POSUDEK VEDOUCÍHO NA BAKALÁŘSKOU PRÁCI LENKY MIŠÁNIKOVÉ *VEŘEJNÁ MINCE*

Tématem práce psané ve slovenštině je vztah interaktivních protokolů se soukromou náhodností na jedné straně a veřejnou na straně druhé.

Práce vrcholí důkazem ekvivalence těchto dvou uspořádání. Text je srozumitelný, bez velkého množství překlepů. Oceňuji, že studentka se pokusila přiblížit problematiku neformálním popisem, který doplňuje formální důkazy.

Některé kroky v důkazech jsou poněkud nevyvážené, co do obtížnosti. Např. na str. 24 uprostřed je kostrbatě dokazována triviální množinová nerovnost

$$\sum_{i \leq l} |h_i(C)| \leq \sum_{i \leq l} |H(C)|\,,$$

zatímco ne zcela samozřejmá nerovnost

$$|C| \leq \sum_{i \leq l} |h_i(C)|\,,$$

která hraje v důkazu důležitou roli, je ponechána bez komentáře.

Uvítal bych také (např. v závěru) informaci o tom, odkud autorka důkazy čerpala a do jaké míry je modifikovala.

Drobnosti.

- V tvrzení 2.a) Lemmatu 16 je obrácená nerovnost.
- Raději Goldwasserov-Sipserov protokol (nebo alespoň Goldwasser-Sipserov protokol) namísto anglizujícího Goldwasser-Sipser protokol.
- Před vylučovacím *alebo* se píše čárka.

Práce splňuje požadavky kladené na bakalářskou práci.

Praha 31. srpna 2008

Štěpán Holub

[redacted]

Mám k ní „výborné"