

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 dihedralních 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 verifying an identity validity (e.g. commutativity, associativity, etc.) for an algebra (group, ring,...). However, this algorithm has exponential time complexity in the length 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 summarize 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