Title: Search problems and search for collisions in hash functions
Author: Samuel Čarnoký
Department: The Department of Algebra
Supervisor: prof. RNDr. Jan Krajíček, DrSc.
Supervisor's e-mail address: krajicek@karlin.mff.cuni.cz

Abstract: Central points of this work are NP search problems and the existence of reductions amog them in the relativised world. Absolute separation would separate N from NP. In particular, we talk about the problem of finding collisions in hash functions that must exist due to the famous pigeonhole principle. We present a brief introduction into the topic, we define various NP search problems and recall reductions and separations. Reduction of weak version of PHP to a problem of finding a homogeneous subgraph is described and our own results are presented in the form of reduction of another variant of PHP to a problem related to finding paths in a graph. We talk about reducing the task of finding collisions in multiple functions into finding a collision in one function.

Keywords: NP search, reductions, pigeonhole principle, oracles