

Generování náhodných čísel na základě jaderného rozpadu

K. Klojda*, J. Podloučka**, D. Ryšánek***

*Gymnázium Jana Palacha 804, Turnov 511 01

**SPŠ a VOŠ Sokolská, Brno

***SPŠE V Úžlabině 320, Praha 10

*klojda@email.cz, **jan@podloucka.eu,

***dennis-rysanek@email.cz

Abstrakt:

Motivací je zjištění, jak sestavit generátor náhodných čísel na fyzickém procesu (jaderném rozpadu), jak ho sestrojít a čísla ověřit. Kvalitní generátor čísel se nám sestrojít nepodařilo, při porovnání s pseudonáhodným generátorem Excelu bylo zřejmé, že Excel čísla vygeneroval lépe, náhodněji. Pokus byl tedy částečně neúspěšný.

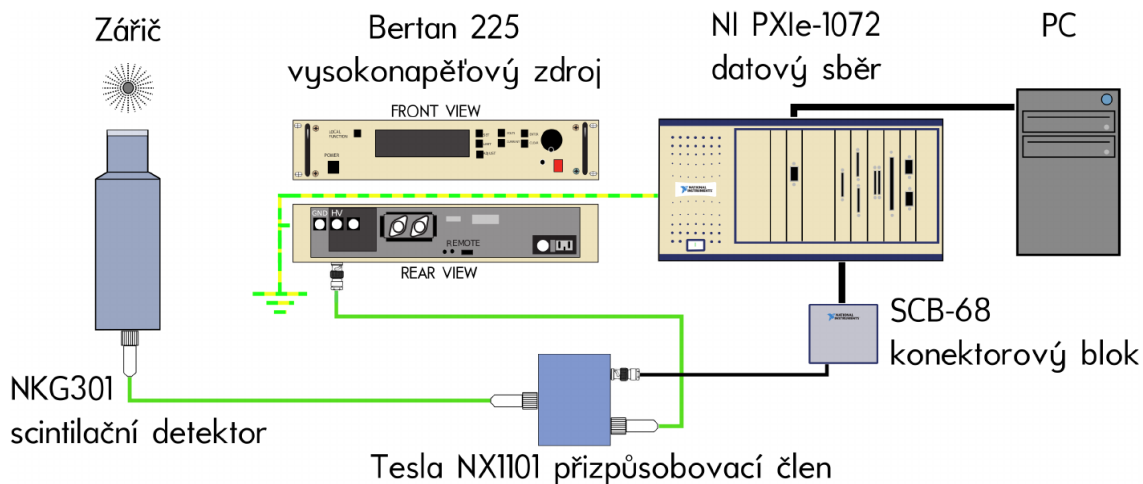
1. Úvod

S potřebou generace náhodných čísel se v dnešní době setkáváme na mnoha místech a s přibývajícím trendem digitalizace, více než kdy dříve. Jako příklad můžeme uvést online sázkové hry, počítačové simulace, ale i šifrování. Avšak ne všechna čísla jsou skutečně náhodná, existují i takzvaná pseudonáhodná čísla, jež se zdají být náhodná, ale jejich náhodnost lze pomocí testů vyvrátit. Tato čísla jsou generovaná počítačem na základě jednoduššího či složitějšího algoritmu, ale ani nejsložitější algoritmus nám nikdy nezaručí jejich naprostou náhodnost. Naprostá náhodnost se dá zaručit pouze pomocí náhodného fyzikálního procesu. Jedním z těchto procesů je jaderný rozpad. A tímto způsobem generace jsme se zabývali.

2. Generování

Metoda a aparatura generování

Ke generaci náhodných čísel jsme použili aparaturu znázorněnou na obr. 1 skládající se ze zářiče (Kobalt 57 a Baryum 133), scintilačního detektoru NKG301, přizpůsobovacího členu Tesla NX1101, vysokonapětového zdroje Bertan 225, konektorového bloku SCB-68, datové sběrný NI PXIe-1072 a PC, které data zpracovává. Pro zpracování dat byly využity programy LabVIEW, Microsoft Excel 2010 a GNUPlot. Proces probíhal následovně: Při rozpadu radioaktivních jader zářiče dochází k vyzáření vysokoenergetického fotonu. Foton naráží do materiálu detektoru a ztrácí svou energii excitací elektronů. Při následné deexcitaci dochází k vyzáření fotonů viditelného světla. Tyto fotony naráží na fotokatodu detektoru a uvolňují z ní elektrony. Pomocí vysokého napětí jsou tyto elektrony ve fotonásobiči urychleny a lavinovitě zesíleny. Na výstupu z fotonásobiče obdržíme elektrický impuls, který zaznamenáváme aparaturou pro sběr dat. Impuls je softwarově zpracován pomocí programu vytvořeného v prostředí LabVIEW a na základě délky intervalů mezi jednotlivými impulsy

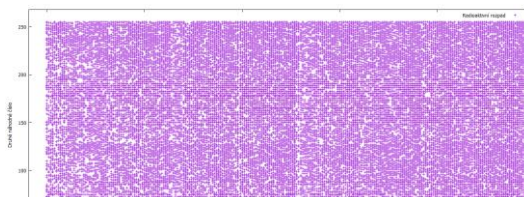


Obrázek 1: Aparatura

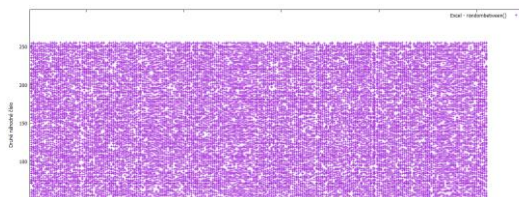
jsou generována náhodná čísla. Pokud označíme T_1 dobu mezi prvním a druhým impulsem a T_2 dobu mezi druhým a třetím impulsem a délka T_1 je vyšší než T_2 , generujeme číslo 1, v opačném případě generujeme číslo 0. V případě, že jsou délky shodné, negenerujeme nic. Pravděpodobnost, že T_1 je vyšší než T_2 je stejná jako, že je nižší (vyplývá to ze zákona radioaktivního rozpadu). Dále je možnost použít např. John von Neumannův dekorelátor odebírající dvojici bitů a nahrazující je takto: Je-li dvojice bitů shodná (00 nebo 11), pak se bity zahodí. V případě, že je dvojice bitů 01 pak výstupní bit je 0, v posledním případě, je-li dvojice bitů 10, výstupní bit je 1. Tento dekorelátor námi nebyl použit. Z posloupnosti 8 vygenerovaných bitů vytvoříme jedno 8-bitové číslo (0-255). Tato čísla jsou poté exportována do textového souboru. Ověření náhodnosti čísel je provedeno graficky vykreslením do roviny, kde každá dvě po sobě jdoucí čísla představují souřadnici X a Y , v případě, že jsou čísla skutečně náhodná, tak by se měl prostor rovnoměrně zaplnit a neměla by být pozorovatelná žádná struktura.

Výsledky, závěr

Bohužel se nám nepovedlo nastavit diskriminační hladinu tak, abychom úplně odstranili pozadí, které pochází jednak z detekce kosmického záření a jednak z elektronického šumu. Nicméně i o tomto pozadí můžeme předpokládat, že vzniká na základě náhodných procesů. Vygenerovali jsme zhruba 100 000 čísel. Bohužel jsme v těchto číslech při ověřování našli viditelné struktury. Abychom vyloučili, že se jedná jen o problém grafického zobrazení počítače, učinili jsme i srovnávací pokus a náš výsledek porovnali se zabudovaným pseudonáhodným generátorem v MS Excel, kde jsme vygenerovali také cca 100 000 čísel. Tato čísla vykazovala méně viditelné struktury a grafický efekt jako hlavní příčinu pozorovaných struktur tedy můžeme vyloučit. Výsledky jsou viditelné na obr. 2 a 3. Dalším vysvětlením tedy může být neplatnost našeho předpokladu o náhodnosti jevů způsobujících vznik pozadí.



Obrázek 2: Rozložení čísel v rovině po generaci na základě rad. rozpadu



Obrázek 3: Rozložení čísel v rovině po generaci v Excelu

3. Shrnutí

Podářilo se nám zjistit, jak sestavit generátor náhodných čísel, i jak tato čísla zpracovat a ověřit, náš generátor náhodných čísel však bohužel nefungoval, jak by měl fungovat.

Náš vzorek náhodných čísel totiž vykazoval zřetelné periodické struktury. To si vysvětlujeme tím, že elektronický šum, jenž se nám nepodařilo plně odfiltrovat je zřejmě periodický a značně snižuje náhodnost generovaných bitů.

Poděkování

Děkujeme Fakultě Jaderné a Fyzikálně Inženýrské Českého Vysokého Učení Technického za možnost účastnit se na týdnu vědy na Jaderce. Zároveň děkujeme panu Janu Rusňákovi za vedení miniprojektu.

Reference:

- [1] KERBEC, J.: *Generování náhodných čísel založené na radioaktivním rozpadu*, FJFI ČVUT PRAHA.
- [2] HOTOVEC, P. – MATOUŠ, P.: *Týden vědy na Jaderce – Sborník příspěvků*, FJFI ČVUT PRAHA, 2015, 168-171.