Oponentský posudek bakalářské práce

Rudolf Barczi: Perfektní neinteraktivní důkaz s nulovou znalostí

Bakalářská práce popisuje konstrukci prvního neinteraktivní argumentu s perfektní nulovou znalostí. Tato konstrukce byla publikována v článku autoru Groth, Ostrovsky a Sahai.

Výsledek je sepsán přehledne, s nevelkým množstvím překlepu, pekným a srozumitelným jazykem. Jedinou vážnejší výhradu mám k ponekud přehnané stručnosti práce. Neformální vysvetlení definic by značne zjednodušilo čtení textu. Konkrétne definice úplnosti a správnosti neinteraktivního dukazového systému, nulové znalosti, rekonstrukce cti dokazovatele (a pojem simulátoru), definice "predpoklad neefektivnosti rozhodování náležení podgrupe" jsou zapsány bud' s príliš krátkou vysvetlující poznámkou, nebo pouze formálne. Chybí jakékoliv vysvetlení pojmu booleovského obvodu.

Pres uvedenou výhradu považuji práci Rudolfa Bareziho za dobrou. **Doporucuji ji** proto **k obhajobe** a navrhuji ohodnotit stupnem **výborne**.

V Praze dne 30.8.2007

Mgr. Libor Barto, Ph.D.