Oponentský posudek diplomové práce

Název: **Jedno užití polynomů nad konečnými tělesy**
Autor: **Jiří Jandl**
Studijní obor: **Učitelství matematiky pro 2. stupeň ZŠ**
Katedra: **Katedra matematiky, fyziky a technické výchovy Fakulty pedagogické ZČU**
Vedoucí práce: **doc. RNDr. Jaroslav Hora, CSc.**
Rok odevzdání: **2017**
Oponent: **PhDr. Lukáš Honzík, Ph.D.**

Předložená práce s názvem *Jedno užití polynomů nad konečnými tělesy*, představující čtenáři zajímavou oblast použití polynomů v běžném životě, je rozdělena do sedmi kapitol. V první kapitole jsou nejprve připomenuta konečná tělesa a aritmetické operace v nich (sčítání a odečítání modulo p). Na to následně navazuje kapitola o polynomech nad konečnými tělesy a o operacích s nimi. Třetí kapitolu autor věnoval ireducibilitě mnohočlenů v $Z[x]$ a v $Z_p[x]$. V souvislosti s tím představuje Eisensteinovo kritérium ireducibility, Kroneckerův algoritmus a Berlekampův algoritmus. Ve čtvrté kapitole jsou zmíněny minimální a primitivní polynomy. Zbývající tři části práce pak popisují některé kódy (lineární, Hammingův) a příklady využití samoopravných kódů.

Práce tak nabízí náhled do velmi zajímavé oblasti matematiky, která našla široké uplatnění v běžném životě, přičemž lidé si tuto skutečnost leckdy ani neuvědomují. Text práce přitom spojuje jakýsi krátký historický exkurz týkající se práce s polynomy v době, kdy ještě neexistovaly počítače, jak je známe dnes, se současnou situací, kdy je užívání počítačů a komunikace na velké vzdálenosti běžnou záležitostí.

Na druhou stranu je bohužel nutné konstatovat, že se v textu vyskytují i nějaké chyby (vizte přílohu posudku), jimiž kvalita práce trpí. Navíc nelze opomenout, že některé pasáže práce jsou často bez větších změn zkopírovány (a to včetně uvedených příkladů, se kterými si snad autor mohl dát tu práci a vymyslet nějaké vlastní) z několika zdrojů – jmenovitě například:

- kapitoly 3.1 a 3.2 obsahují text převzatý z *Projekt VS-14-029* [online]. Dostupné z: http://fpe.zcu.cz/kmt/kmt/projekty/projekt_VS_14.html
- kapitola 4 je částečně převzata ze SÝKORA, Jiří. *Ireducibilní polynomy nad konečnými tělesy*. Praha, 2010. Bakalářská práce. Univerzita Karlova. Vedoucí práce Mgr. Libor Barto, Ph.D. Dostupné z: https://dspace.cuni.cz/bitstream/handle/20.500.11956/37693/BPTX_2009_1_11320_NSZZ027_236468_0_77395.pdf?sequence=1 (tento zdroj ani není uvedený ve zdrojích na konci práce),
- kapitola 7 obsahuje pasáže z elektronických skript TŮMA, Jiří. *Lineární algebra*. [online]. Praha: Univerzita Karlova, 2002. Dostupné z: http://www.karlin.mff.cuni.cz/~tuma/2002/NLinalg8.pdf

Práce i přes výhrady splňuje požadavky kladené na úroveň diplomové práce, a proto ji doporučuji uznat jako práci diplomovou, avšak vzhledem k výše uvedenému ji navrhuji klasifikovat stupněm **dobře**.

V Plzni dne 20. VII. 2017 PhDr. Lukáš Honzík, Ph.D.

