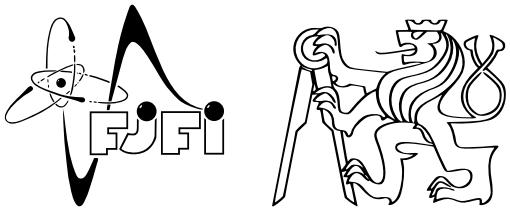
SPECIALIZOVANÉ PRAKTIKUM II
FJFI ČVUT v Praze

Generování náhodných čísel založené na radioaktivním rozpadu.



Jméno: **Krapivin Denis** Kolega: **Roman Jnovčik**

Datum měření: **10.04.2025** Klasifikace:

---

1 Pracovní úkoly

- Zvolte hladinu h_1, od které usoudíte, že došlo k detekci na scintilačním detektoru, a určete počet detekcí za sekundu r_1. Určete průměrnou dobu mezi dvěma detekcemi jako $T_1 = \frac{1}{r_1}$. Vytvořte histogramy počtu detekcí zaznamenaných za doby T_1, $5T_1$ a $500T_1$ a nafitujte je Poissonovým rozdělením. V případě $500T_1$ proveďte fit i Gaussovským rozdělením. Diskutujte kvalitu fitu a zejména vztah směrodatné odchylky a střední hodnoty, který by mělo Poissonovo rozdělení splňovat.

- Zvolte hladinu h_2, od které usoudíte, že došlo k detekci na prvním jednofotonovém detektoru. Určete také hladinu h_3 pro druhý jednofotonový detektor. Pokud počty detekcí nejsou podobné, pokuste se nastavit hladiny tak, aby se rozdíl počtu detekcí lišil maximálně do 10 %. Podobně jako v předešlém úkolu určete průměrné doby mezi detekcemi T_2, resp. T_3, a zobrazte histogramy četnosti detekcí za doby $5T_2$ a $100T_2$, resp. $5T_3$ a $100T_3$. Fitujte Poissonovým rozdělením.

- Z detekcí ze scintilačního detektoru sestavte binární řadu b_1 podle podkapitoly 2.2 *Náhodné bity z gama záření ve zdroji* [1].

- Z detekcí na jednofotonových detektorech sestavte binární řadu b_2, kde bit 0 odpovídá detekci na prvním detektoru a bit 1 detekci na druhém detektoru.

- Vytvořte intervaly délky T_1 a proložte jimi časové záznamy detekcí na scintilačním detektoru. Každý interval rozdělte na dvě poloviny. Pokud se v intervalu nachází právě jedna detekce a ta je v první polovině, generujte bit 0. Pokud je v druhé polovině, generujte bit 1. Intervaly bez detekce, nebo s více detekcemi, nevyužijete. Tímto způsobem sestavte binární řadu b_3.

- Vykreslete autokorelační funkci [2] pro binární řady b_1, b_2 a b_3. Vysvětlete, jaké vlastnosti obecné časové řady lze pomocí autokorelační funkce pozorovat. Sestavte histogramy pro jednotlivé binární řady a vypočítejte jejich informační entropii. Informační entropii lze spočítat z četností bitů 0 (n_0) a bitů 1 (n_1) podle vztahu:

$$H = -p_0 \log_2 p_0 - p_1 \log_2 p_1,$$

kde

$$p_0 = \frac{n_0}{n_0 + n_1}, \quad p_1 = \frac{n_1}{n_0 + n_1}.$$

2 Teoretický úvod

Generování náhodných bitů je založeno na fyzikálně náhodných procesech, jako je radioaktivní rozpad. Radioaktivní rozpad je typický svým náhodným charakterem, a proto je vhodný jako zdroj entropie pro generátory náhodných bitů.

2.1 Generování bitů na základě detekce rozpadů

Rozpad měříme scintilačním detektorem, který zaznamenává jednotlivé rozpady jako napěťové pulsy. Generování bitů je založeno na měření časových intervalů mezi detekcí po sobě jdoucích rozpadů.

Pro vygenerování jednoho bitu je potřeba detekovat čtyři pulsy. Časový interval mezi prvními dvěma pulsy T_1 může být s rovnoměrnou pravděpodobností delší nebo kratší než interval mezi druhými dvěma pulsy T_2. Pravidlo pro generování bitů je následující:

- Pokud $T_1 > T_2$, generovaný bit je 0.
- Pokud $T_1 < T_2$, generovaný bit je 1.
- Pokud $T_1 = T_2$, událost se zahodí.

