**Egyetemi doktori (PhD) értekezés tézisei**

# Az egyenletmegoldhatóság probléma bonyolultsága véges csoportok felett

**Földvári Attila**

Témavezető: Dr. Horváth Gábor
egyetemi docens


DEBRECENI EGYETEM

Matematika- és Számítástudományok Doktori Iskola

Debrecen, 2017.

# Tézisek

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 $f, g$ input polinomokra az $f = g$ egyenlet megoldható-e. Azaz létezik-e olyan helyettesítés melyre az $f$ és $g$ polinomok értékei megegyeznek. Egy másik hasonló kérdés, hogy az input polinomok értékei *minden* helyettesítésre azonosake. Az $\mathcal{R}$ véges gyűrű feletti *ekvivalencia* probléma azt kérdezi, hogy az $f, g$ input polinomok ekvivalensek-e $\mathcal{R}$ felett (jelölésben $\mathcal{R} \models f \approx g$). Azaz $f$ és $g$ 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. A bonyolultságot az input polinomok hosszában vizsgáljuk. Egy $f$ polinom *hosszán* az $f$-ben szereplő változók és konstansok multiplicitással vett számát értjük, jele $\|f\|$. Jelölje továbbá a kettes alapú logaritmust log.

Az első eredmények Hunttól és Stearnstől [14] származnak, akik kommutatív gyűrűk felett vizsgálták az ekvivalencia probléma bonyolultságát. 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 ex-

ponenciális is lehet az eredeti polinom hosszában. A polinomok hosszának ez a változása befolyásolhatja az ekvivalencia probléma bonyolultságát. Ez motiválta Lawrence-t és Willardot [16] 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 [18] bebizonyították a sejtés coNP-teljes részét. Horváth [8] kommutatív gyűrűkre igazolta a sejtést. A polinomiális rész teljes bizonyítása Horváth, Lawrence és Willard [10] 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 [18]-ban 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 [10]-ben 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 [7]-ben bebizonyította, hogy ha a gyűrű nilpotens, akkor az egyenletmegoldhatóság probléma polinomidőben eldönthető. Horváth megmutatta, hogy ha $f$ és $g$ 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 $f = g$ egyenletnek van-e megoldása $\mathcal{R}$-ben. Itt a korlát kitevőjében szereplő torony magassága $\mathcal{R}$ nilpotenciaosztálya. Horváth a [7] 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. Wilson [20] karakterizációs tétele segítségével megmutatjuk, hogy egy tetszőleges nilpotens gyűrű feletti egyenlet megoldhatósága eldönthető néhány speciális mátrixgyűrű feletti egyenlet megoldhatóságának vizsgálatával. Majd hatékony eljárást adunk ezen speciális mátrixgyűrűk feletti egyenletmegoldhatóság probléma eldöntésére. Így 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, $f$ és $g$ 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 $f=g$ egyenletnek van-e megoldása $\mathcal{R}$-ben.*

Ezt az eredményt [4]-ben publikáltam. Megemlítjük, hogy egy ettől teljesen független úton, Károlyi és Szabó később tovább javította az időkorlátot [15]-ben.

A véges gyűrűk után természetesen adódott a véges csoportok feletti egyenletmegolthatóság és az ekvivalencia problémák bonyolultságának vizsgálata. Egy $\mathbf{G}$ véges csoport feletti *csoportkifejezés* alatt változók és $\mathbf{G}$-beli elemek formális szorzatát értjük. A $\mathbf{G}$ 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. Célunk ezen döntési problémák számítási bonyolultságának meghatározása adott csoportokra. A bonyolultságot az input kifejezések hosszában vizsgáljuk. Egy $T=t_1\cdots t_n$ csoportkifejezés *hosszát* $n$-nek definiáljuk, jele $\|T\|$.

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 [11] bizonyították a sejtés coNP-teljes részét. A polinomiális részt Horváth és Szabó [13] igazolták olyan $\mathbf{G} \simeq \simeq \mathbf{A} \rtimes \mathbf{B}$ csoportokra melyekre $\mathbf{A}$ és $\mathbf{B}$ Abel csoportok, $\mathbf{A}$ exponense négyzetmentes és $(|\mathbf{A}|, |\mathbf{B}|) = 1$. Később Horváth [9]-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 [9]-ben található.

