Jana Divišová: Mříže a faktorizace celočíselných polynomů

posudek vedoucího práce

V práci jsou srovnány dva algoritmy na faktorizaci celočíselných polynomů. Fungují tak, že se daný polynom rozloží nejprve na bezčtvercové faktory, každý z nich se rozloží modulo nějaké prvočíslo p a výsledek se nahftuje na rozklad modulo p^k. Oba algoritmy se pak liší v tom, jak z tohoto rozkladu rekonstruují rozklad nad **Z**. Klasický BH algoritmus používá brute force, LLL algoritmus používá techniku redukce báze v mřížích. Hrubá síla má složitost v nejhorším případě exponenciální, LLL polynomiální. Práce obsahuje teoretický popis obou algoritmů a experimentální porovnání výpočetního času na náhodných polynomech. Výsledek experimentu potvrzuje hypotézu, že v průměrném případě se rychlost obou algoritmů neliší.

Práci studentka vypracovala zcela samostatně. Teorie je poskládána z pěti zdrojů uvedených v literatuře, testy jsou provedené na algoritmech implementovaných v C++ knihovně NTL. Text se zdá být matematicky korektní. Práce sice není příliš čtivá, chybí komentáře, které by vysvětlovaly formální definice a značení, ovšem u tak technicky náročného tematu by byl v bakalářské práci překvapením spíše opak. Trochu mi chybí hlubší analýza výsledků testů, zejména vysvětlení nerovnoměrného chování jednotlivých pokusů v rámci jednoho testu (mnou očekávané chování má Test 5, podezřelý mi přijde např. nárust času v průběhu Testu 1).

Závěr:
Předloženou práci doporučuji uznat jako bakalářskou a i přes drobné nedostatky se kloním spíše k hodnocení stupněm **výborně.**

V Praze, 31.8.2007
David Stanovský