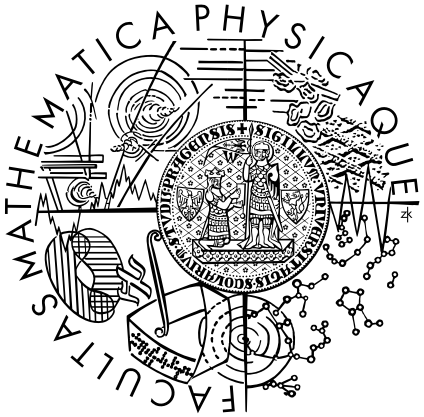
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



František Polach

Testování identit

Katedra algebry

Vedoucí bakalářské práce: RNDr. David Stanovský, Ph.D.
Studijní program: Matematika, obor Obecná matematika

2006

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce.

V Praze dne 21. května 2006 František Polach

Obsah

Název práce: *Testování identit*

Autor: *František Polach*

Katedra (ústav): *Katedra algebry*

Vedoucí bakalářské práce: *RNDr. David Stanovský, Ph.D.*

e-mail vedoucího: *stanovsk@karlin.mff.cuni.cz*

Abstrakt: *Na ověření, zda daná identita (např. komutativita, asociativita, apod.) platí v dané algebře (grupě, okruhu,...), existuje očividný algoritmus, který má exponenciální složitost vzhledem k délce zadané identity (pro fixní algebru). Není těžké nahlédnout, že tento problém je pro libovolnou algebru v třídě* ***co-NP*** *a že existují algebry, pro které je* ***co-NP****-úplný. Na druhou stranu, pro mnoho algeber (např. pro abelovské grupy) existuje algoritmus polynomiální. Existuje mezinárodní projekt, jehož cílem je charakterizovat ty algebry, pro které je tento problém polynomiální, resp.* ***co-NP****-úplný. Cílem této práce je shrnout některé známé výsledky o grupách a okruzích. Konkrétně ukážeme polynomiální algoritmy pro testování identit v nilpotentních i dihedrálních grupách a nilpotentních okruzích, a dokážeme* ***co-NP****-úplnost testování identit v nenilpotentních okruzích.*

Klíčová slova: *testování identit, složitost, grupy, okruhy*

Title: *Identity checking*

Author: *František Polach*

Department: *Department of Algebra*

Supervisor: *RNDr. David Stanovský, Ph.D.*

Supervisor's e-mail address: *stanovsk@karlin.mff.cuni.cz*

Abstract: *There is an obvious algorithm for verifiing an identity validity (e.g. commutativity, asociativity, etc.) for an algebra (group, ring,...). However, this algorithm has exponencial time complexity in the lenght of a given identity (for fixed algebra). It is easy to see that this problem is in* ***co-NP*** *for an arbitrary algebra and that there are algebras such that the problem is* ***co-NP****-complete. Conversely, this problem is polynomial for many algebras (e.g. Abelian groups). There is an international project with the aim of characterization such algebras for which is the problem polynomial or* ***co-NP****-complete. The purpose of this thesis is to summary some known results for groups and rings. Specifically, we'll show polynomial algorithms for the identity checking problem for nilpotent and dihedral groups and nilpotent rings, and we'll prove* ***co-NP****-completeness of the identity checking problem for non-nilpotent rings too.*

Keywords: *Equivalence problem, Complexity, Groups, Rings*

Úvod

Identity jsou podstatné jak pro univerzální algebru, tak i pro teorii složitosti. Navíc mnoho přirozených výpočetních problémů lze nahlédnout jako řešitelnost jistých rovnic nad konečnými algebraickými strukturami, jako jsou například grupy a okruhy.

Základní problém je takový:

> Pro dané dva polynomy $p(x_1, \ldots, x_n)$ a $q(x_1, \ldots, x_n)$ nad fixní algebrou **A** rozhodněte, zda jsou hodnoty p a q rovny pro každé dosazení hodnot z **A**.

Především je podstatné si uvědomit, že tento problém zkoumáme pro fixní algebru (danou tabulkou), která je v algoritmech parametrem. Vstup algoritmů tvoří polynomy (termy), a výstupem je *platí/neplatí* (je to takzvaný rozhodovací problém). Tato úloha je pro každou algebru ve třídě **co-NP**.

Naším cílem je rozhodnout, pro které algebry je tato úloha řešitelná efektivně (tedy polynomiálně) a pro které je neefektivní (tedy **co-NP**-úplná).
V celém textu se zabýváme výhradně konečnými algebrami.

Zde následuje shrnutí některých už známých výsledků:

Nechť je R okruh, pak **Hunt a Stearns** [5] dokázali:

- Pokud je R nilpotentní, pak je testování polynomiálních identit v **P**.
- Pokud je R komutativní a není nilpotentní, pak je testování polynomiálních identit **co-NP**-úplný problém.

Následně **Burris a Lawrence** [2] zobecnili předchozí tvrzení:

- Pokud R není nilpotentní, pak je testování polynomiálních identit **co-NP**-úplný problém.

A pro grupy je dokázáno:

Goldmann, Russel [3]: Pro nilpotentní grupy je testování identit v **P**.

Burris, Lawrence [1]: Pro dihedrální grupy je testování identit v **P**.

Lawrence, Willard [6]: Pro neřešitelné grupy je testování identit **co-NP**-úplný problém.

Horváth, Szabó [4]: Pro metacyklické grupy je testování identit v **P**.

V této práci předvedeme oba důkazy (algoritmy) složitosti testování identit pro okruhy a jeden základní pro nilpotentní grupy a jeden pro dihedrální grupy.

Kapitola 1

Základní pojmy

1.1 Jemný úvod do teorie složitosti

Nyní následuje velice stručný úvod do teorie výpočtové složitosti. Jako podklad byla použita skripta Úvod do složitosti a NP-úplnosti [7] Vladana Majerecha.

Rozhodovací problém je úloha, která pro jistý vstup dává výstup ANO/NE.
Zde se budeme zabývat výhradně rozhodovacími problémy.

Definice. (čas řešení úlohy) Nechť je vstup úlohy kódován v abecedě $\{0,1\}^*$ a n je délka vstupu. Řekneme, že algoritmus $\mathcal{A}$ řeší úlohu (problém) v čase $t_{\mathcal{A}}(n)$, pokud počet kroků algoritmu je nejvýš $t_{\mathcal{A}}(n)$ pro libovolný vstup velikosti nejvýše n.
Čas nedeterministického algoritmu se definuje jako největší hodnota $t(n)$ pro všechny vstupy velikosti nejvýše n.

Definice. (Složitostní třídy **P**, **NP**, **co-NP**) Rozhodovací problém patří do složistostní třídy **P** jestliže existuje deterministický algoritmus, který tento problém rozhoduje a jehož časová náročnost $t(n)$ je polynom v n.
Rozhodovací problém patří do složistostní třídy **NP** jestliže existuje nedeterministický algoritmus, který tento problém rozhoduje a jehož časová náročnost $t(n)$ je polynom v n. (Neboli **NP** obsahuje úlohy řešitelné nedeterministickým polynomiálním algoritmem.)
Do třídy **co-NP** patří takové rozhodovací problémy, jejichž doplněk leží v **NP**.

Definice. (ekvivalentní definice **NP**) *Verifikační algoritmus* $\mathcal{A}$ je takový algoritmus, který má na vstupu binární řetězec x (vstup) a binární řetězec y (ověření). Řekneme, že $\mathcal{A}$ verifikuje x, jestliže existuje takové y, že $\mathcal{A}(x,y) = 1$. Tedy jazyk $L \subseteq \{0,1\}^*$ je v **NP**, pokud existuje verifikační algoritmus $\mathcal{A}$ a polynom p splňující

1. $t_{\mathcal{A}}(x,y) \leq p(|x|)$
2. $x \in L$ právě tehdy, když existuje y takové, že $\mathcal{A}(x,y) = 1$.

Stále otevřenou otázkou je, zda platí, že **P** = **NP**. Kdyby rovnost platila, pak by byla tato práce zbytečná. Proto budeme předpokládat, že **P** $\neq$ **NP**.

