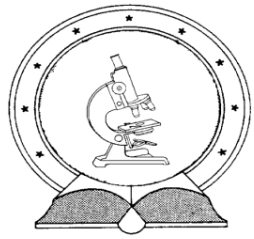
DE TTK



1949

Az egyenletmegoldhatóság probléma bonyolultsága véges csoportok felett

egyetemi doktori (PhD) értekezés

Földvári Attila

Témavezető: Dr. Horváth Gábor

Debreceni Egyetem

Természettudományi Doktori Tanács
Matematika- és Számítástudományok Doktori Iskola

Debrecen, 2017.

Ezen értekezést a Debreceni Egyetem Természettudományi Doktori Tanács Matematika- és Számítástudományok Doktori Iskola *Gyűrűelmélet: csoportalgebrák és egységcsoportok* programja keretében készítettem a Debreceni Egyetem természettudományi doktori (PhD) fokozatának elnyerése céljából.
Nyilatkozom arról, hogy a tézisekben leírt eredmények nem képezik más PhD disszertáció részét.

Debrecen, 2017.

.....
Földvári Attila
jelölt

Tanúsítom, hogy Földvári Attila doktorjelölt 2014 - 2017 között a fent megnevezett Doktori Iskola *Gyűrűelmélet: csoportalgebrák és egységcsoportok* program keretében irányításommal végezte munkáját. Az értekezésben foglalt eredményekhez a jelölt önálló alkotó tevékenységével meghatározóan hozzájárult. Nyilatkozom továbbá arról, hogy a tézisekben leírt eredmények nem képezik más PhD disszertáció részét.
Az értekezés elfogadását javaslom.

Debrecen, 2017.

.....
Dr. Horváth Gábor
témavezető

Az egyenletmegoldhatóság probléma bonyolultsága véges csoportok felett

Értekezés a doktori (Ph.D.) fokozat megszerzése érdekében
a matematika tudományágban

Írta: Földvári Attila okleveles matematikus

Készült a Debreceni Egyetem Matematika- és Számítástudományok
Doktori Iskolája (Gyűrűelmélet: csoportalgebrák és egységcsoportok
doktori programja) keretében

Témavezető: Dr. Horváth Gábor

A doktori szigorlati bizottság:

elnök: Dr. ....
tagok: Dr. ....
Dr. ....

A doktori szigorlat időpontja: 201.. ....

Az értekezés bírálói:

Dr. ....
Dr. ....
Dr. ....

A bírálóbizottság:

elnök: Dr. ....
tagok: Dr. ....
Dr. ....
Dr. ....
Dr. ....

Az értekezés védésének időpontja: 201.. ....

Tartalomjegyzék

1. fejezet

Bevezetés

Az algebra egyik legrégebbi problémája az egyenletek megoldása. Napjainkban a számítógépek elterjedésével sok klasszikus algebrai probléma új megvilágításba kerül. A kutatások egyik fontos iránya az egyenletmegoldhatóság probléma bonyolultságának meghatározása adott véges algebra felett. A dolgozatban véges csoportokra és véges gyűrűkre vizsgáljuk ezt a kérdéskört.

Az $\mathcal{R}$ véges gyűrű feletti *egyenletmegoldhatóság* probléma azt kérdezi, hogy az $\mathcal{R}$ feletti f_1, f_2 input polinomokra az $f_1 = f_2$ egyenlet megoldható-e. Azaz létezik-e olyan helyettesítés melyre az f_1 és f_2 polinomok értékei megegyeznek. Egy másik hasonló kérdés, hogy az input polinomok értékei *minden* helyettesítésre azonosak-e. Az $\mathcal{R}$ véges gyűrű feletti *ekvivalencia* probléma azt kérdezi, hogy az f_1, f_2 input polinomok ekvivalensek-e $\mathcal{R}$ felett (jelölésben $\mathcal{R} \models f_1 \approx f_2$). Azaz f_1 és f_2 ugyanazt a függvényt definiálják-e $\mathcal{R}$ felett. Ezen problémák mindig eldönthetőek a változók összes lehetséges helyettesítésének kiértékelésével. Az érdekesebb kérdés, hogy milyen gyorsan tudunk dönteni, azaz ezen döntési problémák mely bonyolultsági osztályba esnek.

Az első eredmények Hunttól és Stearnstől [17] származnak, akik kommutatív gyűrűk felett vizsgálták az ekvivalencia probléma bonyo-

lultságát. Később Burris és Lawrence [1] nemkommutatív gyűrűkre általánosították Hunt és Stearns módszerét. Igazolták, hogy ha $\mathcal{R}$ nilpotens gyűrű, akkor az ekvivalencia probléma $\mathcal{R}$ felett polinomidőben eldönthető. Továbbá, ha $\mathcal{R}$ nem nilpotens akkor az ekvivalencia probléma $\mathcal{R}$ felett coNP-teljes. Burris és Lawrence bizonyításukban a SAT problémát vezették vissza összegek szorzatának ekvivalenciájára. Ha azonban egy ilyen szorzatot monomok összegére bontunk, akkor az új polinom hossza akár exponenciális is lehet az eredeti polinom hosszában. A polinomok hosszának ez a változása befolyásolhatja az ekvivalencia probléma bonyolultságát. Ez motiválta Lawrence-t és Willardot [20] a *szigma* problémák bevezetésében, melyekben az input polinomok monomok összegeiként adottak. Lawrence és Willard azt sejtették, hogy ha a gyűrű Jacobson-radikál szerinti faktora kommutatív, akkor a szigma ekvivalencia probléma polinomidőben eldönthető. Továbbá, ha a gyűrű Jacobson-radikál szerinti faktora nemkommutatív, akkor a szigma ekvivalencia probléma coNP-teljes. Szabó és Vértesi [24] bebizonyították a sejtés coNP-teljes részét. Horváth [11] kommutatív gyűrűkre igazolta a sejtést. A polinomiális rész teljes bizonyítása Horváth, Lawrence és Willard [13] kéziratában található. Tehát véges gyűrűk felett mind az ekvivalencia mind a szigma ekvivalencia problémák bonyolultsága ismert.

Az alábbiakban összefoglaljuk az egyenletmegoldhatóság és szigma egyenletmegoldhatóság problémákkal kapcsolatos eredményeket. Bár Szabó és Vértesi [24]-ben nem vizsgálták az egyenletmegoldhatóság problémát, de érvelésükből már következik, hogy ha a gyűrű Jacobson-radikál szerinti faktora nemkommutatív, akkor a szigma egyenletmegoldhatóság probléma NP-teljes. Horváth, Lawrence és Willard [13]-ban igazolták, hogy ha a gyűrű nem nilpotens de a Jacobson-radikál szerinti faktora kommutatív, akkor a szigma egyenletmegoldhatóság probléma polinomidőben eldönthető. Az általános esetben, ha a gyűrű nem nilpotens, akkor az egyenletmegoldhatóság probléma NP-teljes Burris és Lawrence [1] ekvivalenciára adott érvelésének következtében.

Horváth [10]-ben bebizonyította, hogy ha a gyűrű nilpotens, akkor az egyenletmegoldhatóság probléma polinomidőben eldönthető. Horváth megmutatta, hogy ha f_1 és f_2 legfeljebb n hosszú polinomok az $\mathcal{R}$ nilpotens gyűrű felett, akkor $O\left(n^{|\mathcal{R}|^{|\mathcal{R}|^{\cdots^{|\mathcal{R}|}}}}\right)$ időben eldönthető, hogy az $f_1 = f_2$ egyenletnek van-e megoldása $\mathcal{R}$-ben. Itt a korlát kitevőjében szereplő torony magassága $\mathcal{R}$ nilpotenciaosztálya. Horváth a [10] cikk 3. problémájának nilpotens gyűrűkkel foglalkozó részében közvetlenül rákérdez, hogy javítható-e ez a korlát. A 3. fejezetben a korlát jelentős csökkentésével megválaszoljuk Horváth 3. problémájának nilpotens gyűrűkre vonatkozó kérdését. Jelölje a kettes alapú logaritmust log. Egy olyan korlátot adunk amelyben a korábbi többszörösen exponenciális kitevő $|\mathcal{R}|^{2\log|\mathcal{R}|}\log^5|\mathcal{R}|$-re csökken.

Tétel (3.1. tétel)**.** *Legyen $\mathcal{R}$ egy nilpotens gyűrű, f_1 és f_2 legfeljebb n hosszú $\mathcal{R}$ feletti polinomok. Ekkor $O\left(n^{|\mathcal{R}|^{2\log|\mathcal{R}|}\log^5|\mathcal{R}|}\right)$ időben eldönthető, hogy az $f_1 = f_2$ egyenletnek van-e megoldása $\mathcal{R}$-ben.*

Ezt az eredményt [5]-ben publikáltam. Megemlítjük, hogy egy ettől teljesen független úton, Károlyi és Szabó később tovább javította az időkorlátot [19]-ben.

A véges gyűrűk után természetesen adódott a véges csoportok feletti egyenletmegolthatóság és az ekvivalencia problémák bonyolultságának vizsgálata. A $\mathbf{G}$ véges csoport feletti *egyenletmegoldhatóság* probléma azt kérdezi, hogy a $\mathbf{G}$ feletti S, T input csoportkifejezésekre (azaz változók és $\mathbf{G}$-beli elemek formális szorzataira) az $S = T$ egyenlet megoldható-e. Más szóval létezik-e olyan helyettesítés melyre S és T kifejezések értékei megegyeznek. A $\mathbf{G}$ feletti *ekvivalencia* probléma azt kérdezi, hogy az S, T input csoportkifejezések ekvivalensek-e $\mathbf{G}$ felett (jelölésben $\mathbf{G} \models S \approx T$). Azaz S és T kifejezések értékei minden helyettesítésre azonosak-e.

Csoportok felett az első eredmények Burristől és Lawrence-től [2] származnak, akik az ekvivalencia probléma bonyolultságát vizsgálták.

Bebizonyították, hogy ha $\mathbf{G}$ nilpotens vagy $\mathbf{G}$ izomorf egy páratlan fokú diédercsoporttal, akkor az ekvivalencia probléma $\mathbf{G}$ felett polinomidőben eldönthető. Burris és Lawrence azt sejtették, hogy ha a csoport feloldható, akkor az ekvivalencia probléma polinomidőben eldönthető. Továbbá, ha a csoport nem feloldható, akkor az ekvivalencia probléma coNP-teljes. Horváth, Lawrence, Mérai és Szabó [14] bizonyították a sejtés coNP-teljes részét. A polinomiális részt Horváth és Szabó [16] igazolták olyan $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$ csoportokra melyekre $\mathbf{A}$ és $\mathbf{B}$ Abel csoportok, $\mathbf{A}$ exponense négyzetmentes és $(|\mathbf{A}|, |\mathbf{B}|) = 1$. Később Horváth [12]-ben általánosította ezt az eredményt olyan $\mathbf{A} \rtimes \mathbf{B}$ szemidirekt szorzatokra melyekre $\mathbf{A}$ és $\mathbf{B}/C_{\mathbf{B}}(\mathbf{A})$ Abel csoportok (itt $C_{\mathbf{B}}(\mathbf{A})$ az $\mathbf{A}$ csoport $\mathbf{B}$-beli centralizátorát jelöli). Feloldható de nem nilpotens csoportok felett csak ezekre a speciális szemidirekt szorzatokra ismert az ekvivalencia probléma bonyolultsága. A három legkisebb csoport melyre az ekvivalencia probléma bonyolultsága a korábbi tételekkel nem eldönthető az $\mathbf{S}_4$, $\mathbf{SL}(2, \mathbb{Z}_3)$ és az $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$ csoportok (utóbbi egy nemkommutatív 54 elemű csoport). Egy részletes lista ezen csoportokról [12]-ben található.

Az egyenletmegoldhatóság probléma bonyolultsága még több csoportra ismeretlen. Goldmann és Russell [7, 8] bebizonyították, hogy ha $\mathbf{G}$ nem feloldható, akkor az egyenletmegoldhatóság probléma $\mathbf{G}$ felett NP-teljes. Továbbá ha $\mathbf{G}$ nilpotens, akkor az egyenletmegoldhatóság probléma $\mathbf{G}$ felett polinomidőben eldönthető. Bizonyításukból azonban nem derül ki nilpotens csoport felett a polinomiális időkorlát pontos kitevője. Számos, a bizonyításban fontos szerepet játszó eredmény Péladeau és Thérien [23, 25] cikkeiből származik. A bizonyítás teljes megértéséhez és a pontos időkorlát meghatározásához tehát több cikk [7, 8, 23, 25] alapos tanulmányozása szükséges. Később Horváth [10] közvetlen bizonyítást adott mely hasonlít a fenti három cikkből összeállítható gondolatmenetre de önmagában is érthető. Megmutatta, hogy ha S és T legfeljebb n hosszú csoportkifejezések a $\mathbf{G}$ nilpo-

tens csoport felett, akkor $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|^{\cdots^{|\mathbf{G}|}}}}\right)$ időben eldönthető, hogy az $S = T$ egyenletnek van-e megoldása $\mathbf{G}$-ben. Itt a korlát kitevőjében szereplő torony magassága $\mathbf{G}$ nilpotenciaosztálya. Horváth a [10] cikk 3. problémájának nilpotens csoportokkal foglalkozó részében közvetlen rákérdez, hogy javítható-e ez a korlát. Az 5. fejezetben a korlát jelentős csökkentésével megválaszoljuk Horváth 3. problémájának nilpotens csoportokra vonatkozó kérdését. Egy olyan korlátot adunk amelyben a korábbi többszörösen exponenciális kitevő $\frac{1}{2}|\mathbf{G}|^2 \log |\mathbf{G}|$-re csökken.

Tétel (5.1. tétel)**.** *Legyen* $\mathbf{G}$ *egy nilpotens csoport,* S *és* T *legfeljebb* n *hosszú csoportkifejezések* $\mathbf{G}$ *felett. Ekkor* $O\left(n^{\frac{1}{2}|\mathbf{G}|^2 \log |\mathbf{G}|}\right)$ *időben eldönthető, hogy az* $S = T$ *egyenletnek van-e megoldása* $\mathbf{G}$*-ben.*

Ezt az eredményt [4]-ben publikáltam.

Feloldható de nem nilpotens csoportok felett csupán néhány speciális esetben ismert az egyenletmegoldhatóság probléma bonyolultsága. Horváth és Szabó bebizonyították, hogy ha a $|\mathbf{G}| = pq$ valamely $p \neq q$ prímekre [16], vagy $\mathbf{G}$ izomorf a negyedfokú alternáló csoporttal [15], akkor az egyenletmegoldhatóság probléma $\mathbf{G}$ felett polinomidőben eldönthető. Később Horváth [12] belátta, hogy az egyenletmegoldhatóság probléma polinomidőben eldönthető minden olyan $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$ szemidirekt szorzatra, ahol $\mathbf{A} \simeq \mathbf{Z}_{p^k}$ vagy $\mathbf{A} \simeq \mathbf{Z}_{2p^k}$ vagy $\mathbf{A} \simeq \mathbf{Z}_p^k$, és $\mathbf{B}$ kommutatív. Tehát minden feloldható de nem nilpotens $\mathbf{G}$ csoportra vonatkozó korábbi eredmény esetén $\mathbf{G} \cong \mathbf{A} \rtimes \mathbf{B}$ úgy, hogy $\mathbf{A}$ és $\mathbf{B}$ is Abel. A három legkisebb csoport melyre sem az ekvivalencia, sem az egyenletmegoldhatóság problémák bonyolultsága nem ismert az $\mathbf{S}_4$, $\mathbf{SL}(2, \mathbb{Z}_3)$ és az $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$ csoportok. Horváth közvetlenül rákérdez ezeknek a problémáknak a bonyolultságára a [12] cikk 3. problémájában az $\mathbf{SL}(2, \mathbb{Z}_3)$ csoport fölött; a [12] cikk 4. problémájában az $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$ csoport fölött.

A 4. fejezetben speciális mátrixcsoportokra, az úgynevezett szemipattern csoportokra határozzuk meg az egyenletmegoldhatóság és ek-

vivalencia problémák bonyolultságát. Egy $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$ csoportot szemipattern csoportnak nevezünk, ha $\mathbf{P}$ a szigorú felső háromszögmátrixok részcsoportja, és $\mathbf{A}$ a diagonális mátrixok részcsoportja. Így többek között megválaszoljuk Horváth $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$ csoportra vonatkozó kérdését [12, 4. probléma].

Tétel (4.1. tétel)**.** *Legyen* $\mathbf{G}$ *egy szemipattern csoport,* S *és* T *legfeljebb* n *hosszú csoportkifejezések* $\mathbf{G}$ *felett. Ekkor* $O\left(n^{|\mathbf{G}| \log^2 |\mathbf{G}|}\right)$ *időben eldönthető az* $S = T$ *egyenlet megoldhatósága* $\mathbf{G}$ *felett, valamint az* $\mathbf{G} \models S \cong T$ *ekvivalencia.*

Ezt az eredményt [5]-ben publikáltam.

A 6. fejezetben egy általános eljárást adunk amely egységesen kezeli a legtöbb olyan feloldható de nem nilpotens csoportot melyre a korábbi tételekkel az egyenletmegoldhatóság probléma eldönthető. Sőt ez az új eljárás sok olyan csoportra is alkalmazható melyre a korábbi eredmények nem mondtak semmit. Így többek között megválaszoljuk Horváth $\mathbf{SL}(2, \mathbb{Z}_3)$ csoportra vonatkozó kérdését [12, 3. probléma].

Tétel (6.1. tétel)**.** *Legyen* $\mathbf{P}$ *egy p-csoport,* $\mathbf{A}$ *egy Abel-csoport. Tekintsünk egy* $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$ *szemidirekt szorzatot. Legyenek* S *és* T *legfeljebb* n *hosszú csoportkifejezések* $\mathbf{G}$ *felett. Ekkor* $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|} \log |\mathbf{G}|}\right)$ *időben eldönthető, hogy az* $S = T$ *egyenletnek van-e megoldása* $\mathbf{G}$*-ben.*

A 6. fejezetben egy hasonlóan általános eredmény bizonyítunk az ekvivalencia problémáról:

Tétel (6.2. tétel)**.** *Legyen* $\mathbf{N}$ *egy nilpotens csoport,* $\mathbf{A}$ *egy Abel-csoport. Tekintsünk egy* $\mathbf{G} = \mathbf{N} \rtimes \mathbf{A}$ *szemidirekt szorzatot. Legyenek* S *és* T *legfeljebb* n *hosszú csoportkifejezések* $\mathbf{G}$ *felett. Ekkor* $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|} \log |\mathbf{G}|}\right)$ *időben eldönthető a* $\mathbf{G} \models S \approx T$ *ekvivalencia.*

Ezeknek az eredményeknek a publikálása folyamatban van.

A 2. fejezetben összefoglaljuk a dolgozatban használt definíciókat és korábbi eredményeket. A 3. fejezetben nilpotens gyűrűk felett vizsgáljuk az egyenletmegoldhatóság probléma bonyolultságát és bebizonyítjuk a 3.1. tételt. A 4. fejezetben szemipattern csoportok felett vizsgáljuk az egyenletmegoldhatóság probléma bonyolultságát és igazoljuk a 4.1. tételt. A 3. és 4. fejezetek eredményeit egyszerzős cikként [5] az *International Journal of Algebra and Computations* folyóiratban publikáltam. Az 5. fejezetben a nilpotens csoportok felett vizsgáljuk az egyenletmegoldhatóság probléma bonyolultságát és bebizonyítjuk az 5.1. tételt. A fejezet eredményeit egyszerzős cikként [4] a *Journal of Algebra* folyóiratban publikáltam. Végül a 6. fejezetben feloldható de nem nilpotens csoportok speciális osztályaira vizsgáljuk az egyenletmegoldhatóság és ekvivalencia problémák bonyolultságát, és bebizonyítjuk a 6.1. és 6.2 tételeket.

2. fejezet

Definíciók, előismeretek

2.1. Csoportok

Legyen $\mathbf{G}$ egy véges csoport. Egy $\mathbf{G}$ csoport feletti *csoportkifejezés* alatt változók és $\mathbf{G}$-beli elemek formális szorzatát értjük. Megjegyezzük, hogy csoportkifejezésekben nem használunk invertálást, az x^{-1} kifejezhető $x^{|\mathbf{G}|-1}$ szorzatként. Egy $T = t_1 \cdots t_n$ csoportkifejezés *hosszát* n-nek definiáljuk, jele $\|T\|$. Az S és T csoportkifejezések *ekvivalens*ek $\mathbf{G}$ felett, ha a változók bármely helyettesítésére S és T értéke megegyezik, jele $\mathbf{G} \models S \approx T$.

