Debreceni Egyetem Természettudományi és Technológiai Kar
Matematikai Intézet

Egyenletmegoldhatóság bonyolultsága szemipattern csoportok felett

Témavezető:
Dr. Horváth Gábor
egyetemi adjunktus
Algebra és Számelmélet tanszék

Készítette:
Földvári Attila
Matematikus MSc hallgató

Debrecen
2013. október 1.

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318202.

A kutatás a TÁMOP 4.2.4.A/2-11-1-2012-0001 azonosító számú „Nemzeti Kiválóság Program – Hazai hallgatói, illetve kutatói személyi támogatást biztosító rendszer kidolgozása és működtetése konvergencia program" című kiemelt projekt keretében zajlott.

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

SZÉCHENYI TERV

Tartalomjegyzék

1. fejezet

Bevezetés

Napjainkban az algebrai problémák számítógépes vizsgálata egyre nagyobb teret hódít. Ezen kutatások egyik iránya egy véges algebra feletti ekvivalencia, illetve egyenletmegoldhatóság problémák bonyolultságának meghatározása.

Adott $\mathcal{A}$ véges algebra feletti ekvivalencia probléma azt kérdezi, hogy tetszőleges $\mathcal{A}$ feletti p és q kifejezések ekvivalensek-e vagy sem, azaz p és q azonos értéket vesznek-e fel bármely $\mathcal{A}$-beli helyettesítésre. Az $\mathcal{A}$ véges algebra feletti egyenletmegoldhatóság probléma azt kérdezi, hogy tetszőleges $\mathcal{A}$ feletti p és q kifejezésekre a $p = q$ egyenlet megoldható-e, azaz létezik-e olyan $\mathcal{A}$-beli helyettesítés, melyre $p = q$. Ezen problémák mindig eldönthetőek a változók összes lehetséges helyettesítésének ellenőrzésével. Az érdekesebb kérdés, hogy milyen gyorsan tudunk dönteni, azaz ezen döntési problémák mely bonyolultsági osztályba esnek.

A kérdés legelőször 1990-ben gyógyszeripari kísérletek összehangolásával kapcsolatban véges kommutatív gyűrűkre merült fel [14]. Az első eredmények megjelenése óta a problémakört erős nemzetközi érdeklődés övezi különböző véges algebrákra. Gyűrűk felett Burris és Lawrence [2], Horváth [7, 9], Horváth, Lawrence és Willard [11], Szabó és Vértesi [24, 25, 26], csoportok felett Burris és Lawrence [3], Goldmann és Russel [5, 6], Horváth, Lawrence, Mérai és Szabó [10], Horváth [8], Horváth és Szabó [12, 13], monoidok és félcsoportok felett Klíma [16, 17, 18], Larose és Zádori [19], Seif [21], Seif és Szabó [22, 23], Tesson és Thérien [27] foglalkozott a késéskörrel. A dolgozat néhány olyan véges mátrixcsoportra vizsgálja az egyenletmegoldhatóság bonyolultságát, melyre az mindeddig megoldatlan volt.

Véges, nilpotens csoportok felett az egyenletmegoldhatóság és az ekvivalencia is P-beli [3, 6]. Véges, nem feloldható csoportok felett az egyenletmegoldhatóság NP-teljes [6], az ekvivalencia coNP-teljes [10]. Véges, feloldható, de nem nilpotens csoportok felett nagyon kevés eredmény ismert

a fenti problémákra. Horváth és Szabó néhány véges, meta-Abel csoportra bizonyította, hogy az egyenletmegoldhatóság és ekvivalencia problémák P-beliek [12, 13]. A dolgozatban néhány olyan véges mátrixcsoport feletti egyenletmegoldhatóság, illetve ekvivalencia probléma bonyolultságát határozzuk meg, amelyre ezek eddig még nem voltak ismertek. A $T(m, \mathbb{F}_q)$ csoport speciális részcsoportjaira, a szemipattern csoportokra vizsgáljuk ezen problémákat. A szemipattern csoportokat, olyan $m \times m$-es felső-háromszög mátrixok alkotják, amelyek főátlójának i-edik eleme az $\mathbb{F}_q^\times$ csoport egy H_i részcsoportjából származik, továbbá a főátló felett néhány, rögzített helyen nulla áll.

1. Tétel. *A szemipattern csoportok feletti egyenletmegoldhatóság, illetve ekvivalencia problémák P-beliek.*

Az 1.1. szakaszban megismerkedünk a probléma tárgyalásához szükséges, alapvető definíciókkal, majd röviden összefoglaljuk a korábbi eredményeket. Az 1. tétel bizonyításának alapötlete szerint egy mátrixcsoport feletti egyenletet visszavezetünk egy véges test feletti, speciális alakú egyenletrendszerre. Ezért az 1.2. szakaszban felidézzük a véges testekre vonatkozó korábbi eredményeket. A 2. fejezetben tetszőleges szemipattern csoport feletti egyenletmegoldhatóságot visszavezetjük egy véges test feletti, speciális alakú egyenletrendszer megoldhatóságára. A fejezet végén a közölt algoritmus futásidejét elemezzük.

1.1. Definíciók, jelölések

Legyen $\mathcal{A}$ véges algebra és jelölje A az $\mathcal{A}$ alaphalmazát. Egy $\mathcal{A}$ feletti n-változós $f(x_1, x_2, \ldots, x_n)$ műveleten egy $f\colon A^n \to A$ függvényt értünk. A dolgozatban polinomokkal foglalkozunk. Az $\mathcal{A}$ feletti $p(x_1, x_2 \ldots, x_n)$ polinomon egy, az $x_1, x_2, \ldots, x_n$ változókból és A elemeiből az algebra alapműveleteivel képzett kifejezést értünk.

Legyen $p(x_1, x_2, \ldots, x_n)$ és $q(x_1, x_2, \ldots, x_n)$ két $\mathcal{A}$-beli polinom. Ekkor p és q polinomokat ekvivalensnek nevezzük $\mathcal{A}$ felett, ha az $x_1, x_2, \ldots, x_n$ változók bármely $(a_1, a_2, \ldots, a_n) \in A^n$ helyettesítésére $p(a_1, a_2, \ldots, a_n) = q(a_1, a_2, \ldots, a_n)$. Jele $\mathcal{A} \models p \approx q$. A $p = q$ egyenletet megoldhatónak nevezzük $\mathcal{A}$ felett, ha az $x_1, x_2, \ldots, x_n$ változóknak létezik, olyan $(a_1, a_2, \ldots, a_n) \in A^n$ helyettesítése, melyre $p(a_1, a_2, \ldots, a_n) = q(a_1, a_2, \ldots, a_n)$.

1.1. Definíció. Az $\mathcal{A}$ véges algebra feletti polinom ekvivalencia (röviden ekvivalencia) probléma bemenete két $\mathcal{A}$ feletti polinom p és q, és azt kérdezi, hogy p és q ekvivalensek-e $\mathcal{A}$ felett, azaz $\mathcal{A} \models p \approx q$ teljesül-e vagy sem. Az $\mathcal{A}$

véges algebra feletti polinom egyenletmegoldhatóság (röviden egyenletmegoldhatóság) probléma bemenete két $\mathcal{A}$ feletti polinom p és q, és azt kérdezi, hogy a $p = q$ egyenlet megoldható-e vagy sem.

