Složitost unifikačních problémů ve varietách idempotentních pologrup

TEZE DISERTAČNÍ PRÁCE

Ondřej Klíma

Katedra Algebry a Geometrie, Přírodovědecká Fakulta Masarykovy Univerzity, Janáčkovo nám. 2a, 662 95 Brno, klima@math.muni.cz

1 Unifikační teorie

Unifikační teorie je částí teoretické informatiky, která se ocitá na pomezí informatiky a univerzální algebry. Aplikace unifikační teorie lze nalézt v takových oborech teoretické informatiky, jako jsou automatické dokazování či logické programování. Jako základní literaturu, ve které se lze seznámit s touto teorií, doporučuji přehledy [3, 4].

Zjednodušeně řečeno, unifikační teorie pojednává o řešení rovnic. Prvním problémem, který se v odborné literatuře objevil, byl „syntaktický unifikační problém“: instancí tohoto problému je dvojice termů nad množinou proměnných obsahující libovolné funkční symboly, a otázkou je, zda existuje substituce, která by oba termy ztotožnila.

Například, nechť $f(x,y) \stackrel{?}{=} f(b,a)$ je instancí problému, kde x a y jsou proměnné, f je binární funkční symbol a a a b jsou konstantní funkční symboly. Hledanou substitucí, která řeší danou rovnici, je potom $\{x \mapsto b, y \mapsto a\}$.

V okamžiku, kdy uvažujeme, že dané funkční symboly vyskytující se v termech, mají jisté sémantické vlastnosti, dostáváme se k pojmu „ekvacionální unifikace“ v jisté „teorii“. Z pohledu univerzální algebry lze takový problém interpretovat tak, že „řešení“ rovnic nehledáme v absolutně volné algebře všech termů daného jazyka, ale v relativně volné algebře ve varietě všech algeber splňujících jistou množinu identit (teorii).

Pokud se vrátíme k předchozímu příkladu a budeme předpokládat, že funkční symbol f je komutativní, neboli splňuje identitu $f(x,y) = f(y,x)$, dostáváme taktéž řešení $\{x \mapsto a, y \mapsto b\}$.

Oproti syntaktickému unifikačnímu problému, který je řešitelný (dokonce v lineárním čase), může být ekvacionální unifikační problém neřešitelný, jak je tomu kupříkladu pro teorii komutativních okruhů, kde je unifikační problém jen jinou formulací známého desátého Hilbertova problému, jehož neřešitelnost dokázal Matiyasevich [16, 6].

Nejdůležitější teorie, ve kterých se ekvacionální unifikační problém studuje jsou teorie binárního symbolu, který je asociativní, komutativní, nebo idempotentní, případně splňuje některé tyto vlastnosti současně. V tomto článku se budeme zabývat pouze těmito teoriemi, proto uvedeme v následující části precizní definici ekvacionální unifikace pouze v rámci teorie asociativního binárního symbolu.

2 Základní definice a výsledky

Pro libovolnou množinu Σ značíme volnou pologrupu nad touto množinou Σ^+. Pro každou varietu pologrup $\mathcal{V}$ a množinu Σ značíme $\sim_{\mathcal{V}}^{\Sigma}$ úplně invariantní kongruenci na volné pologrupě Σ^+, takovou, že $\Sigma^+/_{\sim_{\mathcal{V}}^{\Sigma}}$ je volná pologrupa ve varietě $\mathcal{V}$ nad množinou Σ.

Buď C spočetná množina konstant a X spočetná množina proměnných. *Rovnicí* rozumíme uspořádanou dvojici $(L, R) \in (C \cup X)^+ \times (C \cup X)^+$; píšeme $L \stackrel{?}{=} R$. *Systém* je konečná neprázdná množina rovnic $S = \{L_1 \stackrel{?}{=} R_1, \ldots, L_n \stackrel{?}{=} R_n\}$, přičemž hovoříme o *systému s konstantní pravou stranou* pokud $R_i \in C^+$ pro všechna $i = 1, \ldots, n$.

Řekneme, že zobrazení $\alpha : X \to (C \cup X)^+$ je *substituce*, jestliže *vzor* tohoto zobrazení $\mathrm{Dom}(\alpha) = \{x \in X \mid \alpha(x) \neq x\}$ je konečná množina. Každé zobrazení $\alpha : X \to (C \cup X)^+$ lze jednoznačným způsobem rozšířit na homomorfismus $\overline{\alpha} : (C \cup X)^+ \to (C \cup X)^+$, který se chová na množině konstant C jako identita.