Aby byla posloupnost bitů lépe vyvážená (stejný počet jedniček a nul), používá se John von Neumannův dekorelator. Ten odebírá dvojice bitů a nahrazuje je podle pravidel:

- Dvojice 00 nebo 11 se zahodí.
- Dvojice 01 se převede na výstupní bit 0.
- Dvojice 10 se převede na výstupní bit 1.

2.2 Generování bitů porovnáním signálů jednofotonových detektorů

Druhá metoda generování náhodných bitů využívá principu detekce jednotlivých fotonů. Světelný paprsek z laseru je nasměrován na dělič svazku, který rozděluje fotony mezi dva jednofotonové detektory.

Postup generování bitů je následující:

- Pokud první foton detekuje první detektor, generujeme do binární řady bit 0.
- Pokud první foton detekuje druhý detektor, generujeme do binární řady bit 1.

2.3 Autokorelační funkce a informační entropie

Pro analýzu generovaných binárních posloupností je důležité určit statistické vlastnosti časové řady. Nejprve označíme binární posloupnost jako

$$\mathbf{b} = (b_1, b_2, \ldots, b_n), \quad b_i \in \{0, 1\}.$$

Průměr a rozptyl odhadu posloupnosti označíme jako

$$\tilde{b} = \frac{1}{n}\sum_{i=1}^{n} b_i, \qquad \tilde{\sigma}^2 = \frac{1}{n-1}\sum_{i=1}^{n}(b_i - \tilde{b})^2.$$

Autokorelační funkce $\tilde{c}(\tau)$ pro binární časovou řadu je definována vztahem

$$\tilde{c}(\tau) = \frac{1}{(n-\tau)\,\tilde{\sigma}^2}\sum_{i=1}^{n-\tau}(b_i - \tilde{b})(b_{i+\tau} - \tilde{b}), \quad \tau = 0, 1, \ldots, n-1.$$

Funkce $\tilde{c}(\tau)$ vyjadřuje korelaci mezi i-tým a $(i+\tau)$-tým prvkem posloupnosti.

- $\tilde{c}(\tau) = 0$ znamená, že prvky jsou statisticky nekorelované.
- $\tilde{c}(\tau) > 0$ značí kladnou korelaci – prvky posunuté o τ mají tendenci mít stejnou hodnotu.
- $\tilde{c}(\tau) < 0$ značí zápornou korelaci (antikorelaci) – prvky posunuté o τ mají tendenci být opačné.

Pro binární posloupnost lze odhadnout informační entropii z četností výskytu nul a jedniček:

$$H = -p_0 \log_2 p_0 - p_1 \log_2 p_1,$$

kde p_0 a p_1 jsou relativní četnosti hodnot 0 a 1 v posloupnosti.

Maximální hodnota $H = 1$ odpovídá rovnoměrnému rozdělení a tedy maximální náhodnosti.

3 Výsledky měření

Před zpracováním dat jsme sloučili všechny dostupné soubory s daty. Před samotným sloučením jsme zkontrolovali, že střední hodnota napětí ve všech souborech souhlasí, což nám umožňuje vyloučit rozdíl systematické chyby mezi jednotlivými měřeními.

3.1 Měření na scintilačním detektoru

Při měření na scintilačním detektoru jsme zvolili hodnotu prahové hladiny $h_1 = -0,23$ V. Po sloučení dat jsme získali záznam o délce $T = 755,882$ s a při této prahové hodnotě bylo detekováno celkem 57824 píků. Závislost napětí na scintilačním detektoru v čase s označením píků je zobrazena na Obr.1.

Z těchto dat jsme vypočítali střední počet detekcí za sekundu $r_1 = 76,5$ Hz a střední dobu mezi dvěma píkami $T_1 = 0,013$ s.

Dále jsme sestrojili histogramy počtu detekcí na scintilátoru zaznamenaných za doby T_1, $5T_1$ a $500T_1$ a tyto histogramy jsme nafittovali Poissonovým rozdělením (viz Obr. 2). Pro případ doby $500T_1$ bylo navíc provedeno i Gaussovské rozdělení s parametry $\mu = 498,48$ a $\sigma = 32,73$.

