámú példát ugyanerre. Szabó Csabával [18, 17] igazoltuk, hogy TERM-EQ($M_2(\mathbb{Z}_2)$) és TERM-EQ($M_2(\mathbb{Z}_3)$) coNP-teljes, és ennek kapcsán mutattunk egy 13 elemű példát is. Ezután elkezdődtek a szisztematikus kutatások. Klíma [10] illetve Seif [15] igazolták, hogy a legkisebb elemszámú ilyen félcsoport a hatelemű Brandt monoid. Szabó és Seif [16] pedig megmutatták, hogy kombinatorikus 0-egyszerű félcsoportokra a TERM-EQ mindig P-beli. Nagy kérdés volt, hogy teljesül-e ez minden olyan 0-egyszerű félcsoportra, amely alapcsoportja feloldható. Erre a kérdésre keresem a választ a dolgozat 3.3. fejezetében.

2.3.4. Egy újabb szóprobléma

Pawel Idziak és Szabó Csaba új szemszögből vizsgálták a szóprobléma változatait, arra keresték a választ, hogy mi történik akkor, ha megengedjük bizonyos, véges számú művelet hozzávételét a típushoz (pl. csoport estén a kommutátort). Ez az úgynevezett $*$ problémakör. Az új műveletek, művelettáblái az előkészítés során kiszámíthatóak, majd később bemenetként elfogadhatóak az ezen műveletekkel alkotott kifejezések is. A probléma bonyolultságát ez jelentősen megváltoztatja. Idziak és Szabó megvizsgálták a POL-SAT* probléma bonyolultságát kongruencia moduláris varietásokra. A primhatvány-rendű algebrák direkt összegeként nem előálló kettes típusú nilpotens algebrák kivetélével sikerült dichotomiát bizonyítaniuk.

2.4. 0-egyszerű félcsoportok

Ebben a fejezetben egy rövid leírást adunk a *teljesen 0-egyszerű-* illetve *Rees-mátrix félcsoportokról*, alapvető tulajdonságaikról, bemutatva közben további vizsgálataink fő tárgyát, $\mathcal{M}_{19}$-et. Adott egy G csoport, és egy M mátrix, melynek elemei a $G\cup\{0\}$ halmazból kerülnek ki, és minden sora illetve oszlopa legalább egy nemnulla elemet tartalmaz. Jelölje Λ az M mátrix oszlopainak, I a sorainak indexhalmazát. Az M mátrixhoz tartozó G struktúracsoportú Rees-mátrix félcsoport, $\mathcal{M}(I,\Lambda,G;M)$ alaphalmaza $I\times G\times\Lambda\cup\{0\}$. A 0 elnyelő elemként viselkedik: $0(i,g,\lambda)=(i,g,\lambda)0=0$. A nemnulla elemek szorzását az alábbi képlettel definiáljuk:

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

Ellenőrízhető, hogy a fent definiált szorzás asszociatív, így $\mathcal{M}(I,\Lambda,G;M)$ valóban félcsoport. A félcsoport elemeire az (i,g,λ) jelölés helyett gyakran az $\langle i,\lambda\rangle$ jelölést használjuk, amennyiben a csoportelem nem lényeges. Jelölje π_I,π_G,π_Λ a nemnulla elemek első-, második illetve harmadik korrdinátájára való vetítést. Egy adott Rees-mátrix félcsoportot több különböző mátrixszal is lehet reprezentálni, erről szól az alábbi lemma:

2. lemma. *Legyen $\mathcal{M}(I,\Lambda,G;M)$ egy Rees-mátrix félcsoport, ekkor:*

1. *Az M mátrix két oszlopát illetve sorát felcserélve izomorf Rees-mátrix félcsoportot kapunk;*

2. *Az M mátrix egy oszlopát illetve sorát egy csoportelemmel megszorozva izomorf Rees-mátrix félcsoportot kapunk.*

A Rees-mátrix félcsoportnál a szorzás egyszerűen kiszámolható művelet: amennyiben az eredmény nem 0, csak az első és az utolsó tényezőktől függ az értéke. A következő lemma ezt az összefüggést hívatott formalizálni:

3. lemma. *Legyen $\mathcal{M}(I,\Lambda,G;M)$ egy Rees-mátrix félcsoport, $b=\langle i,\lambda\rangle$, $d=\langle j,\mu\rangle$, $c_1=(i_1,g_1,\lambda_1), c_2=(i_2,g_2,\lambda_2),\ldots,c_n=(i_n,g_n,\lambda_n)\in\mathcal{M}(I,\Lambda,G;M)$, ekkor:*

1. *$b\cdot d=0$ pontosan akkor, ha $M(\lambda,j)=0$;*

2. *$c_1c_2\cdots c_n=0$ pontosan akkor, ha található olyan $k\in\{2,3,\ldots n\}$ index, melyre $c_{k-1}c_k=0$;*

3. *Ha $c_1c_2\cdots c_n\neq 0$, akkor $c_1c_2\cdots c_n=\langle\pi_I(c_1),\pi_\Lambda(c_n)\rangle=\langle i_1,\lambda_n\rangle$.*

A Rees-mátrix félcsoportok definíciója az alábbi, egyszerű példán szemléltethető, amely egyben ezen dolgozat tárgya is:

4. példa. *Legyen $G=\mathbb{Z}_2=\langle a\rangle$, és legyen:*

$$P=\begin{pmatrix}0&1&1\\a&0&1\\1&1&0\end{pmatrix}$$

Ekkor $\Lambda=I=\{1,2,3\}$. Legyen $\mathcal{M}_{19}=\mathcal{M}(I,\Lambda,\mathbb{Z}_2;P)$. $\mathcal{M}_{19}$-ben a szorzás a következőképpen működik: $(1,a,1)(2,1,1)=(1,1,1)$, hiszen $P(1,2)=a$, és mivel $P(2,2)=0$, $\langle 1,2\rangle\langle 2,1\rangle=0$. Általában $\mathcal{M}_{19}$-ben az $\langle i,\lambda\rangle\langle j,\mu\rangle$ szorzat, akkor és csak akkor 0, ha $\lambda=j$.

Van egy jól ismert, klasszikus példa is Rees-mátrix félcsoportokra: $L_n(\mathbb{F})$, a legfeljebb 1 rangú $n\times n$-es mátrixok multiplikatív félcsoportja az $\mathbb{F}$ véges test felett.