Mindkét probléma eldönthető a változók összes lehetséges helyettesítésének ellenőrzésével. Azonnal adódik tehát a kérdés, hogy milyen gyorsan tudunk dönteni ezen problémákról, azaz a fenti döntési problémák mely bonyolultsági osztályba esnek. A számítási bonyolultságot a bemenet hosszának függvényében értelmezzük, így először definiálnunk kell polinomok hosszát.

1.2. Definíció. Az $\mathcal{A}$ algebra feletti p polinom hosszát rekurzívan definiáljuk és $||p||$-vel jelöljük. Ha p egy konstans vagy egyetlen változóból álló polinom, akkor $||p|| = 1$. Ha f egy n-változós alapművelete az $\mathcal{A}$ algebrának, akkor az $f(p_1, p_2, \ldots, p_n)$ polinom hossza $\sum_{i=1}^{n} ||p_i||$. Így speciálisan $||f(x_1, x_2, \ldots, x_n)|| = n$.

Tehát egy polinom hosszán a benne szereplő változók és konstansok multiplicitással vett számát értjük. Az algoritmus futásidejének jellemzéséhez bevezetjük az O jelölést. Legyenek $f, g \colon \mathbb{Z}^+ \to \mathbb{Z}^+$ függvények. Azt mondjuk, hogy $g(k) = O(f(k))$, ha van olyan pozitív egész C, hogy minden pozitív egész k-ra $g(k) \leq C \cdot f(k)$.

Az alábbiakban bevezetjük a főbb bonyolultsági osztályokat. Egy problémát P-belinek nevezünk, ha Turing-géppel polinom időben eldönthető, azaz a probléma a bemenet hosszának polinomidejében eldönthető. Tehát létezik olyan pozitív egész c, hogy a k hosszú bemenetre a probléma $O(k^c)$ időben eldönthető. Egy problémát NP-belinek nevezünk, ha nemdeterminisztikus Turing-géppel polinom időben eldönthető. Ezzel ekvivalens, hogy az igen válaszra létezik polinom méretű tanú és polinom időben ellenőrizhető, hogy a tanú valóban bizonyítja az igen választ. Egy problémát coNP-belinek nevezünk, ha a nem válaszra létezik polinom méretű tanú és polinom időben ellenőrizhető, hogy a tanú valóban bizonyítja a nem választ. A bonyolultsági osztályok precíz definíciója, és a közöttük fennálló összefüggések részletesen [4, 20]-ban megtalálhatóak.

Tetszőleges $\mathcal{A}$ véges algebra feletti $p(x_1, x_2 \ldots, x_n) = q(x_1, x_2 \ldots, x_n)$ egyenletmegoldhatóság probléma NP-beli. Ugyanis, ha $p(x_1, x_2 \ldots, x_n) = q(x_1, x_2 \ldots, x_n)$ megoldható, akkor létezik olyan $(a_1, a_2 \ldots, a_n)$ helyettesítés, melyre $p(a_1, a_2 \ldots, a_n) = q(a_1, a_2 \ldots, a_n)$. Ez a helyettesítés megfelel polinomiális tanúnak. Az $\mathcal{A}$ feletti $p(x_1, x_2, \ldots, x_n) \approx q(x_1, x_2, \ldots, x_n)$ ekvivalencia probléma coNP-beli. Ugyanis, ha $p(x_1, x_2, \ldots, x_n) \not\approx q(x_1, x_2, \ldots, x_n)$, akkor létezik olyan $(a_1, a_2, \ldots, a_n)$ helyettesítés, melyre $p(a_1, a_2, \ldots, a_n) \neq q(a_1, a_2, \ldots, a_n)$. Ez a helyettesítés megfelel polinomiális tanúnak.

A dolgozatban elsősorban véges csoport feletti ekvivalencia és egyenletmegoldhatóság problémákat tárgyalunk. Véges csoport alatt egy nemüres G halmazt értünk, melyen értelmezve van egy asszociatív szorzás művelet. Véges csoport esetén az invertálás kifejezhető megfelelő hatványra történő átírással. Így ezt nem tekintjük a csoport alapműveletének. A továbbiakban a csoportok [15]-ben közölt, alapvető tulajdonságait ismertnek tekintjük.

Egy G véges csoport feletti $p(x_1, \ldots, x_n)$ polinomon egy, az $x_1, \ldots, x_n$ változókból és G elemeiből képzett szorzatot értünk. Tetszőleges $G \models p \approx q$ ekvivalencia pontosan akkor teljesül, ha $G \models pq^{-1} \approx 1$. Tehát véges csoportra az ekvivalencia probléma eldöntéséhez elegendő ellenőrizni, hogy tetszőleges polinom értéke azonosan 1 vagy sem. Hasonlóan a G feletti $p = q$ egyenlet pontosan akkor megoldható, ha $pq^{-1} = 1$ megoldható. Tehet véges csoportra az egyenletmegoldhatóság probléma eldöntéséhez elegendő ellenőrizni, hogy tetszőleges polinom értéke lehet-e 1 vagy sem. Végül a p polinom hosszán a benne szereplő változók és konstansok multiplicitással vett számát értjük.

Az alábbiakban egy ismert, csoport feletti egyenletmegoldhatóság és ekvivalencia bonyolultságának kapcsolatát leíró állítást közlünk.

1.3. Állítás. *Ha egy G véges csoport felett az egyenletmegoldhatóság P-beli, akkor G felett az ekvivalencia is P-beli.*

Bizonyítás. A fenti állítás igazolásához legyen G alaphalmaza $g_1, g_2, \ldots g_N$, ahol $g_1 = 1$. Tekintsük a $G \models p \approx 1$ ekvivalenciát. Vegyük észre, hogy $G \models p \approx 1$ pontosan akkor nem teljesül, ha a $p = g_i$ egyenlet megoldható valamely $i \neq 1$ indexre. Tehát $G \models p \approx 1$ eldönthető $N - 1$ egyenlet megoldhatóságának ellenőrzésével. □

Véges csoport feletti egyenletmegoldhatóság és ekvivalencia problémára a következő bonyolultságelméleti eredmények ismertek.

2. Tétel. *Az alábbi véges csoportok felett az egyenletmegoldhatóság P-beli.*

1. *Nilpotens csoportok [6];*
2. *$G = \mathbb{Z}_p \rtimes B$, ahol B véges kommutatív csoport, p prím [7];*
3. *$G = \mathbb{Z}_4 \rtimes B$, ahol B véges kommutatív csoport [7];*
4. *$G = \mathbb{Z}_2^2 \rtimes B$, ahol B véges kommutatív csoport, $2 \nmid |B|$ [7];*
5. *$G = \mathbb{Z}_p^2 \rtimes \mathbb{Z}_2$, ahol p páratlan prím [7].*

Nem feloldható csoport feletti egyenletmegoldhatóság NP-teljes [6].

3. Tétel. *Az alábbi véges csoportok felett az ekvivalencia P-beli.*

1. *Nilpotens csoportok [6];*

2. $G = A \rtimes B$, *ahol* A *és* B *is Abel [7];*

3. $G = \mathbb{Z}_n \rtimes B$, *ahol a* B *feletti ekvivalencia probléma P-beli [7];*

4. $G = \mathbb{Z}_{n_1} \rtimes (\mathbb{Z}_{n_2} \rtimes \cdots \rtimes (\mathbb{Z}_{n_k} \rtimes (A \rtimes B)))$, *ahol az* n_i*-k pozitív egészek és* A, B *kommutatívak [7].*

Nem feloldható csoportok felett az ekvivalencia probléma coNP-teljes [10].

