Oponentský posudek na doktorskou disertační práci Jána Picha *Complexity theory in Feasible Mathematics*

Předložená práce je soubor dvou článků opatřený krátkým úvodem.

První článek se zabývá otázkou, zda je možno dokázat netriviální dolní odhady na složitost booleovských funkcí ve fragmentech omezené aritmetiky. To je velice zajímavý problém, protože dolní odhady na velikost booleovských obvodů počítajících konkrétní funkce se zatím podařilo dokázat jen pro velmi speciální obvody. Kdyby se podařilo dokázat, že v některých teoriích to nelze, vysvětlilo by to, proč je tento problém tak těžký. I přes velký význam tohoto problému, bylo o tomto problému publikováno jen pár článků. Pichův článek je možná první, který se tímto problémem zabývá systematicky a v tom je jeho velký přínos. Jeho přístup je založen na použití tzv. dosvědčovacích vět v omezené aritmetice. To jsou věty, které říkají, že pokud se dokáže sentence určitého typu v určité teorii, pak lze dosvědčit existenčně kvantifikované číslo pomocí algoritmu resp. obvodu určitého typu. Tím se dá otázka dokazatelnosti převést na otázku existence algoritmů resp. obvodů. Chceme-li dokázat nedokazatelnost, musíme pak argumentovat, že určité algoritmy neexistují. To může být problém, ale je zajímavé něco takového dokázat i s použitím nedokázaných předpokladů, které jsou obecně přijmáné jako pravděpodobně pravdivé. Pich má v práci několik vět tohoto typu, z nichž nejdůležitější je Theorem 1.6.1, který má také poměrně složitý důkaz.

Druhý článek se zabývá formalizací vět z teorie složitosti v omezené aritmetice. Jde zejména o formalizaci tzv. PCP věty. V této oblasti mohl Pich navázat na řadu výsledků v tomto směru, zejména na práce Jeřábka. Ale i když mnoho pojmů už bylo formalizováno, musel ještě mnoho dalších formalizovat, než se dostal k vlastním větám a důkazům. Hlavní výsledky jsou důkaz exponenciální PCP věty (slabší verze PCP věty), PCP věty a formalizace expanderů. Formalizace expanderů potřeboval pro důkaz PCP věty, ale mohou mít využití i v mnoha dalších případech. To, že se dá

PCP věta formalizovat v nějakém fragmentu není překvapivé. O co jde je, zjistit ve kterém nejslabším fragmentu se to dá udělat. To je vlastně základní otázka důkazové složitosti: jaké potřebujeme předpoklady na to, abychom danou větu dokázali. Jak je patrné z textu práce, formalizace byla technicky náročná, ale nejedná se o rutinní práci - bylo potřeba vymyslet vhodné pojmy a formulace lemat a vět.

Pichova práce patří bezesporu k velmi dobrým disertacím. Nemám pochybnosti o výsledcích a jejich významu. Jako oponent, ale cítím povinnost přidat i pár kritických poznámek.

1. Je škoda, že úvod k souboru článků je tak krátký. Myslím si, že je obtížné pro laiky v tomto oboru pochopit význam výsledků a takto krátký, navíc dosti technický, úvod čtenáři moc nepomůže. Doufám, že to autor alespoň částečně napraví tím, že využije obhajobu k tomu, aby vysvětlil své výsledky členům komise, kteří jsou z jiných oborů.
2. Nutnost používat poměrně složitý formalismus je v podstatě věci. Přesto si myslím, že by se dala čitelnost práce zlepšit, kdyby se autor více snažil. Zejména by práci prospělo, kdyby autor zjednodušil formulace hlavních vět a tvrzení (i za cenu toho, že by byly trochu slabší). Např. předpoklad SIZE(nˆk)¥subset NCˆ1 v Proposition 1.6.1, je ekvivalentní předpokladu P/poly¥subset NCˆ1, takže je zřejmé, že by se dalo toto tvrzení formulovat obecněji a srozumitelněji.
3. Další poznámka je podobného druhu. Domnívám se, že by bývalo bylo lepší použít teorie druhého řádu. Je to do značné míry jen formální věc, ale myslím, že by se čtenář v textu orientoval lépe a některé formalizace by mohly být jednodušší.

Shrnutí. Jedná se o velmi kvalitní práci s nertiválními novými výsledky. Ján Pich prokázal schopnost samostatné vědecké práce. Doporučuji udělení titulu PhD.

V Praze, 9.10.14 Prof. RNDr. Pavel Pudlák, DrSc