3.2 Generování bitů ze scintilačního detektoru

Z detekcí ze scintilačního detektoru jsme sestavili surovou binární řadu složenou z $n_0 = 6919$ nul a $n_1 = 6929$ jedniček. Na základě toho jsme určili informační entropii $H_{\text{Raw}} = 1$.

Histogram této binární řady je zobrazen na Obr. 5.a a autokorelační funkce odpovídající této řadě je zobrazena na Obr. 6.a.

Dále jsme s využitím John von Neumannova dekorelatoru sestavili binární řadu složenou z $n_0 = 1784$ nul a $n_1 = 1717$ jedniček. Na základě toho jsme určili informační entropii $H_{\text{Neuman}} = 0{,}999736$.

Histogram této binární řady je zobrazen na Obr. 5.b a autokorelační funkce odpovídající této řadě je zobrazena na Obr. 6.b.

Pro vytvoření další binární řady jsme rozdělili časové záznamy detekcí na intervaly délky T_1. Každý interval byl rozdělen na dvě poloviny. Pokud se v intervalu nacházela právě jedna detekce, pak v první polovině generovala bit 0 a ve druhé polovině bit 1. Intervaly bez detekce nebo s více detekcemi jsme nevyužili.

Tímto způsobem jsme sestavili binární řadu složenou z $n_0 = 10006$ nul a $n_1 = 10234$ jedniček. Na základě toho jsme určili informační entropii $H_{\text{Interval}} = 0{,}999908$.

Histogram této binární řady je zobrazen na Obr. 5.c a autokorelační funkce odpovídající této řadě je zobrazena na Obr. 6.c.

3.3 Měření na jednofotonových detektorech

Při měření na jednofotonových detektorech jsme zvolili hodnotu prahové hladiny pro první detektor $h_0 = 0{,}215$ V a pro druhý $h_1 = 0{,}196$ V. Po sloučení dat jsme získali záznam o délce $T = 762{,}497$ s a při těchto prahových hodnotách bylo detekováno na prvním detektoru 2210 píků a na druhém 2141 píků. Rozdíl v počtu píků je přibližně 3 %. Závislost napětí na prvním a druhém detektoru v čase s označením píků je zobrazena na Obr. 3.

Z těchto dat jsme vypočítali střední počet detekcí za sekundu $r_2 = 2{,}898$ Hz a střední dobu mezi dvěma píkami $T_1 = 0{,}013$ s.

Dále jsme sestrojili histogramy počtu detekcí na prvním detektoru za doby $5T_2$, $50T_2$ a na druhém detektoru za doby $5T_3$, $50T_3$, kde $T_2 = 0{,}345$ s a $T_3 = 0{,}356$ s. Pro všechny histogramy byl proveden fit Poissonovým rozdělením (viz Obr. 4).

3.4 Generování bitů z jednofotonových detektorů

Z detekcí jednofotonovými detektory jsme sestavili surovou binární řadu složenou z $n_0 = 2210$ nul a $n_1 = 2141$ jedniček. Na základě toho jsme určili informační entropii $H_{\text{Foton}} = 0{,}999819$.

Histogram této binární řady je zobrazen na Obr. 5.d a autokorelační funkce odpovídající této řadě je zobrazena na Obr. 6.d.

4 Diskuze

Hlavním problémem všech měření je najít potřebné hodnoty h_1, h_2, h_3 tak, aby odfiltrovaly šum a zároveň aby počet špiček byl dostatečný pro statistické zpracování pro všechny hodnoty intervalů.

Pro malé intervaly (T_1, T_2, T_3) je rozptyl blízký střední hodnotě μ, což odpovídá Poissonovu rozdělení. S rostoucím intervalem se rozptyl stává výrazně větším než μ, což naznačuje, že data vykazují vyšší fluktuace než čisté Poissonovo rozdělení, možná kvůli experimentálním šumům. Navzdory tomu průměrná hodnota μ odpovídá násobkům střední doby mezi dvěma detekcemi pro všechny experimenty.

Další komplikací bylo také to, že s rostoucím intervalem se počet dat výrazně snižoval, takže u jednofotonových detektorů se nám nepodařilo zvolit hodnoty h_2 a h_3 tak, aby bylo dost dat pro intervaly $100T_2$ a $100T_3$, a proto jsme se omezili na intervaly $50T_2$ a $50T_3$.