Megjegyezzük, hogy a szemipattern csoportok feletti egyenletmegoldhatóság és ekvivalencia problémák bonyolultsága ezen tételek segítségével többnyire nem eldönthető.

1.2. Véges testek feletti egyenletmegoldhatóság bonyolultsága

Az 1. tétel bizonyításának alapötlete szerint egy mátrixcsoport feletti egyenletet visszavezetünk egy véges test feletti, speciális alakú egyenletrendszerre. Az alábbiakban két ismert, véges testekre vonatkozó bonyolultságelméleti tételt idézünk fel. Ezen eredmények általánosabban [7, 9, 11]-ben találhatóak meg. A következő speciális esetek áttekintésével az olvasó a teljes algoritmust megismerheti a hivatkozások fellapozása nélkül.

1.4. Lemma. *Legyen* $\mathbb{F}_q$ *a* q *elemű test, ahol* q *egy prímhatvány. Legyenek* $H_1, H_2, \ldots, H_d$ *részcsoportok* $\mathbb{F}_q^\times$*-ben,* $|H_k| = h_k$ *minden* $1 \leq k \leq d$ *esetén. Legyen* $p = p(x_1, x_2, \ldots, x_n, y_{1,1}, y_{1,2}, \ldots, y_{1,m_1}, y_{2,1}, \ldots y_{d,m_d})$ *egy* $\mathbb{F}_q$*-beli, monomok összegeként adott polinom, ahol az* $x_1, x_2, \ldots, x_n$ *változók* $\mathbb{F}_q$*-beli, az* $y_{k,1}, y_{k,2}, \ldots, y_{k,m_k}$ *változók* H_k*-beli értéket vehetnek fel* $(n, m_k \in \mathbb{N})$*. Ekkor* $\mathbb{F}_q \models p \approx 0$ *eldöntése* $O(||p||)$ *időt igényel.*

Bizonyítás. Az alábbiakban egy $O(||p||)$ idejű algoritmust adunk, mellyel $\mathbb{F}_q \models p \approx 0$ eldönthető. Az $\mathbb{F}_q$ véges test minden a elemére $a^q = a$ teljesül. A H_k csoport rendje h_k, így Lagrange tétele szerint minden b elemére $b^{h_k} = 1$ teljesül $(1 \leq k \leq d)$. Ezért $\mathbb{F}_q \models x_i^q \approx x_i$ bármely $1 \leq i \leq n$ indexre és $y_{k,j}^{h_k}$ minden H_k-beli helyettesítésen 1-et vesz fel bármely $1 \leq j \leq \leq m_k$ indexre. Egy $\mathbb{F}_q$ feletti x_i, $y_{k,j}$ változóktól függő polinomot nevezzünk *egyszerű polinomnak*, ha minden benne szereplő x_i változó kitevője eleme az $\{1, 2, \ldots, q-1\}$ halmaznak és minden benne szereplő $y_{k,j}$ változó kitevője eleme a $\{0, 1, 2, \ldots, h_k - 1\}$ halmaznak. Minden $\mathbb{F}_q$ feletti polinom átírható

egy vele ekvivalens egyszerű polinommá az x_i, $y_{k,j}$ változók kitevőinek cseréjével. Az így kapott egyszerű polinom az adott polinom $x_i^q - x_i$ és $y_{k,j}^{h_k} - 1$ polinomokkal vett osztási maradéka. Írjuk át a p polinomot vele ekvivalens egyszerű polinommá. A lehetséges összevonások elvégzése után így kapott polinomot jelöljük $\widetilde{p}$-mal. Ekkor $\mathbb{F}_q \models p \approx \widetilde{p}$. Tehát $\mathbb{F}_q \models p \approx 0$ akkor és csakis akkor teljesül, ha $\mathbb{F}_q \models \widetilde{p} \approx 0$ teljesül.

Most a változók száma szerinti teljes indukcióval belátjuk, hogy $\mathbb{F}_q \models \widetilde{p} \approx \approx 0$ pontosan akkor teljesül, ha $\widetilde{p}$ a konstans 0 polinom. Ha $\widetilde{p}$ változó nélküli, akkor ez nyilván igaz. Tegyük fel, hogy bármely legfeljebb l változós, egyszerű $\widetilde{p}$ polinomra $\mathbb{F}_q \models \widetilde{p} \approx 0$ pontosan akkor teljesül, ha $\widetilde{p}$ minden együtthatója 0. Legyen most $\widetilde{p}$ egy $l+1$ változós, egyszerű polinom. Legyen z a $\widetilde{p}$ polinom egy változója és tekintsük $\widetilde{p}$-t ebben a változóban. Két esetet különböztetünk meg: $z = x_i$, illetve $z = y_{k,j}$ valamely i, k, j indexre.

Ha $z = x_i$ valamely i indexre, akkor $\widetilde{p} = s_{q-1} \cdot z^{q-1} + s_{q-2} \cdot z^{q-2} + \cdots + + s_1 \cdot z + s_0$, ahol $s_0, s_1, \ldots, s_{q-1}$ legfeljebb l változós, z-től független, egyszerű polinomok. Tekintsük egy tetszőleges helyettesítését a nem z változóknak. Az így kapott polinomot jelöljük $\widehat{p}(z)$-vel. Ekkor $\widehat{p}(z)$ csak z-től függ, és $\mathbb{F}_q \models \widehat{p}(z) \approx 0$ teljesül. Tehát $\widehat{p}(z)$ egy legfeljebb $q-1$ fokú polinom, aminek q darab gyöke van. Ez csak úgy lehet, ha $\widehat{p}(z)$ maga a 0 polinom. Tehát a nem z változók tetszőleges helyettesítésére az s_i együtthatók mindegyike 0. Tehát $\mathbb{F}_q \models s_i \approx 0$ teljesül. Így az indukciós feltevés szerint az összes s_i egyszerű polinom minden együtthatója 0. Tehát $\widetilde{p}$ minden együtthatója 0.

A $z = y_{k,j}$ esetet hasonlóan bizonyítjuk. Ekkor $\widetilde{p} = t_{h_k-1} \cdot z^{h_k-1} + + t_{h_k-2} \cdot z^{h_k-2} + \cdots + t_1 \cdot z + t_0$, ahol $t_0, t_1, \ldots, t_{h_k-1}$ legfeljebb l változós, z-től független, egyszerű polinomok. Tekintsük egy tetszőleges helyettesítését a nem z változóknak. Az így kapott polinomot jelöljük $\widehat{p}(z)$-vel. Ekkor $\widehat{p}(z)$ csak z-től függ, és minden H_k-beli helyettesítésre 0-át vesz fel. Tehát $\widehat{p}(z)$ legfeljebb egy $h_k - 1$ fokú polinom, aminek h_k darab gyöke van. Ez csak úgy lehet, ha $\widehat{p}(z)$ maga a 0 polinom. Tehát a nem z változók tetszőleges helyettesítésére a t_i együtthatók mindegyike 0. Tehát $\mathbb{F}_q \models t_i \approx 0$ teljesül. Így az indukciós feltevés szerint az összes t_i egyszerű polinom minden együtthatója 0. Tehát $\widetilde{p}$ minden együtthatója 0.