Az egyenletmegoldhatóság probléma bonyolultsága még több csoportra ismeretlen. Goldmann és Russell [5, 6] 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 [17, 19] cikkeiből származik. A bizonyítás teljes megértéséhez és a pontos időkorlát meghatározásához tehát több cikk [5, 6, 17, 19] alapos tanulmányozása szükséges. Később Horváth [7] közvetlen bizonyítást adott mely hasonlít a fenti három cikkből összeállítható gon-

dolatmenetre de önmagában is érthető. Megmutatta, hogy ha $S$ és $T$ legfeljebb $n$ hosszú csoportkifejezések a $\mathbf{G}$ nilpotens 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 [7] 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. Ehhez egy $\mathbf{G}$ nilpotens csoport feletti egyenletmegoldhatóság problémát visszavezetünk a $\mathbf{G}$ csoport $p$-Sylow részcsoportjai feletti egyenletmegoldhatóság problémákra. Majd a $p$-csoportok policiklikus reprezentációját alkalmazva egy $p$-csoport felett adott csoportkifejezést $\mathbb{Z}_p$ test feletti polinomok segítségével jellemzünk. Ezzel a módszerrel hatékonyan tudunk dönteni az egyenletmegoldhatóságról nilpotens csoportok felett. Így 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 [3]-ban 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 [13], vagy $\mathbf{G}$ izomorf a negyedfokú alternáló csoporttal [12], akkor az egyenletmegoldhatóság probléma $\mathbf{G}$ felett polinomidőben eldönthető. Később Horváth [9] 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 [9] cikk 3. problémájában az $\mathbf{SL}(2, \mathbb{Z}_3)$ csoport fölött; a [9] 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 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 dolgozatban a felső háromszögmátrixok szorzatát a mátrixok elemei segítségével jellemezük. Így egy szemipattern csoport felett adott csoportkifejezés leírható a kifejezés szorzatmátrixának elemei segítségével. Ezzel a módszerrel hatékonyan tudunk dönteni a szemipattern csoport feletti egyenlet megoldhatóságáról. Így többek között megválaszoljuk Horváth $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$ csoportra vonatkozó kérdését [9, 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 [4]-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 [9, 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 a* $\mathbf{G}$ *csoport 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.*

Megjegyezzük, hogy ez az általános eljárás a szemipattern csoportokra is alkalmazható, azonban $|\mathbf{G}|^{|\mathbf{G}|}\log|\mathbf{G}|$ az időkorlátjának kitevője, szemben a speciálisan szemipattern csoportokra adott $|\mathbf{G}|\log^2|\mathbf{G}|$ kitevővel.

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.

# Theses

One of the oldest problems of algebra is the equation solvability problem over a given algebraic structure. Nowadays, many such classical problems arise in a new perspective, namely to consider their computational complexity. In this paper we investigate the complexity of the equation solvability problem over finite groups and rings.

The *equation solvability problem* over a finite ring $\mathcal{R}$ asks whether or not two polynomials can attain the same value for some substitution over $\mathcal{R}$. In other words, for the equation solvability problem, one needs to decide if there exists at least one substitution satisfying the equation. Another interesting problem is whether or not *all* substitutions satisfy the equation. The *equivalence problem* over a finite ring $\mathcal{R}$ asks whether or not two polynomials $f$ and $g$ are equivalent over $\mathcal{R}$ (denoted by $\mathcal{R} \models f \approx g$) that is whether or not $f$ and $g$ determine the same function over $\mathcal{R}$. We investigate the complexities of these problems in the length of the input polynomials. The length of a polynomial $f$ is the number of constants and variables occurring in the polynomial $f$ with multiplicity (denoted by $||f||$). Let log denote the base 2 logarithm.