Definice. Řekneme, že jazyk L_1 je *polynomiálně transformovatelný* na jazyk L_2, píšeme $L_1 \leq_P L_2$, jestliže existuje polynomiálně vypočítatelná funkce $f : \{0,1\}^* \to \{0,1\}^*$ taková, že pro všechna $x \in \{0,1\}^*$ platí: $x \in L_1 \iff f(x) \in L_2$.

Definice. Jazyk L je ***NP**-těžký*, když

$$\forall L' \in \mathbf{NP}, L' \leq_P L.$$

Definice. Jazyk L je ***NP**-úplný*, pokud

- L $\in$ **NP**
- L je **NP**-těžký

Tvrzení 1.1. *Relace $\leq_P$ je tranzitivní.*

Díky této vlastnosti se **NP**-úplnost a těžkost nejrůznějších problémů dokazují transformací (resp. redukcí) ze známých **NP**-úplných problémů.

Definice. *Booleovské formule* definujeme následovně:

1. proměnné jsou booleovské formule,
2. pokud φ je booleovská formule, pak jí je i $\neg\varphi$,
3. pokud φ_1, φ_2 jsou booleovské formule, pak jimi jsou i $\varphi_1 \vee \varphi_2$ a $\varphi_1 \wedge \varphi_2$.

Definice. Řekneme, že formule f je v *konjunktivní normální formě* (*CNF*), pokud je tvaru

$$f = \bigwedge_i \bigvee_j a_{i,j}$$

kde $a_{i,j} = x_k$ nebo $a_{i,j} = \neg x_k$, $x_k \in X$.
Formule f je v *3-CNF*, pokud

$$f = \bigwedge_i \bigvee_{j=1}^{3} a_{i,j}$$

kde $a_{i,j} = x_k$ nebo $a_{i,j} = \neg x_k$, $x_k \in X$.

Problém splnitelnosti 3-CNF formule je, jak známo, **NP**-úplný. Jeho doplňkem je tzv. problém platnosti 3-CNF formule.

1.2 Algebraická terminologie

Definice. *Grupou* $\mathbf{G} = (G, \cdot, ^{-1}, e)$ nazveme množinu G s jednou asociativní binární operací, jednou unární (inverz) a jednou nulární (jednotka) operací.
Okruhem $\mathbf{R} = (S, +, -, \cdot, 0)$ nazýváme takovou algebraickou strukturu, pro kterou platí:

- $(S, +, -, 0)$ je Abelova grupa;
- binární operace $\cdot$ je asociativní (tj. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$) a distributivní vzhledem k operaci + (tj. $x(y + z) = xy + xz$, $(y + z)x = yx + zx$);
- $\forall x \in S : x \cdot 0 = 0 \cdot x = 0$.

Tedy okruh neobsahuje nutně multiplikativní jednotku. Dále uvažujeme jen netriviální okruhy, což jsou okruhy, jejichž kardinalita je alespoň 2.

Definice. *Term* pro grupu v multiplikativním zápise $\mathbf{G} = (G, \cdot, ^{-1}, e)$ je induktivně definován takto:

1. proměnné jsou termy,
2. e je term,
3. t je term implikuje (t^{-1}) je term,
4. s, t jsou termy implikuje $(s \cdot t)$ je term.

Definice. Pro danou grupu **G** definujeme *polynomy* **G** jako termy, do kterých substituujeme prvky grupy za nějaké proměnné,

1. proměnné jsou polynomy,
2. g jako prvek G je polynom,
3. p je polynom implikuje (p^{-1}) je polynom,
4. p, q jsou polynomy implikuje $(p \cdot q)$ je polynom.

Definice. *Term* pro okruh $\mathbf{R} = (S, +, -, \cdot, 0)$ je definován rekurzivně takto:

1. proměnné jsou termy,
2. 0 je term,
3. F je term implikuje $(-F)$ je term,
4. pokud F_i, $1 \leq i \leq n$ jsou termy, pak jimi jsou i $(F_1 + \cdots + F_n)$ a $(F_1 \cdot \ldots \cdot F_n)$.

Definice. *Polynomy* okruhu **R** definujeme rekurzivně takto:

1. proměnné jsou polynomy,
2. prvky S jsou polynomy,
3. F je polynom implikuje $(-F)$ je polynom,
4. pokud F_i, $1 \leq i \leq n$, jsou polynomy, pak jimi jsou i $(F_1 + \cdots + F_n)$ a $(F_1 \cdot \ldots \cdot F_n)$.

Definice. *Velikost* polynomu (resp. termu) $|F|$ definujeme jako počet výskytů symbolů v polynomu F, kde symbolem je každá proměnná, konstanta, závorka a operátor.

Příklad. $|((x_1 \cdot x_2) + c_1)| = 9$.

Jelikož nehrozí záměna významů, značíme zde velikost polynomu i mohutnost množiny (tj. počet jejích prvků) stejně.

Definice. Nechť **A** je nějaká algebra (např. grupa, okruh) a t_1 a t_2 jsou termy definované na **A**. Řekneme, že t_1 a t_2 *splňují identitu* na A, pokud pro všechna $\vec{a} \in \mathbf{A}$ platí $t_1(\vec{a}) = t_2(\vec{a})$.

Definice. *Testování identit* grupy **G** znamená rozhodnout, zda dva dané termy s, t definují stejnou funkci na **G**, tedy zda identita $s \approx t$ platí na **G**.

Testování polynomiálních identit grupy **G** znamená rozhodnout, zda dva dané polynomy p, q definují stejnou funkci na **G**, tedy zda identita $p \approx q$ platí na **G**.
Analogicky se definuje testování identit okruhu.

Poznámka. Protože testování identit grupy $\mathbf{G} \models p \approx q$ je ekvivalentní testování, zda $\mathbf{G} \models p \cdot q^{-1} \approx e$, budeme dále uvažovat jen identitu $\mathbf{G} \models p \approx e$. Obdobně pro okruhy.

Problém testování identit je řešitelný algoritmem, který pro všechna možná dosazení prvků z algebry za proměnné termu ověřuje, zda je term roven nulovému prvku. Tento algoritmus je však exponenciální vzhledem k počtu proměnných (vzhledem k velikosti identity), neboli jeho složitost je $O(|G|^m)$, kde m označuje počet proměnných termu. Pro konkrétní prvky $a_1, \ldots, a_n$, otestovat, zda $p(\vec{a}) = e$, je polynomiální problém.

Protože má podmínka tvar: pro všechny prvky z **A** otestuj, zda splňují jistou polynomiální podmínku, tak tento problém leží v **co-NP** složitostní třídě.

Kapitola 2

Testování identit v konečných grupách

Tato kapitola je zpracována podle článku [1] Burrise a Lawrence. Doplněno bylo pouze Lemma 2.1 a jeho důkaz, použito k tomu bylo Lemma 33.35, str. 86, z knihy [8] od Hanny Neumann.

2.1 Terminologie

Definice. *Komutátor* grupy **G** je zobrazení $[\cdot, \ldots, \cdot] : \mathbf{G} \times \cdots \times \mathbf{G} \to \mathbf{G}$, jenž je definováno rekurzivně pro $x_1, \ldots, x_n \in G$:

1. $[x_1, x_2] = x_1^{-1} x_2^{-1} x_1 x_2$
2. $[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$.

Definice. Komutátor tvaru $[\ldots [[x_1, x_2], x_3], \ldots, x_k]$ nazýváme *levonormovaný* a obvykle značíme $[x_1, x_2, \ldots, x_k]$.

Definice. Grupa **G** je *nilpotentní*, pokud pro nějaké n splňuje identitu

$$[x_0, \ldots, x_n] \approx e \tag{2.1}$$

O nilpotentní grupě **G** řekneme, že je *nilpotentní třídy c*, pokud c je nejmenší n takové, že identita (2.1) platí.

Příklad. Abelovské grupy jsou definovány identitou $[x, y] = 1$ pro libovolné prvky x, y. Tedy jsou to nilpotentní grupy třídy 1.

V následující definici značí $[\cdot, \cdot]$ komutátor ve smyslu binární operace.

Definice. Množina PC (*čisté komutátorové polynomy*) je definována:

1. proměnné patří do PC
2. pokud $g \in G$, pak $g \in PC$
3. pokud $p, q \in PC$, pak $[p, q] \in P$.

Definice. Na množině PC definujeme funkci *lc* takto:

1. $lc(x) = 1$, pokud je x proměnná

2. $lc(g) = 1$, pokud $g \in G$

3. $lc([s,t]) = lc(s) + lc(t)$.