Binární řady získané všemi způsoby obsahují téměř stejný počet nul a jedniček. Hodnota entropie je – což je poněkud překvapivé – nejvyšší u surové binární řady ($H_{\text{Raw}} = 1$), přestože jsme očekávali, že Neumannova dekorelace by měla entropii zvýšit $H_{\text{Neuman}} = 0{,}999736$. Měli jsme pochybnosti o správnosti zpracování dat, avšak po kontrole vše odpovídalo, takže lze předpokládat, že Neumannova dekorelace dává smysl až při větším množství dat. Další možností je, že šum může ovlivnit hodnotu entropie, a proto jsme získali u surové řady entropii vyšší než u Neumannovy řady.

Hodnoty autokorelační funkce se prakticky rovná nule (maximum $\pm 0{,}03$ na většině intervalů). Na velkých intervalech však dochází k výraznému nárůstu, což je způsobeno malým počtem párů pro výpočet. To naznačuje, že všechny řady mají téměř náhodné chování.

Hodnoty všech vypočtených veličin, včetně průměru μ a směrodatné odchylky σ, lze nalézt ve výstupním souboru na Obr. 7.

5 Závěr

V rámci této práce jsme analyzovali různé metody generování náhodných binárních posloupností založené na fyzikálně náhodných procesech. Byly použity čtyři přístupy:

1. Časové intervaly mezi rozpady měřené scintilačním detektorem, včetně aplikace John von Neumannova dekorelatoru.
2. Detekce jednotlivých fotonů pomocí jednofotonových detektorů s děličem svazku.
3. Intervalová metoda založená na dělení časových intervalů délky T_1 na dvě poloviny a generování bitů podle polohy jediné detekce.
4. Sestavení binárních řad přímo z detekcí jednotlivých zařízení a jejich statistická analýza.

Pro všechny metody jsme určili:

- Počet nul a jedniček v generovaných binárních řadách.
- Informační entropii, která se ve všech případech blížila maximální hodnotě $H \approx 1$, což potvrzuje vysokou náhodnost posloupností.

- Histogramy počtu detekcí a jejich fit pomocí Poissonova a Gaussovského rozdělení.
- Autokorelační funkce, která byla ve všech případech blízká nule, což indikuje minimální korelace mezi po sobě jdoucími bity.

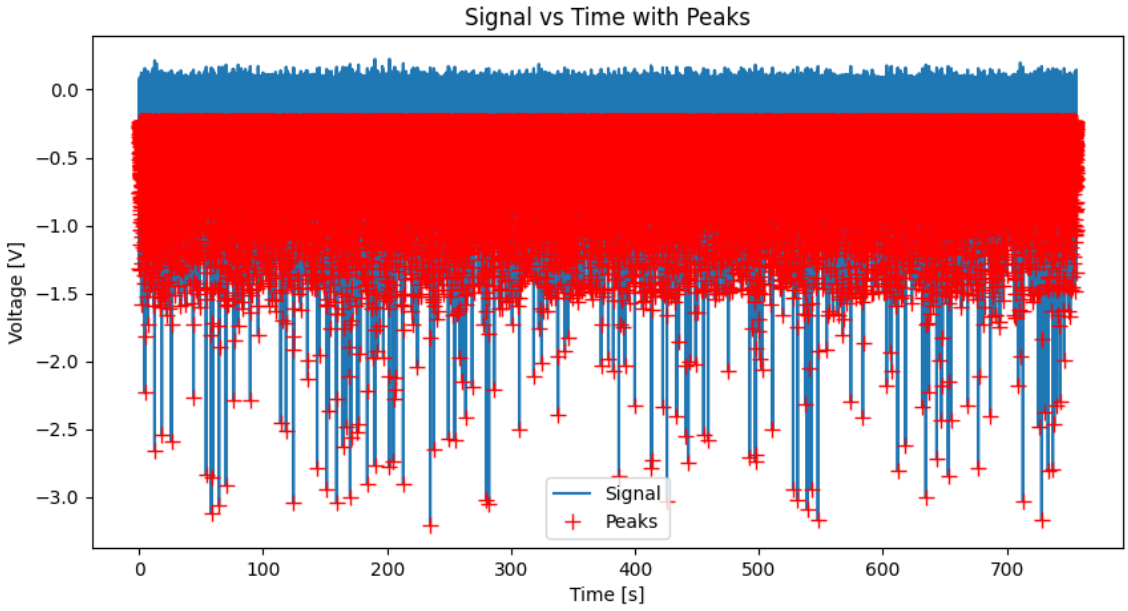
Výsledky ukazují, že všechny použité metody generují binární posloupnosti vhodné pro experimentální využití.