5. tétel. *$L_n(\mathbb{F})$ Rees-mátrix félcsoport.*

Bár a bizonyítás ismert, és nem is nehéz, a teljesség kedvéért álljon itt.
Bizonyítás: Legyen $V=\mathbb{F}^n$, legyenek $\{l_i=\langle v_i\rangle : i\in I\}$, V egydimenziós alterei, azaz $|I|=\frac{|\mathbb{F}|^n-1}{|\mathbb{F}|-1}$. Legyen továbbá $I=\Lambda$. Definiáljuk az M $|\Lambda|\times|I|$-as mátrixot $\mathbb{F}^*\cup\{0\}$ felett a következőképpen: $M(\lambda,i)=v_\lambda^Tv_i$. Minden A 1 rangú mátrix diád, így egyértelműen írható fel $A=\alpha v_iv_\lambda^T$ alakban, ahol $\alpha\in\mathbb{F}^*, i\in I,\lambda\in\Lambda$. Az $A=\alpha v_iv_\lambda^T\mapsto(i,\alpha,\lambda)$ és a $0\mapsto 0$ leképezés izomorfizmust létesít $L_n(\mathbb{F})$ és az $\mathcal{M}(I,\Lambda,\mathbb{F}^*;M)$ Rees-mátrix félcsoport között. $\square$

A Rees-mátrix félcsoportoknak van egy kevésbé formális tárgyalásmódja is, az úgynevezett szendvicsmátrixos reprezentáció. Ekkor $\mathcal{M}(I,\Lambda,G;M)$ elemei a legfeljebb 1 nemnulla elemet tartalmazó $|I|\times|\Lambda|$-es mátrixok, szorzásukat pedig a szokásos mátrixszorzásból öröklik az M, mint szendvicsmátrix beiktatásával. Pontosabban:

$$A \circ B = AMB$$

A dimenziókat összehasonlitva rögtön látszik, hogy a szorzás értelmes. A $\circ$ művelet asszociativitása a mátrixok szorzásának asszociativitásából azonnal következik. A két definíció valóban ugyanaz: a 0 mátrixnak feleljen meg a 0, egyébként egy $A \neq 0$-nak pontosan egy eleme nemnulla, legyen pl. a λ-adik sor i-edik eleme g, feleltessük meg ekkor A-nak (i,g,λ) félcsoportelemet. Ez tényleg izomorfizmust ad. Az előbbi példa a szendvicsmátrixos terminológiában:

6. példa.

$$\begin{pmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ a & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

A *kombinatorikus teljesen 0-egyszerű félcsoportok* olyan Rees-mátrix félcsoportok, melyeknek struktúracsoportja triviális. Tehát egy adott M, csupa 0 sort illetve oszlopot nem tartalmazó $|\Lambda| \times |I|$-as 0-1 mátrixhoz tartozó $S_M = \mathcal{M}(I,\Lambda,1;M)$ kombinatorikus teljesen 0-egyszerű félcsoport alaphalmaza:

$$I \times \Lambda \cup \{0\} = \{\langle i,\lambda\rangle : i \in I, \lambda \in \Lambda\} \cup \{0\}$$

A 0 elnyelő elem, azaz $0\langle i,\lambda\rangle = \langle i,\lambda\rangle 0 = 0$, a többi elem szorzata pedig:

$$\langle i,\lambda\rangle\langle j,\mu\rangle = \begin{cases} \langle i,\mu\rangle & \text{ha } M(\lambda,j) \neq 0, \\ 0 & \text{egyébként} \end{cases}.$$

Minden $S = \mathcal{M}(I,\Lambda,G;M)$ Rees-mátrix félcsoport redukálható kombinatorikus 0-egyszerű félcsoporttá: egyszerűen az M struktúramátrix minden nemnulla elemét kicseréljük egyesre, jelölje ezt $M|_1$, legyen ekkor a kombinatorikus redukált $S|_1 = S_{M|_1}$. Így például 4. példában tárgyalt félcsoport kombinatorikus redukáltja az

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

mátrixhoz tartozó S_A teljesen kombinatorikus 0-egyszerű félcsoport. Definiálható általában egy tetszőleges $\vartheta : G \to H$ csoporthomomorfizmus szerinti redukált is: Legyen $M|_\vartheta$, az a mátrix, melyet M-ből úgy kapunk, hogy M-ben minden $g \in G$ elemet kicserélünk $\vartheta(g)$-re, ekkor S ϑ-redukáltja $S|_\vartheta = \mathcal{M}(I, \Lambda, H; M|_\vartheta)$. Természetes módon definiálható egy $\widehat{\vartheta} : S \to S|_\vartheta$ félcsoporthomomorfizmus is, a $\widehat{\vartheta}(0) = 0, \widehat{\vartheta}((i, g, \lambda)) = (i, \vartheta(g), \lambda)$ képlettel. A redukált félcsoport elég sok információt megőriz az eredeti félcsoportról, például egy kifejezés nemnullaságát. Így ha csak erre vagyunk kíváncsiak, akkor elég csak a kombinatorikus teljesen 0-egyszerű félcsoportokat vizsgálni.

7. megjegyzés. *Tetszőleges $S = \mathcal{M}(I, \Lambda, G; M)$ Rees-mátrix félcsoportra:*

1. TERM-EQ$(S|_\vartheta) \preceq_P$ TERM-EQ(S);
2. POL-EQ$(S|_\vartheta) \preceq_P$ POL-EQ(S);
3. TERM $\equiv 0(S|_\vartheta) \preceq_P$ TERM $\equiv 0(S)$;
4. POL $\equiv 0(S|_\vartheta) \equiv_P$ POL $\equiv 0(S)$.

2.4.1. Miért épp $\mathcal{M}_{19}$?

Mivel a teljesen 0-egyszerű félcsoportok olyan építőkövei a félcsoportoknak, mint a csoportok körében az egyszerű csoportok (mindkét esetben a struktúra fő faktorairól van szó). Így remélhető, hogy azon 0-egyszerű félcsoportok karakterizálása, amelyekre a TERM-EQ polinomiális, segíthet a félcsoportok általános karakterizálásában is, ez a dolgozat tekinthető egy kezdő lépésnek ebben az irányban. Természetes kérdés, hogy van-e egyáltalán olyan 0-egyszerű félcsoport, amelyre TERM-EQ coNP-teljes? Mi lehet, a legegyszerűbb ilyen félcsoport? A kombinatorikus teljesen 0-egyszerű félcsoportokra TERM-EQ polinomiális, így köztük nem is érdemes a példát keresni. Ha egy 0-egyszerű fécsoport struktúramátrixában nem is jelennek meg az 1-en kívül más csoportelemek, akkor felette a szóprobléma ekvivalens a kombinatorikus redukáltja, és a struktúracsoportjabeli szóproblémával. Mivel a csoportok szóproblémájáról még kevesebbet tudunk, mint a félcsoportokéról, és amúgy is inkább félcsoportokról szóló eredményt szeretnénk bizonyítani, így ezektől az esetektől is eltekintünk. Fogadjuk el, hogy egy 0-egyszerű félcsoport annál egyszerűbb, minél több nullát tartalmaz a struktúramátrixa, és minél egyszerűbb a struktúracsoportja. A 2. lemma többszöri alkalmazásával, megmutatható, hogy a fennmaradó 0-egyszerű félcsoportok közül a legegyszerűbb valóban $\mathcal{M}_{19}$.