Tedy funkce lc nám spočítá listy stromu, pokud se na prvek PC podíváme jako na binární strom.

2.2 Nilpotentní grupy

Lemma 2.1. *Nechť $p \in PC$, $lc(p) = n$. Pak existuje $r \geq 1$ a levonormované $q_1, \ldots, q_r \in PC$ (případně konjugované nebo inverzní), $lc(q_i) = n$ pro $i = 1, \ldots, r$, takové, že $p \approx q_1 \cdot \ldots \cdot q_r$.*

Důkaz. K důkazu potřebujeme několik základních komutátorových rovností:

1. $[xy, zt] = [x,t]^y \cdot [y,t] \cdot [x,z]^{yt} \cdot [y,z]^t$;

2. $[x^{-1}, z] = [z,x]^{x^{-1}}$, $[x, y^{-1}] = [y,x]^{y^{-1}}$, $[x^{-1}, y^{-1}] = [x,y]^{y^{-1}x^{-1}}$;

3. $[x, y^{-1}, z]^y \cdot [y, z^{-1}, x]^z \cdot [z, x^{-1}, y]^x = 1$;

kde $[x,y]^z = z^{-1} \cdot [x,y] \cdot z$ (konjugace) a $[x,y]^{-1} = [y,x]$ (inverz).

Použijeme indukci dle $lc(p) =: n$. Pro $n = 1, 2$ tvrzení platí triviálně. Položme $c = [u,v]$, kde $u, v \in PC$ a $lc(u) = k$ a $lc(v) = l$, $k + l = n$. Předpokládejme, že tvrzení platí pro všechny $p \in PC$, $lc(p) < n$. Pomocí rovností (1) a (2) dostaneme c do tvaru $c = \prod [u_i, v_i]^{w_i}$, kde u_i a v_i jsou levonormované. Ať $[u,v] = [u, [v_1, t]]$, kde $lc(v_1) = l - 1$, $l \neq 1$. Přepíšeme c do potřebného tvaru, použijeme k tomu rovnosti (2) a (3) aplikované na $z = u, x = v_1, y = t^{-1}$:

$$\begin{aligned} [u, [v_1, t]]^{-t^{-1}} &= [t^{-1}, u^{-1}, v_1]^u \cdot [u, v_1^{-1}, t^{-1}]^{v_1} = \\ &= [[u, t^{-1}]^{u^{-1}}, v_1]^u \cdot [[v_1, u]^{v_1^{-1}}, t^{-1}]^{v_1} = [[u, t^{-1}], v_1^u] \cdot [[v_1, u], t^{-v_1}]. \end{aligned}$$

Dostali jsme násobek levonormovaných komutátorů, druhý z nich je tvaru $[c', t']$, kde $lc(c') = n - 1$, tedy $lc([c', t']) = n$. První je tvaru $[u', v']$, kde $lc(u') = k + 1$ a $lc(v') = l - 1$, proto $lc([u', v']) = k + l = n$. □

Lemma 2.2. *Pokud je $\mathbf{G}$ nilpotentní grupa třídy c a $p \in PC$, platí:*

1. *$lc(p) = c$ implikuje $\mathbf{G} \models p \cdot z \approx z \cdot p$, kde z je proměnná, nevyskytující se v polynomu p,*

2. *$lc(p) > c$ implikuje $\mathbf{G} \models p \approx e$.*

Důkaz. Aplikací předchozího Lemmatu (přímým dosazením, zde $n = c$) dostaneme:

- $p \cdot z \approx q_1 \ldots q_r \cdot z = q_1 \ldots q_{r-1} \cdot z \cdot q_r \cdot \underbrace{[q_r, z]}_{=1} = \cdots = z \cdot q_1 \cdot [q_1, z] \ldots q_r = z \cdot q_1 \ldots q_r \approx z \cdot p$;

- $p \approx q_1 \ldots q_r \approx e$, neboť $q_1 \approx e, \ldots, q_r \approx e$ ($lc(q_i) > n,\ i = 1, \ldots, r$).

□

Definice. Pro daný polynom p značí symbol $var(p)$ množinu proměnných p.

Lemma 2.3. *Nechť* $\mathbf{G}$ *je konečná nilpotentní grupa třídy* c, $p(x_1, \ldots, x_k)$ *je polynom* $\mathbf{G}$. *Ať* $\mathcal{S}$ *je množina všech nejvýše* c*-prvkových podmnožiny množiny* $\{1, \ldots, k\}$ *a očíslujme prvky* $\mathcal{S}$ *do posloupnosti* $S_1, \ldots, S_m$ *takové, že platí:* $i < j \Rightarrow |S_i| \leq |S_j|$. *Pro* $1 \leq i \leq k$ *předpokládejme* $S_i = \{i\}$. *Pak pro každou* S_i *existuje* n_i *a prvek* $\gamma_i = \prod_{j=1}^{n_i} p_{ij}$, *kde* $p_{ij} \in PC$, *takový, že platí*

- $var(p_{ij}) = \{x_s : s \in S_i\}$, *pro všechny* i, j ;
- $\mathbf{G} \models p(x_1, \ldots, x_k) \approx \gamma_0 \ldots \gamma_m$.

Důkaz. Nejprve přepíšeme polynom $p(x_1, \ldots, x_k)$ do tvaru $y_1^{e_1} \ldots y_l^{e_l}$, $e_i \in \{1, -1\}$, kde y_i je z množiny $\{x_1, \ldots, x_k\}$ nebo označuje prvek grupy $\mathbf{G}$. Nyní použijeme grupovou identitu:

$$x \cdot y \approx y \cdot x \cdot [x, y].$$

Pomocí této identity dostaneme $y_1^{e_1} \ldots y_l^{e_l}$ do tvaru

$$g_0 \cdot x_1^{n_1} \cdot s(x_1) \ldots x_k^{n_k} \cdot s(x_k) \cdot s(x_1, x_2) \ldots s(x_2, x_3) \ldots s(x_1, \ldots, x_k),$$

kde $g_0 \in \mathbf{G}$ a $s(x_1), \ldots, s(x_1, \ldots, x_k)$ jsou čisté komutátorové polynomy, v nichž postupně přibývá proměnných. Pokud tyto polynomy označíme p_i, pak $lc(p_i) \leq c$, $|var(p_i)| \geq 1$ pro každý z nich.

Položme $\gamma_0 = g_0$, $\gamma_i = x_i^{n_i} \cdot s(x_i)$, pro $1 \leq i \leq k$, kde komutátory obsahují právě jednu proměnnou. Dále $\gamma_{k+1} = s(x_1, x_2)$, $\gamma_{k+2} = s(x_1, x_3)$, $\ldots$, $\gamma_{2k} = s(x_2, x_3)$, $\gamma_{k+1+\binom{k}{2}} = s(x_1, x_2, x_3), \ldots$ atd., a nakonec i poslední $\gamma_{k+\binom{k}{2}+\cdots+\binom{k}{k-1}+1} = s(x_1, \ldots, x_k)$. □

Lemma 2.4. *Nechť* $\mathbf{G}$ *je nilpotentní grupa třídy* c, *a* $p(x_1, \ldots, x_k)$ *je polynom* $\mathbf{G}$. *Nechť* $\gamma_0, \ldots, \gamma_m$ *jsou stejné jako v předchozím lemmatu. Pak platí*

$$G \models p(x_0, \ldots, x_k) \approx e \iff \mathbf{G} \models \gamma_i \approx e, \tag{2.2}$$

pro všechna $1 \leq i \leq m$.

