



## ZADANIE BAKALÁRSKEJ PRÁCE

Študent: **Daniel Jahodka**  
ID študenta: 80332  
Študijný program: aplikovaná informatika  
Študijný odbor: 9.2.9. aplikovaná informatika  
Vedúci práce: doc. Ing. Pavol Zajac, PhD.  
Miesto vypracovania: Ústav informatiky a matematiky

Názov práce: **Heuristické riešenie MRHS rovníc**

Jazyk, v ktorom sa práca vypracuje: slovenský jazyk

Špecifikácia zadania:

MRHS rovnice umožňujú efektívne zapísať problém riešenia sústavy nelineárnych Booleovských rovníc. Problém ich riešenia je NP ťažký. Predpokladáme však, že v špecifických prípadoch existuje efektívne riešenie.

Úlohy:

1. Naštudujte známe algoritmy riešenia MRHS rovníc.
2. Navrhните možnosti využitia heuristik na ich zefektívnenie
3. Implementujte navrhnuté algoritmy.
4. Otestujte a štatisticky vyhodnoťte účinnosť heuristik.

Zoznam odbornej literatúry:

1. Zajac, P. A New Method to Solve MRHS Equation Systems and its Connection to Group Factorization. *Journal of Mathematical Cryptology*, 7. s. 367–381. ISSN 1862-2976.
2. Zajac, P. MRHS equation systems that can be solved in polynomial time. *Tatra Mountains Mathematical Publications*, 67. s. 205–219.
3. H. Raddum and P. Zajac: MRHS Solver Based on Linear Algebra and Exhaustive Search. Preprint