

Posudek bakalářské práce

Ján Jančo: Nastavenie konštant pri hľadaní polynómov pre Číselne teoretické síto

Bakalářská práce Jána Janči zabývajúcej sa optimalizáciou nastavení algoritmu pro hledání polynomů v číselném sítu je ve své textové části rozdělena na tři kapitoly.

V úvodní kapitole je čtenář seznámen s algoritmem číselného síta a zejména s klíčovou úlohou, kterou hraje polynom vybíraný v první fázi algoritmu. Popis algoritmu je poměrně hrubý a zjednodušený, což je vzhledem ke značné komplikovanosti algoritmu a pokročilé teorii, na níž je algoritmus postaven, pochopitelné a správné. Autorovi se daří vystihnout základní podstatu algoritmu pro nezasvěceného čtenáře, ale například podmínka nedělitelnosti $[Z_K:Z(\theta)]$ prvočíslem zmíněná později v druhé kapitole na stránce 18 je pak zcela bez kontextu (dokonce i se samotným značením Z_K se zde čtenář setkává poprvé a naposledy). A protože u ní ani není explicitní odkaz do literatury, pátral by takový čtenář po jejím smyslu asi jen obtížně.

Druhá část práce nejprve popisuje jediný zkoumaný algoritmus pro získávání polynomů, z kterých je posléze vybírán ideální polynom, totiž m -base metodu. Dále jsou srozumitelně popsány způsoby hodnocení polynomu, které si kladou za cíl vyjádřit užitečnost polynomu pro algoritmus číselného síta a na základě kterých je prováděn výběr nejlepšího polynomu. Způsob, jakým jsou polynomy hodnoceny, je teoreticky poděřen. Hlavními sledovanými faktory jsou kořenové vlastnosti a velikost polynomiálních hodnot. S ohledem na tyto faktory jsou vysvětleny také parametry hledacího algoritmu, jejichž ideální hodnoty jsou předmětem hledání v poslední část práce.

Třetí část, kterou lze považovat za hlavní výstup práce, popisuje provedené experimenty a naměřené hodnoty včetně jejich interpretace. Kontroverzní je autorovo rozhodnutí porovnávat výsledné vybrané polynomy opět podle umělých kritérií, nikoliv podle skutečné doby běhu číselného síta inicializovaného daným polynomem. Lze přepokládat, že provedení všech měření s celým poctivým prosíváním pokládal autor za nemožné vzhledem k tomu, že by taková měření zabrala výrazně více strojového času, na druhou stranu provedené zjednodušení by si zasloužilo alespoň explicitní zmínku v abstraktu, aby nemohl vzniknout mylný dojem, že autor skutečně změnil, jaké parametry jsou pro reálný běh síta nejlepší.

Samotné experimenty jsou provedeny dobře, volba testovacích parametrů i interpretace naměřených výsledků svědčí o pochopení tématu. Na přiloženém CD jsou k dispozici nezpracovaná naměřená data, ale pokusy samotné jsou jen obtížně opakovatelné, neboť testovací skripty ani implementace síta samotného přiloženy nejsou. Ani není v práci zmínka či odkaz na konkrétní verzi použité implementace síta, což je vzhledem k probíhajícímu vývoji podstatná informace, a také schází informace o hardware, na kterém testy probíhaly.

Text práce je čtivý s minimem překlepů, grafická úprava v pořádku. Poslední drobností, která zarazí, je tak skutečnost, že dvě položky z odkazované literatury jsou články z anglické verze internetové encyklopedie Wikipedie. Domnívám se, že autor odborné práce by se neměl opírat o amatérskou všeobecnou encyklopedii s nízkou důvěryhodností, ale měl by se opírat opět o odborné prameny, které jistě lze k tématu najít.

Vzhledem k výše uvedeným výtkám, které nejsou zásadní, nicméně kvalitu práce snižují, doporučuji hodnotit práci známkou velmi dobře.

V Praze, 14.9.2009, Jan Zvánovec