Důkaz. ($\Longleftarrow$) Stačí dosadit do Lemmatu 2.3.
($\Longrightarrow$) Z Lemmatu 2.3 máme $G \models p \approx e \Rightarrow G \models \gamma_0 \ldots \gamma_m \approx e$. Protože e komutuje se vším, můžeme použít následující postup. Položíme-li všechny proměnné rovny e, dostaneme $\gamma_0 = e$. Nyní položíme všechny proměnné až na x_i rovny e, vyjde nám $G \models \gamma_i \approx e$, pro $1 \leq i \leq k$. Tedy $\mathbf{G} \models \gamma_{k+1} \ldots \gamma_m \approx e$. Nechť $var(\gamma_{k+1}) = \{x_{i_1}, x_{i_2}\}$. Položením všech proměnných kromě x_{i_1} a x_{i_2} rovno e, máme $\gamma_{k+1} \approx e$. A takto pokračujeme dále. □

Tvrzení 2.5. *Nechť* $\mathbf{G}$ *je konečná nilpotentní grupa třídy* c *a* $p(x_1, \ldots, x_k)$ *je polynom grupy* $\mathbf{G}$. *Pak pro všechna* σ *splňující*

- $\sigma x_i \in \{x_i, e\}$
- $|\{i : \sigma x_i \neq e\}| \leq c$,

platí:

$$\mathbf{G} \models p(x_1, \ldots, x_k) \approx e \text{ právě tehdy, když } \mathbf{G} \models p(\sigma x_1, \ldots, \sigma x_k) \approx e.$$

Důkaz. ($\Longrightarrow$) Zřejmé.
($\Longleftarrow$) Nechť σ splňuje podmínky tvrzení. Zvolme $S_0, \ldots, S_m$ a $\gamma_0, \ldots, \gamma_m$ stejně jako v Lemmatu 2.3. Nechť j je takové, že $S_j = \{i : \sigma x_i \neq e\}$. Pak z Lemmatu 2.3 plyne

$$\mathbf{G} \models p(\sigma x_1, \ldots, \sigma x_k) \approx \prod_{S_i \subseteq S_j} \gamma_i,$$

tedy

$$\mathbf{G} \models \prod_{S_i \subseteq S_j} \gamma_i \approx e.$$

Když předchozí postup zopakujeme pro všechna možná σ, zjistíme, že poslední identita platí pro všechna $j \leq m$.
Projdeme-li popořadě množiny S_j, vyjde nám pro $j \leq m$

$$\mathbf{G} \models \gamma_j \approx e$$

Nyní již můžeme použít Lemma 2.4, abychom dostali

$$\mathbf{G} \models p(x_1, \ldots, x_k) \approx e.$$

□

Věta 2.6. *Nechť* **G** *je konečná nilpotentní grupa. Pak testování polynomiálních identit v* **G** *má polynomiální časovou složitost.*

Důkaz. Nechť c je třída nilpotence. Uvažujme polynom $p(x_1, \ldots, x_k)$ na **G**. Definujme

$$T = \{(a_1, \ldots, a_k) : |\{i : a_i \neq e\}| \leq c\}.$$

Pomocí Tvrzení 2.5 dostáváme

$$\mathbf{G} \models p(\vec{x}) \approx e \Longleftrightarrow \forall \vec{a} \in T : \ p(\vec{a}) = e.$$

Není těžké si rozmyslet, že

- $|T| = \sum_{i \leq c} \binom{k}{i} (|G| - 1)^i$, tedy T má polynomiální velikost vzhledem k počtu proměnných p, složitost: $O(k^c)$;
- nalezení T je polynomiální procedura vzhledem k počtu proměnných p, složitost: $O(k^c)$;
- test, zda $p(\vec{a}) = e$ je lineární procedura vzhledem k počtu proměnných p, složitost: $O(k)$.

ALGORITMUS: test, zda platí $p(\vec{a}) = e$ pro všechny $\vec{a} \in T$.

VSTUP: množina T, polynom p
VÝSTUP: ano / ne

n:=0,

1. n:=n+1,

2. pokud n=$|T|$+1, pak VÝSTUP:=ano a KONEC, jinak do p dosaď $\vec{a}_n \in T$,
3. zkontroluj, zda $p(\vec{a}_n) = e$,
4. pokud $p(\vec{a}_n) = e$ platí, zopakuj celý algoritmus od začátku, jinak VÝSTUP:=ne a KONEC.

- korektnost: algoritmus zřejmě počítá to, co má,
- složitost: algoritmus proběhne nanejvýš $|T|$-krát, proto celková složitost je $O(k^{c+1})$.

Tedy máme algoritmus, který v polynomiálním čase ($O(k^c) + O(k^{c+1}) = O(k^{c+1})$) zjistí, zda $\mathbf{G} \models p \approx e$. □

2.3 Dihedrální grupy

Definice. *Dihedrální grupa* $\mathbf{D}_n$ je definována jako grupa symetrií pravidelného n-úhelníka. Jeden prvek $\mathbf{D}_n$ je rotace R n-úhelníka o $360°/n$ kolem středu. Řád tohoto prvku je n. Další prvek $\mathbf{D}_n$ je souměrnost D n-úhelníka dle osy úhlu u některého vrcholu. Tento prvek má řád 2. Dohromady R a D generují $2n$ různých symetrií.
Grupa $\mathbf{D}_n$ má $2n$ prvků, které se dají zapsat jako: $e, R, R^2, \ldots, R^{n-1}, D, RD, \ldots, R^{n-1}D$.
$\mathbf{D}_n$ je možné zapsat také jako $\langle a, b | a^n = 1, b^2 = 1, bab = a^{-1} \rangle$, je to největší taková grupa.

Věta 2.7. *Nechť $n \in \mathbb{N}$, testování polynomiálních identit v dihedrální grupě $\mathbf{D}_n$ má polynomiální časovou složitost.*

Důkaz. Důkaz rozdělíme na dvě části podle toho, zda je n liché či sudé.

Nechť je n liché. Ať $a, b \in D_n$, $o(a) = n, o(b) = 2$. Pak všechny prvky $\mathbf{D}_n$ je možno psát ve tvaru $a^u b^v$, kde u, v jsou celá čísla. Protože platí

$$ba^r b = \underbrace{bab \cdot bab \ldots bab}_{r} = a^{-r}, \quad neb \quad b^2 = 1 \quad a \quad bab = a^{-1},$$

pro dva libovolné prvky z D_n dostaneme

$$(a^{u_1} b^{v_1})(a^{u_2} b^{v_2}) = a^{u_1 + (-1)^{v_1} u_2} b^{v_1 + v_2}.$$

Dále použijeme zkratku (u, v) namísto $a^u b^v$.

Pomocí indukce máme

$$(u_1, v_1) \ldots (u_l, v_l) = (u_1 + (-1)^{v_1} u_2 + \cdots + (-1)^{v_1 + \cdots + v_{l-1}} u_l, v_1 + \cdots + v_l). \quad (2.3)$$

Nechť $p(x_1, \ldots, x_k)$ je polynom $\mathbf{D}_n$. Není problém jej v polynomiálním čase přepsat do tvaru $y_1 \cdot \ldots \cdot y_l$, kde každé $y_i \in \{x_1, \ldots, x_k\} \cup D_n$. Nechť zobrazení $\alpha : \{1, \ldots, l\} \Longrightarrow \{1, \ldots, k\} \cup D_n$ je takové, že

- $y_i = x_{\alpha i}$, pokud y_i je proměnná, a
- $y_i = \alpha i$, pokud $y_i = g \in D_n$.

Každé y_i nahradíme $(u_{\alpha i}, v_{\alpha i})$, což značí:

1. dvojici proměnných (nad celými čísly), pokud $\alpha i \in \{1, \ldots, k\}$, nebo
2. dvojici celých čísel, pokud $\alpha i = a^{u_{\alpha i}} b^{v_{\alpha i}} \in D_n$.

