Posudek vedoucího na bakalářskou práci
Václava Zvoníčka nazvanou
Schoof's algorithm for Weierstrass curves

Jde o velmi pěknou práci, která kombinuje nelehkou oblast matematiky s implementací pracující s knihovnou pro výpočty s libovolnou přesností (multiprecision arithmetic). Vhodnost zadání byla předem konzultována s garantem bakalářského oboru informatika docentem Ondřejem Čepkem.

V prvních třech kapitolách, v rozsahu 15 stran, student popisuje sčítání bodů na hladké Weierstraßově křivce a znalosti o struktuře této grupy, které jsou potřebné pro popis Schoofova algoritmu. Tyto kapitoly jsou napsány přesně a srozumitelně. Daly by se o něco zkrátit, neboť výkladu projektivních bodů by bylo možné se vyhnout. Považuji však za adekvátní respektovat přání studenta látku vyložit tak, aby bylo patrné, že bod v nekonečnu není formálním konstruktem, ale má své přirozené zdůvodnění.

Výkladu Schoofova algoritmu je věnováno šest stran. Výklad se opírá o dříve uvedený popis dělících polynomů, o Hasseho větu a o charakteristickou rovnici Frobeniova endomorfismu. Bez pochopení těchto pojmů a výsledků se nedá Schoofův algoritmus vysvětlit. S jejich znalostí se naopak vyjeví, že jde vlastně o poměrně jednoduchou záležitost, a to zejména v té více frekventované větvi základní smyčky. Ta méně frekventovaná větev, jejíž vynechání by na průměrnou dobu běhu algoritmu mělo jen malý vliv, je pro pochopení a popis náročnější. I tato větev je v práci správně a srozumitelně popsána, což je dobře, protože ona je jakýmsi mostem k následnému a výkonnějšímu algoritmu SEA.

Popisu složitosti Schoofova algoritmu jsou věnovány strany dvě. Považuji za přínosné, že tato složitost je popsána parametricky, tedy v závislosti na složitosti násobení polynomů nad daným tělesem.

Implementace a výsledky měření jsou popsány na sedmi stranách. Určitý prostor je věnován zdůvodnění volby knihovny a popisu organizace kódu. To je následováno komentářem některých detailů implementace a popisem naměřených hodnot.

Kvalitu programu a dokumentaci vnímám jako plně vyhovující. Podrobnosti v tomto směru jistě doplní oponent. Rád bych ale uvedl, že pokud se pracuje jen s malými prvočísly, tak je možné Schoofův algoritmus naprogramovat o dost úsporněji, protože není nutné využívat určitých redukcí, které jsou při tom pro účinnost algoritmu při větších prvočíslech zásadního významu. Program vytvořený studentem vnímám jako poloprofesionální – kód sám o sobě je v pořádku; pro plné využití potenciálu algoritmu by však bylo potřeba mít implementaci umožňující masivní paralelizaci.

Níže následují drobné výhrady a jedna či dvě žádosti. Ty by však neměly podle mého soudu mít významný vliv na hodnocení práce.

1. V úvodu mě zarazilo tvrzení, že "it is advised to use a prime-order subgroup of the group of an elliptic curve". Zní to podivně v kontextu, kdy v kryptografii založené na eliptických křivkách se pracuje výhradně s grupami prvočíselného řádu. To, aby grupa dané křivky měla prvočíselnou podgrupu malinkého indexu je základní požadavek, ze kterého se nikdy neslevuje.

2. Během přípravy práce jsem opakovaně narážel na tendenci studenta uvádět různá zajímavá fakta, která nebyla úplně nutná pro výklad daného

tématu. Něco málo z toho v práci přetrvalo. Například nebyla nutná diskuse přechýlených (to jest *twisted*) křivek.

3. V jednom místě (Proposition 1.4.2) by mělo být psáno $\phi_q \ominus [1]$ spíše než $\phi_q - 1$.

4. Nelíbí se mi zápis čísla jako $6.18e-07$. To snad bylo možno konvertovat do čitelnějšího tvaru.

5. Rád bych, aby se student pokusil najít vhodnou délku prvočísla tak, aby algoritmus trval třeba dvě, tři hodiny, a toto srovnal se vzorcem uvedeným na obrázku 5.6. Není mi úplně jasné, proč se omezil na běhy trvající nejvýše 40 vteřin.

6. Pokud student narazil při přípravě práce i na jiné implementace, tak by asi bývalo vhodné se o nich v práci zmínit, případně srovnat výkonnost své implementace s tím, co na webu nalezl. Vnímám to jako svoji chybu, že jsem ho na toto včas neupozornil.

Navrhuji, aby práce byla přijata jako práce bakalářská a hodnocena stupněm *výborně*.

Aleš Drápal

V Karlíně 26. května 2023