Posudek oponenta bakalářské práce

předložené na Matematicko-fyzikální fakultě Univerzity Karlovy

Autor:	Václav Zvoníček
Název práce:	Schoof's algorithm for Weierstrass curves
Stud. program a zaměření:	informatika, obecná informatika
Rok odevzdání:	2023
Jméno a tituly vedoucího:	Mgr. Martin Mareš, Ph.D.
Pracoviště:	Katedra aplikované matematiky
Kontaktní e-mail:	mares@kam.mff.cuni.cz

Popis práce

Předložená práce se zabývá Schoofovým algoritmem, který stanovuje počet racionálních bodů eliptické křivky nad konečným tělesem. Na těchto křivkách je založena velká část moderní kryptografie a počet racionálních bodů je zásadní pro posouzení bezpečnosti konkrétní křivky.

Jelikož je k vybudování algoritmu potřeba velké množství konceptů z teorie algebraických křivek, první tři kapitoly se věnují jejich vysvětlení. Postupně jsou představeny Weierstrassovy křivky v afinním i projektivním pojetí, grupy eliptických křivek, endomorfismy, torzní podgrupy, Hasseho věta a Frobeniova stopa.

Ve čtvrté kapitole je odvozen samotný Schoofův algoritmus: nejprve základní myšlenky, které k němu vedou, poté samotný algoritmus. Následně je rozebrána jeho asymptotická složitost.

Pátá kapitola se zabývá vlastní implementací algoritmu v jazyce C++. Kromě popisu implementace diskutuje návrhová rozhodnutí, zejména volbu knihoven pro práci s polynomy nad konečnými tělesy. Také popisuje experimenty, kterými byla ověřována správnost implementace a rychlost při reálném použití.

Hodnocení

Práce vybočuje z množiny běžných informatických bakalářských prací. Věnuje se sice problému, který je svou povahou zřetelně informatický – analýze a implementaci algoritmu, navíc zásadnímu pro bezpečnost moderních počítačových systémů. Na druhou stranu ale vyžaduje obsáhlé matematické pozadí teorie algebraických křivek, a to už pro samu formulaci úlohy. Tím se z ní nevyhnutelně stává práce převážně matematická, navíc na úrovni výrazně převyšující doporučené kurzy bakalářského studia.

Oceňuji, že autor zvládl tomuto obtížnému tématu porozumět a na necelých 20 stranách textu čtenáři představit potřebné části teorie. Nejsou to přitom jen suché definice a znění vět přepsaných z literatury, často je uvedena alespoň stručná motivace a jednodušší tvrzení jsou dokázána.

Občas se přeci jenom stane, že nějaká notace není zavedena pořádně a čtenář nealgebraik tápe. Například:

- značení $(x : y : z)$ pro body projektivní roviny,

- několik různých použití hranatých závorek (zejména ve vztahu (3.1) znamenají něco úplně jiného než vzápětí v (3.4)),
- $\overline{K}$ pro algebraický uzávěr tělesa (aniž by bylo vysvětleno, proč vůbec uzávěr potřebujeme),
- úvaha o stupních polynomů ψ_n v oddílu 2.2 se nejspíš odkazuje na jiné polynomy zavedené později.

S takto vybudovaným aparátem je sice popis Schoofova algoritmu stále nesnadný, ale rozhodně funkční a srozumitelný. Analýza složitosti je příjemně detailní. Trochu ji kazí chybná úvaha o Euklidovu algoritmu pro polynomy (3. odrážka na str. 25), ale i po opravení se složitost tohoto kroku stále schová do složitosti ostatních operací.

Implementace algoritmu je čistá a přímočará. Oceňuji, jakou pozornost autor věnoval ověřování korektnosti porovnáváním výsledků s jinými implementacemi.

Za důležité místo práce považuji experimenty s dobou výpočtu pro různě velké vstupy a prokládání funkcí naměřenými hodnotami. To ukázalo, že algoritmus je výrazně rychlejší, než předpověděl teoretický rozbor. Důvod byl nalezen podrobnějším zkoumáním algoritmů pro polynomiální aritmetiku v knihovně NTL.

Celkově práci považuji za zdařilou i po informatické stránce. Implementace a její popis sice nejsou rozsáhlé a na neznalého čtenáře by mohly působit jednoduše. Ale napsat korektní a efektivní program tohoto druhu vyžaduje hluboké porozumění problematice – bez něj by program bylo prakticky nemožné odladit.

Práce je napsána čtivou angličtinou takřka bez jazykových chyb. Po odborné stránce bych vytkl větší množství drobných faktických chyb a používání pojmů a značení, které nebyly pořádně zavedeny.

Použité zdroje jsou korektně citovány. Jen v úvodu, který čerpá převážně z monografie Lawrence Washingtona, bych uvítal odkazy alespoň na konkrétní kapitoly.

Práci doporučuji přijmout jako bakalářskou.

Celkové hodnocení: velmi dobře

Práci navrhuji na zvláštní ocenění: ne

V Praze dne 20. června 2023
Martin Mareš