Řešení systému $S = \{L_1 \stackrel{?}{=} R_1, \ldots, L_n \stackrel{?}{=} R_n\}$ ve varietě pologrup $\mathcal{V}$ je substituce $\alpha : X \to (C \cup X)^+$ taková, že $\overline{\alpha}(L_i) \sim_{\mathcal{V}}^{C \cup X} \overline{\alpha}(R_i)$ pro všechna $i = 1, \ldots, n$.

Definice 1 *Buď $\mathcal{V}$ varieta pologrup. $\mathcal{V}$-unifikační problém má jako instanci daný systém rovnic a otázkou je, zda existuje řešení tohoto systému ve varietě $\mathcal{V}$. $\mathcal{V}$-matching problém je speciálním případem $\mathcal{V}$-unifikačního problému, kde uvažujeme pouze systémy s konstantní pravou stranou.*

Prvotním úkolem unifikační teorie je zjistit, zda je pro danou teorii (varietu) unifikační problém řešitelný. Pokud ano, objevují se dva směry úvah, kterými se lze dále ubírat — složitost problému a popis množiny všech řešení. Základním pojmem v druhém směru úvah je potom unifikační typ, který se definuje následovně.

Na množině všech substitucí lze přirozeným způsobem zavést kvaziuspořádání: pro $\alpha, \beta : X \to (C \cup X)^+$ klademe $\alpha \leq \beta$, pokud existuje substituce $\gamma : X \to (C \cup X)^+$ taková, že $\overline{\gamma} \circ \alpha = \beta$. Řešení α daného systému S se nazývá *minimální*, pokud pro libovolné řešení β systému S platí $\beta \leq \alpha \implies \alpha \leq \beta$. Množina minimálních řešení M systému S se nazývá *úplná*, jestliže pro každé řešení β systému S existuje $\alpha \in M$, $\alpha \leq \beta$.

Řekneme, že varieta $\mathcal{V}$ má unifikační typ *unitární*, pokud má každý řešitelný systém jednoprvkovou úplnou množinu minimálních řešení; má unifikační typ *finitární*, pokud má každý systém konečnou úplnou množinu minimálních řešení; má unifikační typ *infinitární*, pokud má každý systém úplnou množinu minimálních řešení (ta může být i nekonečná); a konečně, má unifikační typ *nula*, pokud existuje systém, pro nějž úplná množina minimálních řešení neexistuje.

Pro ilustraci uveďme, že varieta všech pologrup $\mathcal{S}$ má unifikační typ infinitární, což ukázal Plotkin [19] — například rovnice $xy \stackrel{?}{=} yx$ má minimální řešení $\alpha(x) = z^k, \alpha(y) = z^l$, kde k, l jsou navzájem nesoudělná přirozená čísla. Varieta $\mathcal{C}$ všech komutativních pologrup má unifikační typ finitární (viz. [22]). Základní výsledky o unifikaci dávají, že syntaktická unifikace je typu unitárního (viz. [20]). První příklad teorie s unifikačním typem nula popsali Fages a Huet [7], avšak později Baader [1] a Schmidt-Schauss [21] popsali nezávisle mnohem přirozenější příklad teorie typu nula, kterým je varieta všech idempotentních pologrup (bandů) $\mathcal{B}$. Tím se tato varieta stala pro unifikační teorii důležitou.

Dříve něž přistoupíme k prezentaci vlastních výsledků, zmíníme se stručně o známých výsledcích ve varietách $\mathcal{S}$, $\mathcal{C}$ a $\mathcal{SL}$ (varietě všech polosvazů, tj. idempotentních komutativních pologrup).

První, značně komplikovaný, algoritmus řešící $\mathcal{S}$-unifikační problém, o němž nebylo po dlouhou dobu známo zda je vůbec řešitelný, popsal Makanin [15] v roce 1977. Po mnoho let byl tento algoritmus vylepšován, až byla snížena původní nedeterministická trojitě exponenciální časová složitost na exponenciální prostorovou složitost. V posledních době publikoval Plandowski [18] nový algoritmus, který je ve třídě PSpace. Na druhou stranu není obtížné ukázat, že $\mathcal{S}$-unifikační problém je NP-těžký, přičemž se všeobecně očekává, že se nakonec podaří ukázat, že jde o problém NP-úplný. Více informací lze nalézt v přehledu [14].