Tedy polynom $p(x_1, \ldots, x_k)$ odpovídá

$$(a^{u_{\alpha 1}} b^{v_{\alpha 1}}) \ldots (a^{u_{\alpha l}} b^{v_{\alpha l}}),$$

zkráceně:

$$(u_{\alpha 1}, v_{\alpha 1}) \ldots (u_{\alpha l}, v_{\alpha l}).$$

Pomocí (2.3):

$$\mathbf{D}_n \models p(x_1, \ldots, x_k) \approx e$$

platí, jestliže je splněno

$$\begin{aligned} u_{\alpha 1} + (-1)^{v_{\alpha 1}} u_{\alpha 2} + \cdots + (-1)^{v_{\alpha 1} + \cdots + v_{\alpha (l-1)}} u_{\alpha l} &\equiv 0 \pmod{n} \\ v_{\alpha 1} + \cdots + v_{\alpha l} &\equiv 0 \pmod{2}. \end{aligned}$$

Dosadíme-li 0 za všechny proměnné $u_{\alpha i}$, získáme z předchozích dvou rovnic rovnici (2.4). Dosadíme-li 0 za všechny proměnné kromě jedné, za niž dosadíme 1, získáme z předchozích dvou rovnic rovnici (2.5). Je vidět, že předchozí rovnice platí právě tehdy, když jsou splněny (2.4) a (2.5) a (2.6).

$$\sum_{\alpha i \in D_n} (-1)^{v_{\alpha 1} + \cdots + v_{\alpha (i-1)}} u_{\alpha i} \equiv 0 \pmod{n} \tag{2.4}$$

$$\sum_{\alpha i = s} (-1)^{v_{\alpha 1} + \cdots + v_{\alpha (i-1)}} \equiv 0 \pmod{n}, \text{ pro } 1 \leq s \leq k \tag{2.5}$$

$$v_{\alpha 1} + \cdots + v_{\alpha l} \equiv 0 \pmod{2}. \tag{2.6}$$

Protože je každé $v_{\alpha 1} + \cdots + v_{\alpha (i-1)}$ součtem proměnných a celých čísel, můžeme rovnice (2.4) a (2.5) přepsat ve tvaru

$$\varepsilon_1 \cdot (-1)^{a_{11} v_1 + \cdots + a_{1k} v_k} + \cdots + \varepsilon_r \cdot (-1)^{a_{r1} v_1 + \cdots + a_{rk} v_k} \equiv 0 \pmod{n}, \tag{2.7}$$

kde $\varepsilon_i \in \{0, \ldots, n-1\}$, $a_{ij} \in \{0, 1\}$, a žádné dva řádky matice (a_{ij}) (velikosti $r \times k$) nejsou stejné.
Nechť $\eta_i = (-1)^{v_i}$, a definujme okruhový polynom $q \in \mathbb{Z}_n[w_1, \ldots, w_k]$ následovně

$$q(w_1, \ldots, w_k) = \sum_{1 \leq i \leq r} \varepsilon_i \cdot \prod_{1 \leq j \leq k} w_j^{a_{ij}}.$$

Protože η_i nabývá nezávisle jen hodnoty z $\{1, -1\}$, rovnice (2.7) je ekvivalentní

$$q \equiv 0 \pmod{n}, \text{ pokud } w_i \text{ nabývá hodnot z } \{1, -1\}.$$

Poslední část polynomiálního algoritmu spočívá v uvědomění si, že předchozí tvrzení platí, pokud

$$q(c_1, \ldots, c_k) = 0 \quad \forall c_i \in \{1, -1\}. \tag{2.8}$$

Důkaz (2.8) se provádí indukcí dle k, a to pokud q není nulový polynom, pak pro nějaké dosazení hodnot $c_i \in \{1, -1\}$ za w_i dostaneme, že $q(c_1, \ldots, c_k) \neq 0$ v $\mathbb{Z}_n$.

Dále důkaz pokračuje tak, že napíšeme polynom $q(w_1, \ldots, w_k)$ jako

$$q'(w_1, \ldots, w_{k-1}) + (1 - w_k) \cdot q''(w_1, \ldots, w_{k-1}),$$

a všimneme si, že pokud q není nulový polynom, lze vybrat takové $c_1, \ldots, c_{k-1} \in \{1, -1\}$, že jeden z q' a q'' se po dosazení hodnot nevynuluje v $\mathbb{Z}_n$. Protože n je liché, $w_k = 1$ nebo $w_k = -1$ nám dá takovou hodnotu, že $q(w_1, \ldots, w_k)$ je nenulový. Z (2.8) dostaneme polynomiální algoritmus, který rozhoduje, zda platí (2.4) a (2.5). Rozhodnout, zda platí (2.6), je snadné.

Nyní předpokládejme, že $n = 2^k \cdot m$, kde m je liché a $k \geq 1$. Pak $\mathbf{D}_n$ lze vnořit do $\mathbf{D}_{2^k} \times \mathbf{D}_m$, a $\mathbf{D}_{2^k}$ i $\mathbf{D}_m$ lze vnořit do $\mathbf{D}_n$.
Protože $\mathbf{D}_n$ má $2n$ prvků a kartézský součin $\mathbf{D}_{2^k}$ a $\mathbf{D}_m$ má celkem $2^{k+1} \cdot 2m = 4n$ prvků, použije se k reprezentaci $\mathbf{D}_n$ v $\mathbf{D}_{2^k} \times \mathbf{D}_m$ jen polovina prvků součinu.
Ať

$$\begin{aligned}
\mathbf{D}_n &= \{e, a, a^2, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\}, \\
\mathbf{D}_{2^k} &= \{e, c, c^2, \ldots, c^{2^k-1}, d, cd, \ldots, c^{2^k-1}d\}, \\
\mathbf{D}_m &= \{e, f, f^2, \ldots, f^{m-1}, g, fg, \ldots, f^{m-1}g\}.
\end{aligned}$$

Pak vnoření popíšeme například takto: $e \sim e \cdot e$, $a \sim c \cdot e$, $a^2 \sim c^2 \cdot e$, $\ldots$, $a^{2^k-1} \sim c^{2^k-1} \cdot e$, $a^{2^k} \sim c \cdot f$, $\ldots$, $a^{n-1} \sim c^{2^k-1} \cdot f^{m-1}$, $b \sim d \cdot e$, $ab \sim cd \cdot e$, $\ldots$, $a^{2^k-1}b \sim c^{2^k-1}d \cdot e$, $\ldots$, $a^{n-1}b \sim c^{2^k-1}d \cdot f^{m-1}$.
Podobně je možné popsat vnoření $\mathbf{D}_{2^k}$ a $\mathbf{D}_m$ do $\mathbf{D}_n$.

Tedy máme polynomiální algoritmus pro $\mathbf{D}_n$, neboť jej máme pro $\mathbf{D}_m$ (předchozí část důkazu) a také pro $\mathbf{D}_{2^k}$, díky Větě 2.6 (protože $\mathbf{D}_{2^k}$ je nilpotentní).

□

Kapitola 3

Testování identit v konečných okruzích

Oddíl 3.2 a Věta 3.5 čerpá z článku [5] Hunta a Stearnse, Lemma 3.1 a zbytek oddílu 3.3 je zpracován podle článku [2] Burrise a Lawrence.

3.1 Terminologie

Definice. *Jacobsonův radikál* okruhu **R** je ideál, který vznikne průnikem všech maximálních levých ideálů **R**. Značíme jej $J(\mathbf{R})$.

Definice. Prvek r okruhu **R** nazveme *nilpotentní* pokud pro něj existuje přirozené číslo k_r takové, že platí $r^{k_r} = 0$. Ideál I okruhu **R** nazveme *nil-ideál* pokud každý prvek I je nilpotentní. Řekneme, že ideál I okruhu **R** je *nilpotentní stupně k*, pokud pro všechna $a_1, \ldots, a_k \in S$ ($a_1, \ldots, a_k$ nemusí být různá) platí $a_1 \cdot \ldots \cdot a_k = 0$. Jelikož je celý okruh ideálem, můžeme hovořit o nil-okruhu, resp. nilpotentním okruhu.

Každý netriviální okruh s jednotkou je samozřejmě nenilpotentní. Každý nilpotentní okruh je taktéž nil-okruh. A pro konečné okruhy, platí i obrácená implikace. Tedy platí následující

Lemma 3.1. *Nechť* **R** *je konečný okruh. Pak* **R** *je nil-okruh právě tehdy, když* **R** *je nilpotentní okruh.*

Definice. *Booleova algebra* $\mathbf{B} = (B, \vee, \wedge, \neg, 0, 1)$ je částečně uspořádaná množina se dvěma binárními, dvěma nulárními a jednou unární operací, která pro všechna $x, y, z \in B$ splňuje:

1. $(B, \vee)$, $(B, \wedge)$ jsou komutativní idempotentní pologrupy;
2. $x \wedge (y \vee x) = x = x \vee (y \wedge x)$ (absorpce);
3. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, (distributivita $\wedge$ a $\vee$);
4. $\forall x \in B : 0 \leq x \leq 1$;
5. $\forall x \in B : x \wedge \neg x = 0$ & $x \vee \neg x = 1$.