Ezzel beláttuk, hogy $\mathbb{F}_q \models \widetilde{p} \approx 0$ pontosan akkor teljesül, ha $\widetilde{p}$ a konstans 0 polinom. A p polinom $\widetilde{p}$ egyszerű polinommá való átírása során kicseréltük az x_i, $y_{k,j}$ változók kitevőit, majd elvégeztük a lehetséges összevonásokat. Ez $O(||p||)$ idő alatt megtehető. Tehát a most közölt algoritmus időigénye $O(||p||)$. Tehát $\mathbb{F}_q \models p \approx 0$ eldöntése $O(||p||)$ időt igényel. □

4. Tétel. *Legyen $\mathbb{F}_q$ a q elemű test, ahol q egy prímhatvány. Legyenek $H_1, H_2 \ldots H_d$ részcsoportok. Legyen l természetes szám. Legyenek $p_1, p_2, \ldots, p_l$ monomok összegeként adott, $x_1, x_2, \ldots, x_n, y_{1,1}, y_{1,2}, \ldots, y_{1,m_1}, y_{2,1}, \ldots y_{d,m_d}$-től füg-*

gő, $\mathbb{F}_q$*-beli polinomok, ahol* $x_1, x_2, \ldots, x_n$ *változók* $\mathbb{F}_q$*-beli,* $y_{k,1}, y_{k,2}, \ldots y_{k,m_k}$ *változók* H_k*-beli értéket vehetnek fel minden* $1 \leq k \leq d$ *esetén* $(n, m_k \in \mathbb{N})$*. Legyen* $N = max\{||p_i|| : 1 \leq i \leq l\}$*. Ekkor a* $p_1 = 0, p_2 = 0, \ldots, p_l = 0$ *egyenletrendszer megoldhatósága* $O\left(N^{lq}\right)$ *időben eldönthető.*

Bizonyítás. Legyen r_i az a polinom, melyet úgy kapunk, hogy az $1 - p_i^{q-1}$ polinomot monomok összegére bontjuk $(1 \leq i \leq l)$. Az r_i polinom hossza legfeljebb N^q és p_i-ből $O\left(N^q\right)$ időben kiszámolható. Vegyük észre, hogy r_i lehetséges értéke egy helyettesítésnél 0 vagy 1. Továbbá r_i valamely helyettesítésre pontosan akkor vesz fel 1-et értékként, ha a p_i polinom értéke 0 ugyanezen a helyettesítésen. Legyen r az a polinom, melyet úgy kapunk, hogy az $r_1 r_2 \ldots r_l$ polinomot monomok összegére bontjuk. Az r polinom hossza legfeljebb N^{lq} és $O\left(N^{lq}\right)$ időben kiszámítható. Vegyük észre, hogy $\mathbb{F}_q \models r \approx 0$ pontosan akkor *nem* teljesül, ha van olyan helyettesítés, melyre minden r_i polinom 1-et vesz fel értékként $(1 \leq i \leq l)$. Tehát, ha van olyan helyettesítés melyre $p_1 = 0, p_2 = 0, \ldots, p_l = 0$ egyenletek egyszerre oldhatók meg. Az 1.4. lemma szerint $\mathbb{F}_q \models r \approx 0$ eldöntése $O\left(||r||\right)$ időben tehető meg. Tehát a $p_1 = 0, p_2 = 0, \ldots, p_l = 0$ egyenletrendszer megoldhatósága $O\left(N^{lq}\right)$ időben eldönthető. □

2. fejezet

Egyenletmegoldhatóság bonyolultsága szemipattern csoportban

2.1. Szemipattern csoport

Legyen $\mathbb{F}_q$ egy véges test, és tekintsük azon $m \times m$-es $\mathbb{F}_q$ feletti mátrixokat amelyek főátlója alatt csupa nulla, főátlóban csupa nem nulla elem szerepel. E mátrixok csoportot alkotnak a szorzásra nézve, melyet $T(m, \mathbb{F}_q)$-val jelölünk:

$$T(m,\mathbb{F}_q) = \left\{ \begin{pmatrix} h_1 & a_{1,2} & a_{1,3} & \dots & a_{1,m} \\ 0 & h_2 & a_{2,3} & \dots & a_{2,m} \\ 0 & 0 & h_3 & \dots & a_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & h_m \end{pmatrix} : h_i \in \mathbb{F}_q^\times, a_{i,j} \in \mathbb{F}_q, 1 \le i < j \le m \right\}.$$

Jelölje I_m az $m \times m$-es egységmátrixot, $E_{i,j}$ azt az $m \times m$-es mátrixot, amely i-edik sorának j-edik eleme egy, minden más eleme nulla. Legyen $B(m) = \{E_{i,j} : 1 \le i < j \le m\}$, $X \subseteq B(m)$. A $T(m, \mathbb{F}_q)$ csoport egy

$$\{I_m + \sum_{E_{i,j} \in X} a_{i,j} E_{i,j} : a_{i,j} \in \mathbb{F}_q\}$$

alakú részcsoportját *pattern* csoportnak nevezzük és $U_X(m, \mathbb{F}_q)$-val jelöljük [1]. Legyenek $H_1, H_2, \dots, H_m$ részcsoportok $\mathbb{F}_q^\times$-ben, legyen továbbá $Y = \{(i, H_i) : H_i \neq \{1\}, 1 \le i \le m\}$. Tekintsük azon $m \times m$-es $\mathbb{F}_q$ feletti mátrixokat amelyek főátlójának i-edik eleme H_i-beli, minden más eleme nulla. E

mátrixok normálosztót alkotnak $T(m,\mathbb{F}_q)$-ben, amelyet $N_Y(m,\mathbb{F}_q)$-val jelölünk:

$$N_Y(m,\mathbb{F}_q)=\left\{\begin{pmatrix} h_1 & 0 & 0 & \dots & 0\\ 0 & h_2 & 0 & \dots & 0\\ 0 & 0 & h_3 & \dots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \dots & h_m \end{pmatrix} : h_1\in H_1, h_2\in H_2,\dots,h_m\in H_m\right\}.$$

A $T(m,\mathbb{F}_q)$ csoport $U_X(m,\mathbb{F}_q)N_Y(m,\mathbb{F}_q)$ részcsoportját *szemipattern* csoportnak nevezzük és $T_{X,Y}(m,\mathbb{F}_q)$-val jelöljük.

1. Példa. A $T(3,\mathbb{F}_3)$ csoport

$$T_{B(3),\{(2,\mathbb{F}_3^\times)\}}(3,\mathbb{F}_3)=\left\{\begin{pmatrix} 1 & a & b\\ 0 & h & c\\ 0 & 0 & 1 \end{pmatrix} : a,b,c\in\mathbb{F}_3, h\in\mathbb{F}_3^\times\right\}$$

részcsoportja egy 54 elemű szemipattern csoport.

A 2. fejezeteben szemipattern csoport feletti egyenletmegoldhatóság, illetve ekvivalencia probléma bonyolultságát fogjuk meghatározni. Ezen problémák bonyolultsága eddig még az 1. példában szereplő csoportra sem volt ismert.

A most következő lemmákban a $T(m,\mathbb{F}_q)$-beli mátrixszorzást a mátrixok elemei segítségével jellemezük. Így egyszerű képletet kapunk a $T(m,\mathbb{F}_q)$ csoportban történő számolásokhoz.

