Milan Straka: Faktorizace polynomů nad konečnými tělesy

posudek oponenta

V práci je vyloženo zajímavým a obsažným způsobem téma faktorizace polynomů nad konečnými tělesy. V první části jsou podány dva nejznámnější algoritmy ve své základní, snadno srozumitelné verzi. Ve druhé části je pak jeden z těchto algoritmů optimalizován ve snaze získat subkvadratickou složitost. Součástí práce je i zdařilá implementace, používající rozumný kompromis mezi asymptoticky optimálními a reálně použitelnými algoritmy (řada asymptoticky rychlých algebraických algoritmů je v praxi pomalejší než algoritmy naivní).

Hlavním přínosem práce je přehledné a čtivé zpracování problému, který není takto komplexně podán v žádné mně známé učebnici. Je zřejmé, že student musel zpracovat větší množství samostatných článků. Téma dalece přesahuje nejen obsah přednášky ze základů algebry, ale i specializovaného kurzu Počítačová algebra, který pokrývá pouze základní algoritmus na bezčtvercovou faktorizaci a algoritmus Berlekampův. Sám budu předkládanou práci doporučovat studentům tohoto kurzu jako doplňující čtení. Dobrým nápadem je jistě rozdělení práce na dvě části: první umožňuje algoritmy rychle pochopit a technické detaily nutné k optimalizaci složitosti jsou ponechány na později.

Je nutno podotknout, že práce obsahuje zcela zanedbatelné množství překlepů a jazykových chyb. Vytknout lze pouze několik drobných nepřesností, uveďme např. tyto: definice ireducibilního polynomu uvedená na str. 6 zahrnuje i polynomy konstantní, které se však za ireducibilní nepovažují; na str. 15 ve druhém zvýrazněném vzorci má být místo mod f spíše mod f / ten součin; str. 19 dole: není pravda, že z $M(n)>n$ plyne $M(n)+M(m)<M(m+n)$, což je chyba, která se opakuje na řadě míst; naštěstí je vždy použita v kontextu funkce $x^{k+sigma(1)}$, pro kterou je nerovnost splněna; str. 18,29 místo „očekávaný počet" se česky říká spíše „střední hodnota"; s tím souvisí nejasnost, co to je složitost pravděpodobnostního algoritmu v nejhorším případě - nejsem odborník na složitost, ale zdá se mi, že by to mělo být spíše něco jako „střední složitost"; str. 34, Graf 4.1: není jasné, nad kterým tělesem výpočet probíhá (mimochodem, závislost rychlosti faktorizace daného polynomu na q také mohla dát zajímavý graf). Žádná z těchto nepřesností však čtenáře nemůže vyvést z rovnováhy a jejich počet je vzhledem k rozsahu práce velmi nízký.

Předloženou práci považuji za vynikající a jednoznačně ji doporučuji uznat jako bakalářskou a ohodnotit stupněm **výborně.**

V Laramie (Wyo.), 22.6.2006

David Stanovský