First Hunt and Stearnes [14] investigated the equivalence problem for finite commutative rings. Later Burris and Lawrence [1] generalized their result to non-commutative rings. They proved that if $\mathcal{R}$ is nilpotent then the equivalence problem over $\mathcal{R}$ is solvable in polynomial time, while if $\mathcal{R}$ is not nilpotent then the equivalence problem over $\mathcal{R}$ is coNP-complete. The proof of Burris and Lawrence reduces the satisfiability (SAT) problem to the equivalence problem by using long products of sums of variables. Nevertheless, if we expand this polynomial into a sum of monomials then the length of the new polynomial may become exponential in the length of the original polynomial. Such a change in the length suggests that the complexity of the equivalence problem might be

different if the input polynomials are restricted to be written as sums of monomials. This motivated Lawrence and Willard [16] to introduce the *sigma problems*, where the input polynomials are given as sums of monomials. Lawrence and Willard conjectured that if the factor by the Jacobson radical is commutative then the sigma equivalence problem is solvable in polynomial time. While if the factor by the Jacobson radical is not commutative then the sigma equivalence problem is coNP-complete. Szabó and Vértesi proved the coNP-complete part of the conjecture in [18]. Horváth confirmed the conjecture for commutative rings in [8]. The polynomial part of this conjecture is completely proved in the manuscript [10]. Therefore the complexity of the equivalence problem and the sigma equivalence problem was completely characterized.

Now, we summarize the results for the equation solvability and the *sigma* equation solvability. Using the method of Szabó and Vértesi [18] it is easy to prove that if the factor by the Jacobson radical is not commutative then the sigma equation solvability problem is NP-complete. Horváth, Lawrence and Willard [10] proved that if the ring is not nilpotent but its factor by the Jacobson radical is commutative then the sigma equation solvability problem is solvable in polynomial time. For the general equation solvability, arguments of Burris and Lawrence from [1] yield that if the ring is not nilpotent then the problem is NP-complete. Horváth in [7] proved that if the ring is nilpotent then the equation solvability problem is solvable in polynomial time. He proved that if $f$ and $g$ are polynomials over a finite nilpotent ring $\mathcal{R}$ with length at most $n$, then it can be decided in $O\left(n^{|\mathcal{R}|^{|\mathcal{R}|^{\cdots^{|\mathcal{R}|}}}}\right)$ time whether or not the equation $f = g$ has a solution in $\mathcal{R}$. Here, the height of the tower is the nilpotency class of $\mathcal{R}$. Horváth explicitly asks in [7, Problem 3] whether the exponent of the time complexity can be bounded by a polynomial in the size of the ring $\mathcal{R}$. In Chapter 3 we answer Horváth's question [7, Problem 3] for nilpotent rings by

significantly decreasing the exponent of the time complexity. Wilson [20] characterizes nilpotent rings with the help of special kind of nilpotent matrix rings. We give an efficient method for deciding the equation solvability problem over these special matrix rings. In particular, we show that equation solvability over a nilpotent ring $\mathcal{R}$ can be decided in polynomial time, where the degree of the polynomial is $|\mathcal{R}|^{2\log|\mathcal{R}|}\log^5|\mathcal{R}|$.

**Theorem** (Theorem 3.1.)**.** *Let $\mathcal{R}$ be a nilpotent ring. Let $f$ and $g$ be polynomials over $\mathcal{R}$ with length at most $n$. Then it can be decided in $O\left(n^{|\mathcal{R}|^{2\log|\mathcal{R}|}\log^5|\mathcal{R}|}\right)$ time whether or not the equation $f = g$ has a solution in $\mathcal{R}$.*

This result is published in [4]. Later Károlyi and Szabó [15] further decreased the exponent.

After investigating finite rings, it is natural to consider finite groups. The *equation solvability problem* over a finite group $\mathbf{G}$ asks whether or not two group expressions (i.e. products of variables and elements of $\mathbf{G}$) can attain the same value for some substitution over $\mathbf{G}$. In other words, for the equation solvability problem, one needs to find if there exists at least one substitution satisfying the equation. The *equivalence problem* over a finite group $\mathbf{G}$ asks whether or not two group expressions $S$ and $T$ are equivalent over $\mathbf{G}$ (denoted by $\mathbf{G} \models S \approx T$), that is whether or not $f$ and $g$ determine the same function over $\mathbf{G}$. We investigate the complexities of these problems in the length of the input group expressions, that is in the number of variables and constants occurring in them. We denote the length of an expression $T$ by $||T||$.

