Posudek diplomové práce

Název: The BSS model and Cryptography

Autorka: Bc. Kristina Hostáková

Tématem diplomové práce slečny Hostákové je studium pojmu jednosměrné funkce v kontextu reálných čísel a výpočetního modelu navrženého L.Blumovou, M.Shubem a S.Smalem v r.1989 (tzv. BSS model). Grigoriev a Nikolenko v r.2012 studovali spojité jednosměrné funkce na realných číslech motivováni možnými aplikacemi v biometrii. Definovali několik více proměnných funkcí, které by mohly mít vhodné vlastnosti, ale nedokázali žádný spodní odhad, který by jejich hypotézy podpořil.

Práce slečny Hostákové je teoretická a jejím cílem bylo dokázat aspoň nějaký netriviální spodní odhad na složitost invertování nějaké funkce v BSS modelu, a to bez dodatečných hypotéz. BSS model umožňuje studovat netriviální situace, které v obvyklém binárním světě Turingových strojů nemají obdoby (např. funkce počítané v konstantním čase či uvažovat pouze vstupy délky 1). Obtížnost této práce neleží v nějakých komplikovaných kombinatorických úvahách, ale v tom, že je třeba propojit různé oblasti: výpočetní modely, semialgebraickou geometrii a ideje ze základů kryptografie.

Slečna Hostáková dosáhla zajímavých výsledků. V kapitole 3 ukázala, že funkci druhá mocnina, kterou lze v BSS modelu spočítat v konstantním čase, nelze (v žádném čase) invertovat přesně (Cor.3.2) a ani přibližné invertování nelze provést v konstatním čase (Thm.3.3), nýbrž je třeba čas log log y či invertující stroj musí použít nějaké realné konstanty různé od 0,1 – toto je obdoba neuniformních algoritmů z binárního světa (Cor.3.19). Tento spodní odhad je doplněn podobným horním odhadem získaným netriviální analýzou Newtonovy metody (Thm. 3.15); jednodušší odhad O(log y) je dokázán zvlášť (Thm.3.5). V kapitole 4 pak slečna Hostáková dokázala podobný horní odhad pro invertování všech funkcí 1 realné proměnné počítané BSS strojem v konstantním čase. Prezentace argumentů v těchto kapitolách je pečlivá a je doplněna ilustrací obecných situací konkrétními příklady. U několika tvrzení je důkaz podán dlouhým elementárním výpočtem: to je z důvodu odvození horního odhadu na čas BSS stroje (který provádí jen elementární kroky).

Toto jádro diplomové práce je doplněno stručným a jasným úvodem do BSS modelu (kap.2) a dále diskusí o dalším možném směru výzkumu (kap.5): zde slečna Hostáková prezentuje dvě funkce, které jsou definované jednoduchými (ale nekonstantními) BSS stroji a pro které metody této práce nedávají žádný horní odhad na jejich invertování – jsou tedy možnými kandidáty na funkce obtížně invertovatelné.

Podle mého názoru napsala slečna Hostáková velmi pěknou diplomovou práci a doporučuji, aby ji úspěšně obhájila.

Jan Krajíček
školitel, KA

22.5.2016