Még egy ok, amiért talán érdemes $\mathcal{M}_{19}$-et vizsgálni, hogy van egy természetes reprezentációja transzformációkkal. Vegyük ehhez a három elemen ható transzformáció-félcsoportot, T_3-at ($|T_3| = 3^3 = 27$). Soroljuk az elemeit rangjuk szerint 3 csoportba: $T_3(3) = S_3$ a 3 rangúak, $T_3(2)$ a 2 rangúak és $T_3(1)$ az 1 rangúak. Mivel kompozíció során a rang nem nőhet, így $T_3(1)$ ideál T_3-ban. Vegyük $T_3(2)$ $T_3(1)$ szerinti Rees-faktorát, azaz húzzuk össze $T_3(1)$-et egyetlen 0-elemmé. A kapott félcsoport 19 elemű, és mint az Clifford és Preston [3] híres félcsoportelméleti könyvébenben bizonyítva van, izomorf $\mathcal{M}_{19}$-cel. A dolgozatban a következő tételt látjuk be:

8. tétel. TERM-EQ($\mathcal{M}_{19}$) *coNP-teljes.*

Végezetül leírjuk $\mathcal{M}_{19}$ néhány fontos tulajdonságát:

9. lemma. *Legyen* $b = \langle i, \lambda \rangle, d = \langle j, \mu \rangle \in \mathcal{M}_{19}$ *és* $c_1 = (i_1, g_1, \lambda_1), c_2 = (i_2, g_2, \lambda_2), \ldots, c_n = (i_n, g_n, \lambda_n) \in \mathcal{M}_{19}$*, ekkor:*

1. $b \cdot d = 0$ *pontosan akkor, ha* $P(\lambda, j) = 0$*, azaz ha* $\lambda = i$*;*
2. $\mathcal{M}_{19}$ *idempotens elemei:* $\{(i, g, \lambda) : \lambda \neq i\}$*;*
3. $c_1 c_2 \cdots c_n = 0$ *pontosan akkor, ha található olyan* $k \in \{2, 3, \ldots n\}$ *index, melyre* $c_{k-1} c_k = 0$*, azaz* $\lambda_{k-1} = i_k$ *;*
4. *Jelölje* $l = |\{1 \leq k \leq n-1 : i_k = 1, \lambda_{k+1} = 2\}|$ *(a szorzatban fellépő „extra" a-k számát). Ekkor, ha* $c_1 c_2 \cdots c_n \neq 0$*, akkor*

$$c_1 c_2 \cdots c_n = (i_1, g_1 g_2 \cdots g_n \cdot a^l, \lambda_n) \ .$$

3. fejezet

Mi könnyű? Mi nehéz?

A számítástudomány szemszögéből könnyű az, amire van polinomiális algoritmus, azaz P-ben van, nehéz pedig, ami coNP-teljes. A továbbiakban a szóproblémát próbáljuk ebből a nézőpontból vizsgálni, különös figyelmet fordítva eredeti témánkra, a Rees-mátrix félcsoportok szóproblémájára.

3.1. P-beli problémák

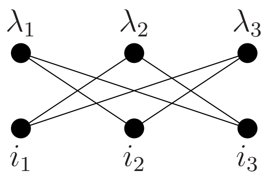
Azt, hogy egy adott struktúrára a szóprobléma P-beli, mi sem bizonyítja jobban, mint hogy megadunk egy tényleges polinomidejű algoritmust az eldöntésére. Általában ez az algoritmus, mint az alábbi 3.1.1. fejezetben is, az azonosságok pontos karakterizációját használja. Nem mindig szükséges a teljes karakterizáció, elég azt belátni, hogy csak polinomsok behelyettesítést kell ellenőrizni, az azonosság igazolásához, a „Brute Force” exponenciálissok helyett. Goldmann és Russel [6] például ezt a módszert alkalmazza a nilpotens csoportok szóproblémájának P-beliségének bizonyításához.

3.1.1. TERM-EQ(S_A)

A továbbiakban teljesen kombinatorikus 0-egyszerű félcsoportok feletti azonosságokat vizsgálunk. Mint látszani fog, egy jó megközelítés adódik ehhez a gráfokon keresztül. Ezért most az eddigi fogalmakat átültetjük a gráfelmélet területére.

Tetszőleges S_M kombinatorikus teljesen 0-egyszerű félcsoporthoz természetes módon definiálható egy $H_M(\Lambda, I, F)$ páros gráf: az a gráf, melynek szomszédsági mátrixa épp M, igy például a 2.4. fejezetben definiált S_A-hoz tartozó páros gráf, épp egy hatszög:

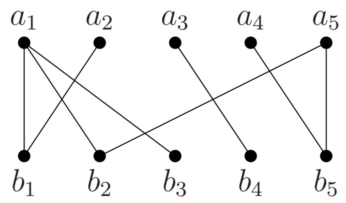
H_6 :



Ismert, hogy a félcsoportok felett egy term egyszerűen $t = x_1x_2 \cdots x_n$ alakú, ahol az x_i-k nem feltétlenül különbözőek. Jelölje $X_t = \{x_1, x_2, \ldots, x_n\}$ a t-ben előforduló változók halmazát. Tetszőleges t termhez konstruálunk egy $G_t(A_t, B_t, E_t)$ páros gráfot a következőképpen: legyen $A_t = \{a_x : x \in X_t\}$, $B_t = \{b_x : x \in X_t\}$ és fusson él a_x és b_y között, ha az xy kifejezés részszava t-nek. A könnyebb érthetőség kedvéért álljon itt egy példa erre.

10. példa. *Legyen* $t = x_1x_2{x_1}^2x_3x_4{x_5}^2x_2{x_1}^2x_2x_1x_2$. *A* t*-hez tartozó gráf:*

G_t :



Ezen gráf-konstrukciók segítségével vizsgálhatjuk az S_M feletti termeket:

11. lemma. *Legyen* $t = x_1x_2 \cdots x_n$*, ahol az* x_i*-k nem feltétlenül különbözőek. Legyen továbbá* $\varepsilon : X_t \to S_M$ t *egy kiértékelése. Ekkor a fenti jelölésekkel:*

1. $\varepsilon(t) \neq 0$ *akkor és csak akkor, ha* $\varepsilon(xy) \neq 0$ t *semelyik* xy *alakú részszavára sem;*

2. *Ha* $\varepsilon : X_t \to S_M$ *nem veszi fel a 0-át semilyen* x*-re sem, akkor definiálható egy* $\varphi_t : G_t \to H_M$ *leképezés a következő formulával:* $\varphi_t(a_x) = \pi_\Lambda(\varepsilon(x))$ *és* $\varphi_t(b_x) = \pi_I(\varepsilon(x))$*;*

3. $\varepsilon(t) \neq 0$ *pontosan akkor, ha* ε *nem veszi fel a* 0*-át, és az ekkor definiálható* $\varphi_t : G_t \to H_M$ *leképezés gráfhomomorfizmus.*

Ezen leírás segítségével, már pontososan karakterizálhatóak S_A azonosságai. A pontos leírást Szabó es Seif [16] cikke tartalmazza, most az egyszerűség kedvéért ezeket az eredményeket már csak az előbbi példában adott S_A félcsoportra tárgyaljuk.

12. állítás. *Legyen $t = x_1x_2 \ldots x_n$, $s = y_1y_2 \ldots y_m$ termek. Ekkor a fent bevezetett jelölésekkel $t \equiv s$ pontosan akkor teljesül S_A-ban, ha mindkét alábbi feltétel teljesül:*

(I) $G_t = G_s$;

(II) $x_1 = y_1$ *és* $x_n = y_m$.