First Burris and Lawrence [2] investigated the complexity of the equivalence problem over finite groups. They proved that if a group $\mathbf{G}$ is nilpotent or $\mathbf{G} \simeq \mathbf{D}_n$, the dihedral group for odd $n$, then the equivalence problem for $\mathbf{G}$ has polynomial time complexity. They conjectured that if $\mathbf{G}$ is solvable then the equivalence

problem over $\mathbf{G}$ is in P, and if $\mathbf{G}$ is not solvable then the equivalence problem over $\mathbf{G}$ is coNP-complete. Horváth, Lawrence, Mérai and Szabó [11] proved the coNP-complete part of the conjecture. Horváth and Szabó [13] confirmed the conjecture for $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ and $\mathbf{B}$ are Abelian groups such that the exponent of $\mathbf{A}$ is squarefree and $(|\mathbf{A}|, |\mathbf{B}|) = 1$. Later Horváth [9] generalized this result to semidirect products $\mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ and $\mathbf{B}/C_{\mathbf{B}}(\mathbf{A})$ are Abelian groups (here $C_{\mathbf{B}}(\mathbf{A})$ denotes the centralizer of $\mathbf{A}$ in $\mathbf{B}$). But the complexity of the equivalence problem over many solvable, not nilpotent groups is not determined, yet. Three of the smallest groups, for which this complexity is not known, are $\mathbf{S}_4$, $\mathbf{SL}(2, \mathbb{Z}_3)$ and $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$ (this third group is a non-commutative group of order 54). See [9] for a more comprehensive list.

Even less is known about the equation solvability problem. Goldmann and Russell [5, 6] proved that if $\mathbf{G}$ is not solvable, then the equation solvability problem is NP-complete, while if $\mathbf{G}$ is nilpotent then the equation solvability problem over $\mathbf{G}$ is solvable in polynomial time. In their papers, they reduce the equation solvability problem over a finite nilpotent group $\mathbf{G}$ to recognizing languages by non-uniform finite automata over $\mathbf{G}$. In their reduction they apply the results of Péladeau and Thérien [17, 19] in a fundamental manner. This way, it is easy to get lost in the chain of thoughts if one wants to recover how the algorithm of Goldmann and Russell manipulates the input group expressions $S$ and $T$ in order to determine whether or not the equation $S = T$ has a solution over $\mathbf{G}$. Furthermore, the algorithm is known to be polynomial in the sizes of $S$ and $T$, but the degree of this polynomial is not explicitly stated. The reduction in [5, 6] applies Ramsey's theorem, suggesting that the degree of the polynomial is multiply exponential. Later Horváth [7] gave a straight proof for nilpotent groups only using group expressions and directly arriving at the Ramsey argument. He proved that if $S$ and $T$ are group expressions over a finite nilpotent group $\mathbf{G}$ with length at most $n$,

then it can be decided in $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|^{\cdots^{|\mathbf{G}|}}}}\right)$ time whether or not the equation $S = T$ has a solution in $\mathbf{G}$. Here, the height of the tower is the nilpotency class of $\mathbf{G}$. Horváth explicitly asks in [7, Problem 3] whether the exponent of the time complexity can be bounded by a polynomial in the size of the group $\mathbf{G}$. In Chapter 5 we answer Horváth's question [7, Problem 3] for nilpotent groups by significantly decreasing the exponent of the time complexity. With the polycyclic presentation of $p$-groups we give a completely new approach to representing group expressions. In particular, we show that equation solvability over a nilpotent group $\mathbf{G}$ can be decided in polynomial time, where the degree of the polynomial is $O\left(n^{\frac{1}{2}|\mathbf{G}|^2 \log |\mathbf{G}|}\right)$.

