Přírodovědecká
fakulta

Posudek oponenta bakalářské práce

Jan Jašek: Generace náhodných čísel prostřednictvím lavinových fotodiod

Bakalářské práce „Generace náhodných čísel prostřednictvím lavinových fotodiod“ se zabývá realizací zdroje náhodných dat s cílem vyprodukovat sekvence splňující kritéria pro použití v náročných aplikacích. Je rozdělena na dvě hlavní části.

První část „Principy a metody“ popisuje motivaci, shrnuje požadavky a uvádí některé algoritmy a testy, které se využívají k úpravám a k ověření kvality náhodných dat. Zmiňuje fyzikální principy, které mohou být použity pro experimentální generaci náhodných dat. Druhá část „Experimentální část a výsledky“ je zaměřena na praktickou realizaci generátorů náhodných dat celkem třemi způsoby, dva s využitím temných detekcí lavinových fotodiod pracujících v Geigerově módu a jeden s pomocí ohlašované detekce jednotlivých fotonů po průchodu polopropustným děličem svazku (realizovaným s pomocí polarizačního hranolu). Naměřené bitové sekvence jsou přeneseny do počítače a dále upravovány různými algoritmy tak, aby bylo dosaženo uniformity (vyváženého poměru jedniček a nul) při zachování jejich náhodnosti. Výsledná data jsou testována programovým balíkem NIST Statistical Test Suite, který vyhodnocuje, zda splňují kritéria pro kryptografické účely. Jako demonstrace je rovněž počítána hodnota čísla π metodou Monte Carlo s použitím vygenerovaných náhodných dat. Práci uzavírá podrobný seznam literatury.

Rozsah práce velmi dobře odpovídá tématu, jazyková úroveň je uspokojivá, místy se však vyskytují poněkud neobratné formulace. Dílo obsahuje minimum jazykových chyb[1], větší pozornost mohla být věnována popisům v tabulkách výsledků NIST STS testů, které mají nejednotné gramatické pády a nesourodé použití velkých písmen. Rovněž tak bych dal přednost některým zaužívanějším pojmům (hašení v el. obvodech → zhášení, uniformnost → uniformita, počítadlo → čítač). Občas se zaměňují termíny ‘uniformita’ a ‘náhodnost’. Jeden a půl chyby se vyskytl ve zdrojového kódu programu (2.1). Výsledky jsou v souladu s vytčenými cíli.

Práci doporučuji k obahjobě, navrhuji kvalifikovat stupněm **A**. K diskusi nicméně předkládám tyto body.

- V kapitole 1.6 „Shannonova entropie“ se operuje s pojmy ‘entropie’ a ‘informace’, které jsou si blízké, avšak neznamenají totéž. Je možné objasnit jejich souvislost?
- U algoritmu „XOR (2x)“ (kapitola 2.2.5) se spojují čtyři sousední bity vstupu do jednoho bitu na výstupu. Pokud je binární přepis dat z čítače maximálně čtyřbitový, obsahuje každý výstupní bit aspoň jeden nejméně významný bit

[1] Jako kuriozitu lze uvést rozdělení čísla 50 100 na straně 25 na dva řádky (50-100).

(t.j. sudá/lichá) z hodnoty čítače. Potom by byl blízký algoritmu „Sudá/Lichá“ (2.2.1). Je možno uvést bitovou hloubku (počet bitů) binárního přepisu dat z čítače? Rovněž by nás zajímal počet bitů použitých při výpočtu inverzní Box-Müllerovy transformace (obrázky 2.5 a 2.6; histogramy Z1, Z2 jsou úzké ve srovnání s histogramem na obrázku 2.2).

V Olomouci dne 24. května 2017 .....

Václav Michálek
oponent bakalářské práce

Společná laboratoř optiky Univerzity Palackého a FzÚ AV ČR
Přírodovědecká fakulta Univerzity Palackého v Olomouci
17. listopadu 50A | 772 07 Olomouc | T: 585 631 502