Částečné uspořádání na B definujeme předpisem $x \leq y$, pokud $x \wedge y = x$ (ekvivalentně $x \vee y = y$). Tedy $x \vee y = \sup(x, y)$, $x \wedge y = \inf(x, y)$.
Svaz $(B, \vee, \wedge)$ je částečně uspořádaná množina B uzavřená na binární operace $\vee, \wedge$ splňující body (1) a (2).

Definice. *Booleovský okruh* je okruh $\mathbf{R} = (R, +, -, \cdot, 0, 1)$, v němž platí:

$$\forall r \in R : r^2 = r.$$

Tvrzení 3.2. *"Booleovy okruhy odpovídají vzájemně jednoznačně Booleovým algebrám."*

1. *Nechť* $\mathbf{B}_1 = (B, \vee, \wedge, \neg, 0, 1)$ *je Booleova algebra. Definujme okruh* $\mathbf{B}_2 = (B, +, \cdot, -, 0, 1)$, *kde*

$$\begin{aligned} x + y &= (x \wedge \neg y) \vee (\neg x \wedge y), \\ x \cdot y &= x \wedge y, \\ -x &= x. \end{aligned}$$

   Pak $\mathbf{B}_2$ *je Booleovský okruh.*

2. *A naopak, nechť* $\mathbf{R}_1 = (R, \vee, \wedge, \neg, 0, 1)$ *je Booleovský okruh. Definujme* $\mathbf{R}_2 = (R, +, \cdot, -, 0, 1)$, *kde*

$$\begin{aligned} x \vee y &= x + y - x \cdot y, \\ x \wedge y &= x \cdot y, \\ \neg x &= 1 - x. \end{aligned}$$

   Pak $\mathbf{R}_2$ *je Booleova algebra.*

Důkaz. Přímočarým ověřením. □

Definice. SP ("sum product") polynomem (resp. termem) nazveme polynom na **R** tvaru $(F_1 + \cdots + F_n)$, pro $n \geq 1$, kde každý polynom F_i na **R** je tvaru $(F_{i1} \cdot \ldots \cdot F_{ij})$ nebo $(-F_{i1} \cdot \ldots \cdot F_{ij})$, pro $j \geq 1$, a každá F_{ik} je nějaká proměnná nebo konstanta.
Obdobně se definuje polynom **PSP** ("product sum product") jako polynom tvaru $(F_1 \cdot \ldots \cdot F_n)$, kde každý polynom F_i je **SP** polynom.

Poznámka. Obvykle se slovem polynom označuje to, čemu my říkáme **SP** polynom (navíc se polynomy obvykle uvažují komutativní). Tato terminologie odpovídá terminologii z předchozí kapitoly.

3.2 Nilpotentní okruhy

Tvrzení 3.3. *Nechť* $\mathbf{R} = (S, +, -, \cdot, 0)$ *je konečný nilpotentní okruh stupně* k. *Pak problém testování polynomiálních identit na* **R** *je deterministicky rozhodnutelný v polynomiálním čase.*

Důkaz. K důkazu tvrzení nám stačí ukázat následující:

> Existuje deterministický algoritmus pracující v polynomiálním čase, jehož vstupem je polynom F na **R** obsahující pouze proměnné, závorky, +, -, ·, a prvky z S, který rozhoduje, zda $F = 0$ na **R**.

Algoritmus:

Polynom F se převede na ekvivalentní **SP** polynom F' obsahující pouze proměnné, +, -, ·, a prvky z S. Převod je možný pomocí opakované aplikace distributivních zákonů s tím, že se každý součin o k a více členech nahradí 0. Tedy $|F'| = O(|F|^{2^{k-1}})$ a F' se získá ve stejném asymptotickém čase.

A samotný algoritmus testování probíhá následovně:

1. Pokud F' nemá proměnné, otestuje se, zda $F' = 0$, jinak se vybere jedna proměnná x v F' a F' se rozdělí na dvě části F'_1 a F'_2, kde
   - F'_1 je součet všech členů F', ve kterých se nejméně jednou vyskytuje x, a
   - F'_2 je součet zbývajících členů F', nebo je roven 0, pokud žádné další členy nezbyly.
2. Pro každý prvek $a \in S$ se na $F'_1[x = a]$, což je polynom F'_1 s dosazenou hodnotou a za vybranou proměnnou x, provede celý algoritmus testování znovu, tj. od kroku (1). A taktéž na polynom F'_2 se provede znovu celý algoritmus.
3. $F = 0$ na **R** právě tehdy, když všechny testy ($F' = 0$) v (1) skončily úspěchem.

Nutnou podmínkou úspěchu je, že polynom F nemá konstantní člen. Protože samozřejmě $0 \in S$, můžeme F' rozdělit na F'_1 a F'_2, a oba menší polynomy otestovat algoritmem zvlášť. Takže algoritmus pracuje korektně.

Tedy zbývá ukázat, že algoritmus pracuje v deterministickém polynomiálním čase vzhledem k $|F|$. Pro každou hodnotu a má polynom $F'_1[x = a] = 0$ aspoň o jednu proměnnou méně v každém členu. Proto maximální počet rekurzivních volání algoritmu testování je omezen hodnotou $k - 1$. Abychom odhadli složitost, omezíme nyní počet opakování algoritmu. Nechť $C(n, d)$ je počet rekurzivních volání algoritmu, tj. kroků (1)-(3), pro daný polynom s n členy, v nichž je v každém nanejvýš d proměnných. Pak pro $C(n, d)$ platí

$$\begin{aligned} C(n,0) &= 1 \\ C(n,d) &\leq |S| \cdot C(n_1, d-1) + C(n_2, d), \text{ pro } n_1 > 0, n_2 \geq 0,\ n_1 + n_2 = n. \end{aligned}$$

Jelikož víme, že $d \leq k - 1$ (k je stupeň nilpotence), indukcí můžeme ověřit, že platí

$$C(n,d) \leq n \cdot |S|^d \leq n \cdot |S|^{k-1}.$$

Jistě platí $n < |F'|$. Převod F na F' a rozdělení F' na F'_1 a F'_2 (krok (1)) má časovou složitost $O(|F'|)$. Tedy celkový čas algoritmu je nejvýše

$$O(|F'|) + O(|F'| \cdot |S|^{k-1}) \cdot O(|F'|) = O(|F|^{2^k} \cdot |S|^{k-1}) = O(|F|^{2^k}).$$

□

3.3 Nenilpotentní okruhy

Lemma 3.4. *Pro každý konečný okruh* $\mathbf{R}$ *existuje kladné celé číslo* n *takové, že platí* $\mathbf{R} \models x^{2n} \approx x^n$.

Důkaz. Uvažujme všechna zobrazení $\mathbf{R} \to \mathbf{R}$, $x \mapsto x^k$, $k \in \mathbb{N}$. Protože těchto různých zobrazení je jen konečně mnoho, existují $k, l \in \mathbb{N}, k > 2l$, taková, že platí $x^k = x^l$ pro všechna $x \in S$. Nechť $n = k - l$. Pak $x^n \cdot x^n = x^k \cdot x^{k-2l} = x^l \cdot x^{k-2l} = x^{l+k-2l} = x^n$. □

Nyní následuje technika důkazu, že v libovolném nenilpotentním okruhu je testování identit **co-NP**-těžký problém. Základem bude následující věta pro komutativní okruhy, kterou dále zobecníme.

Věta 3.5. *Nechť* $\mathbf{R}$ *je konečný nenilpotentní komutativní okruh. Pak testování identit pro* ***PSP*** *termy v* $\mathbf{R}$ *je* ***co-NP****-těžký problém.*

Důkaz. Myšlenka je taková: pro daný nenilpotentní okruh $\mathbf{R}$ redukujeme známý **NP**-úplný problém 3SAT (neboli splnitelnost 3CNF formulí ve 2-prvkové Booleově algebře) na negaci problému testování identit v $\mathbf{R}$.

