Posudek vedoucího na bakalářskou práci

Igor Eržiak: Counting the points on elliptic curves over finite fields

Hlavním cílem předložené práce je popis a implementace Schoofova algoritmu—prvního polynomiálního algoritmu pro výpočet řádu eliptické křivky nad konečným tělesem. Z technických důvodů se práce omezuje na tělesa charakteristiky různé od 2 a 3. Práce je členěna na tři hlavní části. V první je přehled základních pojmů souvisejících s eliptickými křivkami a grupovou operací, ve druhé je pak stručně popsána teorie nutná k pochopení Schoofova algoritmu (endomorfismy křivky a jejich konkrétní popis, Frobeniovo zobrazení a jeho charakteristický polynom a Hasseho odhad na řád křivky). Třetí část se zabývá samotným algoritmem.

Zadání práce považuji za splněné. Autor se musel vyrovnat s nedostatky zdrojů, kde je často dobře vysvětlena základní myšlenka Schoofova algoritmu, ale různé technické detaily, kterých se při pokusu o implementaci vyskytne řada, ošetřeny nejsou. Musel také najít vhodnou rovnováhu mezi teorií (ta je rozsáhlá a její zpracování by vydalo na řadu studentských prací) na jedné straně a potřebou dovést do zdárného konce vlastní jednoduchou implementaci na straně druhé.

Moje hlavní připomínka směřuje k tomu, že některé podstatné detaily implementace musí čtenář luštit z komentářů kódu v SAGE (byť komentáře jsou ke cti autora v kódu hojně přítomny). Dále také není dotaženo do konce vysvětlení na konci str. 13, proč a jak přesně algoritmus funguje při nalezení faktoru dělícího polynomu $\psi_l(x)$ (dlužno ovšem říci, že v tento problém je zděděný už z použitých zdrojů).

Práci **doporučuji k obhajobě** a návrh hodnocení přikládám zvlášť.

V Praze dne 1. 9. 2018 doc. RNDr. Jan Šťovíček, Ph.D.