Posudek oponenta na diplomovou práci Jakuba Skalického: Efektivní aritmetika eliptických křivek nad konečnými tělesy

Práce má tři části. Polovina práce (kapitola 1) je věnována úvodu do teorie eliptických křivek. Kapitola 2 (7 stran) seznamuje s různými metodami reprezentace bodů projektivních eliptických křivek. Dalších 12 stran (kapitola 3) je věnováno Edwardsovým křivkám. Závěrečné čtyři strany jsou věnovány tabulkám měření rychlosti a úvahám, proč Edwardsovy křivky (a eliptické křivky vůbec) nejsou v praxi využívány tak, jak by odpovídalo jejich efektivitě. Z textu práce je zcela nejasné zda tabulky uvedené v závěru jsou odněkud přejaté nebo jsou výsledkem měření, které autor provedl. Zadání práce naznačuje, že k implementaci dojít mělo. Práce se však od zadání výrazně odchýlila – o řešení problému diskrétního logaritmu v práci zmínka není buď vůbec, nebo je tak marginální, že jsem ji přehlédl.

Práce je napsána, s výjimkou některých míst třetí kapitoly, co se týče srozumitelnosti výjimečně dobře. Angličtina je téměř až vybraná. Formálních chyb je málo, byť zcela ojedinělé také nejsou (co se týče angličtiny tak tu a tam je špatně třetí osoba jednotného čísla, typicky *exist* místo *exists*). Co se týče zvyklostí typických v odborném textu, tak je to snad jedině mylné užívání malého písmena v referencích (*proposition 1.1* místo *Proposition 1.1* atd.) a používání *respectively* na všech místech výskytu v závorce uváděných alternativ (píše se jen u posledního výskytu a v případě umístění alternativ do závorek se i zde poslední dobou spíše vypouští).

K první kapitole lze vznést jako obecnou výhradu, že nejde za rámec standardního kursu. Nevidím to jako chybu, že je uvedena – koneckonců to není úplně snadná látka. Těžko ale zde spatřovat nějaký přínos. Navíc při zběžném listování lze mít pocit, že látka je kompletně vyložena. A ono to tak není – tu a tam je odkaz na externí referenci. Bylo by bývalo lepší třeba jen menší okruh předložit v úplné formě a zbytek uvést bez důkazů s odkazem na literaturu.

První kapitola není bez věcných nedostatků, většinou formálních: Na straně 4 nahoře je naprosto nesmyslná definice $\tilde{K}$. Zavedené značení homogenních souřadnic je vícekrát porušeno (na straně 4 dole, v poznámce 1.1.8 a asi i jinde). Definice f^* je závislá na indexu i, pracuje se s ní od definice 1.1.9 jakoby i bylo pevné (což odpovídá standardnímu použití, musí se to ale deklarovat). V definici 1.2.2 by mělo jít o *diskrétní* valuační okruh. Valuace $v_P(x)$ jsou použity bez toho, že by byly definovány. Podobně chybí definice $\deg(P)$ a $\mathrm{Princ}(F/K)$. Uvedení tvrzení 1.2.6 bez komentáře může vzbudit dojem, že jde o důsledek Riemannovy věty. Na straně 7 dole by dvakrát mělo být $w(x, y)$ v kontextu $w(x, y) = 0$. V důkazu tvrzení 1.2.9 chybí na počátku vysvětlení, proč je dimenze $\mathcal{L}(P)$ kladná. Na straně 12 je podivná formulace "over $\bar{K}$ even". V lemmatu 1.4.11 má být opakovaně $v_\alpha(l)$, nikoliv jen v_α. Toto

lemma a dvě následující je uvedeno bez důkazu. To samo o sobě nevadí, chybí ale vysvětlující komentář, proč tomu tak je. V druhém řádku důkazu 1.4.15 je použita špatná operace. V tvrzení 1.4.17 nejsou uvedeny všechny předpoklady.

Navzdory uvedeným nedostatkům však považuji zpracování kapitoly 1 za uspokojivé.