A $\mathbf{G}$ csoport feletti *egyenletmegoldhatóság* probléma inputja két $\mathbf{G}$ feletti csoportkifejezés S és T, és a kérdés, hogy az $S = T$ egyenlet megoldható-e. A $\mathbf{G}$ feletti *ekvivalencia* probléma inputja szintén két $\mathbf{G}$ feletti csoportkifejezés S, T, és a kérdés, hogy S és T ekvivalensek-e $\mathbf{G}$ felett (azaz $\mathbf{G} \models S \approx T$). Ezen problémák mindig eldönthetőek a változók összes lehetséges helyettesítésének kiértékelésével. Az érdekesebb kérdés, hogy mely bonyolultsági osztályba esnek ezen döntési problémák. Az algoritmusok futásidejének jellemzéséhez bevezetjük az O jelölést. Legyenek $f, g \colon \mathbb{Z}^+ \to \mathbb{Z}^+$ függvények. Azt mondjuk, hogy

$g(n) = O(f(n))$, ha van olyan pozitív egész C, hogy minden pozitív egész n-re $g(n) \leq C \cdot f(n)$. Jelölje a kettes alapú logaritmust log. A bonyolultságelméleti alapfogalmak megtalálhatóak például [6, 22]-ben.

Az 5. és 6. fejezetben a kommutátor és a konjugált alapvető tulajdonságait fogjuk használni. Az $x, y \in \mathbf{G}$ elemek *kommutátora* $[x, y] = xyx^{|\mathbf{G}|-1}y^{|\mathbf{G}|-1}$. Így

$$xy = xyx^{|\mathbf{G}|-1}y^{|\mathbf{G}|-1}yx = [x, y]\, yx. \tag{2.1}$$

Az y elem x elemmel vett *konjugáltja* $y^x = xyx^{|\mathbf{G}|-1}$. Így

$$xy = xyx^{|\mathbf{G}|-1}x = y^x x. \tag{2.2}$$

Legyen $\mathbb{F}_q$ egy véges test. Tekintsük azon $m \times m$-es $\mathbb{F}_q$ feletti mátrixokat amelyek főátlója alatt csupa nulla, főátlójában csupa nem nulla elem szerepel. E mátrixok csoportot alkotnak a szorzásra nézve melyet $\mathbf{T}(m, \mathbb{F}_q)$-val jelölünk. A következő lemmában $\mathbf{T}(m, \mathbb{F}_q)$-beli mátrixok szorzatát a mátrixok elemei segítségével jellemezzük. Ezt az eredményt a 4.1. tétel bizonyításában fogjuk alkalmazni.

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

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

Legyen

$$A_1 \cdots A_n = \begin{pmatrix} \alpha_1 & \eta_{1,2} & \eta_{1,3} & \dots & \eta_{1,m} \\ 0 & \alpha_2 & \eta_{2,3} & \dots & \eta_{2,m} \\ 0 & 0 & \alpha_3 & \dots & \eta_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \alpha_m \end{pmatrix}.$$

Ekkor

– *bármely* $i = 1, \ldots, n$ *indexre*

$$\alpha_i = \prod_{k=1}^{n} a_{i,k};$$

– *bármely* $1 \leq i < j \leq m$ *indexre*

$$\eta_{i,j} = \sum_{b=0}^{j-i-1} \sum_{i<l_1<\ldots<l_b<j} \sum_{k_{b+1}=b+1}^{n} \sum_{k_b=b}^{k_{b+1}-1} \cdots \sum_{k_2=2}^{k_3-1} \sum_{k_1=1}^{k_2-1} \left(\prod_{c_0=1}^{k_1-1} a_{i,c_0} \right) h_{i,l_1,k_1} \left(\prod_{c_1=k_1+1}^{k_2-1} a_{l_1,c_1} \right) h_{l_1,l_2,k_2} \left(\prod_{c_2=k_2+1}^{k_3-1} a_{l_2,c_2} \right) h_{l_2,l_3,k_3} \left(\prod_{c_3=k_3+1}^{k_4-1} a_{l_3,c_3} \right) \cdots h_{l_{b-1},l_b,k_b} \left(\prod_{c_b=k_b+1}^{k_{b+1}-1} a_{l_b,c_b} \right) h_{l_b,j,k_{b+1}} \left(\prod_{c_{b+1}=k_{b+1}+1}^{n} a_{j,c_{b+1}} \right). \tag{2.3}$$

A (2.3) formula hossza $O\left(n^m\right)$.

Bizonyítás. A lemma n szerinti teljes indukcióval igazolható. E technikai bizonyítás helyett azonban elmagyarázzuk, hogyan kapható meg a (2.3) formula.

Tekintsük az $A_1 \cdots A_n$ mátrix i-edik sorának j-edik elemét az $\eta_{i,j}$ elemet ($1 \leq i < j \leq m$). Az $\eta_{i,j}$ elem kifejezhető alkalmas szorzatok összegeként. Minden ilyen szorzatban minden egyes A_k ($1 \leq k \leq n$) mátrixból egy elem szerepel. (Az utolsó index jelöli, hogy egy $a_{l_c,k}$

vagy egy $h_{l_{c-1},l_c,k}$ tényező mely mátrixból származik.) Továbbá minden szorzatban minden egyes tényező oszlopindexe megegyezik a következő tényező sorindexével. (Tehát egy $a_{l_c,\cdot}$ vagy $h_{l_{c-1},l_c,\cdot}$ alakú tényezőt egy $a_{l_c,\cdot}$ vagy $h_{l_c,l_{c+1},\cdot}$ alakú tényező követ.) Minden szorzat első tényezőjének sorindexe i, utolsó tényezőjének oszlopindexe j. Mivel $A_1, \ldots, A_n$ felső háromszögmátrixok, így minden szorzat minden egyes tényezőjének sorindexénél nagyobb vagy egyenlő az adott tényező oszlopindexe. (Tehát minden főátló feletti $h_{l_c,l_{c+1},\cdot}$ alakú tényezőre $l_c < l_{c+1}$.) Tehát az $A_1 \cdots A_n$ mátrix i-edik sorának j-edik eleme az $\eta_{i,j}$ elem, n tényezős szorzatok összege úgy, hogy minden szorzatban

- az első tényező sorindexe i, az utolsó tényező oszlopindexe j;
- minden egyes tényező oszlopindexe megegyezik a következő tényező sorindexével;
- minden egyes tényező sorindexénél nagyobb vagy egyenlő az adott tényező oszlopindexe.

Vegyük észre, hogy minden n tényezős szorzatot egyértelműen meghatároznak azok a tényezői melyek sor- és oszlopindexe különböző. Legyen h_{l_{c-1},l_c,k_c} és $h_{l_c,l_{c+1},k_{c+1}}$ a szorzat két ilyen egymást követő tényezője. (Itt $i \leq l_{c-1} < l_c < l_{c+1} \leq j$ és $1 \leq k_c < k_{c+1} \leq n$.) Ekkor h_{l_{c-1},l_c,k_c} és $h_{l_c,l_{c+1},k_{c+1}}$ között a szorzat tényezőinek sor és oszlopindexe egyaránt l_c és a tényezők utolsó indexe k_c-nél nagyobb de k_{c+1}-nél kisebb. Tehát a h_{l_{c-1},l_c,k_c} és $h_{l_c,l_{c+1},k_{c+1}}$ tényezők között az $a_{l_c,k_c+1} \cdot a_{l_c,k_c+2} \cdot \cdots a_{l_c,k_{c+1}-1}$ szorzatnak kell állnia. Ezzel igazoltuk a (2.3) formulát.

A továbbiakban a (2.3) formula hosszát jellemezzük. A (2.3) formula szorzatok összege. Minden szorzat n tényezős, így elegendő a szorzatok számát meghatároznunk. Vegyük észre, hogy egy szorzatot egyértelműen meghatároznak az adott szorzat tényezőinek oszlopindexei. Pontosabban elegendő az első $n-1$ tényező oszlopindexét ismernünk, ugyanis az utolsó tényező oszlopindexe mindenképp j. Ezeket az indexeket az $\{i, i+1, \ldots, j-1, j\}$ halmazból választhatjuk. A kiválasztás

sorrendje nem számít. Elegendő azt tudnunk, hány indexet választunk i-nek, $i+1$-nek, …, j-nek. Tehát egy $j-i+1$ elemű halmazból $n-1$ elemet kell kiválasztanunk úgy, hogy lehetséges ismétlődés. Így a szorzatok száma

$$\binom{n-1+j-i+1-1}{n-1} = \binom{n+j-i-1}{j-i}.$$

Mivel minden szorzat hossza n, a (2.3) formula hossza

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

□

2.2. Gyűrűk

Legyen $\mathcal{R}$ egy véges gyűrű. Egy $\mathcal{R}$ feletti f *polinom* alatt egy változókból és $\mathcal{R}$ elemeiből a gyűrű alapműveleteivel képzett kifejezést értünk. (A polinomokban szereplő változókat pontosvesszőkkel választjuk el a hagyományosan használt vesszők helyett.) Egy f polinom *hosszán* az f-ben szereplő változók és konstansok multiplicitással vett számát értjük, jele $\|f\|$.

Az $\mathcal{R}$ gyűrű feletti *egyenletmegoldhatóság* probléma inputja két $\mathcal{R}$ feletti f_1, f_2 polinom, és a kérdés, hogy az $f_1 = f_2$ egyenlet megoldható-e $\mathcal{R}$ felett. Az $\mathcal{R}$ gyűrű feletti *szigma egyenletmegoldhatóság* probléma inputja két $\mathcal{R}$ feletti monomok összegeként adott f_1, f_2 polinom, és a kérdés, hogy az $f_1 = f_2$ egyenlet megoldható-e $\mathcal{R}$ felett.

Legyenek $S, S_1, \ldots, S_\beta \subseteq \mathcal{R}$. Legyenek $n, n_1, \ldots, n_\beta$ pozitív egészek, és legyenek $X = \{ x_k \ : \ 1 \leq k \leq n \}$, $Y_j = \{ y_{j,k} \ : \ 1 \leq k \leq n_j \}$, $1 \leq j \leq \beta$ páronként diszjunkt halmazok. Legyenek f_1, f_2 polinomok $\mathcal{R}[X; Y_1; \ldots; Y_\beta]$ felett. Azt mondjuk, hogy az $f_1 = f_2$ *egyenlet* $S, S_1, \ldots, S_\beta$*-beli helyettesítésre megoldható* $\mathcal{R}$ *felett* (vagy $f_1|_{S,S_1,\ldots,S_\beta}$

$= f_2|_{S,S_1,\ldots,S_\beta}$ megoldható $\mathcal{R}$ felett) ha léteznek olyan $s_1,\ldots,s_n \in S$, $s_{1,1},\ldots,s_{1,n_1} \in S_1$, …, $s_{\beta,1},\ldots,s_{\beta,n_\beta} \in S_\beta$ elemek melyekre

$$f_1(s_1;\ldots;s_n;s_{1,1};\ldots;s_{1,n_1};\ldots;s_{\beta,1};\ldots;s_{\beta,n_\beta}) =$$
$$= f_2(s_1;\ldots;s_n;s_{1,1};\ldots;s_{1,n_1};\ldots;s_{\beta,1};\ldots;s_{\beta,n_\beta}).$$

Jelölje $\mathbb{F}_q$ a q elemű testet. Egy $f \in \mathbb{F}_q[x_1;\ldots;x_n]$ polinomot *redukáltnak* nevezünk, ha

$$f(x_1;\ldots;x_n) = \sum_{0\le s_1,\ldots,s_n\le q-1} c_{s_1,\ldots,s_n} x_1^{s_1}\cdots x_n^{s_n}$$

alakú, ahol $c_{s_1,\ldots,s_n} \in \mathbb{F}_q$ $(0 \le s_k \le q-1,\ 1 \le k \le n)$. Ha $f(x_1;\ldots;x_n)$ a nulla polinom, akkor f foka 0, egyébként f foka az a maximális $s_1+\cdots+s_n$ összeg melyre a $c_{s_1,\ldots,s_n}$ együttható nem 0. Bármely n változós $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$ függvényhez létezik egy $\mathbb{F}_q[x_1;\ldots;x_n]$-beli redukált polinom mely az adott f függvényt reprezentálja [21].

A következő Wilsontól származó tételben a prímhatvány karakterisztikájú gyűrűket fogjuk jellemezni. Ezt az eredményt a 3.1. tétel bizonyításában alkalmazzuk majd.

2.2. Tétel ([26])**.** *Legyen $\mathcal{R}$ egy p^α karakterisztikájú véges nilpotens gyűrű. Tegyük fel, hogy az $\mathcal{R}$ gyűrűnek van m elemű független generátorrendszere $\mathbb{Z}_{p^\alpha}$ felett. Legyen $\mathcal{M}$ azon $m\times m$-es $\mathbb{Z}_{p^\alpha}$ feletti mátrixok gyűrűje melyek minden főátlóbeli és főátló alatti eleme a (p) ideálból származik. Ekkor $\mathcal{R}$ az $\mathcal{M}$ gyűrű homomorf képe.*

A következő 2.3. és 2.4. tételben, valamint 2.5. következményben néhány speciális egyenletrendszer-megoldhatóságra ismert eredményt idézünk fel. A 2.3. tételben olyan $\mathbb{Z}_{p^\alpha}$ feletti egyenletrendszerek megoldhatóságát jellemezzük, melyekben a változókat a $\mathbb{Z}_{p^\alpha}$ gyűrűből helyettesíthetjük. A 2.3. tételt a 3. fejezetben fogjuk alkalmazni. A 2.4. té-

telben olyan $\mathbb{F}_q$ feletti egyenletrendszerek megoldhatóságát jellemezzük, melyekben az X halmazból származó változókat a $\mathbb{F}_q$ testből helyettesíthetjük, az Y_i halmazból származó változókat az adott $\mathbf{S}_i \leq \mathbb{F}_q^\times$ csoportból helyettesíthetjük. A 2.4. tételt a 4. és 5. fejezetekben fogjuk alkalmazni. A 2.5. következményben olyan $\mathbb{F}_q$ feletti egyenletrendszerek megoldhatóságát jellemezzük, melyekben az X halmazból származó változókat csak a $\mathbb{Z}_p$ *résztestből* helyettesíthetjük, az Y_i halmazból származó változókat az adott $\mathbf{S}_i \leq \mathbb{F}_q^\times$ csoportból helyettesíthetjük. A 2.5. következményt a 6. fejezetben fogjuk alkalmazni.

2.3. Tétel ([13])**.** *Tekintsük a $\mathbb{Z}_{p^\alpha}$ gyűrűt. Legyen*

$$X = \{ x_k \ : \ 1 \leq k \leq n \}.$$

Legyenek $f_1, \ldots, f_k \in \mathbb{Z}_{p^\alpha}[X]$ redukált polinomok. Ekkor az

$$\begin{aligned} f_1 &= 0 \\ &\vdots \\ f_k &= 0 \end{aligned}$$

egyenletrendszer megoldhatósága $O\left(max_{1\leq i\leq k}||f_i||^{\alpha^2 k \cdot p^{2\alpha^2}}\right)$ időben eldönthető $\mathbb{Z}_{p^\alpha}$ felett.

2.4. Tétel ([12, 221 oldal, (d) eset])**.** *Legyen $\mathbb{F}_q$ véges test. Legyenek $\mathbf{S}_1, \ldots, \mathbf{S}_\beta$ az $\mathbb{F}_q^\times$ részcsoportjai. Legyenek*

$$X = \{ x_k \ : \ 1 \leq k \leq n \}, \quad Y_j = \{ y_{j,k} \ : \ 1 \leq k \leq n_j \}, \quad 1 \leq j \leq \beta$$

páronként diszjunkt halmazok. Legyenek továbbá $f_1, \ldots, f_m$ redukált polinomok $\mathbb{F}_q[X; Y_1; \ldots; Y_\beta]$ felett. Ekkor az

$$\begin{aligned} f_1|_{\mathbb{F}_q, \mathbf{S}_1, \ldots, \mathbf{S}_\beta} &= 0 \\ &\vdots \\ f_m|_{\mathbb{F}_q, \mathbf{S}_1, \ldots, \mathbf{S}_\beta} &= 0 \end{aligned} \tag{2.4}$$

egyenletrendszer megoldhatósága $O\left(max_{1\leq i\leq m}\|f_i\|^{(q-1)m}\right)$ *időben eldönthető* $\mathbb{F}_q$ *felett.*

2.5. Következmény. *Legyen* $\mathbb{F}_q$ *egy* p *karakterisztikájú test. Legyen* C *egy pozitív egész. Legyenek*

$$X = \{\, x_k \;:\; 1 \leq k \leq n \,\}, \quad Y_j = \{\, y_{j,k} \;:\; 1 \leq k \leq n_j \,\}, \quad 1 \leq j \leq \beta$$

páronként diszjunkt halmazok. Legyenek továbbá $f_1, \ldots, f_m$ *olyan redukált polinomok* $\mathbb{F}_q[X; Y_1; \ldots; Y_\beta]$ *felett, melyek bármely monomja legfeljebb* C *darab* X*-beli változót tartalmaz (multiplicitással együtt). Ekkor az*

$$\begin{aligned} f_1|_{\mathbb{Z}_p,\mathbf{s}_1,\ldots,\mathbf{s}_\beta} &= 0 \\ &\vdots \\ f_m|_{\mathbb{Z}_p,\mathbf{s}_1,\ldots,\mathbf{s}_\beta} &= 0 \end{aligned} \tag{2.5}$$

egyenletrendszer megoldhatósága $\mathbb{F}_q$ *felett* $O\left(max_{1\leq i\leq m}\|f_i\|^{(q-1)m}\right)$ *időben eldönthető.*

Bizonyítás. Legyen π egy olyan $\mathbb{F}_q$ feletti redukált polinom mely értékkészlete $\mathbb{Z}_p$. Legyen $X^\pi = \{\, \pi(x_k) \;:\; 1 \leq k \leq n \,\}$ polinomhalmaz és legyen $\tilde{f}_i(X; Y_1; \ldots; Y_\beta)$ az az $\mathbb{F}_q$ feletti redukált polinom melyre

$$\tilde{f}_i(X; Y_1; \ldots; Y_\beta) \approx f_i(X^\pi; Y_1; \ldots; Y_\beta) \qquad (1 \leq i \leq m).$$

Az f_i polinom bármely monomja legfeljebb C darab X-beli változót tartalmaz, így

$$\left\|\tilde{f}_i\right\| \leq \|f_i\| \cdot \|\pi\|^C = O\left(\|f_i\|\right).$$

Vegyük észre, hogy az

$$f_i|_{\mathbb{Z}_p,\mathbf{s}_1,\ldots,\mathbf{s}_\beta} = 0, \qquad 1 \leq i \leq m$$

egyenletrendszer pontosan akkor megoldható $\mathbb{F}_q$ felett, ha az

$$\tilde{f}_i|_{\mathbb{F}_q,\mathbf{s}_1,\ldots,\mathbf{s}_\beta} = 0, \qquad 1 \leq i \leq m$$

egyenletrendszer megoldható $\mathbb{F}_q$ felett. Tehát a (2.5) egyenletrendszer megoldhatósága

$$O\left(max_{1\leq i\leq m}\left\|\tilde{f}_i\right\|^{(q-1)m}\right) = O\left(max_{1\leq i\leq m}\left\|f_i\right\|^{(q-1)m}\right)$$

időben eldönthető. □

3. fejezet

Nilpotens gyűrűk

Ebben a fejezetben nilpotens gyűrűk felett vizsgáljuk az egyenletmegoldhatóság probléma bonyolultságát. Horváth bebizonyította, hogy ha f_1 és f_2 legfeljebb n hosszú polinomok egy $\mathcal{R}$ nilpotens gyűrű felett, akkor $O\left(n^{|\mathcal{R}|^{|\mathcal{R}|^{\cdots^{|\mathcal{R}|}}}}\right)$ időben eldönthető, hogy az $f_1 = f_2$ egyenletnek van-e megoldása $\mathcal{R}$-ben. Itt a korlát kitevőjében szereplő torony magassága $\mathcal{R}$ nilpotenciaosztálya. Wilson 2.2. tétele segítségével jelentősen javítjuk az ismert időkorlátot:

3.1. Tétel. *Legyen $\mathcal{R}$ egy nilpotens gyűrű, f_1 és f_2 legfeljebb n hosszú $\mathcal{R}$ feletti polinomok. Ekkor $O\left(n^{|\mathcal{R}|^{2\log|\mathcal{R}|}\log^5|\mathcal{R}|}\right)$ időben eldönthető, hogy az $f_1 = f_2$ egyenletnek van-e megoldása $\mathcal{R}$-ben.*

3.1. Egyenletmegoldhatóság probléma nilpotens gyűrűk felett

3.2. Lemma. *Legyen $\mathcal{M}$ azon $m \times m$-es $\mathbb{Z}_{p^\alpha}$ feletti mátrixok gyűrűje melyek minden főátlóbeli és főátló alatti eleme a (p) ideálból származik.*

Legyen f egy monomok összegeként adott polinom $\mathcal{M}$ felett. Ekkor $O\left(||f||^{\alpha^2 \cdot m^2 \cdot p^{2\alpha^2}}\right)$ időben eldönthető az $f = 0$ egyenlet megoldhatósága $\mathcal{M}$ felett.