2.1. Lemma. *Legyen n egy természetes szám. Legyen minden $1\le k\le n$ esetén*

$$A_k=\begin{pmatrix} h_{1,k} & a_{1,2,k} & a_{1,3,k} & \dots & a_{1,m,k}\\ 0 & h_{2,k} & a_{2,3,k} & \dots & a_{2,m,k}\\ 0 & 0 & h_{3,k} & \dots & a_{3,m,k}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \dots & h_{m,k} \end{pmatrix}\in T(m,\mathbb{F}_q).$$

Ekkor az $A_1A_2\dots A_n$ szorzat i-edik sorának j-edik eleme:

- *0, ha $i>j$;*
- *$\prod_{k=1}^n h_{i,k}$, ha $i=j$;*

–

$$\sum_{b=0}^{j-i-1} \sum_{i<l_1<\dots<l_b<j} \sum_{k_{b+1}=b+1}^{n} \sum_{c=1}^{b} \sum_{k_c=c}^{k_{c+1}-1} \prod_{d_0=1}^{k_1-1} h_{i,d_0} a_{i,l_1,k_1} \prod_{d_1=k_1+1}^{k_2-1} h_{l_1,d_1}$$

$$\prod_{e=2}^{b} a_{l_{e-1},l_e,k_e} \prod_{d_e=k_e+1}^{k_{e+1}-1} h_{l_e,d_e} a_{l_b,j,k_{b+1}} \prod_{d_{b+1}=k_{b+1}+1}^{n} h_{j,d_{b+1}},$$

ha $i < j$.

A 2.1. lemma bizonyítása megtalálható az A. függelékben. A lemma az 1. példában szereplő $m = 3$ esetben az alábbi módon egyszerűsödik.

2.2. Lemma. *Legyen* n *egy természetes szám. Legyen minden* $1 \le k \le n$ *esetén* $A_k = \begin{pmatrix} d_k & a_k & b_k \\ 0 & e_k & c_k \\ 0 & 0 & f_k \end{pmatrix} \in T(3, \mathbb{F}_q)$. *Ekkor*

$$A_1 A_2 \dots A_n = \begin{pmatrix} \prod_{k=1}^{n} d_k & \sum_{k=1}^{n} \prod_{i=1}^{k-1} d_i a_k \prod_{j=k+1}^{n} e_j & b \\ 0 & \prod_{k=1}^{n} e_k & \sum_{k=1}^{n} \prod_{i=1}^{k-1} e_i c_k \prod_{j=k+1}^{n} f_j \\ 0 & 0 & \prod_{k=1}^{n} f_k \end{pmatrix},$$

ahol

$$b = \sum_{k=1}^{n} \prod_{i=1}^{k-1} d_i b_k \prod_{j=k+1}^{n} f_j + \sum_{l=2}^{n} \sum_{m=1}^{l-1} \prod_{i=1}^{m-1} d_i a_m \prod_{j=m+1}^{l-1} e_j c_l \prod_{k=l+1}^{n} f_k.$$

Bizonyítás. A lemma n szerinti teljes indukcióval igazolható.

Az $n = 1$ eset triviális.

Tegyük fel, hogy n-re igaz az állítás.

Jelölje az $A_1 A_2 \dots A_n$ szorzatot

$$A = \begin{pmatrix} d & a & b \\ 0 & e & c \\ 0 & 0 & f \end{pmatrix}.$$

Ekkor az indukciós feltevés szerint $d = \prod_{k=1}^{n} d_k$, $e = \prod_{k=1}^{n} e_k$, $f = \prod_{k=1}^{n} f_k$,

$$a = \sum_{k=1}^{n} \prod_{i=1}^{k-1} d_i a_k \prod_{j=k+1}^{n} e_j,$$
$$c = \sum_{k=1}^{n} \prod_{i=1}^{k-1} e_i c_k \prod_{j=k+1}^{n} f_j,$$
$$b = \sum_{k=1}^{n} \prod_{i=1}^{k-1} d_i b_k \prod_{j=k+1}^{n} f_j + \sum_{l=2}^{n} \sum_{m=1}^{l-1} \prod_{i=1}^{m-1} d_i a_m \prod_{j=m+1}^{l-1} e_j c_l \prod_{k=l+1}^{n} f_k.$$

Jelölje az $A_1 A_2 \dots A_n A_{n+1}$ szorzatot

$$A' = \begin{pmatrix} d' & a' & b' \\ 0 & e' & c' \\ 0 & 0 & f' \end{pmatrix}.$$

Ekkor, $A' = AA_{n+1}$, így a főátlóbeli elemekre triviális az állítás, továbbá

$$a' = \prod_{k=1}^{n} d_k a_{n+1} + a e_{n+1} = \prod_{k=1}^{n} d_k a_{n+1} + \sum_{k=1}^{n} \prod_{i=1}^{k-1} d_i a_k \prod_{j=k+1}^{n} e_j e_{n+1} =$$
$$= \sum_{k=1}^{n+1} \prod_{i=1}^{k-1} d_i a_k \prod_{j=k+1}^{n+1} e_j,$$
$$c' = \prod_{k=1}^{n} e_k c_{n+1} + c f_{n+1} = \prod_{k=1}^{n} e_k c_{n+1} + \sum_{k=1}^{n} \prod_{i=1}^{k-1} e_i c_k \prod_{j=k+1}^{n} f_j f_{n+1} =$$
$$= \sum_{k=1}^{n+1} \prod_{i=1}^{k-1} e_i c_k \prod_{j=k+1}^{n+1} f_j,$$
$$b' = \prod_{k=1}^{n} d_k b_{n+1} + a c_{n+1} + b f_{n+1} = \prod_{k=1}^{n} d_k b_{n+1} + \sum_{k=1}^{n} \prod_{i=1}^{k-1} d_i a_k \prod_{j=k+1}^{n} e_j c_{n+1} +$$
$$\sum_{k=1}^{n} \prod_{i=1}^{k-1} d_i b_k \prod_{j=k+1}^{n} f_j f_{n+1} + \sum_{l=2}^{n} \sum_{m=1}^{l-1} \prod_{i=1}^{m-1} d_i a_m \prod_{j=m+1}^{l-1} e_j c_l \prod_{k=l+1}^{n} f_k f_{n+1} =$$
$$= \sum_{k=1}^{n+1} \prod_{i=1}^{k-1} d_i b_k \prod_{j=k+1}^{n+1} f_j + \sum_{l=2}^{n+1} \sum_{m=1}^{l-1} \prod_{i=1}^{m-1} d_i a_m \prod_{j=m+1}^{l-1} e_j c_l \prod_{k=l+1}^{n+1} f_k.$$

□

2.3. Következmény. *A 2.1. lemmában szereplő $A_1A_2\dots A_n$ szorzat i-edik sorának j-edik elemét jellemző kifejezés hosszát n függvényeben vizsgáljuk. Vegyük észre, hogy az $i<j$ esetén szereplő képletben $b=k$ választásnál $\binom{j-i-1}{k}O\left(n^{k+1}\right)$ darab n hosszú szorzat összege szerepel. Így ezen képlet hossza*

$$O\left(\sum_{b=0}^{j-i-1}\binom{j-i-1}{b}n^{b+1}\cdot n\right)=O\left(n^{j-i+1}\right).$$

Tehát a szorzatmátrix elemeit jellemző kifejezések hosszának maximuma $O\left(n^m\right)$. Az m kitevő csak a szemipattern csoporttól függ, n-től független.

2.2. Egyenletmegoldhatóság szemipattern csoportokban

Legyen $T_{X,Y}(m,\mathbb{F}_q)$ egy szemipattern csoport. Legyen továbbá $T=T_1T_2\dots T_n$ egy $T_{X,Y}(m,\mathbb{F}_q)$ feletti polinom. Tehát T_k egy konstanst vagy változót jelölhet $T_{X,Y}(m,\mathbb{F}_q)$ felett $(1\leq k\leq n)$. Természetesen különböző indexű T_k-k jelölhetik ugyanazon változót vagy konstanst is.