Příloha oponentského posudku diplomové práce

Název: **Jedno užití polynomů nad konečnými tělesy**
Autorka: **Jiří Jandl**

4 - poslední odstavec úvodu: „se zmíníme se“ – přebývá jedno „se“;
5 - poslední věta definice 1.1: místo tělesa K je uvedeno těleso E;
- konec definice 1.1: mělo by být rozlišování mezi množinou T a tělesem $(T, +, \cdot)$;
7 - první odstavec: místo „ekvivalence“ má být „kongruence“?
- $x \equiv x' \equiv y \equiv y'$ je zvláštní podmínka, místo toho bude pro platnost rovnosti $[x + y] = [x' + y']$ stačit jen $x \equiv x'$ a $y \equiv y'$;
8 - operační tabulka $\otimes$: výsledek $4 \otimes 1$ není 1 ale 4;
- řešení příkladu 1.1: „Pomocí řádkovými úpravami“ – špatně sestavená věta;
9 - první odstavec: první věta je nevhodně sestavena, může dojít k představě, že ke 3. řádku matice je třeba přičíst dvojnásobek 1. řádku (to by pak ale 3. řádek po úpravě vyšel 1, 0, 1, 2, 2, 0, nikoliv 0, 2, 2, 0, 2, 0);
12 - poslední odstavec: poslední věta je trochu problematická, lze ji pochopit tak, že z primitivního polynomu nejde vytknout nic jiného než konstantu ±1, jinými slovy že nejde rozložit v součin polynomů nižších stupňů, avšak například polynom $x^2 + 3x + 2$ je primitivní, neboť $D(1, 3, 2) = 1$, ale zároveň jej lze rozložit v součin faktorů $(x + 1)\cdot(x + 2)$;
13 - část b): správně má být $\sum_{i=0}^{l}(a_i - b_i)x^i$, nikoliv $\sum_{i=0}^{l}(a_i + b_i)x^i$;
15 - výpočet polynomu $f_3(x) = R(x)$: zbytek má (tak jako ve schématu dělení) vyjít $26x - 13$, nikoliv $23x - 13$;
- konec popisu dělení polynomu polynomem: „Jelikož polynom $Q(x) \neq 0$, není polynom $f(x)$ dělitelný $g(x)$.“ – to není pravda, nezáleží na polynomu $Q(x)$, ale na zbytku $R(x)$;
- poslední věta: „schématu, který“ – slovo schéma je středního rodu, takže „které“ místo „který“;
16 - konec popisu dělení polynomu polynomem: polynom $f_2(x)$ se nerovná polynomu $Q(x)$, nýbrž polynomu $R(x)$;
- schéma dělení: trochu nepořádek ve znaménkách v řádcích $-(-5x^3 + 10x^2 - 5x + 25)$ a $5x^3 - 10x^2 + 5x - 25$;
18 - řešení příkladu 2.6: „psát posloupnosti jejich v pořadí“ – chybí slovo „koeficientů“;
19 - řešení příkladů 2.7 a 2.8: v popisu postupu by bylo vhodnější nemíchat praktickou a teoretickou stránku výpočtu (zarovnání posloupností nul a jedniček a jejich pouhé sčítání $\times$ informace o polynomech $x^n \cdot g(x)$);
23 - první věta: obor integrity polynomů s racionálními koeficienty budeme značit $Q[x]$;
- část a) Kroneckerova algoritmu: místo „$\left[\frac{n}{2}\right]$ značí tzv. celou část čísla $\left[\frac{n}{2}\right]$“ má být „$\left[\frac{n}{2}\right]$ značí tzv. celou část čísla $\frac{n}{2}$“;
29 - část 1. Berlekampova algoritmu: věta „Pomocí kongruence (…) a dopočítáme…“ je zvláštně formulovaná;
38 - definice: „$f(0)$ ą 0“ má být „$f(0) \neq 0$“, dále „$g(0)$ ą 0“ má být „$g(0) \neq 0$“, podobně na další stránce „$f = ag_1^{m1} \times\times\times ag_n^{mn}$“ má být „$f = ag_1^{m1} \cdots ag_n^{mn}$“, „$m_1,\ldots, m_n$ Î N“ má být „$m_1,\ldots, m_n \in N$“ nebo „pl ł $\max(m_1,\ldots, m_n)$“ má být „$pl \geq \max(m_1,\ldots, m_n)$“ – podobné nesrovnalosti se nacházejí i na dalších stránkách a vznikly zřejmě nepečlivým zkopírováním z bakalářské práce SÝKORA, Jiří. *Ireducibilní polynomy nad konečnými tělesy*.

43 - část věnovaná lineárním kódům mi přijde jako jakýsi pelmel nejrůznějších informací bez nějakého hlubšího propojení (na rozdíl od předchozích kapitol není pořádně vysvětleno, k čemu jednotlivé kódy slouží, co a jak se dělá a podobně);

70 - druhý odstavec: přetržení magnetické pásky, přeslech u telefonních linek či překlepy při psaní už nejsou ani tak šumem ve smyslu poruchy fyzikálního prostředí, jako spíše chybou vysílače či přijímače (např. přetržení pásky pak ani nejde opravit při dekódování);

- poslední odstavec: „Bez něho (šumu) by teorie kódování nebyla třeba.“ – to není tak docela pravda, kódování se užívá například při kompresi, kde nejde o šum ale o snížení datové velikosti (konkrétně třeba pro zmenšení velikosti obrázku při zachování rozumné kvality);

74 - druhý odstavec kapitoly 7.3: celý odstavec je poměrně divný, věty jsou zvláštně až nesmyslně formulovány - „Konvoluční kódy a s kombinací Reed-Solomonovy kódy jsou používány…“, „Tyto signály jsou rušeny (…) prostřednictvím vesmíru.“, „…závisí právě na dvou různých kódech používaných v kombinaci těchto kódů.“;

75 - třetí odstavec: „Dalším algoritmem (…) se nazývá Berlekampův…“ – divná věta

Otázky k obhajobě:

1. Je nutné hlídat oboustranně existenci neutrálního prvku (0 a 1) v axiomech A3 a M3? (str. 5)
2. O jakou binární operaci definovanou na stránce 17 vlastně jde?
3. Jaký další problém se může objevit v závěru Kroneckerova algoritmu kromě objevení polynomu nultého stupně nebo polynomu, který v $Z[x]$ nedělí zadaný polynom $f(x)$? (str. 23-27)
4. Jaký je zdroj tabulky na straně 44 a 45? Nikde se mi nic takového nepodařilo najít.