Bizonyítás. Legyen az f polinom egy tetszőleges monomja $t_1 \cdots t_n$. Azaz t_k $(1 \leq k \leq n)$ egy változó vagy $\mathcal{M}$ egy eleme. Minden $1 \leq k \leq$ $\leq n$ indexre kicseréljük t_k-t a

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

mátrixra az alábbi módon:

- Ha t_k az $\mathcal{M}$ egy eleme, akkor legyenek $x_{i,j,k}$ $(1 \leq i < j \leq m)$ és $y_{i,j,k}$ $(1 \leq j \leq i \leq m)$ a $\mathbb{Z}_{p^\alpha}$ olyan elemei melyekre $t_k = T_k$ és cseréljük ki t_k-t T_k-ra.

- Ha t_k egy $\mathcal{M}$ feletti változó, akkor $x_{i,j,k}$ $(1 \leq i < j \leq m)$ jelöljön egy $\mathbb{Z}_{p^\alpha}$ feletti változót úgy, hogy x_{i_1,j_1,k_1} és x_{i_2,j_2,k_2} pontosan akkor jelölje ugyanazt a változót (valamely $1 \leq i_1 < j_1 \leq m$, $1 \leq i_2 < j_2 \leq m$, $1 \leq k_1, k_2 \leq n$ indexekre) ha t_1 és t_2 ugyanazt a változót jelölik $\mathcal{M}$ felett és $i_1 = i_2$, $j_1 = j_2$. Hasonlóan, $y_{i,j,k}$ $(1 \leq j \leq i \leq m)$ jelöljön egy $\mathcal{M}$ feletti változót úgy, hogy y_{i_1,j_1,k_1} és y_{i_2,j_2,k_2} pontosan akkor jelölje ugyanazt a változót (valamely $1 \leq j_1 \leq i_1 \leq m$, $1 \leq j_2 \leq i_2 \leq m$, $1 \leq k_1, k_2 \leq n$ indexekre) ha t_1 és t_2 ugyanazt a változót jelölik $\mathcal{M}$ felett és $i_1 = i_2$, $j_1 = = j_2$. Ahogy $x_{i,j,k}$ és $y_{i,j,k}$ értékei végigfutnak $\mathbb{Z}_{p^\alpha}$ elemein, úgy T_k értékei végigfutnak $\mathcal{M}$ elemein. Cseréljük ki t_k-t a T_k formális mátrixra.

Így a T monom az alábbi alakra hozható:

$$T_1 \cdots T_n = \begin{pmatrix} y_{1,1,1} \cdot p & x_{1,2,1} & x_{1,3,1} & \cdots & x_{1,m,1} \\ y_{2,1,1} \cdot p & y_{2,2,1} \cdot p & x_{2,3,1} & \cdots & x_{2,m,1} \\ y_{3,1,1} \cdot p & y_{3,2,1} \cdot p & y_{3,3,1} \cdot p & \cdots & x_{3,m,1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y_{m,1,1} \cdot p & y_{m,2,1} \cdot p & y_{m,3,1} \cdot p & \cdots & y_{m,m,1} \cdot p \end{pmatrix} \cdots$$
$$\cdots \begin{pmatrix} y_{1,1,n} \cdot p & x_{1,2,n} & x_{1,3,n} & \cdots & x_{1,m,n} \\ y_{2,1,n} \cdot p & y_{2,2,n} \cdot p & x_{2,3,n} & \cdots & x_{2,m,n} \\ y_{3,1,n} \cdot p & y_{3,2,n} \cdot p & y_{3,3,n} \cdot p & \cdots & x_{3,m,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y_{m,1,n} \cdot p & y_{m,2,n} \cdot p & y_{m,3,n} \cdot p & \cdots & y_{m,m,n} \cdot p \end{pmatrix}.$$

A f polinom összes monomjának átírása $O(||f||)$ időt igényel. Jelölje F az átírás után kapott polinomot.

Jelölje a $T_1, \cdots, T_n$ mátrixok szorzatát

$$T_1 \cdots T_n = \begin{pmatrix} g_{1,1} & g_{1,2} & g_{1,3} & \cdots & g_{1,m} \\ g_{2,1} & g_{2,2} & g_{2,3} & \cdots & g_{2,m} \\ g_{3,1} & g_{3,2} & g_{3,3} & \cdots & g_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{m,1} & g_{m,2} & g_{m,3} & \cdots & g_{m,m} \end{pmatrix}.$$

A 2.1. lemmához hasonlóan kiszámíthatnánk a $g_{i,j}$ polinomokat. Azonban nem szükséges részletesen ismernünk ezeket a formulákat, elegendő azt megértenünk hogyan épülnek fel. Legyenek $1 \leq i, j \leq m$ rögzített indexek. A $g_{i,j}$ polinom $\mathbb{Z}_{p^\alpha}$ feletti monomok összege. Minden monomban minden egyes T_k $(1 \leq k \leq n)$ mátrixból egy elem szerepel. Így minden monom hossza n. Tehát, a mátrixszorzás szabálya szerint, a $g_{i,j}$ polinom legfeljebb m^{n-1} monom összege. Azonban minden nemzéró monom legfeljebb $\alpha - 1$ olyan tényezőt tartalmazhat mely a

főátlóból vagy a főátló alól származik, mivel $\mathbb{Z}_{p^\alpha}$ karakterisztikája p^α. Tehát minden nemzéró monom az alábbi alakú:

$$\underbrace{x_{i,i_1,1} \cdot x_{i_i,i_2,2} \cdots x_{i_{k_1-1},i_{k_1},k_1}}_{k_1 \text{ darab tényező}} \cdot y_{i_{k_1},l_1,k_1+1} \cdot p \cdot \underbrace{x_{l_1,\bar{i}_1,k_1+2} \cdot x_{\bar{i}_1,\bar{i}_2,.} \cdots x_{\bar{i}_{k_2-1},\bar{i}_{k_2},.}}_{k_2 \text{ darab tényező}}$$

$$\cdot y_{\bar{i}_{k_2},l_2,.} \cdot p \cdots y_{\hat{i}_{k_{b-1}},l_{b-1},.} \cdot p \cdot \underbrace{x_{l_{b-1},\tilde{i}_1,.} \cdots x_{\tilde{i}_{k_b-1},\tilde{i}_{k_b},n}}_{k_b \text{ darab tényező}},$$

ahol $1 \leq b \leq \alpha$ és $0 \leq k_1, \ldots, k_b$. Vegyük észre, hogy itt $k_1, \ldots, k_b \leq$ $\leq m-1$. Valóban, bármely $x_{i,j,k}$ tényező a főátló felül származik, így $i < j$. Ezért $1 < i_1 < i_2 < \ldots < i_{k_1} \leq m$, tehát $k_1 \leq m-1$. Hasonlóan $k_2, \ldots, k_b \leq m-1$. Így minden nemzéró monom hossza legfeljebb $(m-1) \cdot \alpha + \alpha - 1 = m\alpha - 1$. Speciálisan, ha $m\alpha - 1 <$ $< n$, akkor $g_{i,j}$ minden monomja zéró. Tehát a $g_{i,j}$ polinom legfeljebb $m^{m\alpha-2}$ monom összege és így $||g_{i,j}|| \leq (m\alpha-1) \cdot m^{m\alpha-2} < \alpha \cdot m^{m\alpha-1}$.

Az F polinom legfeljebb $||F|| = ||f||$ monom összege. Legyen

$$F = \begin{pmatrix} f_{1,1} & f_{1,2} & f_{1,3} & \cdots & f_{1,m} \\ f_{2,1} & f_{2,2} & f_{2,3} & \cdots & f_{2,m} \\ f_{3,1} & f_{3,2} & f_{3,3} & \cdots & f_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_{m,1} & f_{m,2} & f_{m,3} & \cdots & f_{m,m} \end{pmatrix}.$$

Bármely $1 \leq i, j \leq m$ indexekre az $f_{i,j}$ polinom legfeljebb $||f||$ darab $g_{i,j}$ polinom összege. Tehát $||f_{i,j}|| \leq ||f|| \cdot \alpha m^{m\alpha-1} = O(||f||)$, mivel α és m függetlenek f-től. Az $f_{i,j}$ polinomok $O(||f||)$ időben elkészíthetőek.

A mátrixalak egyértelműsége miatt az $F = 0$ egyenlet pontosan akkor megoldható $\mathcal{M}$ felett, ha az

$$f_{i,j} = 0 \qquad\qquad i, j \in \{1, \ldots, m\} \tag{3.1}$$

egyenletrendszer megoldható $\mathbb{Z}_{p^\alpha}$ felett. A 2.3. tétel segítségével a (3.1) egyenletrendszer megoldhatósága $\mathbb{Z}_{p^\alpha}$ felett $O\left(||f||^{\alpha^2 \cdot m^2 \cdot p^{2\alpha^2}}\right)$ időben eldönthető.

Az algoritmus időigénye:

- $O(||f||)$ időt igényel F elkészítése;
- $O(||f||)$ időt igényel a (3.1) egyenletrendszer elkészítése;
- $O\left(||f||^{\alpha^2 \cdot m^2 \cdot p^{2\alpha^2}}\right)$ időt igényel a (3.1) egyenletrendszer megoldhatóságának eldöntése.

Tehát az $f = 0$ egyenlet megoldhatósága $\mathcal{M}$ felett

$$O\left(||f|| + ||f|| + ||f||^{\alpha^2 \cdot m^2 \cdot p^{2\alpha^2}}\right) = O\left(||f||^{\alpha^2 \cdot m^2 \cdot p^{2\alpha^2}}\right)$$

időben eldönthető. □

A 3.1. tétel bizonyítása. Először megmutatjuk, hogy egy tetszőleges nilpotens gyűrű feletti egyenletmegoldhatóság probléma eldönthető néhány speciális nilpotens mátrixgyűrű feletti szigma egyenletmegoldhatóság probléma segítségével. Ha $\mathcal{R}$ egy nilpotens gyűrű, akkor $\mathcal{R}$ felett az egyenletmegoldhatóság probléma és a *szigma* egyenletmegoldhatóság probléma bonyolultsága megegyezik. Ugyanis a t nilpotenciaosztályú $\mathcal{R}$ felett egy tetszőleges f polinom $O(||f||^t)$ időben szorzatok összegére bontható. Itt $t = \log|\mathcal{R}|$. Így, cserébe egy extra $\log|\mathcal{R}|$ faktorért a futásidő kitevőjében, feltehető, hogy az inputként kapott polinomok monomok összegei. Másrészt az egyenletmegoldhatóság problémát elegendő prímhatvány karakterisztikájú nilpotens gyűrűkre vizsgálnunk, hiszen bármely véges gyűrű előáll prímhatvány karakterisztikájú gyűrűk direkt összegeként és az egyenletmegoldhatóság probléma komponensenként kezelhető. Wilson a 2.2. tételben jellemezte a prímhatvány karakterisztikájú nilpotens gyűrűket speciális $\mathcal{M}$ mátrixgyűrűk segítségével.

Legyen $\mathcal{M}$ egy 2.2. tételben szereplő mátrixgyűrű. Azaz $\mathcal{M}$ azon $m \times m$-es $\mathbb{Z}_{p^\alpha}$ feletti mátrixok gyűrűje melyek minden főátlóbeli és főátló alatti eleme a (p) ideálból származik. Legyen $\mathcal{R} \cong \mathcal{M}/\mathcal{I}$. Legyenek f_1 és f_2 legfeljebb n hosszú $\mathcal{R}$ feletti polinomok. Legyen $f = f_1 - f_2$. Ekkor az $f_1 = f_2$ egyenletnek pontosa akkor van megoldása $\mathcal{R}$-ben, ha létezik olyan helyettesítés melyre f értéke 0. Itt $\|f\| \leq 2 \cdot n = O(n)$. A továbbiakban az $f = 0$ egyenletet vizsgáljuk $\mathcal{R}$ felett.

Legyen F egy olyan monomok összegeként adott $\mathcal{M}$ feletti polinom amely $\mathcal{R} \cong \mathcal{M}/\mathcal{I}$ izomorfizmusnál vett képe ekvivalens az f polinommal. A 2.2. tétel szerint $\mathcal{R}$ karakterisztikája p^α, így $\alpha \leq \log|\mathcal{R}|$. Továbbá $m \leq \log|\mathcal{R}|$, $p^\alpha \leq |\mathcal{R}|$. Ezért $\alpha^2 \cdot m^2 \cdot p^{2\alpha^2} \leq |\mathcal{R}|^{2\log|\mathcal{R}|} \log^4|\mathcal{R}|$. Tehát az $F = 0$ egyenlet megoldhatósága $\mathcal{M}$ felett $O\left(||F||^{|\mathcal{R}|^{2\log|\mathcal{R}|}\log^4|\mathcal{R}|}\right)$ időben eldönthető a 3.2. lemma alkalmazásával. Így az $f = 0$ egyenlet megoldhatósága $\mathcal{R} \cong \mathcal{M}/\mathcal{I}$ felett $O\left(|\mathcal{I}| \cdot ||F||^{|\mathcal{R}|^{2\log|\mathcal{R}|}\log^4|\mathcal{R}|}\right)$ időben eldönthető. Itt $|\mathcal{I}| \leq |\mathcal{M}| \leq (p^\alpha)^{m^2} = O\left(|\mathcal{R}|^{\log^2|\mathcal{R}|}\right)$. Vegyük észre, hogy ha f monomok összegeként adott, akkor $||F|| = O(||f||)$. Ha azonban f tetszőleges polinom akkor f monomok összegére bontásával egy extra $\log|\mathcal{R}|$ kitevőt kapunk, így $||F|| = O\left(||f||^{\log|\mathcal{R}|}\right)$. Tehát egy tetszőleges $\mathcal{R}$ nilpotens gyűrű felett az $f = 0$ egyenlet megoldhatósága $O\left(||f||^{|\mathcal{R}|^{2\log|\mathcal{R}|}\log^5|\mathcal{R}|}\right)$ időben eldönthető. □

4. fejezet

Szemipattern csoportok

Ebben a fejezetben speciális mátrixcsoportokra, az úgynevezett szemipattern csoportokra vizsgáljuk az egyenletmegoldhatóság és ekvivalencia problémák bonyolultságát. Egy $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$ csoportot szemipattern csoportnak nevezünk, ha $\mathbf{P}$ a szigorú felső háromszögmátrixok részcsoportja, és $\mathbf{A}$ a diagonális mátrixok részcsoportja. A felső háromszögmátrixok szorzatát jellemző 2.1. lemma segítségével igazoljuk a következő állítást:

4.1. Tétel. *Legyen* $\mathbf{G}$ *egy szemipattern csoport,* S *és* T *legfeljebb* n *hosszú csoportkifejezések* $\mathbf{G}$ *felett. Ekkor* $O\left(n^{|\mathbf{G}|\log^2|\mathbf{G}|}\right)$ *időben eldönthető az* $S = T$ *egyenlet megoldhatósága* $\mathbf{G}$ *felett, valamint az* $\mathbf{G} \models S \cong T$ *ekvivalencia.*

Később a 6. fejezetben egy általános eljárást adunk mely segítségével az egyenletmegoldhatóság és ekvivalencia problémák egységesen kezelhetőek bármely $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$ csoportra, ahol $\mathbf{P}$ egy p-csoport és $\mathbf{A}$ egy Abel csoport. Ez az eljárás a szemipattern csoportokra is alkalmazható, azonban az általános módszer időkorlátjának kitevője $|\mathbf{G}|^{|\mathbf{G}|}\log|\mathbf{G}|$, szemben a speciálisan szemipattern csoportokra ebben a fejezetben adott $|\mathbf{G}|\log^2|\mathbf{G}|$ kitevővel.

4.1. Szemipattern csoportok

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

$$\mathbf{T}(m, \mathbb{F}_q) =$$
$$\left\{ \begin{pmatrix} a_1 & h_{1,2} & h_{1,3} & \dots & h_{1,m} \\ 0 & a_2 & h_{2,3} & \dots & h_{2,m} \\ 0 & 0 & a_3 & \dots & h_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_m \end{pmatrix} \ : \ a_i \in \mathbb{F}_q^{\times}, h_{i,j} \in \mathbb{F}_q, 1 \le i < j \le m \right\}.$$

Jelölje E 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 $H \subseteq \{ E_{i,j} \ : \ 1 \le i < j \le m \}$. Legyen

$$\mathbf{P}_H = \{E + \sum_{E_{i,j} \in H} h_{i,j} E_{i,j} : h_{i,j} \in \mathbb{F}_q\}.$$

Azaz $\mathbf{P}_H$ azon szigorú felső háromszögmátrixok halmaza melyekben a főátló felett nulla áll minden olyan (i, j) pozícióban melyre $E_{i,j}$ nem eleme H-nak. Ha $\mathbf{P}_H$ egy részcsoport $\mathbf{T}(m, \mathbb{F}_q)$-ban, akkor *pattern* csoportnak nevezünk. A pattern csoportok részletes leírása megtalálható [3, 18]-ban. Legyenek $\mathbf{S}_1, \dots, \mathbf{S}_m$ az $\mathbb{F}_q^{\times}$ részcsoportjai. Gyűjtsük össze azokat az $(i, \mathbf{S}_i)$ párokat, melyekre $\mathbf{S}_i \neq \{1\}$. Legyen $D = \{ (i, \mathbf{S}_i) \ : \ \mathbf{S}_i \neq \{1\}, 1 \le i \le m \}$. Legyen $\mathbf{A}_D$ azon $m \times m$-es $\mathbb{F}_q$ feletti mátrixok halmaza melyek főátlójának i-edik eleme $\mathbf{S}_i$-beli $(1 \le i \le m)$,

minden más eleme nulla:

$$\mathbf{A}_D = \left\{ \begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ 0 & 0 & a_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_m \end{pmatrix} \ : \ a_i \in \mathbf{S}_i, 1 \leq i \leq m \right\}.$$

Ha $\mathbf{P}_H$ egy pattern csoport, akkor a $\mathbf{P}_H \cdot \mathbf{A}_D$ csoport $\mathbf{T}(m, \mathbb{F}_q)$ egy részcsoportja. Ekkor a $\mathbf{P}_H \cdot \mathbf{A}_D$ csoportot *szemipattern csoportnak* nevezünk, jele $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$. Megjegyezzük, hogy $\mathbf{P}_H \lhd \mathbf{P}_H \cdot \mathbf{A}_D$ és így $\mathbf{P}_H \cdot \mathbf{A}_D \cong \mathbf{P}_H \rtimes \mathbf{A}_D$. Horváth [12] cikkének 4. problémájában definiált $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$ csoport egy példa szemipattern csoportra:

$$\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times = \left\{ \begin{pmatrix} 1 & h & k \\ 0 & a & l \\ 0 & 0 & 1 \end{pmatrix} \ : \ a \in \mathbb{Z}_3^\times, h, k, l \in \mathbb{Z}_3 \right\}.$$

4.2. Egyenletmegoldhatóság probléma szemipattern csoportok felett

Ebben az alfejezeteben a szemipattern csoportok feletti egyenletmegoldhatóság illetve ekvivalencia problémák bonyolultságát fogjuk meghatározni. Ezen problémák bonyolultsága eddig még az $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$ csoportra sem volt ismert.

4.2. Lemma. *Legyen $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ egy szemipattern csoport, és T egy tetszőleges, n hosszú csoportkifejezés $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ felett. Ekkor a $T = \mathrm{id}$ egyenlet megoldhatósága $O\left(n^{m(q-1)(|H|+|D|)}\right)$ időben eldönthető $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ felett.*

Bizonyítás. Legyen $T = t_1 \cdots t_n$ egy csoportkifejezés $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ felett, azaz t_k $(1 \leq k \leq n)$ egy változó vagy $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ egy eleme.

Legyen

$$T_k = \begin{pmatrix} y_{1,k} & x_{1,2,k} & x_{1,3,k} & \dots & x_{1,m,k} \\ 0 & y_{2,k} & x_{2,3,k} & \dots & x_{2,m,k} \\ 0 & 0 & y_{3,k} & \dots & x_{3,m,k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & y_{m,k} \end{pmatrix}. \tag{4.1}$$

Minden $1 \leq k \leq n$ indexre kicseréljük t_k-t a T_k mátrixalakjára az alábbi módon:

- Ha t_k az $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ egy eleme, akkor legyenek $x_{i,j,k}$ $(1 \leq \leq i < j \leq m)$ az $\mathbb{F}_q$ és $y_{i,k}$ $(1 \leq i \leq m)$ az $\mathbf{S}_i \leq \mathbb{F}_q^\times$ olyan elemei melyekre a t_k elem mátrixalakja T_k és cseréljük ki t_k-t a T_k mátrixra.