Nechť $f = c_1 \wedge \cdots \wedge c_m$ je 3CNF formule a $x_1, \ldots, x_p$ jsou proměnné v f. Nechť V_j je množina literálů (tj. prvků x nebo $\neg x$, $x \in X$) v c_j, n je nejmenší n z předchozího Lemmatu a z je proměnná, nevyskytující se v f. Term $F[f]$ zkonstruujeme takto:

1. Pro $1 \leq i \leq p$, $F[x_i]$ je ${x_i}^n \cdot z^n$ a $F[\neg x_i]$ je $z^n + (-{x_i}^n \cdot z^n)$.
2. Pro $1 \leq j \leq m$, $F[c_j]$ je rovno

   $$F[l_{j1}] + F[l_{j2}] + (-F[l_{j1}] \cdot F[l_{j2}]), \quad \textit{pokud } V_j = \{l_{j1}, l_{j2}\},$$

   a $F[c_j]$ je rovno

   $$F[l_{j1}] + F[l_{j2}] + F[l_{j3}] + (-F[l_{j1}] \cdot F[l_{j2}]) + (-F[l_{j1}] \cdot F[l_{j3}]) + (-F[l_{j2}] \cdot F[l_{j2}]) + F[l_{j1}] \cdot F[l_{j2}] \cdot F[l_{j3}], \quad \textit{pokud } V_j = \{l_{j1}, l_{j2}, l_{j3}\}.$$

3. $F[f] = F[c_1] \cdot \ldots \cdot F[c_m]$.

Je zřejmé, že $F[f]$ je **PSP** term bez konstant. Předchozí konstrukcí se f prodlouží nejvýše konstantněkrát, přesněji: existuje konstanta $c > 0$ nezávislá na f taková, že $|F[f]| \leq c \cdot |f|$, a $F[f]$ je zkonstruovatelný z f v deterministickém polynomiálním čase.

Tvrzení: $F[f] \neq 0$ v $\mathbf{R} \iff f$ je splnitelná.

Díky tomuto tvrzení je testování identit **PSP** termů bez konstant v $\mathbf{R}$ **co-NP**-těžký problém. Následuje důkaz tohoto tvrzení.

Všimněme si, že je $v[F[f]] = 0$ pro všechna přiřazení hodnot v z S za proměnné $F[f]$ taková, že $v[z^n] = 0$. Nechť v je nějaké přiřazení hodnot z S za proměnné $F[f]$ takové, že $v[z^n] \neq 0$. Označme $\beta = v[z^n]$, $T_v = \{v[x_i^n] \cdot \beta | 1 \leq i \leq p\} \cup \{0, \beta\}$.

Definujme operace g, h, i na S následovně: $g(x, y) = x + y + (-x \cdot y)$, $h(x, y) = x \cdot y$, $i(x) = \beta + (-x)$. Nechť $\hat{T}_v$ je uzávěr T_v na operace g, h, i a $\mathbf{g}, \mathbf{h}, \mathbf{i}$ jsou po řadě restrikce g, h, i na $\hat{T}_v$. Pak

$\mathbf{B}_v = (\hat{T}_v, \mathbf{g}, \mathbf{h}, \mathbf{i}, 0, \beta)$ je netriviální Booleova algebra.

Důkaz probíhá takto: pro všechna nezáporná celá čísla i, definujeme množiny T_i induktivně jako

1. $T_0 = T_v$
2. $T_i = T_{i-1} \cup \{z \in S | \exists x, y \in T_{i-1} : \ z = g(x,y), \ nebo \ z = h(x,y), \ nebo \ z = i(x)\}$.

Pak $\hat{T}_v = \cup_{i \geq 0} T_i$. Matematickou indukcí se dá dokázat, že pro všechna $i \geq 0$ a všechna $x, y \in T_i$ platí $x = x \cdot x, \ x \cdot y = y \cdot x, \ x \cdot \beta = \beta \cdot x = x$. Tedy rovnosti platí i pro všechna $x, y \in T_v$. Proto $(T_v, \mathbf{g}, \mathbf{h})$ je netriviální distributivní svaz. Navíc ale pro všechna $x \in \hat{T}_v$ platí $g(0,x) = x$, $g(\beta, x) = \beta$, $g(x, i(x)) = 0$. Tedy $(\hat{T}_v, \mathbf{g}, \mathbf{h}, \mathbf{i}, 0, \beta)$ je distributivní svaz s mezemi $0, \beta$, a tedy Booleova algebra.

Jestliže f není splnitelná, pak $f = 0$ na dvouprvkové Booleově algebře a tedy $f = 0$ na každé netriviální Booleově algebře.

Díky konstrukci $F[f]$ existuje nějaké přiřazení hodnot w z $\hat{T}_v$ do proměnných f, konkrétně $w[x_i] = v[x_i^n] \cdot \beta$ pro $1 \leq i \leq p$, takové, že $w[f] = v[F[f]]$.

Nechť $v[F[f]] = 0$ na $\mathbf{R}$ pro všechna přiřazení v hodnot z S za proměnné $F[f]$. Předpokládejme, že f je splnitelná pro nějaké ohodnocení w z množiny $\{0,1\}$ za proměnné f. Nechť v je právě to přiřazení hodnot z S za proměnné $F[f]$, jenž splňuje pro $1 \leq i \leq p$

- $v[x_i] = v[z]$, když $w[x_i] = 1$, a
- $v[x_i] = 0$, když $w[x_i] = 0$.

Pak pro $1 \leq i \leq p$, $(v[x_i])^n \cdot \beta = \beta$, pokud $w[x_i] = 1$ a $(v[x_i])^n \cdot \beta = 0$, pokud $w[x_i] = 0$.

Nechť $\mathbf{g}', \mathbf{h}', \mathbf{i}'$ jsou ve stejném pořadí restrikce g, h, i na $\{0, \beta\}$. Pak $(\{0, \beta\}, \mathbf{g}', \mathbf{h}', \mathbf{i}', 0, \beta)$ je izomorfní dvouprvkové Booleově algebře. A tedy $v[F[f]] = \beta \neq 0$. Proto $F[f] \neq 0$ v $\mathbf{R}$.

□

Definice. Nechť $\mathbf{R}$ je konečný okruh. Množina *centrálních idempotentů* je množina

$$CE(\mathbf{R}) = \{r \in S : r^2 = r, rs = sr, s \in S\}.$$

Množina $CE(\mathbf{R})$ je uzavřená na operace $\vee, \wedge, \neg$ definované v Tvrzení 3.2 (neboť $\forall x \in CE(\mathbf{R}) : (\neg x)^2 = (1-x)^2 = 1 - 2x + x^2 = 1 - 2x + x = 1 - x$; $(1-x)s = s - xs = s - sx = s(1-x), \forall s \in S$. Obdobně se ověří i obě binární operace). Tedy $\mathbf{CE(R)} = \langle CE(\mathbf{R}), \vee, \wedge, \neg, 0, 1 \rangle$ je Booleova algebra.

Definujme λ_R jako nejmenší n z Lemmatu 3.4. Protože je $J(\mathbf{R})$ nilpotentní, je taktéž nil-ideálem, tedy sestává výhradně z nilpotentních prvků, proto platí:

$$\begin{aligned} J(\mathbf{R}) &\models x^{\lambda_R} \approx 0, \\ \mathbf{R}/I &\models x^{2\lambda_R} \approx x^{\lambda_R}, \end{aligned}$$

pro libovolný ideál I okruhu $\mathbf{R}$.

Z Lemmatu 3.4 plyne fakt, že pro každý *komutativní* okruh $\mathbf{R}$

existuje term $f(x)$ (tvaru x^n), jehož obor hodnot je $CE(\mathbf{R})$.

K zobecnění pro libovolný okruh nám stačí pouze následující:

existuje term $f(x_1, \ldots, x_k)$, jehož obor hodnot je alespoň dvouprvková množina centrálních idempotentů $\mathbf{R}$.

Definice. $\mathcal{BA}$ bude značit třídu Booleových algeber. Pro Booleovu algebru $\mathbf{B}$ a neprázdnou podmnožinu U algebry $\mathbf{B}$ budeme značit

$$\mathbf{B}|_U \models s(x_1, \ldots, x_n) \approx t(x_1, \ldots, x_n),$$

pokud $s(a_1, \ldots, a_n) = t(a_1, \ldots, a_n)$ platí pro libovolné prvky $a_1, \ldots, a_n \in U$.

Lemma 3.6. *Nechť U je aspoň dvouprvková podmnožina Booleovy algebry $\mathbf{B}$. Pak*

$$\mathcal{BA} \models s \approx t \iff \mathbf{B}|_U \models s \approx t,$$

pro libovolnou rovnici $s \approx t$ v jazyce Booleových algeber.

