MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

10. června 2021

Věc: Oponentský posudek na diplomovou práci Jana Václavka „On search complexity of discrete logarithm“

Diplomová práce Jana Václavka představuje podivuhodný počin. Jedná se o práci vynikající kvality, přinášející nové poznatky v teorii složitosti. Práce se zabývá úplnými problémy pro tzv. třídy PPP a PWPP. Ukazuje úplnost některých známých problémů pro tyto třídy a zároveň zavádí problémy nové, které jsou pro ně též úplné a které upravují potíže s dříve definovanými problémy podobného typu. Práce tak zodpovídá některé známé otevřené problémy. Je zcela nepochybné, že výsledky v práci obsažené jsou publikovatelné v předních časopisech a konferencích teoretické informatiky.

Práce je psána pečlivě, svěží angličtinou a težko ji lze něco vytknout. Ukazuje na vyzrálou matematickou osobnost autora.

Osobně bych pouze doporučil přeskupit důkaz lematu 3 tak, aby začínal částí ze strany 14 "*We can now proceed*..." a teprve pak se vrátil k otázce implementace funkce f_0 a f_1. Při současném uspořádání důkazu nemá čtenář před sebou jasný cíl a neví například, co si představit pod hodnotami *m* a *s*. Kromě těchto drobností byla radost práci číst.

Mohu tak jednoznačně konstatovat, že práci doporučuji schválit jako diplomovou a navrhnout na ocenění.

Prof. Mgr. Michal Koucký, Ph.D.

Informatický ústav Univerzity Karlovy
Malostranské nám. 2/25, 118 00 Praha 1
telefon: 951554230, fax: 257531014
e-mail: sekretariat@iuuk.mff.cuni.cz