- Ha t_k egy $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ feletti változó és az (i, j) pozícióra $E_{i,j} \notin H$ (azaz $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ minden elemének mátrixalakjában az i-edik sor j-edik eleme 0), akkor legyen $x_{i,j,k} = 0$ $(1 \leq i < j \leq m)$. Ha az (i, j) pozícióra $E_{i,j} \in H$, akkor $x_{i,j,k}$ $(1 \leq i < j \leq m)$ jelöljön egy $\mathbb{F}_q$ feletti változót úgy, hogy x_{i_1,j_1,k_1} és x_{i_2,j_2,k_2} pontosan akkor jelölje ugyanazt a változót (valamely $1 \leq i_1 < j_1 \leq m$, $1 \leq i_2 < j_2 \leq m$, $1 \leq k_1, k_2 \leq n$ indexre) ha t_1 és t_2 ugyanazt a változót jelölik $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ felett és $i_1 = i_2$, $j_1 = j_2$. Hasonlóan, ha az i indexre $(i, \mathbf{S}_i) \notin D$ (azaz $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ minden elemének mátrixalakjában a főátló i-edik eleme 1) akkor legyen $y_{i,k} = 1$ $(1 \leq i \leq m)$. Ha az i indexre $(i, \mathbf{S}_i) \in D$, akkor $y_{i,k}$ $(1 \leq i \leq m)$ jelöljön egy $\mathbf{S}_i$ feletti változót úgy, hogy y_{i_1,k_1} és y_{i_2,k_2} pontosan akkor jelölje ugyanazt a változót (valamely $1 \leq \leq i_1, i_2 \leq m$, $1 \leq k_1, k_2 \leq n$ indexre) ha t_1 és t_2 ugyanazt a változót jelölik $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ felett és $i_1 = i_2$. Mivel minden csoportelem mátrixalakja egyértelmű, ezért ahogy $x_{i,j,k}$ értékei végigfutnak $\mathbb{F}_q$ elemein ($E_{i,j} \in H$ esetén) és $y_{i,k}$ értékei $\mathbf{S}_i$ elemein ($(i, \mathbf{S}_i) \in D$ esetén), úgy a T_k formális mátrix értékei vé-

gigfutnak $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ elemein. Cseréljük ki t_k-t a T_k formális mátrixra.

A T szorzat átírása a tényezők mátrixalakra történő cseréjével $O(n)$ időt igényel.

Így a T csoportkifejezés az alábbi alakra hozható:

$$T = \begin{pmatrix} y_{1,1} & x_{1,2,1} & x_{1,3,1} & \dots & x_{1,m,1} \\ 0 & y_{2,1} & x_{2,3,1} & \dots & x_{2,m,1} \\ 0 & 0 & y_{3,1} & \dots & x_{3,m,1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & y_{m,1} \end{pmatrix} \dots \\ \dots \begin{pmatrix} y_{1,n} & x_{1,2,n} & x_{1,3,n} & \dots & x_{1,m,n} \\ 0 & y_{2,n} & x_{2,3,n} & \dots & x_{2,m,n} \\ 0 & 0 & y_{3,n} & \dots & x_{3,m,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & y_{m,n} \end{pmatrix}. \quad (4.2)$$

A szorzást elvégezve 2.1. lemma alapján

$$T = \begin{pmatrix} f_1 & g_{1,2} & g_{1,3} & \dots & g_{1,m} \\ 0 & f_2 & g_{2,3} & \dots & g_{2,m} \\ 0 & 0 & f_3 & \dots & g_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & f_m \end{pmatrix}, \quad (4.3)$$

ahol

$$f_i = \prod_{k=1}^{n} y_{i,k},$$

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

Speciálisan, ha $(i, \mathbf{S}_i) \notin D$, akkor $f_i = 1$, ha $E_{i,j} \notin H$, akkor $g_{i,j} = 0$. A 2.1. lemma szerint $\|g_{i,j}\| = O(n^m)$. Továbbá az f_i és $g_{i,j}$ polinomok $O(n^m)$ időben elkészíthetőek.

A mátrixalak egyértelműsége miatt a $T = \mathrm{id}$ egyenletnek pontosan akkor van megoldása, ha az

$$\begin{aligned} f_i|_{\mathbb{F}_q,\mathbf{S}_1,\ldots,\mathbf{S}_m} &= 1 \qquad (1 \le i \le m, (i,\mathbf{S}_i) \in D) \\ g_{i,j}|_{\mathbb{F}_q,\mathbf{S}_1,\ldots,\mathbf{S}_m} &= 0 \qquad (1 \le i < j \le m, E_{i,j} \in H) \end{aligned} \tag{4.4}$$

egyenletrendszer megoldható $\mathbb{F}_q$ felett. A 2.4. tétel szerint a (4.4) egyenletrendszer megoldhatósága $\mathbb{F}_q$ felett eldönthető az alábbi időkorláton belül:

$$O\left(\left(max_{1\le i<j\le m}\{\|f_i\|, \|g_{i,j}\|\}\right)^{(q-1)(|H|+|D|)}\right) =$$
$$O\left(\left(n^m\right)^{(q-1)(|H|+|D|)}\right) = O\left(n^{m(q-1)(|H|+|D|)}\right).$$

Az algoritmus időigénye:

- $O(n)$ időt igényel a t_k $(1 \le k \le n)$ tényezők cseréje a mátrixalakjukra;
- $O(n^m)$ időt igényel a (4.4) egyenletrendszer elkészítése;

– $O\left(n^{m(q-1)(|H|+|D|)}\right)$ időt igényel a (4.4) egyenletrendszer megoldhatóságának eldöntése.

Tehát a $T = \mathrm{id}$ egyenlet megoldhatósága $\mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ felett

$$O\left(n + n^m + n^{m(q-1)(|H|+|D|)}\right) = O\left(n^{m(q-1)(|H|+|D|)}\right)$$

időben eldönthető. □

A 4.1. tétel bizonyítása. Legyenek $S = x_1 \cdots x_k$ és $T = y_1 \cdots y_n$ csoportkifejezések $\mathbf{G}$ felett úgy, hogy $k \leq n$. Tekintsük továbbá a $T' = x_k^{|\mathbf{G}|-1} \cdots x_1^{|\mathbf{G}|-1} y_1 \cdots y_n$ formális szorzatot. Ekkor az $S = T$ egyenletnek pontosa akkor van megoldása $\mathbf{G}$-ben, ha létezik olyan helyettesítés melyre T' értéke id. Hasonlóan $\mathbf{G} \models S \approx T$ pontosan akkor, ha minden helyettesítésre T' értéke id. Itt $\|T'\| \leq |\mathbf{G}| \cdot n = O(n)$, mivel $|\mathbf{G}|$ sem S-től sem T-től nem függ, így n-től is független. A továbbiakban a $T' = \mathrm{id}$ egyenletet, valamint a $\mathbf{G} \models T' \approx \mathrm{id}$ ekvivalenciát vizsgáljuk.

A 4.2. lemma szerint a $\mathbf{G} = \mathbf{SP}_{H,D}(m, \mathbb{F}_q)$ feletti $T' = \mathrm{id}$ egyenlet megoldhatósága $O\left(n^{m(q-1)(|H|+|D|)}\right)$ időben eldönthető. Itt $q^{|H|} \cdot 2^{|D|} \leq$ $\leq |\mathbf{G}|$. Így

$$q - 1 < |\mathbf{G}|\,,$$
$$|H| + |D| \leq \log |\mathbf{G}|.$$

Az álalánosság megszorítása nélkül feltehető, hogy

$$m \leq |H| + |D| \leq \log |\mathbf{G}|.$$

Tehát

$$m(q-1)(|H| + |D|) < |\mathbf{G}| \log^2 |\mathbf{G}|.$$

A $\mathbf{G} \models T' \approx \mathrm{id}$ ekvivalencia pontosan akkor *nem* teljesül, ha $T' = g$ megoldható valamely $\mathrm{id} \neq g \in \mathbf{G}$ csoportelemre. Mivel $|\mathbf{G}|$ nem függ n-től, a $\mathbf{G} \models T' \approx \mathrm{id}$ ekvivalencia eldönthető a $\mathbf{G}$ feletti egyenletmegolthatóság probléma időkorlátján belül. □

5. fejezet

Nilpotens csoportok

Ebben a fejezetben nilpotens csoportok felett vizsgáljuk az egyenletmegoldhatóság probléma bonyolultságát. Egy új eljárást adunk amely jelentősen javítja az ismert polinomiális időkorlátot.

5.1. Tétel. *Legyen* $\mathbf{G}$ *egy nilpotens csoport,* S *és* T *legfeljebb* n *hosszú csoportkifejezések* $\mathbf{G}$ *felett. Ekkor* $O\left(n^{\frac{1}{2}|\mathbf{G}|^2 \log |\mathbf{G}|}\right)$ *időben eldönthető, hogy az* $S = T$ *egyenletnek van-e megoldása* $\mathbf{G}$*-ben.*

5.1. p-csoportok

Legyen $\mathbf{P}$ egy p^α elemű csoport. Legyen $\mathbf{P}$ egy maximális centrális lánca $\{\mathrm{id}\} = \mathbf{N}_0 \lhd \mathbf{N}_1 \lhd \cdots \lhd \mathbf{N}_\alpha = \mathbf{P}$. Ekkor $\mathbf{N}_i/\mathbf{N}_{i-1}$ izomorf a p rendű ciklikus csoporttal ($1 \leq i \leq \alpha$). Minden $1 \leq i \leq \alpha$ indexre legyen $b_i \in \mathbf{N}_i \setminus \mathbf{N}_{i-1}$. Ekkor $b_i\mathbf{N}_{i-1}$ az $\mathbf{N}_i/\mathbf{N}_{i-1}$ egy generátora. A $\mathcal{B} = (b_1, \ldots, b_\alpha)$ sorozatot a $\mathbf{P}$ csoport ($\mathbf{N}_0 \lhd \mathbf{N}_1 \lhd \cdots \lhd \mathbf{N}_\alpha$ lánchoz tartozó) *bázisának* nevezünk. Legyen $g \in \mathbf{P}$ tetszőleges csoportelem. Ekkor egyértelműen léteznek olyan $u_1, \ldots, u_\alpha \in \{\, 0, 1, \ldots, p-1 \,\}$ kitevők melyekre

$$g = b_1^{u_1} \cdots b_\alpha^{u_\alpha}. \tag{5.1}$$

A g elem $\mathcal{B}$ bázisra vonatkozó (5.1) előállítását $\mathcal{B}$-*alaknak* nevezünk.

Az 5.2. lemmában kiszámítjuk n csoportelem szorzatának $\mathcal{B}$-alakját az elemek $\mathcal{B}$-alakjaiból redukált $\mathbb{Z}_p$ feletti polinomok segítségével. Itt $\mathbb{Z}_p$ a p-elemű testet jelöli a $\{\,0, 1, \ldots, p-1\,\}$ alaphalmazon. A félreértések elkerülése végett a modulo p összeadást $\oplus$, a modulo p szorzást $\odot$ jelöli, míg a hagyományos, egészek közötti összeadást és szorzást $+$ és $\cdot$ jelöli az 5.2. lemma bizonyításában.

5.2. Lemma. *Legyen* $\mathbf{P}$ *egy* p^α *elemű csoport. Legyen* $\mathbf{P}$ *egy bázisa* $\mathcal{B} = (b_1, \ldots, b_\alpha)$. *Legyen* $C_\alpha = (2p-2)^{\alpha-1}$. *Egy tetszőleges* n *pozitív egészre legyen*

$$X_{n,\alpha} = \{\, x_{k,i} \;:\; 1 \le k \le n, 1 \le i \le \alpha \,\}.$$

Ekkor léteznek olyan $f_1, \ldots, f_\alpha \in \mathbb{Z}_p[X_{n,\alpha}]$ *redukált polinomok, hogy bármely* $g_1, \ldots, g_n \in \mathbf{P}$ *elemekre melyek* $\mathcal{B}$*-alakjai*

$$g_k = b_1^{u_{k,1}} \cdots b_\alpha^{u_{k,\alpha}} \qquad (1 \le k \le n),$$

a $g_1 \cdots g_n$ *szorzat* $\mathcal{B}$*-alakja*

$$g_1 \cdots g_n = b_1^{f_1(u_{1,1};\ldots;u_{n,\alpha})} \cdots b_\alpha^{f_\alpha(u_{1,1};\ldots;u_{n,\alpha})}. \tag{5.2}$$

Bármely $1 \le l \le \alpha$ *indexre az* f_l *polinom foka legfeljebb* C_α, $\|f_l\| = O\left(n^{C_\alpha}\right)$, *és* f_l *kiszámítható* $O\left(n^{C_\alpha}\right)$ *időben.*

Bizonyítás. Az 5.2. lemmát α szerinti teljes indukcióval igazoljuk. Ha $\alpha = 1$, akkor $C_1 = 1$ és $\mathbf{P}$ izomorf a p rendű ciklikus csoporttal. Legyen $\mathbf{P}$ egy generátora b_1, ekkor $\mathcal{B} = (b_1)$ bázis. Legyenek $g_1, \ldots, g_n \in \mathbf{P}$ és jelölje ezen elemek $\mathcal{B}$-alakjait $g_k = b_1^{u_{k,1}} (1 \le k \le n)$. Legyen $f_1(x_1; \ldots; x_n) = x_1 \oplus \cdots \oplus x_n$. Ekkor $g_1 \cdots g_n = b_1^{f_1(u_{1,1};\ldots;u_{n,1})}$. Továbbá f_1 foka 1, $\|f_1\| = O(n)$, és f_1 kiszámítható $O(n)$ időben. Tehát f_1 megfelel az 5.2. lemma feltételeinek.

Tegyük fel, hogy a lemma teljesül bármely p^α rendű csoportra és legyen $\mathbf{P}$ egy $p^{\alpha+1}$ rendű csoport. Legyen $\mathbf{P}$ egy maximális centrális lánca $\{\mathrm{id}\} = \mathbf{N}_0 \lhd \mathbf{N}_1 \lhd \cdots \lhd \mathbf{N}_\alpha \lhd \mathbf{N}_{\alpha+1} = \mathbf{P}$. Legyen $\mathbf{P}$ egy $\mathbf{N}_0 \lhd \lhd \mathbf{N}_1 \lhd \cdots \lhd \mathbf{N}_\alpha \lhd \mathbf{N}_{\alpha+1}$ lánchoz tartózó bázisa $\mathcal{B} = (b_1, \ldots, b_\alpha, b_{\alpha+1})$. Legyenek $g_1, \ldots, g_n \in \mathbf{P}$ tetszőleges csoportelemek és jelölje ezen elemek $\mathcal{B}$-alakjait

$$g_k = b_1^{u_{k,1}} \cdots b_\alpha^{u_{k,\alpha}} b_{\alpha+1}^{u_{k,\alpha+1}} \qquad (1 \leq k \leq n).$$

Ki fogjuk számítani a

$$g_1 \cdots g_n = b_1^{u_{1,1}} \cdots b_\alpha^{u_{1,\alpha}} b_{\alpha+1}^{u_{1,\alpha+1}} \cdots b_1^{u_{n,1}} \cdots b_\alpha^{u_{n,\alpha}} b_{\alpha+1}^{u_{n,\alpha+1}} \tag{5.3}$$

szorzat $\mathcal{B}$-alakját. Először fölvázoljuk a fő lépéseket majd elmagyarázzuk a részleteket.

1. A (2.1)-beli $xy = [x,y]yx$ összefüggést alkalmazva a $b_{\alpha+1}^{u_{k,\alpha+1}}$ $(1 \leq \leq k \leq n)$ tényezőket az (5.3) szorzat jobb oldalára gyűjtjük. Először a $b_{\alpha+1}^{u_{1,\alpha+1}}$ tényezőt visszük jobbra egyenként felcseréve a $b_i^{u_{2,i}}$ $(1 \leq i \leq \alpha)$ tényezőkkel, míg $b_{\alpha+1}^{u_{2,\alpha+1}}$ mellé kerül. Minden ilyen cserével egy $\left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_i^{u_{2,i}}\right]$ kommutátor keletkezik. Így végül $b_{\alpha+1}^{u_{1,\alpha+1}}$ és $b_{\alpha+1}^{u_{2,\alpha+1}}$ egymás mellett állnak a szorzatban. Legyen $\chi \in \mathbb{Z}_p[x;y]$ a modulo p átviteli függvény:

$$\chi(x;y) = \begin{cases} 1, & \text{ha } x+y \geq p, \\ 0, & \text{egyébként.} \end{cases} \tag{5.4}$$

A $b_{\alpha+1}^{u_{1,\alpha+1}}$ és $b_{\alpha+1}^{u_{2,\alpha+1}}$ tényezők egymás mellett szerepelnek a szorzatban, így az alábbi módon össze tudjuk vonni őket:

$$b_{\alpha+1}^{u_{1,\alpha+1}} b_{\alpha+1}^{u_{2,\alpha+1}} = b_{\alpha+1}^{u_{1,\alpha+1}+u_{2,\alpha+1}} = \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})} b_{\alpha+1}^{u_{1,\alpha+1} \oplus u_{2,\alpha+1}}. \tag{5.5}$$

Majd a $b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}$ tényezőt visszük jobbra és így tovább. A k-adik lépésben $(1 \leq k \leq n-1)$ a $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}}$ tényezőt egyenként felcseréljük a $b_i^{u_{k+1,i}}$ $(1 \leq i \leq \alpha)$ tényezőkkel, míg $b_{\alpha+1}^{u_{k+1,\alpha+1}}$ mellé nem kerül. Ezután, összevonjuk $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}}$ és $b_{\alpha+1}^{u_{k+1,\alpha+1}}$ tényezőket (5.5) mintájára:

$$b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}} b_{\alpha+1}^{u_{k+1,\alpha+1}} = b_{\alpha+1}^{(u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1})+u_{k+1,\alpha+1}} =$$
$$= \left(b_{\alpha+1}^{p}\right)^{\chi\left(u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1};u_{2,\alpha+1}\right)} b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}\oplus u_{2,\alpha+1}}. \quad (5.6)$$

Végül, miután az összes $b_{\alpha+1}^{u_{k,\alpha+1}}$ tényezőt jobbra gyűjtöttük $(1 \leq \leq k \leq n-1)$, a szorzat végén $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{n,\alpha+1}}$ szerepel. Jelölje S az (5.3)-ból így kapott formális szorzatot. Ekkor S utolsó tényezője $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{n,\alpha+1}}$. Jelölje T azt a formális szorzatot melyet S-ből az utolsó tényező elhagyásával kapunk. Azaz $S = T b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{n,\alpha+1}}$. Ekkor T tényezői

- b_i hatványok valamely $1 \leq i \leq \alpha$ indexre;
- $\left[b_{\alpha+1}^{x}, b_i^{y}\right]$ alakú kommutátorok melyeket a $b_{\alpha+1}^{x} b_i^{y} = [b_{\alpha+1}^{x}, b_i^{y}] b_i^{y} b_{\alpha+1}^{x}$ cserékből kaptunk;
- $b_{\alpha+1}^{p}$ hatványok melyeket az (5.6)-beli összevonások során kaptunk.

Így T összes tényezője az $\mathbf{N}_\alpha$ részcsoport eleme. Az $\mathbf{N}_\alpha$ csoport p^α rendű és $\mathbf{N}_\alpha$ egy bázisa $\mathcal{B} = (b_1, \ldots, b_\alpha)$. Tehát alkalmazhatjuk az indukciós feltevést a T szorzat $\mathcal{B}$-alakjának meghatározására. Ehhez azonban szükségünk van némi technikai előkészületre a 2. és 3. lépésekben.

2. Meghatározzuk a T szorzatban szereplő $\left[b_{\alpha+1}^{x}, b_i^{y}\right]$ $(x, y \in \mathbb{Z}_p,$ $1 \leq i \leq \alpha)$ kommutátorok $\mathcal{B}$-alakjait. Bebizonyítjuk, hogy létez-

nek olyan redukált $\psi_{i,j}^{(k)} \in \mathbb{Z}_p[x_1;\ldots;x_k;y]$ $(1 \leq i,j \leq \alpha, 1 \leq$ $\leq k \leq n)$ polinomok melyekre

$$\left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}}, b_i^{u_{k+1,i}}\right] =$$
$$= b_1^{\psi_{i,1}^{(k)}\left(u_{1,\alpha+1};\ldots;u_{k,\alpha+1};u_{k+1,i}\right)} \cdots b_\alpha^{\psi_{i,\alpha}^{(k)}\left(u_{1,\alpha+1};\ldots;u_{k,\alpha+1};u_{k+1,i}\right)}. \quad (5.7)$$

Továbbá $\psi_{i,j}^{(k)}$ foka legfeljebb $2p-2$, $\left\|\psi_{i,j}^{(k)}\right\| = O\left(k^{p-1}\right) \leq O\left(n^{p-1}\right)$, és $\psi_{i,j}^{(k)}$ kiszámítható $O\left(k^{p-1}\right) \leq O\left(n^{p-1}\right)$ időben.