Valójában ez az állítás egy az egyben igaz az olyan struktúramátrixú félcsoportokra, amelyek nem csak néhány, csupa 1-esből álló blokkot tartalmaznak, azaz amelyekhez tartozó H_M párosgráf nem teljes páros gráfok diszjunkt uniója.

Bizonyítás: Láttuk, hogy $G_A = H_6$ épp egy hatszög. Ha (I) teljesül, akkor a két termben ugyanazok az xy kifejezések szerepelnek részszóként, azaz 3. lemma 2. pontja alapján t és s ugyanakkor nulla. (II) teljesülése pedig a 3. lemma 3. pontja szerint azt biztosítja, hogy ha egy behelyettesítésre a termek nem nullák, akkor egyenlőek.

A „csak akkor" irányhoz elég konkrét behelyettesítéseket adni, melyekre a két term nem egyenlő.

Tegyük fel, hogy (I) nem teljesül, azaz $G_t \neq G_s$. Ez kétféleképpen fordulhat elő: vagy a két gráf csúcshalmaza különbözik, vagy az élhalmazuk. Az első esetben $X_t \neq X_s$. Az általánosság megszorítása nélkül feltehető, hogy $x \in X_t \setminus X_s$. Tekintsük ekkor a következő behelyettesítést:

$$\varepsilon(z) = \begin{cases} 0 & \text{ha } z = x, \\ \langle 2,3 \rangle & \text{egyébként} \end{cases},$$

ekkor $\varepsilon(t) = 0 \neq \langle 2,3 \rangle = \varepsilon(s)$.

Ha az élhalmaz nem egyezik meg, akkor megint feltehető, hogy $(x, y) \in E_t \setminus E_s$, azaz az xy kifejezés részszava t-nek, de s-nek nem, ekkor az

$$\varepsilon(z) = \begin{cases} \langle 2,1 \rangle & \text{ha } z = x, \\ \langle 1,3 \rangle & \text{ha } z = y, \\ \langle 2,3 \rangle & \text{egyébként} \end{cases}.$$

behelyettesítésre $\varepsilon(t) = 0 \neq \varepsilon(s)$.

Tegyük fel, hogy (II) valamelyike nem teljesül, és tekintsük a következő behelyettesítéseket:

$$\varepsilon(z) = \begin{cases} \langle 1,2 \rangle & \text{ha } z = x_1, \\ \langle 3,2 \rangle & \text{egyébként} \end{cases}.$$

Ha $x_1 \neq y_1$, akkor $\varepsilon(t) = \langle 1,2 \rangle \neq \langle 3,2 \rangle = \varepsilon(s)$.

$$\varepsilon(z) = \begin{cases} \langle 3,2\rangle & \text{ha } z = x_n, \\ \langle 3,1\rangle & \text{egyébként} \end{cases} .$$

Ekkor $x_n \neq y_m$ esetén $\varepsilon(t) = \langle 3,2\rangle \neq \langle 3,1\rangle = \varepsilon(s)$. □

Mivel ezek a tulajdonságok polinom időben tesztelhetőek, így:

13. következmény. TERM-EQ(S_A) *P-beli.*

Az azonosságok hasonló karakterizációjával belátható, hogy:

14. tétel. *Minden teljesen kombinatorikus 0-egyszerű félcsoportra,* TERM-EQ *P-beli.*

3.2. coNP-teljes problémák

A coNP-teljesség bizonyítására lényegében egyetlen módszer létezik: visszavezetjük egy már ismerten coNP-teljes problémára, azaz megmutatjuk, hogy amennyiben az eredeti probléma gyorsan megoldható, akkor az ismert probléma is (ez az úgynevezett Karp-redukció). A bizonyítások csak abban térhetnek el, hogy az eredeti kérdést milyen módszerekkel, és milyen ismert problémára vezetjük vissza.

3.2.1. Az első példa

Popov és Volkov [13] konstruálta az első példát olyan félcsoportra, melyben a szóprobléma coNP-teljes. Mint minden első példa ez is akármilyen bonyolult lehetett. A konstrukció a SAT-ra való visszaveztéssel ment. „Egyszerűen” definiáltak egy olyan félcsoportot, amelyben minden Boole-formula lekódolható , ez két elem által generált $\langle a,b\rangle$ szabad félcsoport egy faktora lesz. A $P_j = ab^{15+j}a^2$ $(0 \leq j \leq 14)$ elemek segítségével adhatóak meg a kifejezések alkotóelemei:

$$(= P_0P_2P_1 \qquad) = P_0P_3P_1$$
$$\neg = P_0P_4P_1 \qquad \vee = P_0P_5P_1 \qquad \wedge = P_0P_6P_1$$
$$1 = P_0P_{10}P_1 \qquad 0 = P_0P_{11}P_1$$

A kifejezések ($\mathcal{L}$):

$$(0), (1), (\neg 0), (\neg 1)$$
$$(V_1 \wedge V_2 \wedge \cdots \wedge V_k),\ \text{ahol } V_i \in \{0,1,\neg 0,\neg 1\}$$
$$W_1 \vee W_2 \vee \cdots \vee W_l,\ \text{ahol } W_j \text{ a fenti alakú}$$

A Relációk:

$$U = W, \text{ ha } U, W \notin \mathcal{L}$$

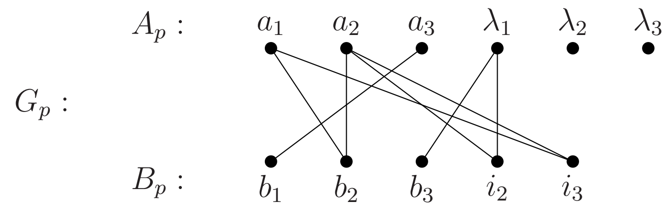
$$\begin{array}{cc}
\neg 0 = 1 & \neg 1 = 0 \\
(0 \wedge 0 = (0 & (0 \wedge 1 = (0 \\
(1 \wedge 0 = (0 & (1 \wedge 1 = (1 \\
\wedge 0 \wedge 0 = \wedge 0 & \wedge 0 \wedge 1 = \wedge 0 \\
\wedge 1 \wedge 0 = \wedge 0 & \wedge 1 \wedge 1 = \wedge 1 \\
(0) \vee (0) = (0) & (0) \vee (1) = (1) \\
(1) \vee (0) = (1) & (1) \vee (1) = (1)
\end{array}$$

Így kapunk egy félcsoportot, ami elkódolja a Boole-formulákat, és mindenesetre teljesülnek benne a Bolle-formulák alapvető azonosságai. A kérdés az, hogy ezektől a relációktól nem esik-e túlságosan össze a félcsoport, azaz a különböző Boole-formulákat tényleg különböző félcsoportelemek reprezentáják-e? Ennek bizonyítása nagyon hosszú és technikai, ezért nem részletezzük. Közben adható egy felső becslés a félcsoport méretére is: kijön, hogy legfeljebb 2^{1700} elemű lehet.