Vezessük be a következő jelölést:

$$T_k=\begin{pmatrix} y_{1,k} & x_{1,2,k} & x_{1,3,k} & \dots & x_{1,m,k}\\ 0 & y_{2,k} & x_{2,3,k} & \dots & x_{2,m,k}\\ 0 & 0 & y_{3,k} & \dots & x_{3,m,k}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \dots & y_{m,k}\end{pmatrix}. \tag{2.1}$$

Ha $T_k\in T_{X,Y}(m,\mathbb{F}_q)$ konstanst jelölt akkor $y_{i,k}$ H_i-beli, $x_{i,j,k}$ $\mathbb{F}_q$-beli konstansok $(1\leq i<j\leq m)$. Hasonlóan, ha $T_k\in T_{X,Y}(m,\mathbb{F}_q)$ változó, akkor $y_{i,k}$ H_i-beli, $x_{i,j,k}$ $\mathbb{F}_q$-beli változók úgy, hogy $T_k=T_l$ akkor és csakis akkor, ha $y_{i,k}=y_{i,l}$ és $x_{i,j,k}=x_{i,j,l}$ teljesül minden $1\leq i<j\leq m$ esetén. Ha $(i,H_i)\notin Y$, akkor $H_i=\{1\}$, így $y_{i,k}=1$ minden $1\leq k\leq n$ indexre. Ha $B_{i,j}\notin X$, akkor a $T_{X,Y}(m,\mathbb{F}_q)$ csoportot alkotó mátrixok i-edik sorának j-edik eleme 0, így $x_{i,j,k}=0$ bármely $1\leq k\leq n$ esetén.

Ezen jelöléssel a T kifejezés az alábbi alakra hozható:

$$T = \begin{pmatrix} y_{1,1} & x_{1,2,1} & x_{1,3,1} & \dots & x_{1,m,1} \\ 0 & y_{2,1} & x_{2,3,1} & \dots & x_{2,m,1} \\ 0 & 0 & y_{3,1} & \dots & x_{3,m,1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & y_{m,1} \end{pmatrix} \begin{pmatrix} y_{1,2} & x_{1,2,2} & x_{1,3,2} & \dots & x_{1,m,2} \\ 0 & y_{2,2} & x_{2,3,2} & \dots & x_{2,m,2} \\ 0 & 0 & y_{3,2} & \dots & x_{3,m,2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & y_{m,2} \end{pmatrix} \dots$$
$$\dots \begin{pmatrix} y_{1,n} & x_{1,2,n} & x_{1,3,n} & \dots & x_{1,m,n} \\ 0 & y_{2,n} & x_{2,3,n} & \dots & x_{2,m,n} \\ 0 & 0 & y_{3,n} & \dots & x_{3,m,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & y_{m,n} \end{pmatrix}.$$

A szorzást elvégezve 2.1. lemma alapján

$$T = \begin{pmatrix} y_1 & x_{1,2} & x_{1,3} & \dots & x_{1,m} \\ 0 & y_2 & x_{2,3} & \dots & x_{2,m} \\ 0 & 0 & y_3 & \dots & x_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & y_m \end{pmatrix}, \tag{2.2}$$

ahol

$$y_i = \prod_{k=1}^{n} y_{i,k},$$
$$x_{i,j} = \sum_{b=0}^{j-i-1} \sum_{i<l_1<\dots<l_b<j} \sum_{k_{b+1}=b+1}^{n} \sum_{c=1}^{b} \sum_{k_c=c}^{k_{c+1}-1} \prod_{d_0=1}^{k_1-1} y_{i,d_0} x_{i,l_1,k_1} \prod_{d_1=k_1+1}^{k_2-1} y_{l_1,d_1}$$
$$\prod_{e=2}^{b} x_{l_{e-1},l_e,k_e} \prod_{d_e=k_e+1}^{k_{e+1}-1} y_{l_e,d_e} x_{l_b,j,k_{b+1}} \prod_{d_{b+1}=k_{b+1}+1}^{n} y_{j,d_{b+1}}.$$

Speciálisan, ha $(i, H_i) \notin Y$, akkor $y_i = 1$, ha $B_{i,j} \notin X$, akkor $x_{i,j} = 0$.

A T polinom pontosan akkor vehet fel I_m-et valamely helyettesítésre, ha y_i 1-et, $x_{i,j}$ 0-t vesz fel ugyanerre a helyettesítésre ($1 \le i < j \le m$). Tehát a $T = I_m$ egyenlet akkor és csakis akkor kielégíthető, ha az $y_i = 1$, $x_{i,j} = 0$ egyenletekből álló egyenletrendszer megoldható $\mathbb{F}_q$ felett. Ez egy speciális $\mathbb{F}_q$ feletti, monomok összegeként felírt egyenletből álló egyenletrendszer, melyben az $y_{i,k}$ változók H_i-ből, az $x_{i,j,k}$ változók $\mathbb{F}_q$-ból származnak ($1 \le k \le n$). Így a 4. tételben leírt módszerrel ezen egyenletrendszer megoldhatósága hatékonyan eldönthető.

2. Példa. Alkalmazzuk a 2.2. szakaszban közölt módszert az 1. példában szereplő $T_{B(3),\{(2,\mathbb{F}_3^\times)\}}(3,\mathbb{F}_3)$ csoportra. Legyen $T = T_1T_2\dots T_n$ egy polinom $T_{B(3),\{(2,\mathbb{F}_3^\times)\}}(3,\mathbb{F}_3)$ felett. Legyen minden $1 \le k \le n$ esetén:

$$T_k = \begin{pmatrix} 1 & u_k & v_k \\ 0 & y_k & w_k \\ 0 & 0 & 1 \end{pmatrix}.$$

Itt y_k $\mathbb{F}_3^\times$-beli, u_k, v_k, w_k $\mathbb{F}_3$-beli konstanst vagy változót jelölhet. Így T a 2.2. lemma alapján az alábbi alakra hozható:

$$T = \begin{pmatrix} 1 & u_1 & v_1 \\ 0 & y_1 & w_1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & u_2 & v_2 \\ 0 & y_2 & w_2 \\ 0 & 0 & 1 \end{pmatrix}\dots\begin{pmatrix} 1 & u_n & v_n \\ 0 & y_n & w_n \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & u & v \\ 0 & y & w \\ 0 & 0 & 1 \end{pmatrix},$$

ahol

$$u = \sum_{k=1}^{n} u_k \prod_{i=k+1}^{n} y_i, \qquad v = \sum_{k=1}^{n} v_k + \sum_{k=2}^{n}\sum_{l=1}^{k-1} u_l \prod_{i=l+1}^{k-1} y_i w_k,$$

$$y = \prod_{k=1}^{n} y_k, \qquad w = \sum_{k=1}^{n}\prod_{i=1}^{k-1} y_i w_k.$$

Tehát a $T = I_3$ egyenlet akkor és csakis akkor megoldható, ha az $y = 1$, $u = 0$, $v = 0$, $w = 0$ egyenletrendszer megoldható $\mathbb{F}_3$ felett. Ez a 4. tételben leírt módszerrel hatékonyan eldönthető.