$\mathcal{C}$-unifikační problém koresponduje s řešením lineárních rovnic nad přirozenými čísly a existuje o něm rozsáhlá literatura. Problém je NP-úplný, pokud však uvažujeme pouze systémy bez konstant, unifikační problém je řešitelný v polynomiálním čase.

Poslední podstatný problém je $\mathcal{SL}$-unifikační problém. Zde se jedná vlastně o řešení rovnic v množinách a snadno se nahlédne, že tento problém je řešitelný v polynomiálním čase. Poznamenejme ještě, že varieta $\mathcal{SL}$ má unifikační typ finitární.

3 Naše výsledky

Výsledky, které zde uvedu byly publikovány v článku [10] (plná verze vyšla jako technický report [11]) a dále jsou obsahem dvou článků na kterých v současné době pracuji [12, 13].

Řešitelnost $\mathcal{B}$-unifikačního problému plyne snadno z faktu, že idempotentní pologrupy jsou lokálně konečné (viz. [8]). Přestože $\mathcal{B}$-unifikační problém byl v unifikační teorii studován, první výsledek týkající se jeho složitosti se objevil až po několika letech.

Věta 1 ([10]) *$\mathcal{B}$-matching problém je NP-úplný.*

Nedeterministický polynomiální algoritmus je založen na faktu, že každý řešitelný systém (s konstantní pravou stranou) má polynomiálně velké řešení. Důkaz tohoto tvrzení používá přepisovací systém, řešící problém identit pro idempotentní pologrupy, který byl objeven Siekmanem a Szabó [23]. Bohužel tato metoda nelze aplikovat na obecné systémy, kde „nejkratší" řešení systému může být i exponenciálně velké v závislosti na velikosti daného systému. Přesto se podařilo (později) nalézt algoritmus, který dává stejný výsledek pro unifikační problém.

Věta 2 ([13]) *$\mathcal{B}$-unifikační problém je NP-úplný.*

Co se týká důkazu NP-těžkosti, je zajímavé, že naše redukce z klasického NP-úplného problému 3-SAT používá pouze tři konstanty. To znamená, že tato redukce dává taktéž NP-těžkost $\mathcal{V}$-unifikačního problému pro libovolnou varietu idempotentních pologrup $\mathcal{V}$, která obsahuje volný band nad tří prvkovou množinou. Kromě takových variet však již existuje jen několik „jednoduchých" variet bandů, takže se nabízelo popsat složitost unifikačních problémů pro všechny variety bandů, což se nakonec též podařilo. Popis svazu všech variet bandů, který je pro důkaz následujícího výsledku nezbytný, lze nalézt v připravovaném článku [12]. My zde uvedeme jednodušší formulaci, která v sobě navíc zahrnuje i předchozí dva výsledky.

Věta 3 ([12]) *Buď $\mathcal{V}$ varieta bandů. Pokud varieta $\mathcal{V}$ splňuje identitu $xyzx = xzyx$, potom je $\mathcal{V}$-unifikační problém řešitelný v polynomiálním čase, a pokud ji nesplňuje, potom je NP-úplný. Pokud varieta $\mathcal{V}$ splňuje identitu $xyxzx = xyzx$, potom je $\mathcal{V}$-matching problém řešitelný v polynomiálním čase, a pokud ji nesplňuje, potom je NP-úplný.*

Poznamenejme, že charakterizaci unifikačního typu pro variety bandů podal již dříve Baader [2].

4 Související otázky — další výzkum

Další problémy, kterými se hodlám v disertační práci zabývat, jsou některé speciální problémy, kdy systém sestává pouze z jedné rovnice, případně obsahuje pouze jednu neznámou.

Podobnou charakterizaci složitosti, jako jsme podali ve větě 3, lze též udat pro obecný unifikační problém, kde se vyskytují další neinterpretované funkční symboly. Kupříkladu, obecný unifikační problém v polosvazech je NP-úplný, jak již bylo dokázáno dříve [9]. Předpokládám, že tato zobecnění budou též součástí disertační práce.

Dalším problémem studovaným v unifikační teorii je problém počtu řešení. Protože unifikační typ idempotentních pologrup je nula, má smysl tento problém uvažovat pouze pro matching problém. Očekávám, že metody používané v důkazu věty 2 povedou k určení složitosti tohoto problému.