**Theorem** (Theorem 5.1.)**.** *Let* $\mathbf{G}$ *be a nilpotent group,* $S, T$ *be group expressions over* $\mathbf{G}$ *with length at most* $n$*. Then it can be decided in* $O\left(n^{\frac{1}{2}|\mathbf{G}|^2 \log |\mathbf{G}|}\right)$ *time whether or not the equation* $S = T$ *has a solution in* $\mathbf{G}$*.*

This result is published in [3].

Not much is known for solvable, non-nilpotent groups. Horváth and Szabó proved that the equation solvability problem over $\mathbf{G}$ is decidable in polynomial time if $|\mathbf{G}| = pq$ for primes $p \neq q$ [13], or if $\mathbf{G}$ is the alternating group acting on four points [12]. Later, Horváth [9] proved that the equation solvability problem over $\mathbf{G}$ is decidable in polynomial time for groups $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A} \simeq \mathbf{Z}_{p^k}$ or $\mathbf{Z}_{2p^k}$ or $\mathbf{Z}_p^k$ and $\mathbf{B}$ is commutative. Note that all results for the equation solvability problem over solvable, not nilpotent groups are about groups $\mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ and $\mathbf{B}$ are Abelian. Three of the smallest groups, for which the complexity of the equivalence and equation solvability problems is not known, are $\mathbf{S}_4$, $\mathbf{SL}(2, \mathbb{Z}_3)$ and $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$. Horváth explicitly asks the complexity of these problems over $\mathbf{SL}(2, \mathbb{Z}_3)$ in [9, Problem 3] and over $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$ in [9, Problem 4].

In Chapter 4 we investigate the the complexity of the equivalence and equation solvability problems over semipattern groups. We say that a group $A \rtimes B$ is a *semipattern group* if $\mathbf{A}$ is a subgroup of the group of upper unitriangular matrices, and $\mathbf{B}$ is a subgroup of the diagonal matrices. With the help of matrix multiplication we reduce the solvability of the input equation over a semipattern group over a finite field to the solvability of a system of equations over the same field. This way, we give an efficient method for deciding the equivalence and equation solvability problems over semipattern groups. This way, we answer Horváth's question [9, Problem 4] for the group $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$.

**Theorem** (Theorem 4.1.)**.** *Let* $\mathbf{G}$ *be a semipattern group,* $S, T$ *be group expressions over* $\mathbf{G}$ *with length at most* $n$*. Then it can be decided in* $O\left(n^{|\mathbf{G}| \log^2 |\mathbf{G}|}\right)$ *time whether or not the equation* $S = T$ *has a solution in* $\mathbf{G}$*. Furthermore it can be decided in* $O\left(n^{|\mathbf{G}| \log^2 |\mathbf{G}|}\right)$ *time whether or not* $\mathbf{G} \models S \approx T$ *holds.*

This result is published in [4].

In Chapter 6 we give a new method for deciding the equation solvability over some solvable, non-nilpotent groups. This method covers most of the cases from [9], and can be applyied for many groups for which the complexity was not yet known. In particular, we answer Horváth's question [9, Problem 3] for the group $\mathbf{SL}(2, \mathbb{Z}_3)$.

**Theorem** (Theorem 6.1.)**.** *Let* $\mathbf{G} \simeq \mathbf{P} \rtimes \mathbf{A}$*, where* $\mathbf{P}$ *is a finite p-group and* $\mathbf{A}$ *is a finite Abelian group. Let* $S, T$ *be group expressions over* $\mathbf{G}$ *with length at most* $n$*. Then it can be decided in* $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|} \log |\mathbf{G}|}\right)$ *time whether or not the equation* $S = T$ *has a solution in* $\mathbf{G}$*.*

**Theorem** (Theorem 6.2.)**.** *Let* $\mathbf{G} \simeq \mathbf{N} \rtimes \mathbf{A}$*, where* $\mathbf{N}$ *is a finite nilpotent group and* $\mathbf{A}$ *is a finite Abelian group. Let* $S, T$ *be group expressions over* $\mathbf{G}$ *with length at most* $n$*. Then it can be decided in* $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|}\log|\mathbf{G}|}\right)$ *time whether or not* $\mathbf{G} \models S \approx T$ *holds.*

Note, that the method describe in Chapter 6 is more general than the one in Chapter 4, and can be applied for semipattern groups, as well. However, the exponent of the time complexity is larger ($|\mathbf{G}|^{|\mathbf{G}|}\log|\mathbf{G}|$) in the general case than in the semipattern case ($|\mathbf{G}|\log^2|\mathbf{G}|$).