3.2.2. POL-EQ(S_A)

Ezt a problémakört is érdemes visszavezetni a gráfokra, ugyanúgy, mint azt a TERM-EQ esetében tettük. A polinomok a félcsoportok körében a következő általános alakba írhatóak: $p = e_1 e_2 \cdots e_n$, ahol az e_i-k ($1 \leq i \leq n$) vagy változók, vagy félcsoportbeli konstansok, és nem feltétlenül különbözőek. Feltehető, hogy p-ben nem szerepel a nulla konstansként, ekkor ugyanis $p \equiv 0$, azaz minden rá vonatkozó kérdés triviálisan eldönthető. Jelölje X_p a p-ben előforduló változók, $C_p \subseteq I \times \Lambda$ a p-beli konstansok halmazát. Definiáljuk továbbá a p-ben szereplő konstasok első illetve utolsó tagjainak halmazát: $I_p = \pi_I(C_p)$ és $\Lambda_p = \pi_\Lambda(C_p)$. Az 3.1.1. fejezetben mutatott konstrukció mintájára most is definiálható egy gráf az adott p polinomhoz. Legyen tehát $G_p(A_p, B_p, E_p)$ a p-hez tartozó gráf, ahol $A_p = \{a_x : x \in X_p\} \cup \Lambda_p$, $B_p = \{b_x : x \in X_p\} \cup I_p$, továbbá $a \in A_p$ és $b \in B_p$ között fusson él, ha az a-nak és b-nek megfelelő változók vagy konstansok egymásmellett szerepelnek p-ben. Persze ha p egy term, akkor ez a konstrukció visszaadja az 3.1.1. fejezetben tárgyalt gráfot. Nézzünk erre is egy példát:

15. példa. *Legyen* $p = x_1 x_2 \langle 2,3\rangle x_2^2 \langle 3,1\rangle \langle 2,1\rangle x_3 x_1 \langle 3,2\rangle$, *a* p*-hez tartozó gráf:*



Ismét azt látjuk, hogy egy polinom nemnullasága egy gráfhomomorfizmus-problémára vezethető vissza, csak ezúttal színezettre.

16. lemma. *Legyen p egy polinom, amelyben a 0 nem szerepel konstansként, ekkor a fenti jelölésekkel:*

1. *$C_p \subseteq I \times \Lambda$, így az identitás definiál egy $f_p : I_p \cup \Lambda_p \to H$ leképezést;*

2. *Ha $p \not\equiv 0$, akkor f_p részleges gráfhomomorfizmus;*

Tegyük fel, hogy f_p részleges gráfhomomorfizmus és legyen $\varepsilon : X_p \to S_M$ p egy kiértékelése, ekkor:

3. *$\varepsilon(p) \neq 0$ akkor és csak akkor, ha $\varepsilon(ef) \neq 0$ p semelyik ef alakú részszavára sem;*

4. *Ha ε nem veszi fel a 0-át semilyen x-re sem, akkor definiálható egy $\varphi_p : G_p \to H$ leképezés a következő formulával: $\varphi|_{I_p \cup \Lambda_p} \equiv f_p$ és $\varphi_p(a_x) = \pi_\Lambda(\varepsilon(x))$ és $\varphi_p(b_x) = \pi_I(\varepsilon(x))$;*

5. *$\varepsilon(t) \neq 0$ pontosan akkor, ε nem veszi fel a 0-át, és az ekkor definiálható $\varphi_t : G_t \to H$ leképezés gráfhomomorfizmus;*

A lemma azonnali következménye:

17. következmény. *$p \not\equiv 0$ pontosan akkor, ha f_p kiterjeszthető G_p-re.*

Láttuk, hogy minden $p \not\equiv 0$ problémához deifiniálható egy színezettgráf-homomorfizmus probléma. Mint azt Seif és Szabó [16] igazolta, ennek a megfordítása is igaz:

18. állítás. *Legyen H_M olyan gráf, melynek szomszédságimátrixa nem tartalmaz csupa nulla sort illetve oszlopot. Ekkor $\mathrm{OAL}(H_M)$ minden input-problémájához definiálható olyan p polinom, amellyel pontosan akkor létezik a színezett homomrfizmus, ha $p \not\equiv 0$.*

Bizonyítás: Legyen $G(V,E)$ és $f : V \to I \cup \Lambda$ részleges homomorfizmus OAL(H_M) egy bemenete. Ha a színezettgráf-homomorfizmus problémának nem triviálisan nincs megoldása (ilyenkor például a $p = (1,1,1)$ polinom megfelel az állításbeli követelményeknek), akkor G páros gráf, és van a csúcsainak egy olyan $V = A \cup B$ felosztása, hogy egyrészt A és B között nem megy él, másrészt $f(A) \subseteq \Lambda$ és $f(B) \subseteq I$. Jelölje az A-beli színezett csúcsokat Λ', a B-belieket I', az A-beli nem színezetteket A' és a B-belieket B'. Esetleg néhány új csúcs hozzávételével feltehető, hogy $|\Lambda'| = |I'|$ és $|A'| = |B'|$. Legyen $X_p = X \cup^\star \{x_e : e \in E\}$ változók egy halmaza, melyre $|X| = |A'| = |B'|$. Ekkor persze A' és B' halmazok indexelhetőek X-szel: $A' = \{a_x : x \in X\}$ $B' = \{b_x : x \in X\}$. Továbbá legyen $|C| = |\Lambda'| = |I'|$, ekkor Λ' és I' indexelhető C-vel: $\Lambda' = \{\lambda_c : c \in C\}$ $I' = \{i_c : c \in C\}$. Jelölje az így kapott páros gráfot $G'(A' \cup^\star \Lambda', B' \cup^\star I', E)$. Definiáljunk minden $e = (a,b) \in E$ élhez egy w_e szót:

$$w_e = \begin{cases} xyx_e & \text{ha } a = a_x \in A' \text{ és } b = b_y \in B', \\ x\langle\lambda_d, i_d\rangle x_e & \text{ha } a = a_x \in A' \text{ és } b = i_d \in I', \\ \langle\lambda_c, i_c\rangle y x_e & \text{ha } a = \lambda_c \in \Lambda' \text{ és } b = b_y \in B', \\ \langle\lambda_c, i_c\rangle\langle\lambda_d, i_d\rangle x_e & \text{ha } a = \lambda_c \in \Lambda' \text{ és } b = i_d \in I', \end{cases} .$$

Legyen

$$p = \prod_{e \in E} w_e \, .$$

Ekkor a p-hez tartozó G_p gráf, G' és még $2|E|$ darab G' egy-egy pontjához kapcsolódó pontokból áll. És, mivel M minden sora illetve oszlopa tartalmaz nem 0 elemet, így a H gráf tetszőleges csúcsának van szomszédja, azaz pontosan akkor létezik $G' \to H_M$ színezettgráf-homomorfizmus, ha van $G_p \to H_M$ színezettgráf-homomorfizmus is. Tehát p megfelel a követelményeknek. $\square$

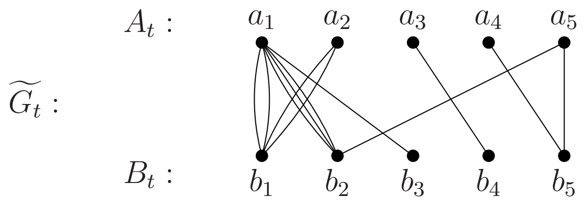
És így mivel POL $\equiv 0 \preceq_P$ POL-EQ, és a 2.2. fejezetbeli megjegyzés szerint OAL(H_6) NP-teljes:

19. tétel. POL-EQ(S_A) *coNP-teljes.*

3.3. TERM-EQ($\mathcal{M}_{19}$)

A 3.1.1. és a 3.2.2. fejezetekhez hasonlóan ez a probléma is sikeresen vizsgálható gráfhomomorfizmusokon keresztül, azonban mivel már nem teljesen kombinatorikus 0-egyszerű félcsoportról van szó, így egy termhez tartozó gráfnak nemcsak az xy részszavakat, hanem azok multiplicitását is kódolnia kell. Ezért most egy t termhez a 3.1.1. fejezetbeli $G_t(A_t, B_t, E_t)$ gráfon kívül egy többszörös éleket is tartalmazó $\widetilde{G_t}(A_t, B_t, \widetilde{E_t})$ páros gráfot is definiálunk: legyen az $(a_x, b_y) \in E_t$ multiplicitása $\widetilde{E_t}$-ben az xy részszó t-beli előfordulásainak száma.