Reference

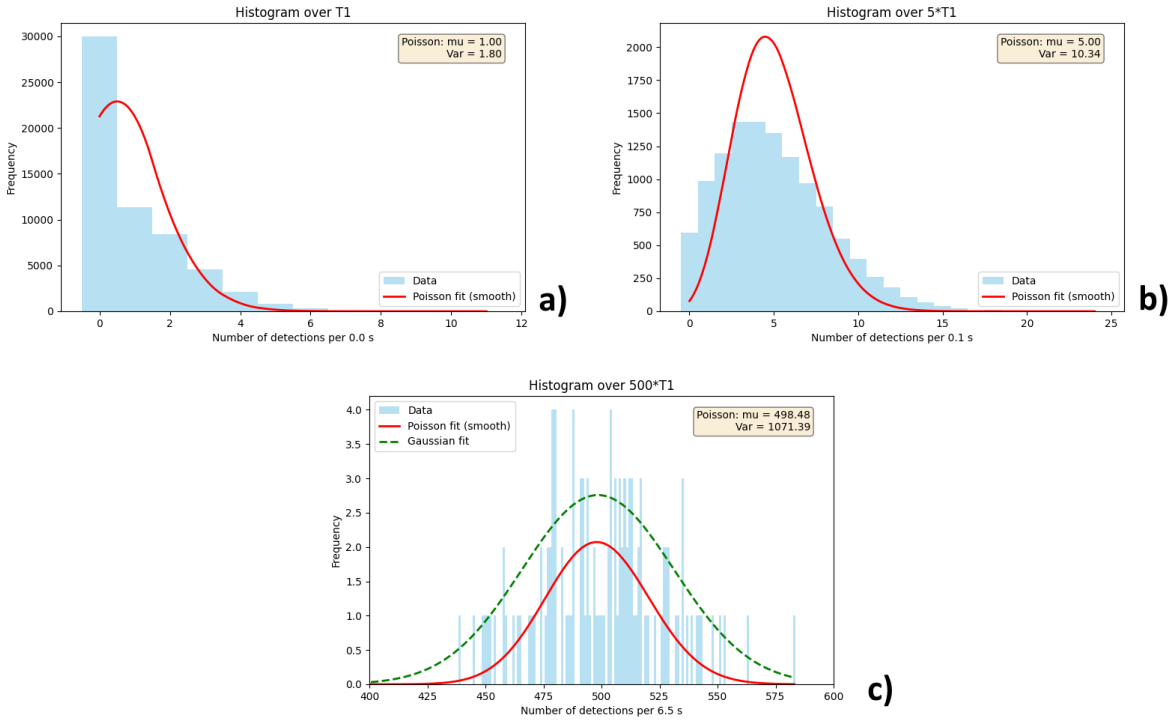
[1] Kolektiv autorů, *Generování náhodných čísel založené na radioaktivním rozpadu*, SPRA01, ČVUT v Praze, FJFI, 2018.

[2] Kolektiv autorů, *Jednofotonový generátor náhodných událostí*, SPRA01, ČVUT v Praze, FJFI, 2020.