2.3. Az algoritmus időigénye

Az algoritmus bemenete egy $T_{X,Y}(m,\mathbb{F}_q)$ feletti $T = T_1T_2\dots T_n$ polinom. Az n számot a T polinom hosszának nevezzük, és ennek függvényében vizsgáljuk algoritmusunk időigényét. Első lépésként a $T_1T_2\dots T_n$ szorzat minden T_k tényezőjét átírjuk (2.1) alakba ($1 \le k \le n$). Ez a lépés $O(n)$ időt igényel. Majd meghatározzuk a $T_1T_2\dots T_n$ szorzatot, így a (2.2) kifejezéshez jutunk. Ha $(i,H_i) \in Y$, akkor a (2.2)-ben szereplő y_i kifejezés hossza $O(n)$, egyébként $y_i = 1$. Ha $B_{i,j} \in X$, akkor az $x_{i,j}$ kifejezés hossza a 2.3. következmény szerint legfeljebb $O(n^m)$, egyébként $x_{i,j} = 0$. Ez a lépés $O(n^m)$ időt igényel.

A $T = I_m$ egyenlet pontosan akkor megoldható, ha a $y_i = 1$, $x_{i,j} = 0$ egyenletrendszer megoldható $\mathbb{F}_q$ felett ($1 \le i < j \le m$). Ez egy $\mathbb{F}_q$ test feletti $|X|+|Y|$ nem triviális egyenletből álló egyenletrendszer, melyben az egyenletek monomok összegeként vannak felírva, és hosszaik maximuma $O(n^m)$. Ennek megoldhatóságáról a 4. tétel szerint $l = |X|+|Y|$, $N = O(n^m)$ paraméterek mellett $O\left(n^{mq(|X|+|Y|)}\right)$ időben dönthetünk. Tehát tetszőleges $T_{X,Y}(m,\mathbb{F}_q)$

feletti T polinom megoldhatósága $O\left(n^{mq(|X|+|Y|)}\right)$ időben eldönthető. A kitevőben szereplő $mq(|X|+|Y|)$ kifejezés csak az $T_{X,Y}(m,\mathbb{F}_q)$ csoporttól függ, n-től független, így az algoritmus valóban polinom idejű.

Az 1.3. állítás szerint, ha egy véges csoport feletti egyenletmegoldhatóság P-beli, akkor az ekvivalencia is az. Tehát $T_{X,Y}(m,\mathbb{F}_q)$ felett az ekvivalencia probléma is polinom időben eldönthető.

3. Példa. A $T_{B(3),\{(2,\mathbb{F}_3^\times)\}}(3,\mathbb{F}_3)$ csoport feletti egyenletmegoldhatóság probléma a 2. példában közölt algoritmussal $O\left(n^{3\cdot3(3+1)}\right) = O\left(n^{36}\right)$ időben eldönthető.

A függelék

Mátrixszorzás $T\left(m, \mathbb{F}_q\right)$-ban

A.1. Lemma. *Legyen n egy természetes szám. Legyen minden $1 \leq k \leq n$ esetén*

$$A_k = \begin{pmatrix} h_{1,k} & a_{1,2,k} & a_{1,3,k} & \dots & a_{1,m,k} \\ 0 & h_{2,k} & a_{2,3,k} & \dots & a_{2,m,k} \\ 0 & 0 & h_{3,k} & \dots & a_{3,m,k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & h_{m,k} \end{pmatrix} \in T\left(m, \mathbb{F}_q\right).$$

Ekkor az $A_1 A_2 \dots A_n$ szorzat i-edik sorának j-edik eleme ($1 \leq i, j \leq m$):

- 0, *ha* $i > j$;
- $\prod_{k=1}^{n} h_{i,k}$, *ha* $i = j$;
- $$\sum_{b=0}^{j-i-1} \sum_{i<l_1<\dots<l_b<j} \sum_{k_{b+1}=b+1}^{n} \sum_{c=1}^{b} \sum_{k_c=c}^{k_{c+1}-1} \prod_{d_0=1}^{k_1-1} h_{i,d_0} a_{i,l_1,k_1} \prod_{d_1=k_1+1}^{k_2-1} h_{l_1,d_1} \prod_{e=2}^{b} a_{l_{e-1},l_e,k_e} \prod_{d_e=k_e+1}^{k_{e+1}-1} h_{l_e,d_e} a_{l_b,j,k_{b+1}} \prod_{d_{b+1}=k_{b+1}+1}^{n} h_{j,d_{b+1}},$$

  ha $i < j$.

Bizonyítás. A lemma n szerinti teljes indukcióval igazolható.

Az $n = 1$ esetben az állítás $i \geq j$-re triviális. Ha $i < j$, akkor

$$\sum_{b=0}^{j-i-1} \sum_{i<l_1<\dots<l_b<j} \sum_{k_{b+1}=b+1}^{1} \sum_{c=1}^{b} \sum_{k_c=c}^{k_{c+1}-1} \prod_{d_0=1}^{k_1-1} h_{i,d_0} a_{i,l_1,k_1} \prod_{d_1=k_1+1}^{k_2-1} h_{l_1,d_1} \prod_{e=2}^{b} a_{l_{e-1},l_e,k_e} \prod_{d_e=k_e+1}^{k_{e+1}-1} h_{l_e,d_e} a_{l_b,j,k_{b+1}} \prod_{d_{b+1}=k_{b+1}+1}^{1} h_{j,d_{b+1}} = \sum_{k_1=1}^{1} \prod_{d_0=1}^{k_1-1} h_{i,d_0} a_{i,j,k_1} \prod_{d_1=k_1+1}^{1} h_{j,d_1} = a_{i,j,1}.$$

Tegyük fel, hogy n-re igaz az állítás.
Jelölje az $A_1A_2\dots A_n$ szorzatot

$$A=\begin{pmatrix} h_1 & a_{1,2} & a_{1,3} & \dots & a_{1,m} \\ 0 & h_2 & a_{2,3} & \dots & a_{2,m} \\ 0 & 0 & h_3 & \dots & a_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & h_m \end{pmatrix}.$$

Ekkor az indukciós feltevés szerint

$$h_i=\prod_{k=1}^{n} h_{i,k},$$

$$a_{i,j}=\sum_{b=0}^{j-i-1}\sum_{i<l_1<\dots<l_b<j}\sum_{k_{b+1}=b+1}^{n}\sum_{c=1}^{b}\sum_{k_c=c}^{k_{c+1}-1}\prod_{d_0=1}^{k_1-1} h_{i,d_0}a_{i,l_1,k_1}\prod_{d_1=k_1+1}^{k_2-1} h_{l_1,d_1}\prod_{e=2}^{b} a_{l_{e-1},l_e,k_e}$$
$$\prod_{d_e=k_e+1}^{k_{e+1}-1} h_{l_e,d_e}a_{l_b,j,k_{b+1}}\prod_{d_{b+1}=k_{b+1}+1}^{n} h_{j,d_{b+1}}.$$

Jelölje az $A_1A_2\dots A_nA_{n+1}$ szorzatot

$$A'=\begin{pmatrix} h_1{}' & a_{1,2}{}' & a_{1,3}{}' & \dots & a_{1,m}{}' \\ 0 & h_2{}' & a_{2,3}{}' & \dots & a_{2,m}{}' \\ 0 & 0 & h_3{}' & \dots & a_{3,m}{}' \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & h_m{}' \end{pmatrix}.$$