20. példa. *Így a 10. példában adott t-hez tartozó gráf:*



Az eddigiekhez hasonlóan G_t és $\widetilde{G_t}$ gráf-konstrukciók segítségével tudjuk vizsgálni az $\mathcal{M}_{19}$ feletti termeket:

21. lemma. *Legyen $t = x_1 x_2 \cdots x_n$, ahol az x_i-k nem feltétlenül különbözőek. Legyen $\varepsilon : X_t \to \mathcal{M}_{19}$ t egy kiértékelése, ekkor a fenti jelölésekkel:*

1. *$\varepsilon(t) \neq 0$ akkor és csak akkor, ha $\varepsilon(xy) \neq 0$ t semelyik xy alakú részszavára sem;*

2. *Ha $\varepsilon : X_t \to \mathcal{M}_{19}$ nem veszi fel a 0-át semilyen x-re sem, akkor definiálható egy $\varphi_t : G_t \to H_6$ és egy $\widetilde{\varphi}_t : \widetilde{G_t} \to H_6$ leképezés a következő formulával: $\varphi_t(a_x) = \widetilde{\varphi}_t(a_x) = \pi_\Lambda(\varepsilon(x))$ és $\varphi_t(b_x) = \widetilde{\varphi}_t(b_x) = \pi_I(\varepsilon(x))$;*

3. *$\varepsilon(t) \neq 0$ pontosan akkor, ha ε nem veszi fel a 0-át, és az ekkor a definiálható $\varphi_t : G_t \to H_6$ illetve $\widetilde{\varphi}_t : \widetilde{G_t} \to H_6$ leképezések gráfhomomorfizmusok;*

4. *Jelölje $l_t = |\{2 \leq k \leq n : \varphi_t(a_{x_k}) = 1, \varphi_t(b_{x_{k+1}}) = 2\}|$, és definiáljuk az $\eta : X_t \to \mathbb{Z}_2$ leképezést a következőképpen: $\eta(x) = \pi_G(\varepsilon(x))$. Ekkor ha $\varepsilon(p) \neq 0$, akkor*
$$\varepsilon(t) = (\varphi_t(a_{x_1}), \eta(x_1)\eta(x_2)\cdots\eta(x_n) \cdot a^{l_t}, \varphi_t(b_{x_n})) \ ;$$

5. *$l_t = |\widetilde{\varphi}_t^{\,-1}(\lambda_1, i_2)|$;*

6. *Ha $\varepsilon(t) \neq 0$, akkor*
$$\varepsilon(t) = (\varphi_t(x_1), \eta(x_1)\eta(x_2)\cdots\eta(x_n) \cdot a^{|\widetilde{\varphi}_t^{\,-1}(\lambda_1, i_2)|}, \varphi_t(x_n)) \ .$$

A további vizsgálathoz egy technikai definicióra van szükségünk. H_6 a 3.1.1. fejezetben definiált hatszög. Legyen $G(A,B,E)$ egy (esetleg többszörös éleket tartalmazó) páros gráf, jelölje $G_i(A_i,B_i,E_i)$ $(1 \le i \le k)$ az összfüggő komponenseit. Azt mondjuk, hogy két $\varphi,\psi : G \to H_6$ homomorfizmus *forgatás-ekvivalens* ($\varphi \sim \psi$), ha vannak a H_6 hatszögnek olyan $\omega_i : H_6 \to H_6$ izomrfiái, melyekre $\varphi|_{G_i} = \omega_i \circ \psi|_{G_i}$. Ekkor φ a ψ egy *elforgatása.* Könnyen látszik, hogy $\sim$ ekvivalencia-reláció a G-ből H_6-ba menő homomorfizmusok halmazán.

22. lemma. *Legyen t egy term, jelölje G_t a t-hez definiált gráfot. Legyen továbbá adva egy $\varphi : G_t \to H_6$ homomorfizmus, ekkor:*

1. *$\varphi : G_t \to H_6$-nek pontosan egy olyan elforgatása van, melyre $\psi(A_t) \subseteq \Lambda$ és $\psi(B_t) \subseteq I$;*

2. *Van egy olyan $\varepsilon : X_t \to \mathcal{M}_{19}$ kiérékelés, amelyhez tartozó $\varphi_t : G_t \to H_6$ homomorfizmus φ egy elforgatottja.*

A következőkben a 12. állításhoz hasonlóan leírjuk $\mathcal{M}_{19}$ azonosságait, majd fokozatosan feltárjuk a TERM-EQ($\mathcal{M}_{19}$) és a 2HOM(H_6) közötti szoros összfüggést.

23. állítás. *Legyen $t = x_1x_2\dots x_n, s = y_1y_2\dots y_m$ termek, a fent bevezetett jelölésekkel: $t \equiv s$ pontosan akkor teljesül $\mathcal{M}_{19}$-ben, ha a következő négy feltétel mindegyike teljesül:*

(I) $G_t = G_s$;

(II) $x_1 = y_1$ *és* $x_n = y_m$;

(III) *Minden változó előfordulásának paritása megeggyezik t-ben illetve s-ben;*

(IV) *Tetszőleges $\mathcal{M}_{19}$ feletti kiértékelésre az egymásutáni $\langle .,2\rangle\langle 1,.\rangle$ tagok előfordulásának paritása megeggyezik t-ben ill. s-ben, azaz $l_t \equiv l_s \pmod 2$ minden behelyettesítésre;*

Bizonyítás: 9. lemma alapján ezek a feltételek tényleg elégségesek. Az (I) és (II) feltételek a 12. állítás szerint már S_A felett is szükségesek voltak, így $\mathcal{M}_{19}$ felett is. A többi feltétel szükségességét konkrét behelyettesítésekkel bizonyítjuk:

Tegyük fel, hogy x nem felel meg a (III) feltételnek, azaz pl. páros sokszor szerepel t-ben, és páratlanszor s-ben. Tekintsük az alábbi behelyettesítést:

$$\varepsilon(z) = \begin{cases} (2,a,3) & \text{ha } z = x, \\ (2,1,3) & \text{egyébként} \end{cases}.$$

Ekkor $\varepsilon(t) = (2,1,3) \neq (2,a,3) = \varepsilon(s)$.
A (IV) feltétel szükséges a (III) feltétel teljesülése és a 16. lemma szerint.