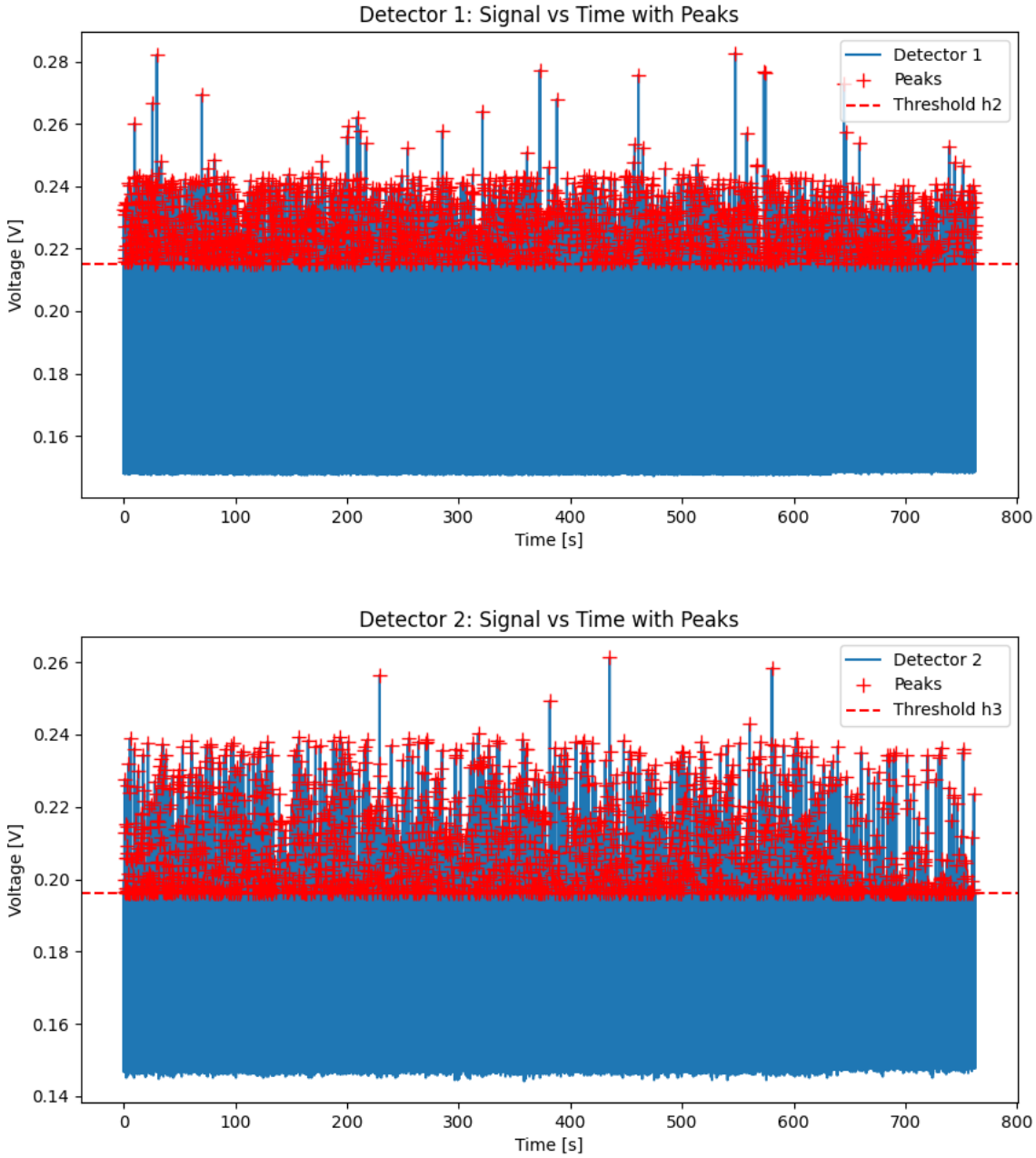
A Příloha



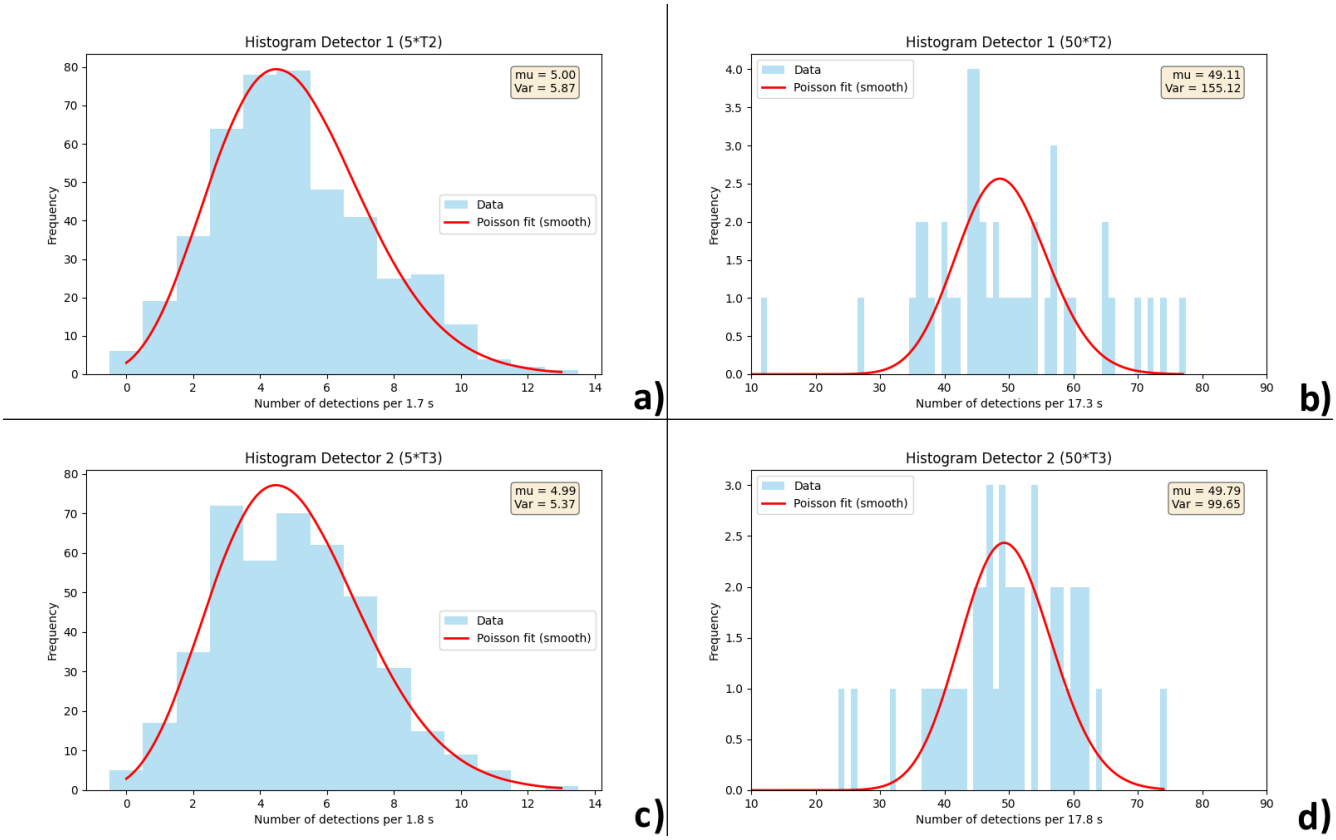
Obr. 1: Závislost napětí na scintilačním detektoru v čase s označením píků, hladina $h_1 = -0,23$ V.



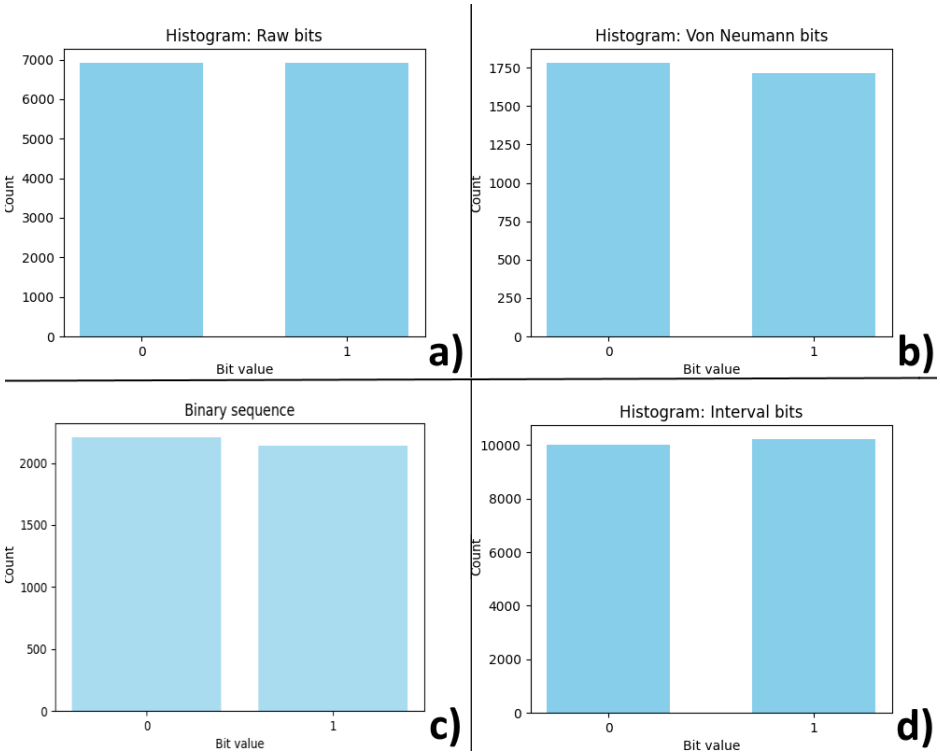
Obr. 2: Histogramy počtu detekcí na scintilátoru zaznamenaných za doby a) T_1, b) $5T_1$, c) $500T_1$, kde $T_1 = 0.013$ s a fitovány Poissonovým rozdělením. Pro případ c) bylo provedeno i Gaussovské rozdělení s parametry $\mu = 498,48$, $\sigma = 32,73$.



