OPONENTSKÝ POSUDEK DIPLOMOVÉ PRÁCE

Autor práce: Bc. Olha Jurečková
Název: Testy generátorů pseudonáhodných čísel
Vedoucí: doc. Mgr. Pavel Příhoda , Ph.D.

Práce Olhy Jurečkové se zabývá otázkou testování generátorů pseudonáhodných bitů. Kromě statistických metod testujících očekávané náhodné chování vygenerované posloupnosti bitů, které tvoří jádro práce, je uveden i test založený na počítání iterací Pollardovy ρ-metody pro výpočet faktorizace celých čísel.

Text je vedle motivačního úvodu a závěru, který sumarizuje výsledky měření, rozčleněn do sedmi kapitol. Zatímco první kapitola práce obsahuje přehled potřebného statistického aparátu, je druhá část věnována popisu používaných pseudonáhodných generátorů. Následující tři kapitoly se postupně zabývají různými typy testování, nejprve standardními testy založenými na výskytu bitů v generované pseudonáhodné posloupnosti (konkrétně frekvenčním monobit testem, poker testem a runs testem), dále testy založenými na zkoumání výskytu monomů algebraické normální formy odpovídající Booleovy funkce a konečně testy založenými na struktuře obecné proudové šifry. Šestá kapitola vysvětluje princip testování pomocí Pollardovy ρ-metody pro výpočet prvočíselných rozkladů. V poslední části textu jsou shrnuty výsledky testů, jejichž implementace je nezanedbatelnou součástí předložené práce.

Ač se téma práce nezdá být příliš obtížné, především množství prezentovaných postupů včetně jejich implementace a měření umožňující srovnání jednotlivých testů vyžadovalo po studentce matematickou a programátorskou práci značného rozsahu. Samotný text je sepsán velmi pečlivě a množství matematických a jazykových nedostatků odpovídá jeho délce. Je škoda, že u drobných komentářů a doporučení týkající se hierarchizace a věrohodnosti testů (viz připomínky níže) není v textu alespoň naznačeno jejich odůvodnění, ať už jsou dány matematicky, statisticky či jen odbornou autoritou citovaného zdroje. Přehledné uvedení do problematiky, korektní použití především statistického aparátu a úspěšná implementace prezentovaných algoritmů ovšem svědčí o autorčině vhledu do problematiky.

Práce Olhy Jurečkové *Testy generátorů pseudonáhodných čísel* podle mého mínění splnila zadání a doporučuji ji uznat jako diplomovou.

v Praze 30.8.2015 Jan Žemlička

Připomínky a otázky:

(1) Jak je míněna poznámka v úvodu, *že procházení některými statistickými testy nemusí být dostatečným důkazem, že daný generátor pseudonáhodných bitů je dobrý.* Co je vlastně v kontextu práce dobrý generátor?

(2) V práci jsou poměrně časté odkazy na literaturu obsahující jistá doporučení (například na s. 24 a 30 s odkazem na položku literatury [9], na s. 39 bez uvedení zdroje, nebo na s. 42, 44, 46 a 48 s odkazem na položku [19]). Na jakém typu úvahy jsou uváděná doporučení založena?

(3) Na s. 12 je obor hodnot funkce ϵ kladný reálný (nikoli $\mathbb{N}$).