□

A (I),(II) és (III) feltételek polinomidőben ellenőrízhetőek, így valójában elég csak a (IV) feltétel ellenőrizésével foglalkozni. És ha ez a három feltétel tényleg teljesül, akkor nem kell minden behelyettesítést külön kezelni:

24. lemma. *Tegyük fel, hogy $t \equiv s$ a* TERM-EQ *egy bemenete, ekkor a* (III)*feltétel teljesülése esetén elég $\langle i, \lambda \rangle$ alakú behelyettesítéseket ellenőrizni $t \equiv s$ azonosság $\mathcal{M}_{19}$-beli teljesülésének bizonyításához.*

A továbbiakban mindent átfogalmazunk a gráfok nyelvére.

(III′) Minden csúcs fokszámának paritása megegyezik $\widetilde{G_t}$-ben illetve $\widetilde{G_s}$-ban;

(IV′) Minden $\mathcal{M}_{19}$ feletti kiértékelésre a (λ_2, i_1) él ősképének paritása megegyezik $\widetilde{\varphi}_t$-nél, illetve $\widetilde{\varphi}_s$-nél, azaz:

$$|\widetilde{\varphi}_t^{-1}(\lambda_2, i_1)| \equiv |\widetilde{\varphi}_s^{-1}(\lambda_2, i_1)| \pmod 2$$

Mivel a hatszög forgásszimmetrikus, így (IV′) feltétel ekvivalens az alábbival:

(IV″) Minden $\mathcal{M}_{19}$ feletti kiértékelésre az összes (λ, i) él ősképének paritása megegyezik $\widetilde{\varphi}_t$-nél, illetve $\widetilde{\varphi}_s$-nél, azaz

$$|\widetilde{\varphi}_t^{-1}(\lambda, i)| \equiv |\widetilde{\varphi}_s^{-1}(\lambda, i)| \pmod 2$$

Jelölje $\widetilde{G_{t\equiv s}}(A_{t\equiv s}, B_{t\equiv s}, \widetilde{E_{t\equiv s}}) = \widetilde{G_t} \uplus \widetilde{G_s}$-t. Ekkor a 22. lemma segítségével újabb ekvivalens feltételek fogalmazhatóak meg:

(III″) Minden $\widetilde{G_{t\equiv s}}$-beli csúcs foka páros.

(IV‴) Minden $\psi : \widetilde{G_{t\equiv s}} \to H_6$ homomorfizmusra az összes (λ, i) él őském páros, azaz

$$|\psi^{-1}(\lambda, i)| \equiv 0 \pmod 2$$

25. megjegyzés. *Az* (IV$'''$) *feltételből következik az* (III$''$) *feltétel.*

Bizonyítás: Tegyük fel, hogy van egy páratlan fokú csúcs: v, az általánosság megszorítása nélkül feltehető, hogy $v \in A_{t\equiv s}$. Vegyük a következő homomorfizmust:

$$\varphi(u) = \begin{cases} \lambda_3 & \text{ha } u = v, \\ i_2 & \text{ha } u \in B, \\ \lambda_2 & \text{egyébként} \end{cases} .$$

Azaz ilyenkor a (IV$'''$) feltétel sem teljesül. □

Arra jutottunk tehát, hogy:

26. állítás. *Legyen* $t = x_1 x_2 \dots x_n, s = y_1 y_2 \dots y_m$ *termek, a fent bevezetett jelölésekkel:* $t \equiv s$ *pontosan akkor teljesül* $\mathcal{M}_{19}$*-ben, ha a* (I),(II) *és* (IV$'''$) *feltétel teljesülnek.*

Kijött tehát, hogy a TERM-EQ($\mathcal{M}_{19}$) minden bemenetéhez társítható egy, a 2.2. fejezetben definiált pároshomomorfizmus-probléma. Most belátjuk, hogy ennek a megfordítása is igaz. Mivel eddig a gráfoknak csak mod 2 tulajdonságait használtuk, így tekinthetünk két gráfot azonosnak, ha mod 2 nem különböznek. Azt mondjuk, hogy $G(V, E_G)$ és $H(V, E_H)$ gráfok mod 2 megegyeznek, $G \equiv H \pmod 2$, ha minden (u, v), csúcspárra az (u, v) él multiplicitásának paritás megegyezik E_G-ben és E_H-ban.

27. állítás. *Legyen* $G(A, B, E)$ *egy páros gráf, melynek minden csúcsának foka páros. Ekkor létezik olyan* $t \equiv s$ *azonosság, amelyre az* (I) *és a* (II) *feltételek teljesülnek, és* $\widetilde{G_{t\equiv s}} \equiv G \pmod 2$.

Bizonyítás: Esetleg néhány új csúcs hozzávételével feltehető, hogy $|A| = |B|$. Definiáljuk a $G_{t\equiv s}(A_{t\equiv s}, B_{t\equiv s}, E)$ gráfot az $A_{t\equiv s} = A \cup^\star \{c\}$ és a $B_{t\equiv s} = B \cup^\star \{d\}$ egyenlőségekkel. Legyen $X \cup^\star \{z\}$ változók egy halmaza úgy, hogy, $|X \cup^\star \{z\}| = |A_{t\equiv s}| = |B_{t\equiv s}|$. Ekkor tehát a csúcsok indexelhetőek $X \cup^\star \{z\}$-vel: $A_{t\equiv s} = \{a_x : x \in X\} \cup^\star \{c\}$ és $B_{t\equiv s} = \{b_x : x \in X\} \cup^\star \{d\}$, és c illetve d tartozzanak z-hez. Egy $e = (a_x, b_y) \in E$ élhez definiáljuk a $w_e = xy$ szót. Legyen

$$h = \prod_{e \in E} (w_e y^2) .$$

Tekintsük a

$$t := y^2 h$$

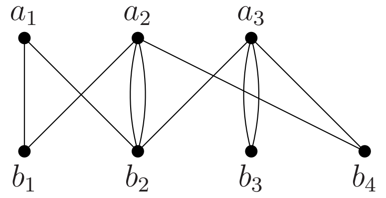
$$s := y^2 hh$$

termeket. Ekkor $G_{t\equiv s} \equiv G \pmod 2$, azaz $t \equiv s$ a feltételeknek megfelelő azonosság. □

A könnyebb érthetőség kedvéért a fenti bizonyítást egy példán keresztül szemléltetjük.