Naprosto odlišný pohled na řešení rovnic je problém EQN_M, který prezentují autoři článků [5, 17], kdy není dána varieta pologrup $\mathcal{V}$, ale konkrétní konečná pologrupa či monoid M (EQN_M má jako instanci systém rovnic s parametry z M a otázkou je, zda má tento systém v M řešení). Zajímavé je, že hranice složitosti mezi polynomiálně řešitelnými a NP-úplnými problémy (ta existuje pokud

P≠NP) vychází pro idempotentní monoidy stejně jako v případě unifikace, přestože se prozatím nedá říci, že jeden výsledek lze obdržet pomocí druhého či naopak. Ze spolupráce s autory zmíněných článků by měl vzejít popis složitosti EQN_M problému pro libovolný monoid (pologrupu) M a jeho analogie pro rovnice s konstantní pravou stranou ($T - EQN_M$). Tyto výsledky by se případně taktéž mohly stát součástí disertační práce, pokud se podaří nalézt podstatné souvislosti.

Reference

[1] Baader F.: The Theory of Idempotent Semigroups is of Unification Type Zero, J. of Automated Reasoning **2** (1986) 283–286.

[2] Baader F.: Unification in Varieties of Idempotent Semigroups, Semigroup Forum **36** (1987) 127–145.

[3] Baader F., Siekmann J. H.: Unification Theory, Handbook of Logic in Artificial Intelligence and Logic Programming (1993), Oxford University Press.

[4] Baader F., Snyder W.: Unification Theory, Handbook of Automated Reasoning (2001), Elsevier Science Publishers.

[5] Barrington D.M., McKenzie P., Moore C., Tesson P., Thérien D.: Equation Satisfiability and Program Satisfiability for Finite Monoids, MFCS'00, Vol. 1893 of LNCS (2000) 172–181.

[6] Davis M.: Hilbert's tenth problem is unsolvable, Am. Math. Mon. **80** (1973) 233–269.

[7] Fages F., Huet G.: Complete Sets of Unifiers and Matchers in Equational Theories, Vol. 159 of LNCS (1983) 205–220.

[8] Green J. A., Rees D.: On Semigroups in which $x^r = x$, Proc. Camb. Phil. Soc. **48** (1952) 35–40.

[9] Kapur D., Narendran P.: NP–completeness of the Set Unification and Matching Problems, CADE'86, Vol. 230 of LNCS (1986) 489–495.

[10] Klíma O., Srba J.: Matching Modulo Associativity and Idempotency is NP-complete, MFCS'00, Vol. 1893 of LNCS (2000) 456–466.

[11] Klíma O., Srba J.: Matching Modulo Associativity and Idempotency is NP-complete, Technical report RS-00-13, BRICS, Aarhus University (2000).

[12] Klíma O.: Complexity of Unification and Matching Problems in the Varieties of Idempotent Semigroups.

[13] Klíma O.: Unification Modulo Associativity and Idempotency is NP-complete.

[14] Lothaire M.: Algebraic Combinatorics on Words, Preliminary version available at `http://www-igm.univ-mlv.fr/~berstel/Lothaire/index.html`

[15] Makanin G. S.: The Problem of Solvability of Equations in a Free Semigroup, Mat. Sbornik. **103(2)** (1977) 147–236. (In Russian) English translation in: Math. USSR Sbornik **32** (1977) 129–198.

[16] Matiyasevich Yu.V.: Diophantine representation of recursively enumerable predicates, Akad. Nauk SSSR, Ser. Mat. **35**, 3–30 (1971).

[17] Moore C., Tesson P., Thérien D.: Satisfiability of Systems of Equations over Finite Monoids, MFCS'01, Vol. 2136 of LNCS, ?? (2001).

[18] Plandowski W.: Solvability of word equations with constants is in P-SPACE, FOCS 1999.

[19] Plotkin G.: Building in Equational Theories, Machine Intelligence **7** (1972) 73–90.

[20] Robinson J. A.: A machine-oriented logic based on the resolution principle, J. Assoc. Comput. Mach. **12**, (1965) 23–41.
[21] Schmidt-Schauss M.: Unification under Associativity and Idempotence is of Type Nullary, J. of Automated Reasoning **2** (1986) 277–281.
[22] Siekmann J.: Unification of commutative terms, EUROSAM'79, Vol. 72 of LNCS (1979) 531–545.
[23] Siekmann J., Szabó P.: A Noetherian and Confluent Rewrite System for Idempotent Semigroups, Semigroup Forum **25** (1982) 83–110.