Kapitola 2 ukazuje, jak lze výpočet zdvojování a sčítání urychlit, jsou-li použity souřadnice projektivní, Jacobiho a Chudnovských. Uvítal bych podrobnější výklad, který by vzal v úvahu kontext nějakého nadřízeného algoritmu, ve kterém ke sčítání dochází, a vyložil v takovém kontextu, jak dalece se vyskytují případy $Z = 1$ a jak dalece má cenu využívat cache v případě souřadnice Chudnovských. Použití cache je podle mého soudu v textu kapitoly 2 vysvětleno nejasně.

Jádro práce se zdá být v kapitole 3. Edwardsovy křivky určitě stojí za podrobné zpracování. Text kapitoly působí zpočátku jako kvalitní, při bližším rozboru se ale ukáže, že není plně promyšlen a je ne zcela dobře strukturován. Nebyl jsem například spokojen s Větou 3.1.5. Už její znění je formálně nesprávné, protože předpoklad o charakteristice tělesa by měl být jasně uveden v textu věty. To ale takový problém není. Spíše mi vadí, že důkaz nebyl rozložen do více oddělených kroků. V důkazu se totiž jedná o něco trochu jiného než je ve znění. Ukazuje se, že $y^2 = f(x)$, kde $\deg(f) = 4$, je možné lineárně lomenou transformací převést do tvaru $y^2 = (x-\phi)(x+1)x(x-1)$ a odsud získat tvar Edwardsovy křivky. Jako speciální případ se pak v závěru vyloží, že polynomy stupně tři se dají převést na polynomy stupně čtyři. Smutné je, že diplomant si zřejmě nevšiml, že uvedenou transformaci lze obrátit a získat polynom stupně tři. (Jde o tvar $(y/x^2)^2 = (1-\phi x^{-1})(1+x^{-1})(1-x^{-1})$.) Kdyby si toho všiml, mohl dokázat větší část tvrzení 3.1.2 a mohl by se na externí zdroj odkázat jenom pro případ vícenásobných kořenů (což ostatně také není těžké ošetřit přímo). Výklad má ještě další nedostatek v tom, že invertibilita lomené lineární transformace není dostatečně okomentována a čtenář se nedozví, jak jejím použitím bude naplněn požadavek ekvivalence. Navíc vůbec není komentováno, proč je podmínka nenulovosti $AD - BC$ při zvolené transformaci splněna.

Znění Věty 3.1.2 asi nebude správně. Odkaz ve mne vzbuzuje pochybnosti. Zdroj [13] jsem nestudoval, takže nevylučuji, že opravdu je tvrzení dokázáno v kapitole “Some quadratic problems”. Prosím o komentář během obhajoby.

Bylo by bylo lepší tvrzení o Edwardsových křivkách dokázat rovnou pro zobecněný tvar. Poznámka 3.1.9 vyžaduje v ”if and only if” formě vysvětlení (k tomu by bylo třeba propojit definici ekvivalence s transformacemi Weierstrassovy rovnice v kapitole 1 – je chyba, že se tak nestalo).

Závěr důkazu tvrzení 3.1.10 ukazuje na určitou nedůslednost při přejímání textu z původního zdroje. Pokud se pohybujeme ve formálním

rámci algebraických funkčních těles, nejsou přece úvahy o výjimečných bodech potřeba. To, že v textu zůstaly, vzbuzuje pochybnost o míře porozumění autora zpracovávané látce.

Nepříliš dobře působí také to, že vazba mezi Edwardsovými křivkami a eliptickými křivkami je zmíněna jakoby mimochodem v důkazu Věty 3.2.5. V této části je také nejasné, proč není použito znaménko $\oplus$.

Použití stopy v závěrečné části kapitoly tři bez komentáře je sporné – není to tak triviální, aby se v textu typu diplomové práce neobjevil podrobnější výklad. Použití alfanumerického znaku pro velikost množiny bez vysvětlení jenom umocňuje celkový dojem, že třetí kapitola, zejména její závěr, byly psány v rychlosti a bez pečlivého rozmyšlení. To je velká škoda.

Práce je na hranici toho, aby byla uznána jako diplomová. Svou kvalitou sama o sobě by si přijetí jako práce diplomová zasluhovala, byť i tak by šlo o práci slabou. Vysvětlení, proč se zpracování významně odchýlilo od zadání jsem v práci nenašel. Lze doufat, že během obhajoby budou sděleny dostatečně přesvědčivé důvody, proč se tak stalo.

V Praze 12. září 2012

Aleš Drápal