3. Hasonlóan meghatározzuk a T szorzatban szereplő $\left(b_{\alpha+1}^p\right)^u$ $(u \in$ $\in \mathbb{Z}_p)$ hatványok $\mathcal{B}$-alakjait. Bebizonyítjuk, hogy léteznek olyan redukált $\chi_i^{(k)} \in \mathbb{Z}_p[x_1;\ldots;x_k;y]$ $(1 \leq i \leq \alpha, 1 \leq k \leq n)$ polinomok melyekre

$$\left(b_{\alpha+1}^p\right)^{\chi\left(u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1};u_{k+1,\alpha+1}\right)} =$$
$$b_1^{\chi_1^{(k)}\left(u_{1,\alpha+1};\ldots;u_{k,\alpha+1};u_{k+1,\alpha+1}\right)} \cdots b_\alpha^{\chi_\alpha^{(k)}\left(u_{1,\alpha+1};\ldots;u_{k,\alpha+1};u_{k+1,\alpha+1}\right)}. \quad (5.8)$$

Továbbá $\chi_i^{(k)}$ foka legfeljebb $2p-2$, $\left\|\chi_i^{(k)}\right\| = O\left(k^{p-1}\right) \leq O\left(n^{p-1}\right)$, és $\chi_i^{(k)}$ kiszámítható $O\left(k^{p-1}\right) \leq O\left(n^{p-1}\right)$ időben.

4. Végül alkalmazzuk az indukciós feltevést a T szorzatra a 2. és 3. lépésekből kapott $\psi_{i,j}^{(k)}$ és $\chi_i^{(k)}$ polinomok felhasználásával, és bebizonyítjuk az 5.2. lemmát az S szorzatra.

Először a szorzat jobb oldalára gyűjtjük a $b_{\alpha+1}^{u_{k,\alpha+1}}$ tényezőket $(1 \leq$ $\leq k \leq n)$. A (2.1)-beli $xy = [x,y]yx$ összefüggést alkalmazzuk $x =$ $= b_{\alpha+1}^{u_{1,\alpha+1}}, y = b_1^{u_{2,1}}$ esetén és felcseréljük az $b_{\alpha+1}^{u_{1,\alpha+1}}$ és $b_1^{u_{2,1}}$ tényezőket a g_1g_2 szorzatban:

$$g_1g_2 = b_1^{u_{1,1}} \cdots b_\alpha^{u_{1,\alpha}} b_{\alpha+1}^{u_{1,\alpha+1}} b_1^{u_{2,1}} b_2^{u_{2,2}} b_3^{u_{2,3}} \cdots b_\alpha^{u_{2,\alpha}} b_{\alpha+1}^{u_{2,\alpha+1}}$$
$$= b_1^{u_{1,1}} \cdots b_\alpha^{u_{1,\alpha}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} b_{\alpha+1}^{u_{1,\alpha+1}} b_2^{u_{2,2}} b_3^{u_{2,3}} \cdots b_\alpha^{u_{2,\alpha}} b_{\alpha+1}^{u_{2,\alpha+1}}.$$

Majd az $xy = [x,y]yx$ összefüggést $x = b_{\alpha+1}^{u_{1,\alpha+1}}, y = b_2^{u_{2,2}}$ esetén alkalmazzuk és felcseréljük $b_{\alpha+1}^{u_{1,\alpha+1}}$ és $b_2^{u_{2,2}}$ tényezőket:

$$g_1 g_2 = b_1^{u_{1,1}} \cdots b_\alpha^{u_{1,\alpha}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_2^{u_{2,2}}\right] b_2^{u_{2,2}} b_{\alpha+1}^{u_{1,\alpha+1}} b_3^{u_{2,3}} \\ b_4^{u_{2,4}} \cdots b_\alpha^{u_{2,\alpha}} b_{\alpha+1}^{u_{2,\alpha+1}}.$$

Ezt az eljárást folyatjuk, míg a $b_{\alpha+1}^{u_{1,\alpha+1}}$ tényező $b_{\alpha+1}^{u_{2,\alpha+1}}$ mellé nem kerül:

$$g_1 g_2 = b_1^{u_{1,1}} \cdots b_\alpha^{u_{1,\alpha}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_2^{u_{2,2}}\right] b_2^{u_{2,2}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_3^{u_{2,3}}\right] \\ b_3^{u_{2,3}} \cdots \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_\alpha^{u_{2,\alpha}}\right] b_\alpha^{u_{2,\alpha}} b_{\alpha+1}^{u_{1,\alpha+1}} b_{\alpha+1}^{u_{2,\alpha+1}}.$$

Így α új kommutátort kapunk: $\left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_i^{u_{2,i}}\right]$ az összes $1 \leq i \leq \alpha$ indexre. Majd összevonjuk a $b_{\alpha+1}^{u_{1,\alpha+1}}$ és $b_{\alpha+1}^{u_{2,\alpha+1}}$ tényezőket $b_{\alpha+1}^{u_{1,\alpha+1}+u_{2,\alpha+1}}$ hatvánnyá. Azonban az $u_{1,\alpha+1} + u_{2,\alpha+1}$ kitevő nem biztos, hogy a $\{0, 1, \ldots, p-1\}$ halmaz eleme. Legyen $\chi\colon \mathbb{Z}_p^2 \to \mathbb{Z}_p$ az (5.4)-ben definiált modulo p átviteli függvény. Ekkor létezik egy olyan $\mathbb{Z}_p[x;y]$-beli redukált polinom mely a χ függvényt reprezentálja [21]. Ezt a redukált polinomot szintén χ jelölje. Megjegyezzük, hogy [9]-ben explicit formulát adtak a χ függvényt reprezentáló redukált polinomra. Számunkra azonban elegendő, hogy a χ polinom foka legfeljebb $2p-2$ és kiszámítható. E polinom elkészítéséhez szükséges idő, csak a $\mathbf{P}$ csoporttól függ, független n választásától. Ekkor

$$b_{\alpha+1}^{u_{1,\alpha+1}+u_{2,\alpha+1}} = \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})} b_{\alpha+1}^{u_{1,\alpha+1} \oplus u_{2,\alpha+1}},$$

és

$$g_1 g_2 = b_1^{u_{1,1}} \cdots b_\alpha^{u_{1,\alpha}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} \cdots \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_\alpha^{u_{2,\alpha}}\right] b_\alpha^{u_{2,\alpha}} \\ \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})} b_{\alpha+1}^{u_{1,\alpha+1} \oplus u_{2,\alpha+1}}.$$

Majd a $b_{\alpha+1}^{u_{1,\alpha+1} \oplus u_{2,\alpha+1}}$ tényezőt felcseréljük $b_1^{u_{3,1}}$ tényezővel a $g_1 g_2 g_3$ szor-

zatban:

$$\begin{aligned} g_1g_2g_3 &= b_1^{u_{1,1}}\cdots b_\alpha^{u_{1,\alpha}}\left[b_{\alpha+1}^{u_{1,\alpha+1}},b_1^{u_{2,1}}\right]b_1^{u_{2,1}}\cdots\left[b_{\alpha+1}^{u_{1,\alpha+1}},b_\alpha^{u_{2,\alpha}}\right]b_\alpha^{u_{2,\alpha}}\\ &\quad \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})}b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}b_1^{u_{3,1}}b_2^{u_{3,2}}\cdots b_\alpha^{u_{3,\alpha}}b_{\alpha+1}^{u_{3,\alpha+1}}\\ &= b_1^{u_{1,1}}\cdots b_\alpha^{u_{1,\alpha}}\left[b_{\alpha+1}^{u_{1,\alpha+1}},b_1^{u_{2,1}}\right]b_1^{u_{2,1}}\cdots\left[b_{\alpha+1}^{u_{1,\alpha+1}},b_\alpha^{u_{2,\alpha}}\right]b_\alpha^{u_{2,\alpha}}\\ &\quad \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})}\left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}},b_1^{u_{3,1}}\right]b_1^{u_{3,1}}b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}\\ &\quad b_2^{u_{3,2}}\cdots b_\alpha^{u_{3,\alpha}}b_{\alpha+1}^{u_{3,\alpha+1}}. \end{aligned}$$

Ezt az eljárást folyatjuk, míg a $b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}$ tényező $b_{\alpha+1}^{u_{3,\alpha+1}}$ mellé kerül:

$$\begin{aligned} g_1g_2g_3 &= b_1^{u_{1,1}}\cdots b_\alpha^{u_{1,\alpha}}\left[b_{\alpha+1}^{u_{1,\alpha+1}},b_1^{u_{2,1}}\right]b_1^{u_{2,1}}\cdots\left[b_{\alpha+1}^{u_{1,\alpha+1}},b_\alpha^{u_{2,\alpha}}\right]b_\alpha^{u_{2,\alpha}}\\ &\quad \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})}\left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}},b_1^{u_{3,1}}\right]b_1^{u_{3,1}}\cdots\\ &\quad \left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}},b_\alpha^{u_{3,\alpha}}\right]b_\alpha^{u_{3,\alpha}}b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}b_{\alpha+1}^{u_{3,\alpha+1}}. \end{aligned}$$

Majd összeszorozzuk $b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}$ és $b_{\alpha+1}^{u_{3,\alpha+1}}$ tényezőket

$$b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}b_{\alpha+1}^{u_{3,\alpha+1}} = \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1}\oplus u_{2,\alpha+1};u_{3,\alpha+1})}b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}\oplus u_{3,\alpha+1}},$$

így tehát

$$\begin{aligned} g_1g_2g_3 &= b_1^{u_{1,1}}\cdots b_\alpha^{u_{1,\alpha}}\left[b_{\alpha+1}^{u_{1,\alpha+1}},b_1^{u_{2,1}}\right]b_1^{u_{2,1}}\cdots\left[b_{\alpha+1}^{u_{1,\alpha+1}},b_\alpha^{u_{2,\alpha}}\right]b_\alpha^{u_{2,\alpha}}\\ &\quad \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})}\left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}},b_1^{u_{3,1}}\right]b_1^{u_{3,1}}\cdots\\ &\quad \left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}},b_\alpha^{u_{3,\alpha}}\right]b_\alpha^{u_{3,\alpha}}\left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1}\oplus u_{2,\alpha+1};u_{3,\alpha+1})}\\ &\quad b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}\oplus u_{3,\alpha+1}}. \end{aligned}$$

Ismét α új kommutátort kapunk: $\left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}},b_i^{u_{3,i}}\right]$ az összes $1\leq i\leq$ $\leq\alpha$ indexre; és egy újabb $b_{\alpha+1}^{p}$ hatványt. Ezután a $b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}\oplus u_{3,\alpha+1}}$

tényezőt visszük jobbra, stb. Általánosan, a k-adik lépésben ($1 \leq k < n-1$) a $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}}$ tényezőt felcseréljük az összes $b_i^{u_{k+1,i}}$, $1 \leq i \leq \alpha$ tényezővel. E cserékkel α új

$$\left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}}, b_i^{u_{k+1,i}}\right] \qquad (1 \leq i \leq \alpha) \tag{5.9}$$

kommutátor keletkezik. Továbbá $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}}$ és $b_{\alpha+1}^{u_{\alpha+1,k+1}}$ egymás mellé kerül a szorzatban. Ekkor összevonjuk $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}}$ és $b_{\alpha+1}^{u_{\alpha+1,k+1}}$ tényezőket:

$$\begin{aligned} &b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}} b_{\alpha+1}^{u_{\alpha+1,k+1}} = \\ &\quad = \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1};u_{k+1,\alpha+1})} b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}\oplus u_{k+1,\alpha+1}}. \end{aligned} \tag{5.10}$$

Ezzel az eljárással az összes $b_{\alpha+1}^{u_{k,\alpha+1}}$ tényezőt ($1 \leq k \leq n$) jobbra gyűjtjük és (5.10) mintájára összevonjuk ezeket. Végül a szorzat utolsó tényezője $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{n,\alpha+1}}$ lesz. Jelölje S az (5.3)-ból így kapott formális szorzatot. Jelölje T azt a formális szorzatot melyet S-ből az utolsó tényező elhagyásával kapunk. Azaz $S = T b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{n,\alpha+1}}$. Ekkor a T szorzat tényezői

- b_i hatványok valamely $1 \leq i \leq \alpha$ indexre;
- $\left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}}, b_i^{u_{k+1,i}}\right]$ alakú kommutátorok melyeket a $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}}$ és $b_i^{u_{k+1,i}}$ tényezők cseréiből kaptunk;
- $b_{\alpha+1}^{p}$ hatványok melyeket az (5.10)-beli összevonások során kaptunk.

Azaz T összes tényezője az $\mathbf{N}_\alpha$ részcsoport eleme. Az $\mathbf{N}_\alpha$ csoport p^α rendű és $\mathbf{N}_\alpha$ egy bázisa $(b_1, \ldots, b_\alpha)$. Tehát, némi technikai előkészület után, alkalmazhatjuk az indukciós feltevést a T szorzat $\mathcal{B}$-alakjának meghatározására.

A 2. lépesben az (5.9) alakú kommutátorok $\mathcal{B}$-alakjainak kiszámításával folytatjuk. Legyen $\psi_{i,j}\colon \mathbb{Z}_p^2 \to \mathbb{Z}_p$ $(1 \leq i,j \leq \alpha)$ az a függvény melyre

$$\left[b_{\alpha+1}^x, b_i^y\right] = b_1^{\psi_{i,1}(x;y)} \cdots b_\alpha^{\psi_{i,\alpha}(x;y)}.$$

Ekkor kiszámítható egy olyan $\mathbb{Z}_p[x;y]$-beli, redukált polinom mely a $\psi_{i,j}$ $(1 \leq i,j \leq \alpha)$ függvényt reprezentálja [21]. Ezt a redukált polinomot szintén $\psi_{i,j}$ jelölje. E polinom elkészítéséhez szükséges idő, csak a $\mathbf{P}$ csoporttól függ, független n választásától. A $\psi_{i,j}$ polinom foka legfeljebb $2p-2$ minden $1 \leq i,j \leq \alpha$ indexre. Speciálisan megadhatóak olyan $c_{s,t} \in \mathbb{Z}_p$ $(0 \leq s,t \leq p-1)$ konstansok, hogy

$$\psi_{i,j}(x;y) = \bigoplus_{t=0}^{p-1} \bigoplus_{s=0}^{p-1} c_{s,t} \odot x^s \odot y^t.$$

Helyettesítsük a $\psi_{i,j}(x;y)$ polinom x változóját az $x_1 \oplus \cdots \oplus x_k$ összeggel, majd bontsuk fel a zárójeleket és végezzük el a lehetséges összevonásokat minden $1 \leq i,j \leq \alpha$ és $1 \leq k < n$ indexre. Jelölje $\psi_{i,j}^{(k)} \in$ $\in \mathbb{Z}_p[x_1;\ldots;x_k;y]$ az így kapott redukált polinomot. Ekkor (5.9) $\mathcal{B}$-alakja

$$\left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus\cdots\oplus u_{k,\alpha+1}}, b_i^{u_{k+1,i}}\right] = \\ = b_1^{\psi_{i,1}^{(k)}(u_{1,\alpha+1};\ldots;u_{k,\alpha+1};u_{k+1,i})} \cdots b_\alpha^{\psi_{i,\alpha}^{(k)}(u_{1,\alpha+1};\ldots;u_{k,\alpha+1};u_{k+1,i})}. \quad (5.11)$$

Továbbá, a polinomiális tétel szerint,

$$\psi_{i,j}^{(k)}(x_1;\ldots;x_k;y) = \bigoplus_{t=0}^{p-1} \bigoplus_{s=0}^{p-1} \bigoplus_{\substack{0\leq s_1,\ldots,s_k \\ s_1+\cdots+s_k=s}} \frac{s!}{s_1!\cdots s_k!} c_{s,t} \odot x_1^{s_1} \odot \cdots \odot x_k^{s_k} \odot y^t.$$

A $\psi_{i,j}^{(k)}$ polinom s-ed fokú monomjainak száma meghatározható k elem s-ed osztályú ismétléses kombinációja segítségével. Így a monomok

száma a $\psi_{i,j}^{(k)}$ polinomban

$$\sum_{s=0}^{p-1} \binom{k+s-1}{s} = O\binom{k+p-1-1}{p-1} = O\left(k^{p-1}\right).$$

A $\psi_{i,j}^{(k)}$ polinom foka legfeljebb $2p-2$. Így $\left\|\psi_{i,j}^{(k)}\right\| \leq O\left(k^{p-1}\right)$. A $\psi_{i,j}^{(k)}$ $(1 \leq i,j \leq \alpha,\ 1 \leq k < n)$ polinomok együttesen $O\left(\sum_{k=1}^{n} k^{p-1}\right) \leq$ $\leq O\left(n^p\right)$ időben kiszámíthatóak.

A 3. lépesben az (5.10)-beli összevonások során kapott p-hatványok $\mathcal{B}$-alakjainak kiszámításával folytatjuk. Mivel $b_{\alpha+1}^p \in \mathbf{N}_\alpha$, ezért egyértelműen léteznek olyan $c_1, \ldots, c_\alpha \in \mathbb{Z}_p$ konstansok melyekre

$$b_{\alpha+1}^p = b_1^{c_1} \cdots b_\alpha^{c_\alpha},$$

azaz

$$\left(b_{\alpha+1}^p\right)^{\chi(x;y)} = b_1^{c_1 \odot \chi(x;y)} \ldots b_\alpha^{c_\alpha \odot \chi(x;y)}.$$

Helyettesítsük a $\chi(x;y)$ polinom x változóját az $x_1 \oplus \cdots \oplus x_k$ összeggel, majd bontsuk fel a zárójeleket és végezzük el a lehetséges összevonásokat minden $1 \leq i \leq \alpha$ és $1 \leq k < n$ indexre. Jelölje $\chi_i^{(k)} \in$ $\in \mathbb{Z}_p\left[x_1; \ldots; x_k; y\right]$ az így kapott redukált polinomot. Ekkor az (5.10)-beli p-hatvány $\mathcal{B}$-alakja

$$\left(b_{\alpha+1}^p\right)^{\chi(u_{1,\alpha+1} \oplus \cdots \oplus u_{k,\alpha+1}; u_{k+1,\alpha+1})} =$$
$$= b_1^{\chi_1^{(k)}(u_{1,\alpha+1};\ldots;u_{k,\alpha+1};u_{k+1,\alpha+1})} \cdots b_\alpha^{\chi_\alpha^{(k)}(u_{1,\alpha+1};\ldots;u_{k,\alpha+1};u_{k+1,\alpha+1})}. \quad (5.12)$$

Továbbá a monomok száma a $\chi_i^{(k)}$ polinomban, a $\psi_{i,j}^{(k)}$ polinomhoz hasonlóan, $O\left(k^{p-1}\right)$. A $\chi_i^{(k)}$ polinom foka legfeljebb $2p-2$. Így $\left\|\chi_i^{(k)}\right\| \leq$ $\leq O\left(k^{p-1}\right)$. A $\chi_i^{(k)}$ $(1 \leq i \leq \alpha,\ 1 \leq k < n)$ polinomok együttesen $O\left(\sum_{k=1}^{n} k^{p-1}\right) \leq O\left(n^p\right)$ időben kiszámíthatóak.

Végül a 4. lépesben alkalmazzuk az indukciós feltevést a T szorzatra. Írjuk át az $(n-1)\cdot\alpha$ darab (5.9) alakú kommutátort és az $(n-1)$ darab (5.10)-beli p-hatványt $\mathcal{B}$-alakjaikra (5.11) és (5.12) alkalmazásával. A T szorzat ezen felül még $n\cdot\alpha$ darab $b_i^{u_{k,i}}$ $(1\le i\le\alpha,\, 1\le k\le n)$ alakú tényezőt tartalmaz. Jelölje $\tilde{n}$ a T tényezőinek számát, ekkor

$$\tilde{n}=\alpha\cdot n+\alpha\cdot(n-1)+n-1=(2\alpha+1)\cdot n-\alpha-1=O(n).$$

A T szorzat minden tényezője $\mathbf{N}_\alpha$-beli, így minden $1\le\tilde{k}\le\tilde{n}$ indexhez léteznek olyan $\tilde{u}_{\tilde{k},1},\dots,\tilde{u}_{\tilde{k},\alpha}\in\mathbb{Z}_p$, hogy a $\tilde{k}$-adik tényező $\mathcal{B}$-alakja $b_1^{\tilde{u}_{\tilde{k},1}}\cdots b_\alpha^{\tilde{u}_{\tilde{k},\alpha}}$. Ha a T szorzat $\tilde{k}$-adik tényezője $b_i^{u_{k,i}}$ valamely $1\le i\le\alpha, 1\le k\le n$ indexekre, akkor

$$\tilde{u}_{\tilde{k},j}=\begin{cases}u_{k,i}, & \text{ha } j=i,\\ 0, & \text{ha } j\neq i.\end{cases}\tag{5.13}$$

Ha a T szorzat $\tilde{k}$-adik tényezője (5.9) alakú kommutátor valamely $1\le i\le\alpha$, $1\le k\le n$ indexekre, akkor

$$\tilde{u}_{\tilde{k},j}=\psi_{i,j}^{(k)}\left(u_{1,\alpha+1};\dots;u_{k,\alpha+1};u_{k+1,i}\right).\tag{5.14}$$

Végül, ha a T szorzat $\tilde{k}$-adik tényezője (5.10)-beli összevonásból származó p-hatvány valamely $1\le k\le n$ indexre, akkor

$$\tilde{u}_{\tilde{k},j}=\chi_j^{(k)}\left(u_{1,\alpha+1};\dots;u_{k,\alpha+1};u_{k+1,\alpha+1}\right).\tag{5.15}$$

Legyen $\tilde{X}_{\tilde{n},\alpha}=\left\{\,\tilde{x}_{\tilde{k},i}\;:\;1\le\tilde{k}\le\tilde{n},1\le i\le\alpha\,\right\}$. Az indukciós feltevés szerint léteznek olyan $\tilde{f}_1,\dots,\tilde{f}_\alpha\in\mathbb{Z}_p\left[\tilde{X}_{\tilde{n},\alpha}\right]$ redukált polinomok, hogy

$$T=b_1^{\tilde{f}_1(\tilde{u}_{1,1};\dots;\tilde{u}_{\tilde{n},\alpha})}\cdots b_\alpha^{\tilde{f}_\alpha(\tilde{u}_{1,1};\dots;\tilde{u}_{\tilde{n},\alpha})}.$$

Továbbá bármely $1\le l\le\alpha$ indexre az $\tilde{f}_l$ foka legfeljebb C_α, $\left\|\tilde{f}_l\right\|=$ $=O\left(\tilde{n}^{C_\alpha}\right)=O\left(n^{C_\alpha}\right)$, és $\tilde{f}_l$ kiszámítható $O\left(\tilde{n}^{C_\alpha}\right)=O\left(n^{C_\alpha}\right)$ időben.