# Irodalomjegyzék/References

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

[4] 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.

[5] 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.

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

[7] 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.

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

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

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

[11] 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.

[12] 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.

[13] 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.

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

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

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

[17] 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.

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

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

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

# Publikációs jegyzék / List of publications

1. Attila Földvári: The complexity of the equation solvability problem over nilpotent groups. *Journal of Algebra*, 2017, megjelenés alatt.

2. Attila Földvári: The complexity of the equation solvability problem over semipattern groups. *International Journal of Algebra and Computation*, 27 (2), 259–272, 2017.

3. Földvári Attila: Egyenletmegoldhatóság bonyolultsága szemipattern csoportok felett (könyvrészlet). *„Együtt a biztosabb tudományos karrierért, a jövőtervezésért": PEME VII. Ph.D. konferencia* 322–345, 2013.

4. Durkó Emília – Földvári Attila: Biomasszából előállított tömörítvények gazdasági értékelése (könyvrészlet). *Interdiszciplináris kutatás – a Debreceni Egyetem Hallgatóinak tanulmányai*, 66–79, 2011.

A disszertációban ismertetett új eredmények az 1–3. publikációkon alapulnak.

# Előadások / List of talks

1. The complexity of the equation solvability problem over groups. *Arbeitstagung Allgemeine Algebra – 93th Workshop on General Algebra*, Bern, Svájc, 2017

2. Egyenletmegoldhatóság bonyolultsága néhány véges csoport felett, *MTA Rényi Intézet, Algebra Szeminárium* (szemináriumi előadás), Budapest, 2017

3. Egyenletmegoldhatóság bonyolultsága véges csoportok felett, *Miskolci Egyetem Matematikai Intézet* (szemináriumi előadás), Miskolc, 2017

4. Egyenletmegoldhatóság bonyolultsága véges csoportok felett. *Eszterházy Károly Egyetem Matematikai és Informatikai Intézet* (szemináriumi előadás), Eger, 2017

5. The complexity of the equation solvability problem over semipattern groups, *CSM – The 4th Conference of PhD Students in Mathematics*, Szeged, 2016

6. The equivalence and equation solvability problems over some finite groups, *The 40th SMS of University of Silesia Session*, Szczyrk, Lengyelország, 2016

7. Egyenletmegoldhatóság bonyolultsága véges csoportok felett, *Debreceni Egyetem Algebra és Számelmélet Tanszék* (szemináriumi előadás), Debrecen, 2016

8. The equivalence and equation solvability problems over some finite groups, *Arbeitstagung Allgemeine Algebra – 87th Workshop on General Algebra*, Linz, Ausztria, 2014

9. The equivalence and equation solvability problems over some finite groups, *The 10th International Students' Conference on Analysis*, Síkfőkút, 2014

DEBRECENI EGYETEM
EGYETEMI ÉS NEMZETI KÖNYVTÁR
H-4002 Debrecen, Egyetem tér 1, Pf.: 400
Tel.: 52/410-443, e-mail: publikaciok@lib.unideb.hu

Nyilvántartási szám: DEENK/337/2017.PL
Tárgy: PhD Publikációs Lista

Jelölt: Földvári Attila
Neptun kód: A42IWL
Doktori Iskola: Matematika- és Számítástudományok Doktori Iskola
MTMT azonosító: 10057599

## A PhD értekezés alapjául szolgáló közlemények

Magyar nyelvű könyvrészletek (1)

1. **Földvári, A.**: Egyenletmegoldhatóság bonyolultsága szemipattern csoportok felett. In: "Együtt a biztosabb tudományos karrierért, a jövőtervezésért" című VII. Ph.D.-Konferencia előadásai (Budapest, 2013. október. 11.). Szerk.: Koncz István, Szova Ilona, Professzorok az Európai Magyarországért Egyesület, Budapest, 322-345, 2013. ISBN: 9789638991508

