Oponentský posudek bakalářské práce

Denis Vald: Důkaz s nulovou znalostí pro isomorfismus grafů

Předložená práce se zabývá tzv. důkazy s nulovou znalostí, tedy protokoly, které umožňují „dokazovateli" přesvědčit „ověřovatele", že disponuje jistou znalostí, aniž by ověřovateli vyzradil jakoukoliv relevantní informaci. V první kapitole je pojem důkazu s nulovou znalostí a různé jeho varianty formalizovány. V druhé kapitole jsou uvedeny příklady protokolů, zejména je (za předpokladu existence jednosměrné funkce) ukázán protokol pro problém 3-obarvitelnosti grafu. Závěrečná kapitola se zabývá otázkou, kdy se sekvenčním a paralelním skládáním protokolů zachovává vlastnost nulové znalosti.

Práci považuji za dobrou a nemám k ní vážnější výhrady. Kromě několika menších formálních nedostatků lze vyčíst špatnou úroveň sazby způsobenou použitým softwarem.

Bakalářskou práci Denise Valda **doporučuji k obhajobě** a navrhuji ohodnotit stupněm **výborně**.

V Praze dne 28.8.2008

Mgr. Libor Barto, Ph.D.