Legyen $X_{n,\alpha+1} = \{\, x_{k,i} \,:\, 1 \le k \le n, 1 \le i \le \alpha+1 \,\}$. Az alábbiakban $1 \le l \le \alpha$ indexre definiáljuk az f_l redukált polinomot, melyet az $\tilde{f}_l$ polinomból kapunk az $\tilde{x}_{\tilde{k},j}$ változók ($1 \le \tilde{k} \le \tilde{n}, 1 \le j \le \alpha$) megfelelő (5.13), (5.14) és (5.15) szerint kapott $\mathbb{Z}_p[X_{n,\alpha+1}]$ feletti redukált polinomokkal való helyettesítésével. Legyen $1 \le \tilde{k} \le \tilde{n}$ rögzített. Ha a T szorzat $\tilde{k}$-adik tényezője $b_i^{u_{k,i}}$, valamely $1 \le i \le \alpha$, $1 \le k \le n$ indexre, akkor

$$\text{az } \tilde{x}_{\tilde{k},j} \text{ változót kicseréljük } \begin{cases} x_{k,i} \text{ változóra,} & \text{ha } j = i, \\ 0\text{-ra,} & \text{ha } j \neq i. \end{cases} \tag{5.16}$$

Ha a T szorzat $\tilde{k}$-adik tényezője (5.9) alakú kommutátor valamely $1 \le i \le \alpha$, $1 \le k \le n$ indexekre, akkor

$$\text{az } \tilde{x}_{\tilde{k},j} \text{ változót kicseréljük a } \psi_{i,j}^{(k)}\left(x_{1,\alpha+1}; \ldots, x_{k,\alpha+1}; x_{k+1,i}\right) \text{ polinomra.} \tag{5.17}$$

Végül, ha a T szorzat $\tilde{k}$-adik tényezője (5.10)-beli összevonásból származó p-hatvány valamely $1 \le k \le n$ indexre, akkor

$$\text{az } \tilde{x}_{\tilde{k},j} \text{ változót kicseréljük a } \chi_j^{(k)}\left(x_{1,\alpha+1}; \ldots, x_{k,\alpha+1}; x_{k+1,\alpha+1}\right) \text{ polinomra.} \tag{5.18}$$

Jelölje f_l azt a redukált polinomot melyet az $\tilde{f}_l$ polinomból (5.16), (5.17), (5.18) helyettesítések után, a zárójelek felbontásával és a lehetséges összevonások elvégzésével kapunk. A T szorzat $\mathcal{B}$-alakja (5.13), (5.14), és (5.15) alapján

$$T = b_1^{f_1(u_{1,1};\ldots;u_{n,\alpha+1})} \cdots b_\alpha^{f_\alpha(u_{1,1};\ldots;u_{n,\alpha+1})}.$$

Legyen

$$f_{\alpha+1}\left(x_{1,1}; \ldots; x_{n,\alpha+1}\right) = \bigoplus_{k=1}^{n} x_{k,\alpha+1},$$

ekkor a $g_1 \cdots g_n$ szorzat $\mathcal{B}$-alakja

$$g_1 \cdots g_n = b_1^{f_1(u_{1,1};\ldots;u_{n,\alpha+1})} \cdots b_\alpha^{f_\alpha(u_{1,1};\ldots;u_{n,\alpha+1})} b_{\alpha+1}^{f_{\alpha+1}(u_{1,1};\ldots;u_{n,\alpha+1})}.$$

Tehát $f_1, \ldots, f_\alpha, f_{\alpha+1}$ eleget tesznek az (5.2) feltételnek.

Mivel $C_\alpha = (2p-2)^{\alpha-1}$, legyen $C_{\alpha+1} = (2p-2)^\alpha$. Az $\tilde{f}_l$ polinom foka legfeljebb C_α a indukciós feltevés szerint. Az f_l polinomot az $\tilde{f}_l$ polinomból a változók helyettesítésével kaptuk. Az $\tilde{f}_l$ egy változóját (5.16) esetén $x_{k,i}$-vel vagy 0-val helyettesítettük, (5.17) esetén $\psi_{i,j}^{(k)}$-val helyettesítettük, (5.18) esetén $\chi_i^{(k)}$-val helyettesítettük. A $\psi_{i,j}^{(k)}$ és $\chi_i^{(k)}$ polinomok foka legfeljebb $(2p-2)$. Tehát f_l foka legfeljebb $(2p-2) \cdot C_\alpha = (2p-2)^\alpha = C_{\alpha+1}$. Másrészt $\left\|\psi_{i,j}^{(k)}\right\| \leq O\left(n^{p-1}\right)$, $\left\|\chi_i^{(k)}\right\| \leq O\left(n^{p-1}\right)$, így $\tilde{f}_l$ bármely monomjának felbontásából legfeljebb $O\left(\left(n^{(p-1)}\right)^{C_\alpha}\right) = O\left(n^{(p-1)C_\alpha}\right)$ darab monom keletkezik. Tehát

$$\|f_l\| \leq O\left(n^{(p-1)C_\alpha}\right)\left\|\tilde{f}_l\right\| \leq O\left(n^{(p-1)C_\alpha}\right) O\left(n^{C_\alpha}\right) \leq$$
$$\leq O\left(n^{(2p-2)C_\alpha}\right) \leq O\left(n^{C_{\alpha+1}}\right).$$

Az $\tilde{f}_l$ polinom változóinak helyettesítése után, a zárójelek felbontása és a lehetséges összevonások elvégzése $O\left(n^{C_{\alpha+1}}\right)$ időben kiszámítható.

Az f_l polinom kiszámításának időigénye:

- $O\left(n^{C_\alpha}\right)$ időt igényel az $\tilde{f}_l$ polinom kiszámítása;
- $O\left(n^p\right)$ időt igényel a $\psi_{i,j}^{(k)}$ polinomok kiszámítása;
- $O\left(n^p\right)$ időt igényel a $\chi_i^{(k)}$ polinomok kiszámítása;
- $O\left(n^{C_{\alpha+1}}\right)$ időt igényel f_l elkészítése az $\tilde{f}_l, \psi_{i,j}^{(k)}$ és $\chi_i^{(k)}$ polinomokból.

Figyelembe véve, hogy $p \leq 2p-2 \leq C_\alpha \leq C_{\alpha+1}$ az f_l polinom kiszámításnak időigénye

$$O\left(n^{C_\alpha} + n^p + n^p + n^{C_{\alpha+1}}\right) = O\left(n^{C_{\alpha+1}}\right).$$

□

5.2. Egyenletmegoldhatóság probléma nilpotens csoportok felett

Ebben a alfejezetben bebizonyítjuk az 5.1. tételt. Ehhez a következő lemmát fogjuk alkalmazni.

5.3. Lemma. *Legyen* $\mathbf{P}$ *egy* p^α *elemű csoport, és* T *egy tetszőleges,* n *hosszú csoportkifejezés* $\mathbf{P}$ *felett. Ekkor* $O\left(n^{\frac{1}{2}(2p-2)^\alpha\alpha}\right)$ *időben eldönthető, hogy a* $T = \mathrm{id}$ *egyenletnek van-e megoldása* $\mathbf{P}$*-ben.*

Bizonyítás. Legyen $\mathbf{P}$ egy bázisa $\mathcal{B} = (b_1, \ldots, b_\alpha)$. Legyen $T = t_1 \cdots t_n$ egy csoportkifejezés $\mathbf{P}$ felett, azaz t_k $(1 \leq k \leq n)$ egy változó vagy $\mathbf{P}$ egy eleme. Minden $1 \leq k \leq n$ indexre kicseréljük t_k-t a $b_1^{x_{k,1}} \cdots b_\alpha^{x_{k,\alpha}}$ szorzatra az alábbi módon:

- Ha t_k a $\mathbf{P}$ egy eleme, akkor legyen $x_{k,i}$ $(1 \leq i \leq \alpha)$ a $\mathbb{Z}_p$ egy olyan eleme melyre t_k $\mathcal{B}$-alakja $t_k = b_1^{x_{k,1}} \cdots b_\alpha^{x_{k,\alpha}}$ és cseréljük ki t_k-t a $b_1^{x_{k,1}} \cdots b_\alpha^{x_{k,\alpha}}$ $\mathcal{B}$-alakra.

- Ha t_k egy $\mathbf{P}$ feletti változó, akkor $x_{k,i}$ $(1 \leq i \leq \alpha)$ jelöljön egy $\mathbb{Z}_p$ feletti változót úgy, hogy x_{k_1,i_1} és x_{k_2,i_2} pontosan akkor jelölje ugyanazt a változót (valamely $1 \leq k_1, k_2 \leq n$, $1 \leq$ $\leq i_1, i_2 \leq \alpha$ indexre) ha t_1 és t_2 ugyanazt a változót jelölik $\mathbf{P}$ felett és $i_1 = i_2$. Mivel minden csoportelem $\mathcal{B}$-alakja egyértelmű, ezért ahogy $x_{k,1}, \ldots, x_{k,\alpha}$ értékei végigfutnak $\mathbb{Z}_p$ elemein, úgy a $b_1^{x_{k,1}} \cdots b_\alpha^{x_{k,\alpha}}$ kifejezés értékei végigfutnak $\mathbf{P}$ elemein. Cseréljük ki t_k-t a $b_1^{x_{k,1}} \cdots b_\alpha^{x_{k,\alpha}}$ formális szorzatra.

A T szorzat átírása a t_k tényezők $\mathcal{B}$-alakjaikra történő cseréjével $O(n)$ időt igényel.

Az 5.2. lemma alkalmazásával jellemezhetjük a $t_1 \cdots t_n$ szorzat $\mathcal{B}$-alakját. Legyen $X_{n,\alpha} = \{ x_{k,i} : 1 \leq k \leq n, 1 \leq i \leq \alpha \}$ és $C_\alpha =$ $= (2p-2)^{\alpha-1}$. Számítsuk ki az 5.2. lemmában szereplő $f_1, \ldots, f_\alpha \in$

$\in \mathbb{Z}_p[X_{n,\alpha}]$ redukált polinomokat. Ez $O\left(n^{C_\alpha}\right)$ időben megtehető. Ekkor $\|f_l\| = O\left(n^{C_\alpha}\right)$ minden $1 \leq l \leq \alpha$ indexre. Az 5.2. lemma szerint a $t_1 \cdots t_n$ szorzat $\mathcal{B}$-alakja

$$t_1 \cdots t_n = b_1^{f_1(x_{1,1};\ldots;x_{n,\alpha})} \cdots b_\alpha^{f_\alpha(x_{1,1};\ldots;x_{n,\alpha})}$$

Az id $\mathcal{B}$-alakja $\mathrm{id} = b_1^0 \cdots b_\alpha^0$. A $\mathcal{B}$-alak egyértelműsége miatt, a $t_1 \cdots t_n = \mathrm{id}$ egyenletnek pontosan akkor van megoldása $\mathbf{P}$-ben, ha az

$$\begin{aligned} f_1(x_{1,1};\ldots;x_{n,\alpha}) &= 0 \\ &\vdots \\ f_\alpha(x_{1,1};\ldots;x_{n,\alpha}) &= 0 \end{aligned} \tag{5.19}$$

egyenletrendszer megoldható $\mathbb{Z}_p$ felett. A 2.4. tétel szerint az (5.19) egyenletrendszer megoldhatósága $\mathbb{Z}_p$ felett eldönthető az alábbi időkorláton belül:

$$O\left(\max_{1\leq l\leq m} \|f_l\|^{(p-1)\alpha}\right) \leq O\left(n^{C_\alpha\cdot(p-1)\cdot\alpha}\right) \leq O\left(n^{(2p-2)^{\alpha-1}\cdot(p-1)\cdot\alpha}\right) = O\left(n^{\frac{1}{2}(2p-2)^\alpha\alpha}\right).$$

Az algoritmus időigénye:

- $O(n)$ időt igényel a t_k $(1 \leq k \leq n)$ tényezők cseréje $\mathcal{B}$-alakjaikra;
- $O\left(n^{C_\alpha}\right) = O\left(n^{(2p-2)^{\alpha-1}}\right)$ időt igényel az f_l $(1 \leq l \leq \alpha)$ redukált polinomok elkészítése;
- $O\left(n^{\frac{1}{2}(2p-2)^\alpha\alpha}\right)$ időt igényel az (5.19) egyenletrendszer megoldhatóságának eldöntése.

Tehát a $\mathbf{P}$ feletti $T = \mathrm{id}$ egyenlet megoldhatósága

$$O\left(n + n^{(2p-2)^{\alpha-1}} + n^{\frac{1}{2}(2p-2)^{\alpha}\alpha}\right) = O\left(n^{\frac{1}{2}(2p-2)^{\alpha}\alpha}\right)$$

időben eldönthető. □

Az 5.1. tétel bizonyítása. Legyenek $S = x_1 \cdots x_k$ és $T = y_1 \cdots y_n$ csoportkifejezések $\mathbf{G}$ felett úgy, hogy $k \leq n$. Tekintsük továbbá a $T' = x_k^{|\mathbf{G}|-1} \cdots x_1^{|\mathbf{G}|-1} y_1 \cdots y_n$ kifejezést. Az $S = T$ egyenletnek pontosa akkor van megoldása $\mathbf{G}$-ben ha létezik olyan helyettesítés melyre T' értéke id. Ekkor $\|T'\| \leq |\mathbf{G}| \cdot n = O(n)$, mivel $|\mathbf{G}|$ sem S-től sem T-től nem függ, így n-től is független. A továbbiakban a $T' = \mathrm{id}$ egyenletet vizsgáljuk.

Először azt az esetet vizsgáljuk, amikor $\mathbf{G}$ egy p^α rendű csoport. Az 5.3. lemma szerint a $T' = \mathrm{id}$ egyenlet megoldhatósága $\mathbf{G}$ felett $O\left(n^{\frac{1}{2}(2p-2)^{\alpha}\alpha}\right)$ időben eldönthető. Itt $|\mathbf{G}| = p^\alpha$, $\alpha \leq \log|\mathbf{G}|$, $2p-2 \leq p^2$, így

$$\frac{1}{2}(2p-2)^{\alpha}\alpha \leq \frac{1}{2}p^{2\alpha}\alpha \leq \frac{1}{2}|\mathbf{G}|^2 \log|\mathbf{G}|.$$

A második esetben $\mathbf{G}$ legyen egy nilpotens csoport és $\mathbf{P}_1, \ldots, \mathbf{P}_m$ a Sylow részcsoportjai. Ekkor $\mathbf{G}$ a Sylow részcsoportok direkt szorzata. Így $T' = \mathrm{id}$ pontosan akkor oldható meg $\mathbf{G}$ felett, ha minden $1 \leq i \leq m$ indexre $T' = \mathrm{id}$ megoldható $\mathbf{P}_i$ felett. Bármely $1 \leq i \leq m$ indexre a $T' = \mathrm{id}$ egyenlet megoldhatósága $\mathbf{P}_i$ felett $O\left(n^{\frac{1}{2}|\mathbf{P}_i|^2 \log|\mathbf{P}_i|}\right) \leq O\left(n^{\frac{1}{2}|\mathbf{G}|^2 \log|\mathbf{G}|}\right)$ időben eldönthető. Így együttesen az összes $1 \leq i \leq m$ indexre $O\left(m \cdot n^{\frac{1}{2}|\mathbf{G}|^2 \log|\mathbf{G}|}\right) = O\left(n^{\frac{1}{2}|\mathbf{G}|^2 \log|\mathbf{G}|}\right)$ időkorlát adódik, mivel m nem függ T'-től, csak a $\mathbf{G}$ csoporttól. □

6. fejezet

$\mathbf{P} \rtimes \mathbf{A}$ csoportok

Ebben a fejezetben az egyenletmegoldhatóság problémát vizsgáljuk olyan $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$ szemidirekt szorzatokra, ahol $\mathbf{P}$ egy p-csoport és $\mathbf{A}$ egy Abel-csoport. Egy általános eljárást adunk amely egységesen kezeli a legtöbb olyan feloldható de nem nilpotens csoportot melyre a korábbi tételekkel az egyenletmegoldhatóság probléma eldönthető. Sőt ez az új eljárás sok olyan csoportra is alkalmazható melyre a korábbi eredmények nem mondtak semmit.

6.1. Tétel. *Legyen* $\mathbf{P}$ *egy* p*-csoport,* $\mathbf{A}$ *egy Abel-csoport. Tekintsünk egy* $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$ *szemidirekt szorzatot. Legyenek* S *és* T *legfeljebb* n *hosszú csoportkifejezések* $\mathbf{G}$ *felett. Ekkor* $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|}\log|\mathbf{G}|}\right)$ *időben eldönthető, hogy az* $S = T$ *egyenletnek van-e megoldása* $\mathbf{G}$*-ben.*

A 6.1. tétel alkalmazásával egy hasonlóan általános eredményt bizonyítunk az ekvivalencia problémáról:

6.2. Tétel. *Legyen* $\mathbf{N}$ *nilpotens csoport,* $\mathbf{A}$ *Abel-csoport. Tekintsünk egy* $\mathbf{G} = \mathbf{N} \rtimes \mathbf{A}$ *szemidirekt szorzatot. Legyenek* S *és* T *legfeljebb* n *hosszú csoportkifejezések* $\mathbf{G}$ *felett. Ekkor* $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|}\log|\mathbf{G}|}\right)$ *időben eldönthető a* $\mathbf{G} \models S \approx T$ *ekvivalencia.*

6.1. $\mathbf{P} \rtimes \mathbf{A}$ csoportok

Az alábbi szakasz sokban emlékeztet az 5.1. szakaszra mely gondolatait és módszereit fogjuk alkalmazni.

Legyen $\mathbf{P}$ egy p^α elemű csoport, $\mathbf{A}$ egy Abel-csoport. Tekintsünk egy $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$ szemidirekt szorzatot. Vegyük $\mathbf{P}$ egy maximális centrális láncát és egészítsük ki ezt $\mathbf{G}$ egy kompozícióláncává: $\{\mathrm{id}\} = \mathbf{N}_0 \lhd \lhd \mathbf{N}_1 \lhd \cdots \lhd \mathbf{N}_\alpha = \mathbf{P} = \mathbf{M}_0 \lhd \mathbf{M}_1 \lhd \cdots \lhd \mathbf{M}_\beta = \mathbf{G}$. Ekkor $\mathbf{N}_i \lhd \mathbf{P}$ minden $1 \leq i \leq \alpha$ indexre, $\mathbf{M}_j \lhd \mathbf{G}$ minden $1 \leq j \leq \beta$ indexre, de $\mathbf{N}_i \lhd \mathbf{G}$ nem feltétlen teljesül. Az $\mathbf{N}_i/\mathbf{N}_{i-1}$ csoport izomorf a p rendű ciklikus csoporttal ($1 \leq i \leq \alpha$) és az $\mathbf{M}_j/\mathbf{M}_{j-1}$ csoport izomorf a p_j rendű ciklikus csoporttal, egy alkalmas p_j prímre ($1 \leq j \leq \beta$). Minden $1 \leq i \leq \alpha$ indexre legyen $b_i \in \mathbf{N}_i \setminus \mathbf{N}_{i-1}$ és minden $1 \leq j \leq \beta$ indexre legyen $c_j \in \in \mathbf{M}_j \setminus \mathbf{M}_{j-1}$. Ekkor $b_i\mathbf{N}_{i-1}$ az $\mathbf{N}_i/\mathbf{N}_{i-1}$ egy generátora és $c_j\mathbf{M}_{j-1}$ az $\mathbf{M}_j/\mathbf{M}_{j-1}$ egy generátora. A $\mathcal{B} = (b_1, \ldots, b_\alpha, c_1, \ldots, c_\beta)$ sorozatot a $\mathbf{G}$ csoport *bázisának* nevezünk. Legyen $g \in \mathbf{G}$ tetszőleges csoportelem. Ekkor egyértelműen léteznek olyan $u_1, \ldots, u_\alpha \in \{\, 0, 1, \ldots, p-1 \,\}$ és $v_1 \in \{\, 0, \ldots, p_1 - 1 \,\}, \ldots, v_\beta \in \{\, 0, \ldots, p_\beta - 1 \,\}$ kitevők melyekre

$$g = b_1^{u_1} \cdots b_\alpha^{u_\alpha} c_1^{v_1} \cdots c_\beta^{v_\beta}. \tag{6.1}$$

A g elem $\mathcal{B}$ bázisra vonatkozó (6.1) előállítását $\mathcal{B}$-*alaknak* nevezünk.