Ekkor $A'=AA_{n+1}$, így

$$h_i{}'=\prod_{k=1}^{n} h_{i,k}h_{i,n+1}=\prod_{k=1}^{n+1} h_{i,k},$$

$$a_{i,j}{}'=h_ia_{i,j,n+1}+\sum_{f=i+1}^{j-1} a_{i,f}a_{f,j,n+1}+a_{i,j}h_{j,n+1}=$$

$$= \prod_{k=1}^{n} h_{i,k} a_{i,j,n+1} + \sum_{f=i+1}^{j-1} \sum_{b=0}^{f-i-1} \sum_{i<l_1<\cdots<l_b<f} \sum_{k_{b+1}=b+1}^{n} \sum_{c=1}^{b} \sum_{k_c=c}^{k_{c+1}-1}$$

$$\prod_{d_0=1}^{k_1-1} h_{i,d_0} a_{i,l_1,k_1} \prod_{d_1=k_1+1}^{k_2-1} h_{l_1,d_1} \prod_{e=2}^{b} a_{l_{e-1},l_e,k_e} \prod_{d_e=k_e+1}^{k_{e+1}-1} h_{l_e,d_e} a_{l_b,f,k_{b+1}}$$

$$\prod_{d_{b+1}=k_{b+1}+1}^{n} h_{f,d_{b+1}} a_{f,j,n+1} + \sum_{b=0}^{j-i-1} \sum_{i<l_1<\cdots<l_b<j} \sum_{k_{b+1}=b+1}^{n} \sum_{c=1}^{b} \sum_{k_c=c}^{k_{c+1}-1}$$

$$\prod_{d_0=1}^{k_1-1} h_{i,d_0} a_{i,l_1,k_1} \prod_{d_1=k_1+1}^{k_2-1} h_{l_1,d_1} \prod_{e=2}^{b} a_{l_{e-1},l_e,k_e} \prod_{d_e=k_e+1}^{k_{e+1}-1} h_{l_e,d_e} a_{l_b,j,k_{b+1}}$$

$$\prod_{d_{b+1}=k_{b+1}+1}^{n} h_{j,d_{b+1}} h_{j,n+1} = \sum_{b=0}^{j-i-1} \sum_{i<l_1<\cdots<l_b<j} \sum_{k_{b+1}=b+1}^{n+1} \sum_{c=1}^{b} \sum_{k_c=c}^{k_{c+1}-1}$$

$$\prod_{d_0=1}^{k_1-1} h_{i,d_0} a_{i,l_1,k_1} \prod_{d_1=k_1+1}^{k_2-1} h_{l_1,d_1} \prod_{e=2}^{b} a_{l_{e-1},l_e,k_e} \prod_{d_e=k_e+1}^{k_{e+1}-1} h_{l_e,d_e} a_{l_b,j,k_{b+1}}$$

$$\prod_{d_{b+1}=k_{b+1}+1}^{n+1} h_{j,d_{b+1}}.$$

□

Irodalomjegyzék

[1] Ery Arias-Castro – Persi Diaconis – Richard Stanley: A superclass walk on upper-triangular matrices. In *Journal of Algebra*, 278. évf. (2004), 739–765. p.

[2] Stanley Burris – John Lawrence: The equivalence problem for finite rings. In *Journal of Symbolic Computation*, 15. évf. (1993), 67–71. p.

[3] Stanley Burris – John Lawrence: Results on the equivalence problem for finite groups. In *Algebra Universalis*, 52. évf. (2005) 4. sz., 495–500. p.

[4] Michael Garey – David S. Johnson: *Computers and Intractability: A Guide to the Theory of NP-completeness.* San Francisco, W. H. Freeman and Company, 1979.

[5] Mikael Goldmann – Alexander Russell: The complexity of solving equations over finite groups. In *Proceedings of the 14th Annual IEEE Conference on Computational Complexity* (konferenciaanyag). Atlanta, Georgia, 1999, 80–86. p.

[6] Mikael Goldmann – Alexander Russell: The complexity of solving equations over finite groups. In *Information and Computation*, 178. évf. (2002), 253–262. p.

[7] Gábor Horváth: *Bonyolultságelméleti problémák algebrai struktúrákban.* Phd értekezés (Eötvös Loránd Tudományegyetem Természettudomyányi Kar). Budapest, 2011.

[8] Gábor Horváth: The complexity of the equivalence end equation solvability problems over nilpotent rings and groups. In *Algebra Universalis*, 2011. 66(4). sz., 391–403. p.

[9] Gábor Horváth: The complexity of the equivalence problem over finite rings. In *Glasgow Mathematical Journal*, 54. évf. (2012) 1. sz., 193–199. p.

[10] Gábor Horváth – John Lawrence – László Mérai – Csaba Szabó: The complexity of the equivalence problem for non-solvable groups. In *Bulletin of the London Mathematical Society*, 39. évf. (2007) 3. sz., 433–438. p.

[11] Gábor Horváth – John Lawrence – Ross Willard: The complexity of the equation solvability problem over finite rings. 2012. kézirat.

[12] Gábor Horváth – Csaba Szabó: The complexity of checking identities over finite groups. In *International Journal of Algebra Computation*, 16. évf. (2006) 5. sz., 931–940. p.

[13] Gábor Horváth – Csaba Szabó: Equivalence and equation solvability problems for the group A_4. In *Journal of Pure and Applied Algebra*, 216. évf. (2012) 10. sz., 2170–2176. p.

[14] H.B. Hunt – R.E. Stearns: The complexity for equivalence for commutative rings. In *Journal of Symbolic Computation*, 10. évf. (1990), 411–436. p.

[15] Emil Kiss: *Bevezetés az algebrába.* Elméleti matematika sorozat, 9. köt. Budapest, Typotex, 2007.

[16] Ondrej Klíma: *Unification modulo associativity and idempotency.* Phd értekezés (Masaryk University). Brno, 2003.

[17] Ondrej Klíma: Complexity issues of checking identities in finite monoids. In *Semigroup Forum*, 79. évf. (2009) 3. sz., 435–444. p.

[18] Ondrej Klíma: Identity checking problem for transformation monoids. In *Semigroup Forum*, 84. évf. (2012) 3. sz., 487–498. p.

[19] Benoit Larose – László Zádori: Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras. In *International Journal of Algebra and Computation*, 16. évf. (2006) 3. sz., 563–581. p.

[20] Christos H. Papadimitriou: *Computational Complexity.* Addison-Wesley Publishing Company, 1994.

[21] Steve Seif: The perkins semigroup has conp-complete term-equivalence problem. In *International Journal of Algebra and Computation*, 15. évf. (2005) 2. sz., 317–326. p.

[22] Steve SEIF – Csaba SZABÓ: Algebra complexity problems involving graph homomorphism, semigroups and the constraint satisfaction problem. In *Journal of Complexity*, 19. évf. (2003) 2. sz., 153–160. p.

[23] Steve SEIF – Csaba SZABÓ: Computational complexity of checking identites in 0-simple semigroups and matrix semigroups over finite fields. In *Semigroup Forum*, 72. évf. (2006) 2. sz., 207–222. p.

[24] Csaba SZABÓ – Vera VÉRTESI: The complexity of checking identities for finite matrix rings. In *Algebra universalis*, 51. évf. (2004), 439–445. p.

[25] Csaba SZABÓ – Vera VÉRTESI: The complexity of the word-problem for finite matrix rings. In *Proceedings of the American Mathematical Society*, 132. évf. (2004), 3689–3695. p.

[26] Csaba SZABÓ – Vera VÉRTESI: The equivalence problem over finite rings. In *International Journal of Algebra and Computation*, 21. évf. (2011), 449–457. p.

[27] Pascal TESSON – Denis THÉRIEN: Monoids and computations. In *International Journal of Algebra and Computation*, 14. évf. (2004) 5–6. sz., 801–816. p.