MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

16. června 2021

Posudek vedoucího práce Bc. Jana Václavka:

Diplomová práce kolegy Václavka s názvem „On search complexity of discrete logarithm“ se zabývá složitostí problému diskrétního logaritmu v kontextu třídy výpočetní složitosti TFNP a jejích podtříd. Hlavními výsledky práce jsou důkazy úplnosti vhodných formulací problému diskrétního logaritmu pro třídy PPP a PWPP. Mimo jiné tedy práce řeší otevřený problém z článku Sotirakiové, Zampetakise a Zirdelise „PPP-Completeness with Connections to Cryptography“ (FOCS 2018).

Výsledky v práci vznikly spoluprací se mnou jako vedoucím. K podílu kolegy Václavka na výsledcích musím zdůraznit, že většina technické části práce je postavena na jeho myšlenkách, které za mé pomoci samostatně rozvedl do rigorózních důkazů. Obzvláště v části ukazující PWPP-těžkost vhodné varianty diskrétního logaritmu nazvané DLOG kolega Václavek prokázal svou matematickou vyspělost. Pro důkaz tohoto tvrzení je definován nový vyhledávací problém DOVE, s jehož pomocí jsou elegantně vyřešeny technické problémy vyvstávající při redukci z PWPP-úplného problému COLLISION na DLOG. Celkově je prezentace dosažených výsledků na výborné úrovni po jazykové i formální stránce. Osobně mám také radost z důkazu PWPP-těžkosti alternativní formulace problému diskrétního logaritmu nazvané INDEX. Zprvu jsem očekával, že takový výsledek ve skutečnosti nelze dokázat a navrhoval kolegovi Václavkovi, aby se pokusil dokázat odpovídající negativní výsledek pomocí separace problémů INDEX a PIGEON.

Výsledky práce jsme společně ve formě článku odeslali k recenznímu hodnocení a případné prezentaci do relevantní konference v teoretické informatice a následně plánujeme publikovat ve vhodném časopise. Věřím tomu, že výsledky této práce budou motivovat další výzkum tříd PPP a PWPP a mohou být použity jako základ pro nové charakterizace těchto tříd.

Doporučuji práci k obhájení jako diplomovou a dle uvážení komise také k navržení na ocenění.

Mgr. Pavel Hubáček, 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