A $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$ csoport p-Sylow részcsoportja normálosztó melyet jelöljön $\mathbf{P}_{Syl}$. A $\mathbf{G}/\mathbf{P}_{Syl}$ csoport Abel melyet jelöljön $\mathbf{B}$. Ekkor $(|\mathbf{P}_{Syl}|, |\mathbf{B}|) = 1$, így a Shur-Zassenhaus tétel szerint $\mathbf{G} \cong \mathbf{P}_{Syl} \rtimes \mathbf{B}$. Tehát $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$ esetén $p \nmid |\mathbf{A}|$ az általánosság megszorítása nélkül feltehető.

A legkisebb p karakterisztikájú testet mely multiplikatív csoportja tartalmaz $p_1, \ldots, p_\beta$ rendű részcsoportokat a $\mathbf{G}$ csoport *alaptestének* nevezünk. Bármely $\mathbf{G}$ csoportnak létezik és kiszámítható az alapteste. Legyen ugyanis m a $p_1, \ldots, p_\beta$ prímek legkisebb közös többszöröse.

Ekkor $p \nmid |\mathbf{A}|$ miatt p és m relatív prímek, így a

$$p^x \equiv 1 \qquad \mod m$$

kongruenciának létezik minimális pozitív egész $x = s$ megoldása. Tehát $\mathbf{G}$ alapteste a p^s elemű test. Megjegyezzük, hogy $s \leq m \leq |\mathbf{A}|$, így

$$p^s \leq p^{|\mathbf{A}|}. \tag{6.2}$$

Legyen a $\mathbf{G}$ csoport alapteste $\mathbb{F}_q$. Legyen $\mathbf{S}_j \leq \mathbb{F}_q^\times$ a p_j elemű ciklikus csoport $(1 \leq j \leq \beta)$. Valamely p_j prímre jelölje a modulo p_j összeadást $\oplus_{p_j}$, a $(\{\, 0, \ldots, p_j - 1 \,\}, \oplus_{p_j})$ csoportot $\mathbf{Z}_{p_j}$ $(1 \leq j \leq \beta)$. Legyen egy rögzített izomorfizmus

$$\varphi_j \colon \mathbf{Z}_{p_j} \to \mathbf{S}_j \qquad\qquad (1 \leq j \leq \beta). \tag{6.3}$$

Legyenek $X_\alpha = \{\, x_i \,:\, 1 \leq i \leq \alpha \,\}, Y_\beta = \{\, y_j \,:\, 1 \leq j \leq \beta \,\}$. Ekkor léteznek olyan $\chi_1, \ldots, \chi_\alpha \in \mathbb{F}_q[X_\alpha; Y_\beta]$ redukált polinomok, hogy bármely $h \in \mathbf{P} \leq \mathbf{G}$ és $a \in \mathbf{A} \leq \mathbf{G}$ elemekre melyek $\mathcal{B}$-alakjai

$$h = b_1^{u_1} \cdots b_\alpha^{u_\alpha} c_1^0 \cdots c_\beta^0, \qquad\qquad a = b_1^0 \cdots b_\alpha^0 c_1^{v_1} \cdots c_\beta^{v_\beta}$$

a h^a konjugált $\mathcal{B}$-alakja

$$h^a = b_1^{\chi_1(u_1;\ldots;u_\alpha;\varphi_1(v_1);\ldots;\varphi_\beta(v_\beta))} \cdots b_\alpha^{\chi_\alpha(u_1;\ldots;u_\alpha;\varphi_1(v_1);\ldots;\varphi_\beta(v_\beta))} c_1^0 \cdots c_\beta^0. \tag{6.4}$$

Legyenek ugyanis $\tilde{\chi}_i \colon \mathbb{F}_q^{\alpha+\beta} \to \mathbb{F}_q$ $(1 \leq i \leq \alpha)$ olyan függvények melyek eleget tesznek a (6.4) feltételnek. Ekkor kiszámíthatóak azok az $\mathbb{F}_q[X_\alpha; Y_\beta]$-beli, redukált χ_i polinom melyek a $\tilde{\chi}_i$ függvényeket reprezentálják [21]. A χ_i polinom foka legfeljebb $(\alpha + \beta) \cdot (q - 1)$ és χ_i legfeljebb $q^{\alpha+\beta}$ monom összege $(1 \leq i \leq \alpha)$.

A 6.3. lemmában kiszámítjuk n darab $\mathbf{G}$-beli csoportelem szorzatának $\mathcal{B}$-alakját az elemek $\mathcal{B}$-alakjaiból redukált $\mathbb{F}_q$ feletti polinomok segítségével. A bizonyítás sokat merít az 5.2. lemma bizonyításának gondolatiból.

6.3. Lemma. *Legyen* $\mathbf{P}$ *egy* p^α *rendű csoport,* $\mathbf{A}$ *egy Abel-csoport. Tekintsünk egy* $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$ *szemidirekt szorzatot. Legyen* $\mathbf{G}$ *egy bázisa* $\mathcal{B} = (b_1, \dots, b_\alpha, c_1, \dots, c_\beta)$*. Legyen* $C_\alpha = (2p-2)^{\alpha-1}$*. Legyen* $\mathbf{G}$ *alapteste* $\mathbb{F}_q$*. Legyenek* $\varphi_1, \dots, \varphi_\beta$ *a (6.3)-beli izomorfizmusok. Egy tetszőleges* n *pozitív egészre legyen*

$$X_{n,\alpha} = \{\, x_{k,i} \;:\; 1 \le k \le n, 1 \le i \le \alpha \,\},$$
$$Y_{n-1,\beta} = \{\, y_{k,j} \;:\; 1 \le k \le n-1, 1 \le j \le \beta \,\}.$$

Ekkor léteznek olyan $f_1, \dots, f_\alpha \in \mathbb{F}_q[X_{n,\alpha}; Y_{n-1,\beta}]$ *redukált polinomok, hogy bármely* $h_1, \dots, h_n \in \mathbf{P} \le \mathbf{G}, a_1, \dots, a_n \in \mathbf{A} \le \mathbf{G}$ *elemekre melyek* $\mathcal{B}$*-alakjai*

$$h_k = b_1^{u_{k,1}} \cdots b_\alpha^{u_{k,\alpha}} c_1^0 \cdots c_\beta^0, \quad a_k = b_1^0 \cdots b_\alpha^0 c_1^{v_{k,1}} \cdots c_\beta^{v_{k,\beta}} \quad (1 \le k \le n)$$

a $h_1 a_1 \cdots h_n a_n$ *szorzat* $\mathcal{B}$*-alakja*

$$\begin{aligned} h_1 a_1 \cdots h_n a_n = & b_1^{f_1(u_{1,1};\dots;u_{n,\alpha};\varphi_1(v_{1,1});\dots;\varphi_\beta(v_{n-1,\beta}))} \cdots \\ & b_\alpha^{f_\alpha(u_{1,1};\dots;u_{n,\alpha};\varphi_1(v_{1,1});\dots;\varphi_\beta(v_{n-1,\beta}))} \cdot \\ & \cdot c_1^{v_{1,1} \oplus_{p_1} \cdots \oplus_{p_1} v_{n,1}} \cdots c_\beta^{v_{1,\beta} \oplus_{p_\beta} \cdots \oplus_{p_\beta} v_{n,\beta}}. \end{aligned}$$

Bármely $1 \le l \le \alpha$ *indexre* $\|f_l\| = O\left(n^{C_\alpha+1}\right)$*, és az* f_l *polinom kiszámítható* $O\left(n^{C_\alpha+1}\right)$ *időben. Továbbá az* f_l *polinom bármely monomja legfeljebb* $\alpha^{C_\alpha}(q-1)^{C_\alpha}$ *darab* $X_{n,\alpha}$*-beli változót tartalmaz.*

Bizonyítás. Először a $h_1 a_1 \cdots h_n a_n$ szorzat jobb oldalára gyűjtjük az a_k tényezőket $(1 \le k \le n)$. Ehhez a (2.2)-beli $xy = y^x x$ összefüggést alkalmazzuk:

$$\begin{aligned} & h_1 a_1 \cdot h_2 a_2 \cdot h_3 a_3 \cdots h_n a_n = h_1 h_2^{a_1} a_1 a_2 \cdot h_3 a_3 \cdots h_n a_n = \\ & = h_1 h_2^{a_1} h_3^{a_1 a_2} a_1 a_2 a_3 \cdots h_n a_n = \underbrace{h_1 h_2^{a_1} h_3^{a_1 a_2} \cdots h_n^{a_1 \cdots a_{n-1}}}_{\in \mathbf{P}} \underbrace{a_1 a_2 a_3 \cdots a_n}_{\in \mathbf{A}}. \end{aligned}$$

Legyen

$$T_{\mathbf{P}} = h_1 h_2^{a_1} \cdots h_n^{a_1 \cdots a_{n-1}}, \qquad T_{\mathbf{A}} = a_1 \cdots a_n. \tag{6.5}$$

Ekkor a $T_{\mathbf{A}}$ szorzat $\mathcal{B}$-alakja:

$$\begin{aligned} T_{\mathbf{A}} = a_1 \cdots a_n &= b_1^0 \cdots b_\alpha^0 c_1^{v_{1,1}} \cdots c_\beta^{v_{1,\beta}} \cdots b_1^0 \cdots b_\alpha^0 c_1^{v_{n,1}} \cdots c_\beta^{v_{n,\beta}} = \\ &= b_1^0 \cdots b_\alpha^0 c_1^{v_{1,1} \oplus_{p_1} \cdots \oplus_{p_1} v_{n,1}} \cdots c_\beta^{v_{1,\beta} \oplus_{p_\beta} \cdots \oplus_{p_\beta} v_{n,\beta}}. \end{aligned} \tag{6.6}$$

Most kiszámítjuk a (6.5)-beli $h_k^{a_1 \cdots a_{k-1}}$ konjugáltak $\mathcal{B}$-alakjait. A feltételek szerint a h_k elem $\mathcal{B}$-alakja

$$h_k = b_1^{u_{k,1}} \cdots b_\alpha^{u_{k,\alpha}} c_1^0 \cdots c_\beta^0. \tag{6.7}$$

Vegyük észre, hogy az $a_1 \cdots a_{k-1}$ szorzat $\mathcal{B}$-alakja:

$$a_1 \cdots a_{k-1} = b_1^0 \cdots b_\alpha^0 c_1^{v_{1,1} \oplus_{p_1} \cdots \oplus_{p_1} v_{k-1,1}} \cdots c_\beta^{v_{1,\beta} \oplus_{p_\beta} \cdots \oplus_{p_\beta} v_{k-1,\beta}}. \tag{6.8}$$

Továbbá a $v_{1,j} \oplus_{p_j} \cdots \oplus_{p_j} v_{k-1,j}$ összeg (6.3)-beli φ_j izomorfizmus általi képe

$$\varphi_j(v_{1,j} \oplus_{p_j} \cdots \oplus_{p_j} v_{k-1,j}) = \varphi_j(v_{1,j}) \cdots \varphi_j(v_{k-1,j}). \tag{6.9}$$

Legyenek $\chi_1, \ldots, \chi_\alpha \in \mathbb{F}_q[X_\alpha; Y_\beta]$ a (6.4)-ben szereplő redukált polinomok. Minden $1 \le i \le \alpha$ és $2 \le k \le n$ indexre helyettesítsük a χ_i polinom összes y_j változóját az $y_{1,j} \cdots y_{k-1,j}$ szorzattal ($1 \le j \le \beta$). Jelölje $\chi_i^{(k)} \in \mathbb{F}_q[X_\alpha; Y_{n-1,\beta}]$ az így kapott redukált polinomot. Ekkor a $h_k^{a_1 \cdots a_{k-1}}$ konjugált $\mathcal{B}$-alakja

$$h_k^{a_1 \cdots a_{k-1}} = b_1^{\tilde{u}_{k,1}} \cdots b_\alpha^{\tilde{u}_{k,\alpha}} c_1^0 \cdots c_\beta^0, \tag{6.10}$$

ahol (6.7), (6.8) és (6.9) alapján

$$\tilde{u}_{k,i} = \begin{cases} u_{k,i}, & \text{ha } k = 1, \\ \chi_i^{(k)}(u_{k,1}; \ldots; u_{k,\alpha}; \varphi_1(v_{1,1}); \ldots; \varphi_\beta(v_{k-1,\beta})), & \text{ha } 2 \le k \le n. \end{cases}$$

Mivel a χ_i polinom legfeljebb $q^{(\alpha+\beta)}$ monom összege, ezért $\chi_i^{(k)}$ szintén legfeljebb $q^{(\alpha+\beta)}$ monom összege. Mivel a χ_i polinom foka legfeljebb $(\alpha+\beta)(q-1)$ ezért $\chi_i^{(k)}$ foka legfeljebb $\alpha(q-1)+\beta(q-1)(k-1) = = O(k)$. Továbbá $\chi_i^{(k)}$ minden monomja legfeljebb $\alpha(q-1)$ darab X_α-beli változót tartalmaz. Így $\left\|\chi_i^{(k)}\right\| = O(k)$. A $\chi_i^{(k)}$ $(1 \le i \le \alpha, 2 \le \le k \le n)$ polinomok együttesen $\sum_{k=2}^{n} \alpha \cdot O(k) \le O(n^2)$ időben kiszámíthatóak.

Végül meghatározzuk a (6.5)-beli $T_{\mathbf{P}}$ szorzat $\mathcal{B}$-alakját az 5.2. lemma alkalmazásával. A $T_{\mathbf{P}}$ szorzat tényezői $h_1, h_2^{a_1}, \ldots, h_n^{a_1 \cdots a_{n-1}}$ mind a $\mathbf{P} \le \mathbf{G}$ részcsoport elemei. A $h_k^{a_1 \cdots a_{k-1}}$ konjugált $\mathcal{B}$-alakját (6.10)-ban jellemeztük. A $\mathbf{G}$ csoport $\mathcal{B} = (b_1, \ldots, b_\alpha, c_1, \ldots, c_\beta)$ bázisának első α tagja $(b_1, \ldots, b_\alpha)$ a $\mathbf{P}$ csoport egy bázisát alkotja. Így az 5.2. lemma alkalmazásával megadhatóak olyan $\tilde{f}_1, \ldots, \tilde{f}_\alpha \in \mathbb{Z}_p[X_{n,\alpha}]$ redukált polinomok, hogy a $T_{\mathbf{P}}$ szorzat $\mathcal{B}$-alakja

$$T_{\mathbf{P}} = b_1^{\tilde{f}_1(\tilde{u}_{1,1};\ldots;\tilde{u}_{n,\alpha})} \cdots b_\alpha^{\tilde{f}_\alpha(\tilde{u}_{1,1};\ldots;\tilde{u}_{n,\alpha})} c_1^0 \cdots c_\beta^0.$$

Legyen $C_\alpha = (2p-2)^{\alpha-1}$. Ekkor az 5.2. lemma szerint bármely $1 \le \le i \le \alpha$ indexre az $\tilde{f}_l$ foka legfeljebb C_α, $\left\|\tilde{f}_l\right\| = O\left(n^{C_\alpha}\right)$, és $\tilde{f}_l$ kiszámítható $O\left(n^{C_\alpha}\right)$ időben.

Mivel $\mathbb{Z}_p \le \mathbb{F}_q$, ezért speciálisan $\tilde{f}_l \in \mathbb{F}_q[X_{n,\alpha}]$. Minden $1 \le l \le \le \alpha$ indexre helyettesítsük az $\tilde{f}_l$ polinom összes $x_{k,i}$ változóját a $\chi_i^{(k)}$ redukált polinommal $(1 \le i \le \alpha, 2 \le k \le n)$, majd bontsuk monomok összegére a helyettesítésből származó polinomokat. Jelölje $f_1, \ldots, f_\alpha \in \in \mathbb{F}_q[X_{n,\alpha}, Y_{n-1,\beta}]$ az így kapott redukált polinomokat. A $T_{\mathbf{P}}$ szorzat $\mathcal{B}_{\mathbf{P}}$-alakja (6.10) alapján

$$\begin{aligned} T_{\mathbf{P}} = & b_1^{f_1(u_{1,1};\ldots;u_{n,\alpha};\varphi_1(v_{1,1});\ldots;\varphi_\beta(v_{n-1,\beta}))} \cdots b_\alpha^{f_\alpha(u_{1,1};\ldots;u_{n,\alpha};\varphi_1(v_{1,1});\ldots;\varphi_\beta(v_{n-1,\beta}))} \cdot \\ & \cdot c_1^0 \cdots c_\beta^0. \end{aligned} \tag{6.11}$$

Tehát a $h_1a_1 \cdots h_na_n$ szorzat $\mathcal{B}$-alakja (6.6) és (6.11) alapján

$$h_1a_1 \cdots h_na_n = T_{\mathbf{P}} \cdot T_{\mathbf{A}} =$$
$$= b_1^{f_1(u_{1,1};\ldots;u_{n,\alpha};\varphi_1(v_{1,1});\ldots;\varphi_\beta(v_{n-1,\beta}))} \cdots b_\alpha^{f_\alpha(u_{1,1};\ldots;u_{n,\alpha};\varphi_1(v_{1,1});\ldots;\varphi_\beta(v_{n-1,\beta}))} \cdot$$
$$\cdot\, c_1^{h_1(v_{1,1};\ldots;v_{n,1})} \cdots c_\beta^{h_\beta(v_{1,\beta};\ldots;v_{n,\beta})}.$$

Az f_l polinomot az $\tilde{f}_l$ polinomból az $x_{k,i}$ változók $\chi_i^{(k)}$ polinomokkal történő helyettesítésével kaptuk. Az 5.2. Lemma szerint az $\tilde{f}_l$ polinom foka C_α. Továbbá $\tilde{f}_l$ legfeljebb $\|f_l\|$ monom összege. A $\chi_i^{(k)}$ polinom foka $O(k) \leq O(n)$ és $\chi_i^{(k)}$ legfeljebb $q^{\alpha+\beta}$ monom összege. Továbbá $\chi_i^{(k)}$ bármely monomja legfeljebb $\alpha \cdot (q-1)$ darab $X_{n,\alpha}$-beli változót tartalmaz. Tehát $\tilde{f}_l$ bármely monomjának felbontásából legfeljebb $\left(q^{\alpha+\beta}\right)^{C_\alpha}$ monom keletkezik, f_l foka legfeljebb $C_\alpha \cdot O(n)$ és

$$\|f_l\| = \left\|\tilde{f}_l\right\| \cdot \left(q^{\alpha+\beta}\right)^{C_\alpha} \cdot C_\alpha \cdot O(n) = O\left(n^{C_\alpha}\right) \cdot O(n) = O\left(n^{C_\alpha+1}\right).$$

Továbbá f_l bármely monomja legfeljebb $\alpha^{C_\alpha} \cdot (q-1)^{C_\alpha}$ darab $X_{n,\alpha}$-beli változót tartalmaz. Az $\tilde{f}_l$ polinom $\chi_i^{(k)}$ polinomokkal történő helyettesítése és a kapott polinom monomok összegére bontása $O\left(n^{C_\alpha+1}\right)$ időben kiszámítható.

Az f_l polinom kiszámításának időigénye:

- $O\left(n^{C_\alpha}\right)$ időt igényel az $\tilde{f}_l$ polinom kiszámítása;
- $O(n^2)$ időt igényel a $\chi_i^{(k)}$ polinomok kiszámítása;
- $O\left(n^{C_\alpha+1}\right)$ időt igényel f_l elkészítése az $\tilde{f}_l$ és $\chi_i^{(k)}$ polinomokból.

Figyelembe véve, hogy $2 \leq C_\alpha$ az f_l polinom kiszámításnak időigénye

$$O\left(n^{C_\alpha} + n^2 + n^{C_\alpha+1}\right) = O\left(n^{C_\alpha+1}\right).$$

□

6.2. Egyenletmegoldhatóság probléma $\mathbf{P} \rtimes \mathbf{A}$ csoportok felett

Ebben az alfejezetben bebizonyítjuk a 6.1. tételt. Ehhez a következő lemmát fogjuk alkalmazni.