Idegen nyelvű tudományos közlemények külföldi folyóiratban (2)

2. **Földvári, A.**: The complexity of the equation solvability problem over nilpotent groups. *J. Algebra. [Epub]*, [1-15], 2017. ISSN: 0021-8693.
DOI: http://dx.doi.org/10.1016/j.jalgebra.2017.10.002
IF: 0.61 (2016)

3. **Földvári, A.**: The complexity of the equation solvability problem over semipattern groups. *Int. J. Algebr. Comput. 27* (02), 259-272, 2017. ISSN: 0218-1967.
DOI: http://dx.doi.org/10.1142/S0218196717500126
IF: 0.396 (2016)

DEBRECENI EGYETEM
EGYETEMI ÉS NEMZETI KÖNYVTÁR
H-4002 Debrecen, Egyetem tér 1, Pf.: 400
Tel.: 52/410-443, e-mail: publikaciok@lib.unideb.hu

## További közlemények

Magyar nyelvű könyvrészletek (1)

4. Durkó, E., **Földvári, A.**: Biomasszából előállított tömörítvények gazdasági értékelése. In: Interdiszciplináris kutatás : a Debreceni Egyetem hallgatóinak tanulmányai. Szerk.: Mező Ferenc, Debreceni Egyetemi K., Debrecen, 66-79, 2011. ISBN: 9789633181201

**A közlő folyóiratok összesített impakt faktora: 1,006**
**A közlő folyóiratok összesített impakt faktora (az értekezés alapjául szolgáló közleményekre): 1,006**

A DEENK a Jelölt által az iDEa Tudóstérbe feltöltött adatok bibliográfiai és tudománymetriai ellenőrzését a tudományos adatbázisok és a Journal Citation Reports Impact Factor lista alapján elvégezte.

Debrecen, 2017.10.27.

UNIVERSITY AND NATIONAL LIBRAY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

Registry number: DEENK/337/2017.PL
Subject: PhD Publikációs Lista

Candidate: Attila Földvári
Neptun ID: A42IWL
Doctoral School: Doctoral School of Mathematical and Computational Sciences
MTMT ID: 10057599

**List of publications related to the dissertation**

Hungarian book chapters (1)

1. **Földvári, A.**: Egyenletmegoldhatóság bonyolultsága szemipattern csoportok felett.
   In: "Együtt a biztosabb tudományos karrierért, a jövőtervezésért" című VII. Ph.D.-Konferencia előadásai (Budapest, 2013. október. 11.). Szerk.: Koncz István, Szova Ilona, Professzorok az Európai Magyarországért Egyesület, Budapest, 322-345, 2013. ISBN: 9789638991508

Foreign language scientific articles in international journals (2)

2. **Földvári, A.**: The complexity of the equation solvability problem over nilpotent groups.
   *J. Algebra. [Epub]*, [1-15], 2017. ISSN: 0021-8693.
   DOI: http://dx.doi.org/10.1016/j.jalgebra.2017.10.002
   IF: 0.61 (2016)

3. **Földvári, A.**: The complexity of the equation solvability problem over semipattern groups.
   *Int. J. Algebr. Comput. 27* (02), 259-272, 2017. ISSN: 0218-1967.
   DOI: http://dx.doi.org/10.1142/S0218196717500126
   IF: 0.396 (2016)

UNIVERSITY AND NATIONAL LIBRAY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

## List of other publications

Hungarian book chapters (1)

4. Durkó, E., **Földvári, A.**: Biomasszából előállított tömörítvények gazdasági értékelése. In: Interdiszciplináris kutatás : a Debreceni Egyetem hallgatóinak tanulmányai. Szerk.: Mező Ferenc, Debreceni Egyetemi K., Debrecen, 66-79, 2011. ISBN: 9789633181201

**Total IF of journals (all publications): 1,006**
**Total IF of journals (publications related to the dissertation): 1,006**

The Candidate's publication data submitted to the iDEa Tudóstér have been validated by DEENK on the basis of Web of Science, Scopus and Journal Citation Report (Impact Factor) databases.

27 October, 2017