

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Representation of complex numbers in redundant numeration systems
Jméno autora:	Adam Blažek
Typ práce:	bakalářská práce
Fakulta:	Fakulta jaderná a fyzikálně inženýrská (FJFI)
Katedra:	Katedra matematiky
Vedoucí práce:	Prof. Ing. Edita Pelantová, CSc.
Pracoviště vedoucího práce:	Katedra Matematiky FJFI

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání a motivace k jeho vyspání	náročnější
<i>Hodnocení náročnosti zadání závěrečné práce a krátké průvodní slovo k motivaci pro zadání práce.</i>	
<p>Reitwiesner v roce 1960 ukázal, že pokud v soustavě s bází $b=2$ připustíme kromě obvyklých cifer 0 a 1 také cifru -1, lze celé číslo reprezentovat tak, že v každé dvojici sousedících cifer je alespoň jedna 0. Takovým reprezentacím se říká NAF (non-adjacent form). V klasické binární soustavě je hustota cifry nula rovna $\frac{1}{2}$, zatímco u NAF je hustota nuly $\frac{2}{3}$. Přitom NAF reprezentace čísla je maximálně o jednu cifru delší než klasická binární reprezentace. Převaha nul v zápisech čísel významně zrychluje násobení, které je klíčovou operací v šifrovacích algoritmech. Koncept NAF-reprezentací byl zobecněn i pro komplexní čísla Heubergerem a Krennem: reprezentace komplexního čísla v soustavě s bází b a množinou cifer D je w-NAF, pokud v každé w-tici po sobě jdoucích cifer dané reprezentace se vyskytuje nanejvýš jediná nenulová cifra. Motivací pro zadání práce byla snaha odvodit pro tyto systémy další vlastnosti.</p>	

Motivací pro zadání práce byla

Splnění zadání	splněno
<i>Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.</i>	
<p>V předložené práci je studován numerační systém pro zápis gaussovských celých čísel. Komplexní báze $b=i-1$ a cifry 0 a 1 umožňují reprezentovat každé gaussovské celé číslo. Rozšíření množiny cifer o cifry -1, i a $-i$ (tedy celkově na 5 cifer) dovoluje reprezentovat každé gaussovské číslo v tzv. 3-NAF tvaru, kdy v každé trojici po sobě jdoucích cifer jsou alespoň 2 nuly. Hustota nuly v tomto numeračním systému je dokonce $\frac{3}{4}$. I když zmíněné vlastnosti báze $b=i-1$ jsou známé více než 15 let, Adam v práci podává jejich nové elegantní důkazy. Práce obsahuje i nový vysoce netriviální výsledek: pro každé gaussovské celé číslo x je určen počet tzv. optimálních reprezentací, tj. reprezentací, které mají stejný počet nenulových cifer jako 3-NAF reprezentace čísla x. Možnost nahradit 3-NAF reprezentaci čísla x náhodně vybranou jinou optimální reprezentací zvyšuje odolnost kryptosystému proti pokusům o prolomení. V práci je odvozen rovněž horní odhad na počet optimálních reprezentací využívajících N nenulových cifer. Adamův výsledek představuje analogii obdobného výsledku pro Reitwiesnerův numerační systém, který prvně odvodili Grabner a Heuberger (2006) a jinou metodou dokázali Vábek a Tůma (2015). Numerační systém studovaný Adamem je však daleko složitější a vyžadoval nové nástroje k řešení.</p>	

Aktivita a samostatnost při zpracování práce	výborná
<i>Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven. Posuďte schopnost studenta samostatně tvůrčí práce.</i>	
<p>Počet schůzek ve složení: student, školitelka a konzultantka, na kterých se studovala tematika bakalářské práce, přesáhl určité číslo 30 a schůzky začaly už rok před zadáním bakalářské práce. Pro Adama bylo hlavní motivací schůzek ne sepsání bakalářské práce, ale vyřešení problému, který jej zaujal. Doufám, že stejně jako pro mě a konzultantku i pro Adama byly schůzky hlavně zábavou s matematikou. Průběh schůzek se nelišil od schůzek,</p>	

kdy s kolegy vědecky pracujeme. Adam přicházel s nápady, aktivně testoval hypotézy, sám si k tomu navrhoval a implementoval algoritmy.

Odborná úroveň

výborná

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Podařilo se vyřešit několik otázek spojených s redundantním numerálním systémem pro reprezentaci gaussovských celých čísel. K tomuto řešení nestačilo využívat znalosti získané studiem, bylo třeba zobecňovat výsledky jiných matematiků pro náš daleko složitější numerální systém a vytvořit nové nástroje pro zvládnutí technických jemností důkazu. Adam nejdříve dokázal rekurentní vztah pro počet reprezentací a s asistencí počítače vytipoval maxima počtu optimálních reprezentací i proměnné, na kterých se maximum nabývá. To vedlo k vyjádření počtu reprezentací ve tvaru tzv. recognisable function. Odvodit maximum této funkce vede na úlohu spojenou s určením společného spektrálního poloměru (joint spectral radius) pěti matic rozměru 9×9 , což bylo velice technicky náročné. Vedlejším produktem Adamova postupu je automat, tj. orientovaný graf s ohodnocenými hranami, který slouží k tomu, aby se z 3-NAF reprezentace gaussovského čísla generovala náhodná optimální reprezentace.

Formální a jazyková úroveň

výborná

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Text je skvěle pedagogicky sepsán se snahou čtenáři vše vysvětlit na příkladech, s uváděním motivace před každou definicí či tvrzením. Také angličtina je na výborné úrovni.

Výběr zdrojů, korektnost citací

výborné

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Adam nejdříve uvádí známe výsledky, u kterých uvede zdroj. Opatřuje je však svými vlastními důkazy. Počínaje kapitolou 3, jsou definice a věty původní.

Další komentáře a hodnocení

Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.

Výsledky Adamova výzkumu byly prezentovány na hlavní konferenci v oboru nestandardních numerálních systému Numeration 2024 v nizozemském Utrechtu. V současnosti připravujeme k publikaci článek. Se svou bakalářskou prací se Adam účastnil česko-slovenské studentské vědecké soutěže (SVOČ) v sekci Teoretická informatika, kde obsadil 2. místo.

Adamem studovaný systém má další významnou výhodu. Sčítání dvou čísel v tomto systému (při dostatečném počtu procesorů) lze provádět v konstantním počtu kroků nezávisle na délce řetězců, které tato čísla reprezentují (Frougny et al. 2011). Lze proto očekávat, že výsledky získané Adamem podpoří širší uplatnění tohoto numerálního systému.

III. CELKOVÉ HODNOCENÍ A NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Případně uveďte otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Práce je vysoce nadstandardní, obsahuje nové výsledky, které se u mezinárodní komunity setkaly s pozitivním ohlasem. Student prokázal nejenom schopnost přicházet s matematickými nápady, ale také schopnost jejich platnost ověřovat a popřípadě dokazovat. Jeho matematické vyjadřování a logické členění textu je už teď profesionální.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **A - výborně**.

Datum: 15.8.2024

Podpis: