Generování náhodných čísel založené na radioaktivním rozpadu

Petr Hotovec
Petr Matouš
Karlínské gymnázium, Praha 8
Petrmatous13@seznam.cz
Petrhotovec10@gmail.com

Abstrakt:

Hlavním cílem našeho projektu bylo vyzkoušet si vygenerovat vlastní náhodná čísla za pomocí generátoru náhodných čísel na principu radioaktivního rozpadu. Sestavili jsme měřící aparaturu a pokoušeli se vyčíst nějaká čísla v binární soustavě. Bohužel se objevila řada problémů hlavně s ukládáním binárních kódů a následným převedením do dekadické soustavy. Na příkladném souboru jsme viděli jak z bitového kódu udělat čísla a zároveň jsme si ověřili, že jsou dostatečně náhodná.

1 Úvod

Naše skupina se zabývala generováním náhodných čísel a použitím tohoto tématu v praktickém životě. S generováním náhodných čísel se setkáváme téměř denně, stačí zapnout počítač a už jen jeho ochrana spočívá hlavně na náhodných číslech. Další oblasti použití jsou například šifrování, simulace fyzikálních procesů, nebo hazardní hry. Už za druhé světové války se šifrovalo pomocí náhodných čísel a tato metoda se používá i v dnešní době, i když je na daleko vyšší úrovni. Vygenerovaná čísla se děli na *pseoudonáhodná* a *náhodná.* Pseudonáhodná tvoří členy složitých matematických posloupností. To znamená, že se s určitou pravděpodobností opakují. Zatím co náhodná tvoří neopakující se, nebo nepravidelně opakující se čísla.

2 Základní pojmy a vztahy

2.1 Radioaktivita

Radioaktivní rozpad je proces přeměny těžkých nestabilních jader na lehčí stabilnější. Radioaktivní zářiče se dělí podle typu vyzařované částice na alfa (jádro helia), beta (elektron a pozitron) a gama (foton). Fyzikální výklad rozpadů byl možný až s příchodem kvantové mechaniky a kvantové teorie pole.

Radioaktivní rozpad je náhodný proces a pravděpodobnost přeměny *n* jader za 1 vteřinu je dána vztahem

$$P(n) = A^n \, e^{-A} / n! \qquad (1)$$

kde *A* je aktivita vzorku, to je průměrný počet částic přeměněných za 1 vteřinu.

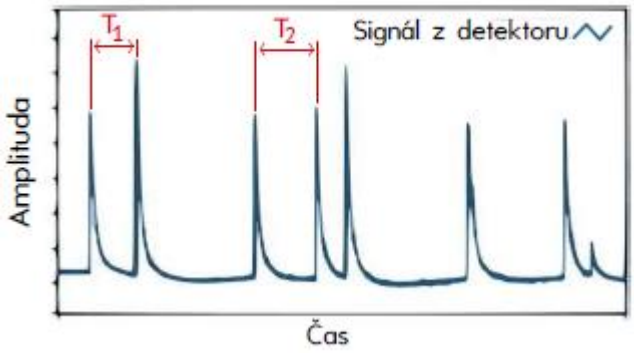
2.2 Generování náhodných bitů

Generování bitů se zakládá na měření doby mezi detekcí jednotlivých rozpadů zobrazených na osciloskopu. Čas mezi detekcí dvou po sobě jdoucích rozpadů je náhodná veličina, nebo pravděpodobnost (1) pro dostatečně velké vzorky nezávisí na počtu již přeměněných jader. Vygenerování jednoho bitu vzniká ze čtyř pulzů (viz obrázek č.1). Čas T_1 může být se stejnou pravděpodobností delší nebo kratší než čas T_2. Pravidla pro generování bitů zní:

- Je-li $T_1 > T_2$ pak generovaný bit je 0.
- Je-li $T_1 < T_2$ pak generovaný bit je 1.
- Je-li $T_1 = T_2$ (dané konečnou vzorkovací frekvencí datového sběru) = událost za hodinu

Z důvodu lepší vyváženosti jedniček a nul je vhodné použít John von Neumannův dekorelátor, který odebírá dvojice bitů a nahrazuje je podle následujících pravidel:

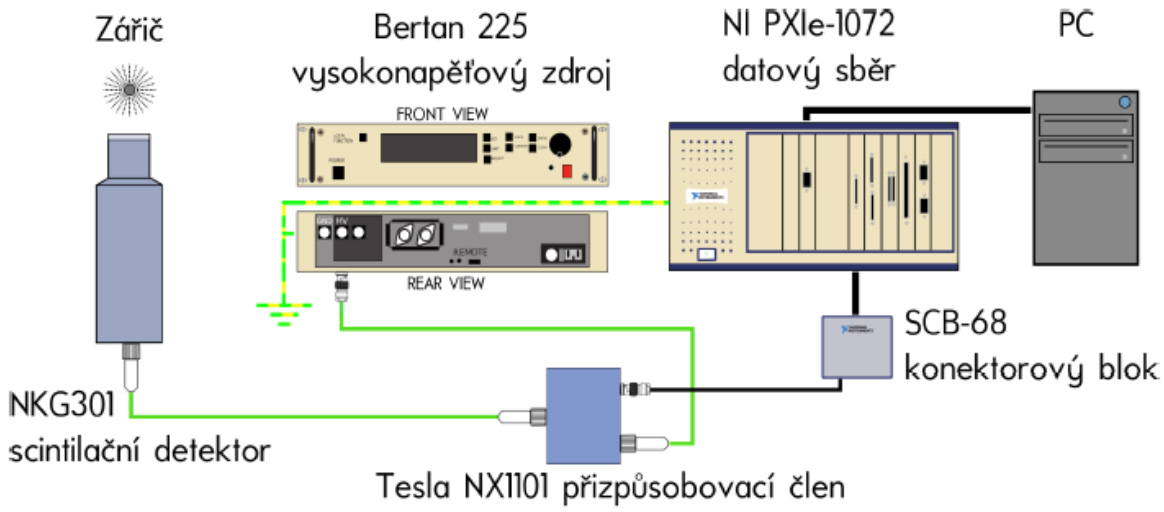
- Je-li dvojice bitů 00 nebo 11 pak se bity zahodí.
- Je-li dvojice bitů 01 pak výstupní bit je 0.
- Je-li dvojice bitů 10 pak výstupní bit je 1.



Obrázek č. 1: Výstupní signál z detektoru

2.3 Uspořádání experimentální sestavy

K vytvoření pokusu je zapotřebí: Zářič, scintilační detektor, přizpůsobovací člen, vysokonapěťový zdroj, konektorový blok, datová sběrna a PC (viz obrázek č.2). Zářič vyzařuje záření do scintilačního detektoru, kde je energie záření převedena na elektrický impulz. Dále musíme zapojit přizpůsobovací člen, do kterého z jedné strany vede záření a z druhé strany napětí cca1000V a konektorový blok. Následuje datový sběrač, který zprostředkovává data a ukládá je do PC, kde se na ně v podobě časového průběhu pulzů můžeme podívat.



Obrázek č. 2: Zapojení soustavy

2.4 Platnost hypotézy

Hodnoty náhodných veličin se dělí na Gaussovo, Poissonovo, Cauchyho a uniformní atd. Kvůli tomu, že nikdy neměříme nekonečné množství hodnost, ale pouze jejich část, nelze na 100% říci, z kterého rozdělení naměřená data pocházejí. K testování hypotéz potřebujeme alternativní hypotézu H_a a testovací hypotézu H_0. Při rozhodování o zamítnutí, nebo schválení hypotézy H_0 mohou nastat tyto případy.

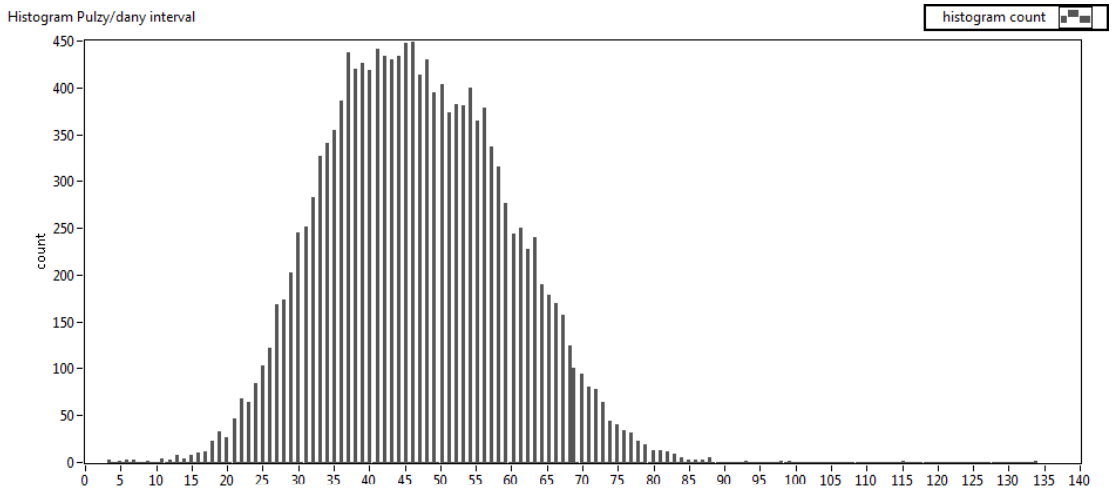
1. Platí H_0 a naše rozhodnutí je nezamítnout H_0.
2. Platí H_0 a naše rozhodnutí je zamítnout H_0 (dopouštíme se chyby prvního druhu).
3. Platí H_a a naše rozhodnutí je nezamítnout H_0 (dopouštíme se chyby druhého druhu).
4. Platí H_a a naše rozhodnutí je zamítnout H_0.

Nulová hypotéza je ta, jejíž zamítnutí na principu chyby prvního druhu je závažnější. Díky tomu můžeme určit, s jakou pravděpodobností se dopouštíme této chyby.

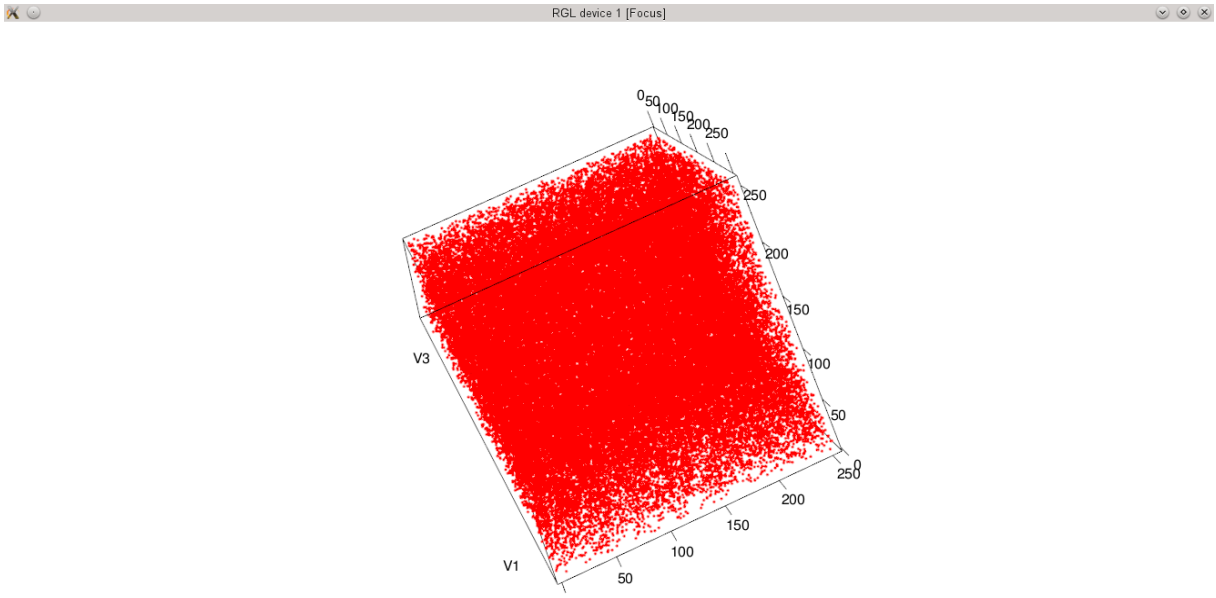
2.5 Ukázka našich výsledků

Ověřili jsme, že počet rozpadů za jednotku času je skutečně náhodná veličina, která se řídí normálním rozdělením (viz obrázek č. 3).

Z náhodných bitů jsme sestavili 8bitová čísla a sestavili je do prostoru (viz obrázek č.4). Čísla rovnoměrně vyplňují celý prostor na rozdíl od pseudonáhodného generátoru, kde by čísla tvořila pouze navzájem oddělené paralelní roviny. Dalším krokem mělo být testování hypotéz náhodnosti generovaných bitů pomocí sady statistických testů sady Diehard. To se bohužel nezdařilo.



Obrázek č. 3: Počet rozpadů za jednotku času



Obrázek č. 4: Náhodná čísla v prostorovém grafu

3 Shrnutí

Za pomocí aparatury pro detekci gama záření jsme sestavili generátor náhodných čísel. Seznámili jsme se s grafickým programovacím jazykem Labview, který byl použit k naprogramování systému sběru dat.

Náhodnost generovaných sekvencí jsme alespoň částečně ověřili vykreslením do prostorového grafu (viz obrázek č.4).

Poděkování

Poděkování Vojtěchu Svobodovi za organizaci týdne vědy a Janu Rusňákovi za konzultace a pomoc při realizaci projektu.

Reference:

[1] The marsaglia random number cdrom including the diehard battery of tests of randomness,
www.stat.fsu.edu/pub/diehard.
[2] National Instruments. Labview user manual,
http://www.ni.com/pdf/manuals/320999e.pdf.
[3] National Instruments. Ground loops and returns, http://www.ni.com/white-paper/3394/en/.
[4] National Institute of Standards and Technology Computer Security Resource Center. Random number generation,
http://csrc.nist.gov/groups/ST/toolkit/rng/index.html.
[5] Robert G. Brown (rgb). Dieharder: A random number test suite,
www.phy.duke.edu/~rgb/General/dieharder.php