6.4. Lemma. *Legyen* $\mathbf{P}$ *egy* p^α *elemű csoport,* $\mathbf{A}$ *egy* $p_1 \cdots p_\beta$ *rendű Abel csoport. Tekintsünk egy* $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$ *szemidirekt szorzatot. Legyen* $C_\alpha = (2p-2)^{\alpha-1}$. *Legyen* $\mathbf{G}$ *alapteste* $\mathbb{F}_q$. *Legyen* T *egy tetszőleges,* n *hosszú csoportkifejezés* $\mathbf{G}$ *felett. Ekkor* $O\left(n^{(C_\alpha+1)(q-1)(\alpha+\beta)}\right)$ *időben eldönthető, hogy a* $T = \mathrm{id}$ *egyenletnek van-e megoldása* $\mathbf{G}$*-ben.*

Bizonyítás. Legyenek az $\mathbf{A}$ csoport kompozíciófaktorai rendre izomorfak a $\mathbf{Z}_{p_1}, \ldots, \mathbf{Z}_{p_\beta}$ ciklikus csoportokkal. Legyen a $\mathbf{G}$ csoport egy bázisa $\mathcal{B} = (b_1, \ldots, b_\alpha, c_1, \ldots, c_\beta)$. Legyen $T = t_1 \cdots t_n$ egy polinom $\mathbf{G}$ felett, azaz t_k $(1 \leq k \leq n)$ egy változó vagy $\mathbf{G}$ egy eleme. Minden $1 \leq k \leq n$ indexre kicseréljük t_k-t a $b_1^{x_{k,1}} \cdots b_\alpha^{x_{k,\alpha}} c_1^{z_{k,1}} \cdots c_\beta^{z_{k,\beta}}$ szorzatra az alábbi módon:

- Ha t_k a $\mathbf{G}$ egy eleme, akkor legyenek $x_{k,i}$ $(1 \leq i \leq \alpha)$ a $\mathbb{Z}_p$ és $z_{k,j}$ a $\mathbf{Z}_{p_j}$ $(1 \leq j \leq \beta)$ olyan elemei melyekre a t_k elem $\mathcal{B}$-alakja $t_k = b_1^{x_{k,1}} \cdots b_\alpha^{x_{k,\alpha}} c_1^{z_{k,1}} \cdots c_\beta^{z_{k,\beta}}$ és cseréljük ki t_k-t erre a $b_1^{x_{k,1}} \cdots b_\alpha^{x_{k,\alpha}} c_1^{z_{k,1}} \cdots c_\beta^{z_{k,\beta}}$ $\mathcal{B}$-alakra.

- Ha t_k egy $\mathbf{G}$ feletti változó, akkor $x_{k,i}$ $(1 \leq i \leq \alpha)$ jelöljön egy $\mathbb{Z}_p$ feletti változót úgy, hogy x_{k_1,i_1} és x_{k_2,i_2} pontosan akkor jelölje ugyanazt a változót (valamely $1 \leq k_1, k_2 \leq n$, $1 \leq i_1, i_2 \leq \leq \alpha$ indexre) ha t_1 és t_2 ugyanazt a változót jelölik $\mathbf{G}$ felett és $i_1 = i_2$. Hasonlóan $z_{k,j}$ jelöljön egy $\mathbf{Z}_{p_j}$ feletti változót $(1 \leq j \leq \leq \beta)$ úgy, hogy z_{k_1,j_1} és z_{k_2,j_2} pontosan akkor jelölje ugyanazt a változót (valamely $1 \leq k_1, k_2 \leq n$, $1 \leq j_1, j_2 \leq \beta$ indexre) ha t_1 és t_2 ugyanazt a változót jelölik $\mathbf{G}$ felett és $j_1 = j_2$. Mivel a $\mathbf{G}$-beli elemek $\mathcal{B}$-alakjai egyértelműek, ezért ahogy $x_{k,1}, \ldots, x_{k,\alpha}$

értékei végigfutnak $\mathbb{Z}_p$ elemein és $z_{k,j}$ értékei a $\mathbf{Z}_{p_j}$ elemein, úgy a $b_1^{x_{k,1}} \cdots b_\alpha^{x_{k,\alpha}} c_1^{z_{k,1}} \cdots c_\beta^{z_{k,\beta}}$ kifejezés értékei végigfutnak $\mathbf{G}$ elemein. Cseréljük ki t_k-t a $b_1^{x_{k,1}} \cdots b_\alpha^{x_{k,\alpha}} c_1^{z_{k,1}} \cdots c_\beta^{z_{k,\beta}}$ formális szorzatra.

A t_k tényezők $\mathcal{B}$-alakjaikra történő cseréje $O(n)$ időt igényel.

Legyen $\varphi_j \colon \mathbf{Z}_{p_j} \to \mathbf{S}_j$ a (6.3)-ban definiált izomorfizmus ($1 \le j \le \beta$). Minden $1 \le k \le n$ és $1 \le j \le \beta$ indexre definiáljuk $y_{k,j}$-t a következőképp:

- Ha $z_{k,j}$ a $\mathbf{Z}_{p_j}$ egy eleme, akkor legyen $y_{k,j} = \varphi_j(z_{k,j})$.
- Ha $z_{k,j}$ egy $\mathbf{Z}_{p_j}$ feletti változó, akkor $y_{k,j}$ jelöljön egy $\mathbf{S}_j$ feletti változót úgy, hogy y_{k_1,j_1} és y_{k_2,j_2} pontosan akkor jelölje ugyanazt a változót (valamely $1 \le k_1, k_2 \le n$, $1 \le j_1, j_2 \le \beta$ indexre) ha z_{k_1,j_1} és z_{k_2,j_2} ugyanazt a változót jelölik $\mathbf{Z}_{p_j}$ felett. Ahogy $z_{k,j}$ értékei végigfutnak $\mathbf{Z}_{p_j}$ elemein, úgy a $\varphi_j(z_{k,j})$ értékei végigfutnak $\mathbf{S}_j$ elemein.

Az $y_{k,j}$-k elkészítése $O(n)$ időt igényel.

A 6.3. lemma segítségével jellemezzük a $t_1 \cdots t_n$ szorzat $\mathcal{B}$-alakját. Számítsuk ki a 6.3. lemmában szereplő $f_1, \ldots, f_\alpha$ redukált $\mathbb{F}_q$ feletti polinomokat. Ez $O\left(n^{C_\alpha+1}\right)$ időben megtehető. Ekkor a 6.3. lemma szerint a $t_1 \cdots t_n$ szorzat $\mathcal{B}$-alakja

$$t_1 \cdots t_n = b_1^{f_1(x_{1,1};\ldots;x_{n,\alpha};y_{1,1};\ldots;y_{n-1,\beta})} \cdots b_\alpha^{f_\alpha(x_{1,1};\ldots;x_{n,\alpha};y_{1,1};\ldots;y_{n-1,\beta})} \cdot c_1^{z_{1,1} \oplus_{p_1} \cdots \oplus_{p_1} z_{n,1}} \cdots c_\beta^{z_{1,\beta} \oplus_{p_\beta} \cdots \oplus_{p_\beta} z_{n,\beta}}.$$

Itt $x_{k,i}$ a $\mathbb{Z}_p$ egy elemét vagy egy $\mathbb{Z}_p$ feletti változót jelöl, $y_{k,j}$ az $\mathbf{S}_j$ egy elemét vagy egy $\mathbf{S}_j$ feletti változót jelöl, és $z_{k,j}$ a $\mathbf{Z}_{p_j}$ egy elemét vagy egy $\mathbf{Z}_{p_j}$ feletti változót jelöl. Az id $\mathcal{B}$-alakja $\mathrm{id} = b_1^0 \cdots b_\alpha^0 c_1^0 \cdots c_n^0$. A $\mathcal{B}$-alak egyértelműsége miatt a $t_1 \cdots t_n = \mathrm{id}$ egyenletnek pontosan

akkor van megoldása, ha az

$$\begin{aligned} f_1|_{\mathbb{Z}_p,\mathbf{S}_1,\ldots,\mathbf{S}_\beta}(x_{1,1},\ldots,x_{n,\alpha},y_{1,1},\ldots,y_{n-1,\beta}) &= 0_{\mathbb{F}_q} \\ &\vdots \\ f_\alpha|_{\mathbb{Z}_p,\mathbf{S}_1,\ldots,\mathbf{S}_\beta}(x_{1,1},\ldots,x_{n,\alpha},y_{1,1},\ldots,y_{n-1,\beta}) &= 0_{\mathbb{F}_q} \\ z_{1,1} \oplus_{p_1} \cdots \oplus_{p_1} z_{n,1} &= 0_{\mathbf{Z}_{p_1}} \\ &\vdots \\ z_{1,\beta} \oplus_{p_\beta} \cdots \oplus_{p_\beta} z_{n,\beta} &= 0_{\mathbf{Z}_{p_\beta}} \end{aligned} \tag{6.12}$$

egyenletrendszernek van olyan megoldása melyre $\varphi_j(z_{k,j}) = y_{k,j}$ minden $1 \leq k \leq n$, $1 \leq j \leq \beta$ indexre. A (6.12) egyenletrendszer első α egyenlete $\mathbb{F}_q$ feletti, míg a következő β egyenlet rendre $\mathbf{Z}_{p_1},\ldots,\mathbf{Z}_{p_\beta}$ feletti. Ez utóbbi β egyenletet lefordítjuk $\mathbb{F}_q$ feletti egyenletekké. Vegyük észre, hogy a (6.3)-beli φ_j izomorfizmus definíciója és az $y_{k,j}$ definíciója alapján bármely $1 \leq j \leq \beta$ indexre

$$z_{1,j} \oplus_{p_j} \cdots \oplus_{p_j} z_{n,j} = 0_{\mathbf{Z}_{p_j}} \qquad \Leftrightarrow \qquad y_{1,j} \cdots y_{n,j} = 1_{\mathbb{F}_q}.$$

Legyen $f(x_1;\ldots;x_n) = \prod_{k=1}^{n} x_k - 1$. Ekkor a (6.12) egyenletrendszernek pontosan akkor van $\varphi_j(z_{k,j}) = y_{k,j}$ $(1 \leq k \leq n, 1 \leq j \leq \beta)$ feltételeknek eleget tevő megoldása, ha az

$$\begin{aligned} f_1|_{\mathbb{Z}_p,\mathbf{S}_1,\ldots,\mathbf{S}_\beta}(x_{1,1},\ldots,x_{n,\alpha},y_{1,1},\ldots,y_{n-1,\beta}) &= 0_{\mathbb{F}_q} \\ &\vdots \\ f_\alpha|_{\mathbb{Z}_p,\mathbf{S}_1,\ldots,\mathbf{S}_\beta}(x_{1,1},\ldots,x_{n,\alpha},y_{1,1},\ldots,y_{n-1,\beta}) &= 0_{\mathbb{F}_q} \\ f|_{\mathbf{S}_1}(y_{1,1};\ldots;y_{n,1}) &= 0_{\mathbb{F}_q} \\ &\vdots \\ f|_{\mathbf{S}_\beta}(y_{1,\beta};\ldots;y_{n,\beta}) &= 0_{\mathbb{F}_q} \end{aligned} \tag{6.13}$$

egyenletrendszer megoldható $\mathbb{F}_q$ felett. A 6.3. lemma szerint az f_i $(1 \leq i \leq \alpha)$ polinom bármely monomja legfeljebb $\alpha^{C_\alpha} \cdot (q-1)^{C_\alpha}$ darab $X_{n,\alpha}$-beli változót tartalmaz. Az $f_1, \ldots, f_\alpha, f$ polinomok hosszának maximuma $O\left(n^{C_\alpha+1}\right)$. Tehát a (6.13) egyenletrendszer megoldhatósága a 2.5. következmény segítségével

$$O\left(n^{(C_\alpha+1)(q-1)(\alpha+\beta)}\right)$$

időben eldönthető.

A $\mathbf{G}$ feletti $T = \mathrm{id}$ egyenlet megoldhatóságát eldöntő algoritmus időigénye:

- $O(n)$ időt igényel a t_k $(1 \leq k \leq n)$ tényezők cseréje $\mathcal{B}$-alakjaikra;
- $O(n)$ időt igényel az összes $y_{k,j}$ $(1 \leq k \leq n, 1 \leq j \leq \beta)$ elkészítése;
- $O\left(n^{C_\alpha+1}\right)$ időt igényel az f_l $(1 \leq l \leq \alpha)$ és f redukált polinomok elkészítése;
- $O\left(n^{(C_\alpha+1)(q-1)(\alpha+\beta)}\right)$ időt igényel a (6.13) egyenletrendszer megoldhatóságának eldöntése.

Tehát a $\mathbf{G}$ feletti $T = \mathrm{id}$ egyenlet megoldhatósága

$$O\left(n + n + n^{C_\alpha+1} + n^{(C_\alpha+1)(q-1)(\alpha+\beta)}\right) = O\left(n^{(C_\alpha+1)(q-1)(\alpha+\beta)}\right)$$

időben eldönthető. □

A 6.1. tétel bizonyítása. Legyenek $S = x_1 \cdots x_k$ és $T = y_1 \cdots y_n$ csoportkifejezések $\mathbf{G}$ felett úgy, hogy $k \leq n$. Tekintsük továbbá a $T' = x_k^{|\mathbf{G}|-1} \cdots x_1^{|\mathbf{G}|-1} y_1 \cdots y_n$ kifejezést. Ekkor az $S = T$ egyenletnek pontosa akkor van megoldása $\mathbf{G}$-ben ha létezik olyan helyettesítés melyre T' értéke id. Itt $\|T'\| \leq |\mathbf{G}| \cdot n = O(n)$, mivel $|\mathbf{G}|$ sem S-től sem T-től

nem függ, így n-től is független. A továbbiakban a $T' = \mathrm{id}$ egyenletet vizsgáljuk.

A 6.4. lemma szerint a $\mathbf{G}$ feletti $T' = \mathrm{id}$ egyenlet megoldhatósága eldönthető $O\left(n^{(C_\alpha+1)(q-1)(\alpha+\beta)}\right)$ időben. Itt $|\mathbf{G}| = p^\alpha p_1 \cdots p_\beta$, így

$$\alpha + \beta \leq \log |\mathbf{G}|,$$
$$C_\alpha + 1 = (2p-2)^{\alpha-1} + 1 \leq 2 \cdot (2p)^{\alpha-1} \leq p^{2\alpha-1}.$$

Másrészt (6.2) szerint $q \leq p^{|\mathbf{A}|}$. Mivel $2\alpha + |\mathbf{A}| \leq 2^\alpha + |\mathbf{A}| \leq |\mathbf{P}| + |\mathbf{A}| \leq |\mathbf{G}| + 1$, így

$$(C_\alpha + 1)(q-1) < p^{2\alpha-1} p^{|\mathbf{A}|} \leq |\mathbf{G}|^{|\mathbf{G}|}.$$

Tehát

$$(C_\alpha + 1)(q-1)(\alpha+\beta) \leq |\mathbf{G}|^{|\mathbf{G}|} \log |\mathbf{G}|.$$

□

6.3. Ekvivalencia probléma $\mathbf{N} \rtimes \mathbf{A}$ csoportok felett

A 6.2. tétel bizonyítása. Legyenek $S = x_1 \cdots x_k$ és $T = y_1 \cdots y_n$ csoportkifejezések $\mathbf{G}$ felett úgy, hogy $k \leq n$. Tekintsük továbbá a $T' = x_k^{|\mathbf{G}|-1} \cdots x_1^{|\mathbf{G}|-1} y_1 \cdots y_n$ kifejezést. Ekkor $\mathbf{G} \models T \approx S$ pontosan akkor, ha minden helyettesítésre T' értéke id. Itt $\|T'\| \leq |\mathbf{G}| \cdot n = O(n)$. A továbbiakban a $\mathbf{G} \models T' \approx \mathrm{id}$ ekvivalenciát vizsgáljuk.

Jelölje az $\mathbf{N}$ nilpotens csoport Sylow részcsoportjait $\mathbf{P}_1, \ldots, \mathbf{P}_m$. Ekkor $\mathbf{N}$ a Sylow részcsoportok direkt szorzata. A $\mathbf{P}_l$ Sylow részcsoport karakterisztikus $\mathbf{N}$-ben, így $\mathbf{P}_l \trianglelefteq \mathbf{G}$ $(1 \leq l \leq m)$. Ezért $\mathbf{A}$ hatása

$\mathbf{N}$-en leírható az $\mathbf{A}$ csoport $\mathbf{P}_1, \ldots, \mathbf{P}_m$ csoportokra gyakorolt hatásaival. Tehát $\mathbf{G} \models T' \approx \mathrm{id}$ pontosan akkor, ha $\mathbf{P}_l \rtimes \mathbf{A} \models T' \approx \mathrm{id}$ különkülön minden $1 \leq l \leq m$ indexre. Valamely l indexre $\mathbf{P}_l \rtimes \mathbf{A} \models T' \approx \mathrm{id}$ pontosan akkor *nem* teljesül, ha $T' = g$ megoldható egy $\mathrm{id} \neq g \in$ $\in \mathbf{P}_l \rtimes \mathbf{A}$ csoportelemre. Mivel $\mathbf{P}_l \rtimes \mathbf{A} \leq |\mathbf{G}|$ nem függ n-től, a $\mathbf{P}_l \rtimes \mathbf{A} \models T' \approx \mathrm{id}$ ekvivalencia eldönthető a $\mathbf{P}_l \rtimes \mathbf{A}$ feletti egyenletmegolthatóság probléma időkorlátján belül. Azaz a 6.1. tétel alkalmazásával $\mathbf{P}_l \rtimes \mathbf{A} \models T' \approx \mathrm{id}$ eldönthető

$$O\left(n^{|\mathbf{P}_l \rtimes \mathbf{A}|^{|\mathbf{P}_l \rtimes \mathbf{A}|} \log|\mathbf{P}_l \rtimes \mathbf{A}|}\right) \leq O\left(n^{|\mathbf{G}|^{|\mathbf{G}|} \log|\mathbf{G}|}\right)$$

időben. Tehát a $\mathbf{G} \models T' \approx \mathrm{id}$ ekvivalencia $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|} \log|\mathbf{G}|}\right)$ időben eldönthető. □

Irodalomjegyzék

[1] S. Burris – J. Lawerence: The equivalence problem for finite rings. *Journal of Symbolic Computation*, 15. évf. (1993), 67–71. p.

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

[3] P. Diaconis – I.M. Isaacs: Counting characters of upper triangular groups. *Trans. Amer. Math. Soc.*, 360. évf. (2008), 2359–2392. p.

[4] A. Földvári: The complexity of the equation solvability problem over nilpotent groups. *Journal of Algebra*, 2017. elfogadva.

[5] A. Földvári: The complexity of the equation solvability problem over semipattern groups. *International Journal of Algebra Computation*, 27. évf. (2017) 2. sz., 259–272. p.

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

[7] M. Goldmann – A. 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.

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

[9] G. Grasegger – G. Horváth – K. A. Kearnes: Polynomial equivalence of finite rings. *Journal of the Australian Math Society*, 96. évf. (2014) 2. sz., 244–257. p.

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

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

[12] G. Horváth: The complexity of the equivalence end equation solvability problems over meta-abelian groups. *Journal of Algebra*, 433. évf. (2015), 208–230. p.

[13] G. Horváth – J. Lawerence – R. Willard: The equation solvability problem over finite rings. 2017. kézirat.

[14] G. Horváth – J. Lawrence – L. Mérai – Cs. Szabó: The complexity of the equivalence problem for non-solvable groups. *Bulletin of the London Mathematical Society*, 39. évf. (2007) 3. sz., 433–438. p.

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

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

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

[18] I.M. Isaacs: Counting characters of upper triangular groups. *Journal of Algebra*, 315. évf. (2007) 2. sz., 698–719. p.

[19] Gy. Károlyi – Cs. Szabó: The complexity of the equation solvablity problem over nilpotent rings. 2017. benyújtva.

[20] J. Lawrence – R. Willard: The complexity of solving polynomial equations over finite rings. 1997. kézirat.

[21] B. R. MacDonald: *Finite rings with identity*. 1974, Marcel Dekker.

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

[23] P. Péladeau – D. Thérien: Sur les langages reconnus par des groupes nilpotents. *Comptes Rendus de l'Académie des Sciences - Series I - Mathematics*, 306. évf. (1988) 2. sz., 93–95. p.

[24] Cs. Szabó – V. Vértesi: The equivalence problem over finite rings. *International Journal of Algebra and Computation*, 21. évf. (2011) 3. sz., 449–457. p.

[25] D. Thérien: Subword counting and nilpotent groups. In *Combinatorics on words (Waterloo, Ont., 1982)*. Toronto, Ont., 1983, Academic Press, 297–305. p.

[26] R. S. Wilson: On the stucture of finite rings. *Compositio Mathematica*, 26. évf. (1973) 1. sz., 79–93. p.