28. példa. *Legyen*

G :



A fenti G gráfhoz konstruált termek a következőképpen néznek ki:

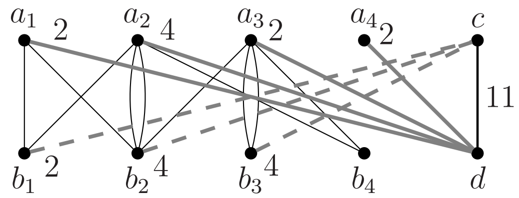
$$h = x_1^2y^2x_1x_2y^2x_2y^2x_2x_1y^2x_2^2y^2x_2^2y^2x_2x_3y^2x_3^2y^2x_3^2y^2x_4x_2y^2x_4x_3y^2$$

$$t = y^2x_1^2y^2x_1x_2y^2x_2y^2x_2x_1y^2x_2^2y^2x_2^2y^2x_2x_3y^2x_3^2y^2x_3^2y^2x_4x_2y^2x_4x_3y^2$$

$$s = y^2x_1^2y^2x_1x_2y^2x_2y^2x_2x_1y^2x_2^2y^2x_2^2y^2x_2x_3y^2x_3^2y^2x_3^2y^2x_4x_2y^2x_4x_3y^2\cdot$$
$$\cdot x_1^2y^2x_1x_2y^2x_2y^2x_2x_1y^2x_2^2y^2x_2^2y^2x_2x_3y^2x_3^2y^2x_3^2y^2x_4x_2y^2x_4x_3y^2$$

Például a t-hez tartozó gráf:

$\widetilde{G_t}$:



Hasonlóan felrajzolható $\widetilde{G_t}$ és $\widetilde{G_{t\equiv s}}$ is.

A 16. és 22. lemmákból az alábbi következik:

29. következmény. *Legyen $G(A, B, E)$ olyan páros gráf, melynek minden fokszáma páros. Ekkor megadható egy az* (I) *és* (II) *feltételeket teljesítő $t \equiv s$ azonosság, melyre $t \equiv s$ igaz $\mathcal{M}_{19}$ felett pontosan akkor, ha minden $\varphi : \widetilde{G_{t\equiv s}} \to H$ homomorfizmus páros.*

Mostantól a 2HOM(H_6) coNP-teljességét szeretnénk belátni. Ehhez, mivel RET(H_6) NP-teljes a 2.2. fejezetbeli megjegyzés szerint, így elég a következőt bizonyítani:

30. állítás. *Minden egy H'_6 hatszöget tartalmazó G egyszerű gráfhoz definiálható egy olyan $\widetilde{G}$ páros gráf, melynek minden fokszáma páros, és pontosan akkor létezik $\varphi : G \to H_6$ retrakció, ha létezik $\psi : \widetilde{G} \to H_6$ nem páros homomorfizmus.*

Bizonyítás: Legyen G az állításbeli páros gráf. Ekkor $\widetilde{G}$-ot úgy kapjuk, hogy G minden nem a H'_6 hatszöghöz tartozó élet megduplázunk. Ekkor persze $\widetilde{G}$ minden csúcsa valóban páros fokú lesz. Azt állitjuk, hogy $\widetilde{G}$ megfelel az állítás követelményeinek.
Tegyük fel, hogy $\varphi : G \to H'_6$ retrakció, ekkor ugyanez a leképezés megad egy $\widetilde{\varphi} : \widetilde{G} \to H_6$ homomorfizmust is. Legyen ekkor $\psi = \omega \circ \widetilde{\varphi}$, ahol ω az izomorfizmus H_6 és H'_6 között.
A másik irányhoz tegyük fel, hogy $\psi : \widetilde{G} \to H_6$ nem páros homomorfizmus. Mivel a hatszög éleit kivéve minden élet megdupláztunk, így $\psi|_{H_6} : H'_6 \to H_6$ szintén egy nem páros homomoprfizmust ad, ami izomorfizmus is, hiszen a hatszög bármely nem szürjektív homomorfizmusa páros. Ekkor $\varphi = (\psi|_{H_6})^{-1} \circ \psi$ G egy H_6-ra való retrakcióját definiálja. □
Az eddigiekkel tehát azt sikerült igazolni, hogy:

31. tétel. 2HOM*(H_6) coNP-teljes.*

Ezekből pedig rögtön következik 8. tétel, miszerint TERM-EQ($\mathcal{M}_{19}$) NP-teljes.

3.4. Záró megjegyzések

Mint az eddigiekből kiderült, a TERM-EQ nehézségének megállapításához nincs egy jól bevállt, mindig működő módszer. Érdekes kérdés, hogy a félcsoportok körében van-e egyáltalán remény a dichotómia bizonyítására, vagy van-e esély legálabb a 0-egyszerű félcsoportok esetében? A továbbiakban egy ezzel kapcsolatos negatív eredményt szeretnénk bizonyítani, mely szerint a probléma nehezebb az eddig még megoldatlan CSP problémakörnél: sejtésünk, hogy minden CSP problémához van olyan 0-egyszerű félcsoport, amelyre a szóprobléma ekvivalens az adott CSP problémával.

Irodalomjegyzék

[1] J. Büki and Cs. Szabó. Colored homomorphisms for direct products of graphs. *Information Processing Letters*, 81/4:175–178, 2002.

[2] S. Burris and J. Lawrence. The equivalence problem for finite rings. *Journal of Symbolic Computation*, 15:67–71, 1993.

[3] A. Clifford and G. Preston. *The Algebraic Theory of Semigroups*, volume 1. American Mathematical Society, 1961.

[4] M.Y. Feder, T. Vardy. Monotone monadic SNP and constraint satisfaction. In *25th Annual ACM Symposium on Theory of Computing*, pages 612–622, 1993.

[5] T. Feder, P. Hell, and J. Huang. List homomorphism and circular arc graphs. *Combinatorica*, 19:487–505, 1999.

[6] M. Goldmann and A. Russel. The complexity of solving equations over finite groups. *Information and Computation*, 178:253–262, 2002.

[7] P. Heel and J. Nešetřil. On the complexity of h-coloring. *Journal of Combinatorial Theory*, B 48:92–110, 1990.

[8] G. Horváth. Véges csoportok azonosságai. TDK dolgozat, 2003.

[9] H. Hunt and R. Stearns. The complexity for equivalence for commutative rings. *Journal of Symbolic Computation*, 10:411–436, 1990.

[10] O. Klíma. On the solvability of equations in semigroups with $x^r = x$. *Contributions to general algebra*, 12:237–245, 1999.

[11] J. Lawrence and R. Willard. The complexity of solving polynomial equations over finite rings. manuscript, 1997.

[12] C.H. Papadimitrou. *Számítási bonyolultság.* Novadat Bt., 1999.

[13] V.Yu. Popov and M.V. Volkov. Complexity of checking identities and quasi-identities in finite semigroups. *Journal of Symbolic logic*, to appear.

[14] L. Rónyai, G. Ivanyos, and R. Szabó. *Algoritmusok*. Typotex, 1999.

[15] S. Seif and Cs. Szabó. Algebra complexity problems involving graph homomorphism, semigroups and the constraint satisfaction problem. *Journal of Complexity*, 19(2):153–160, 2003.

[16] S. Seif and Cs. Szabó. The computational complexity of checking identities in simple semigroups and matrix semigroups over finite fields. Semigroup Forum, elfogadva, 2005.

[17] Cs. Szabó and V. Vértesi. The complexity of checking identities for finite matrix rings. *Algebra Universalis*, 51:439–445, 2004.

[18] Cs. Szabó and V. Vértesi. The complexity of the word-problem for finite matrix rings. *Proceedings of the American Mathematical Society*, 132:3689–3695, 2004.

[19] V. Vértesi. Azonosságok 0-egyszerű félcsoportokban. TDK dolgozat, 2004.

[20] V. Vértesi. Azonosságok gyűrűkben. TDK dolgozat, 2004.