Důkaz. Ze Stoneovy prvoideálové věty pro Booleovy algebry plyne, že existuje homomorfizmus μ z B do dvouprvkové Booleovy algebry 2_{BA} takový, že $\mu|_U$ je taktéž na. Tedy z $B|_U \models s \approx t$ plyne $2_{BA} \models s \approx t$. A to implikuje $\mathcal{BA} \models s \approx t$. □

Definice. Pro daný okruhový term f a okruh $\mathbf{R}$ definujme $Rg_R(f)$ obor hodnot f v $\mathbf{R}$.

Tvrzení 3.7. *Nechť $\mathbf{R}$ je okruh, pro který lze nalézt term $f(x_1, \ldots, x_k)$, jehož obor hodnot je alespoň dvouprvková množina centrálních idempotentů $\mathbf{R}$. Pak testování identit v $\mathbf{R}$ je **co-NP**-těžký problém.*

Důkaz. Stačí pozměnit důkaz Věty 3.5 tak, že změníme definici $F[f]$ takto:

$$\begin{aligned} F[x_i] &\quad je \quad f(x_{i1}, \ldots, x_{ik}) \\ F[\neg x_i] &\quad je \quad f(z_1, \ldots, z_k) + -f(x_{i1}, \ldots, x_{ik}) \cdot f(z_1, \ldots, z_k). \end{aligned}$$

Nechť s je Booleovská formule v 3CNF. Pak

$$\begin{aligned} \mathcal{BA} \models s \approx 0 &\iff CE(\mathbf{R})|_{Rg_R(f)} \models s \approx 0 \quad (Lemma\ 3.6) \\ &\iff \mathbf{R} \models F[s] \approx 0 \quad (definice\ CE(\mathbf{R})), \end{aligned}$$

tedy máme **co-NP**-těžkost testování identit. □

Protože potřebujeme silnější verzi předchozího tvrzení, zadefinujme

$$CE_J(\mathbf{R}) = \{r \in S : \ r/J(\mathbf{R}) \in CE(\mathbf{R}/J(\mathbf{R}))\},$$

což je množina prvků $\mathbf{R}$, jejichž obrazy v $\mathbf{R}/J(\mathbf{R})$ jsou centrální idempotenty.

Lemma 3.8. *Nechť $r \in CE_J(\mathbf{R})$. Pak*

$$r/J(\mathbf{R}) = 0/J(\mathbf{R}) \iff r^{\lambda_R} = 0.$$

Důkaz.

$$\begin{aligned} r/J(\mathbf{R}) = 0/J(\mathbf{R}) &\implies r \in J(R) \\ &\implies r^{\lambda_R} = 0 \\ &\implies r^{\lambda_R}/J(\mathbf{R}) = 0/J(\mathbf{R}) \\ &\implies r/J(\mathbf{R}) = 0/J(\mathbf{R}), \end{aligned}$$

neboť $r/J(\mathbf{R})$ je idempotentní. □

Tvrzení 3.9. *Nechť* $\mathbf{R}$ *je nenilpotentní konečný okruh. Jestliže existuje term* f *takový, že* $Rg_R(f) \subseteq CE_J(\mathbf{R})$ *a* $|Rg_R(f)/J(\mathbf{R})| \geq 2$*, pak testování identit v* $\mathbf{R}$ *je* ***co-NP****-úplný problém.*

Důkaz. Oproti Tvrzení 3.7 máme k dispozici pouze netriviální množinu centrálních idempotentů modulo Jacobsonův radikál. Aby bylo vidět, že to není problém, položme $U = Rg_R(f)/J(\mathbf{R})$. Jelikož $CE(\mathbf{R}/J(\mathbf{R})) = CE_J(\mathbf{R})/J(\mathbf{R})$, dostáváme pro 3CNF Booleovskou formuli s:

$$\begin{aligned} \mathcal{BA} \models s \approx 0 &\iff CE(\mathbf{R}/J(\mathbf{R}))|_U \models s \approx 0 \quad (\textit{Lemma } 3.6) \\ &\iff \mathbf{R}/J(\mathbf{R}) \models F[s] \approx 0 \quad (\textit{definice } CE(\mathbf{R})) \\ &\iff \mathbf{R} \models F[s]^{\lambda_R} \approx 0 \quad (\textit{Lemma } 3.8), \end{aligned}$$

kde $F[s]$ je modifikováno z důkazu Věty 3.5. □

Věta 3.10. *Nechť* $\mathbf{R}$ *je nenilpotentní konečný okruh. Pak testování identit v* $\mathbf{R}$ *je* ***co-NP****-úplný problém.*

Důkaz. Jelikož $\mathbf{R}$ je nenilpotentní, není roven svému Jacobsonovu radikálu $J(\mathbf{R})$, a navíc je $\mathbf{R}/J(\mathbf{R})$ direktní sumou maticových okruhů nad konečnými tělesy. Fixujeme surjektivní homomorfizmus

$$\mu : \mathbf{R} \longrightarrow \prod_{i=1}^{n} M_{k_i}(F_i)$$

s jádrem rovným $J(\mathbf{R})$. Nechť $k = max\{k_i : 1 \leq i \leq n\}$.

Z Formánkova řešení (1972) slavného Kaplanského problému o existenci centrálních polynomů víme, že existuje polynom $p_k(\vec{x})$, který je centrální pro všechna $M_k(F)$, kde F je těleso. Tedy obor hodnot p_k v každém $M_k(F)$ je

- netriviální, a
- obsahuje pouze centrální prvky.

Zřejmě můžeme předpokládat, že p_k nemá absolutní člen (pokud $p_k = q_k + c$, kde q_k nemá absolutní člen, nahradíme p_k za q_k). Takový polynom se musí vynulovat na všech $M_k(F)$ pro $m < k$. Přesvědčíme se o tom tak, že aplikujeme p_k na matice v $M_k(F)$, jejichž nenulové hodnoty leží v prvních m sloupcích a v prvních m řádcích. Velikost matic se nezmění, ale jediná matice takového tvaru, která je centrální v $M_k(F)$ je nulová matice.

Tvrdíme, že term $f(\vec{x}) = p_k(\vec{x})^{\lambda_R}$ splňuje předpoklady Tvrzení 3.9. Pro libovolné prvky $\vec{r}$ z $\mathbf{R}$ platí: $p_k(\vec{r})^{\lambda_R}/J(\mathbf{R})$ je jednak centrální (dle výběru p_k) a jednak idempotentní (máme zde exponent λ_R). Tedy $Rg_R(f) \subseteq CE_J(\mathbf{R})$.

Zbývá ukázat, že $|Rg_R(f)/J(\mathbf{R})| \geq 2$. Jistě $0 \in Rg_R(f)$, tedy stačí najít prvek $r \in Rg_R(f)$ takový, že $r/J(\mathbf{R}) \neq 0/J(\mathbf{R})$. Položme $k_n = k$. Vyberme prvky $\vec{r} \in R$ takové, že pro nějaké nenulové $c \in F_n$ platí: $\mu f(\vec{r})(n) = c \cdot I$, kde I je jednotková matice z $M_k(F_n)$. Pak ale $f(\vec{r})/J(\mathbf{R}) \neq 0/J(\mathbf{R})$. Tím dostáváme, že obor hodnot f modulo $J(\mathbf{R})$ je netriviální. Nyní můžeme použít Tvrzení 3.9.

□

Literatura

[1] Burris S., Lawrence J.: *Results on the equivalence problem for finite groups*, Algebra Universalis **52** (2004), 495-500.

[2] Burris S., Lawrence J.: *The equivalence problem for finite rings*, J. Symbolic Computation **15** (1993), 67-71.

[3] Goldmann M., Russell A.: *The complexity of solving systems of equations over finite groups*, preprint, 1998.

[4] Horváth G., Szabó C.: *The complexity of cheking identities over finite groups*, preprint, 2005.

[5] Hunt III H.B., Stearns R.E.: *The complexity of equivalence for commutative rings*, J. Symbolic Computation **10** (1990), 411-436.

[6] Lawrence J., Willard R.: *The complexity of solving polynomial equations over finite rings*, rukopis, 1997.

[7] Majerech V.: *Úvod do složitosti a NP-úplnosti*, skriptum, 1999.

[8] Neumann H.: *Varieties of Groups*, Springer-Verlag, 1967.