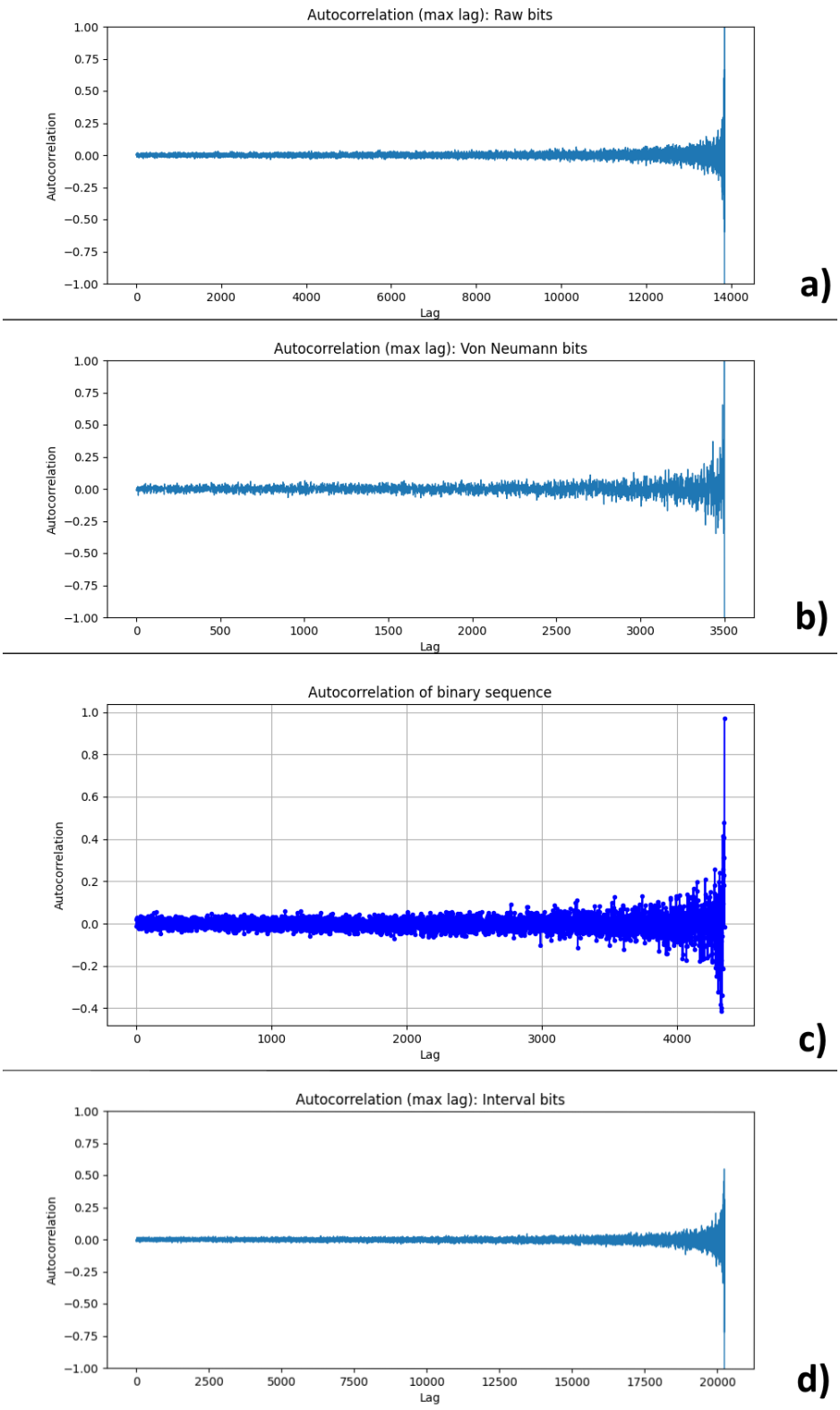
Obr. 3: Závislost napětí na prvním (horní) a druhém (dolní) jednofotonovém detektoru v čase s označením píků, hladiny $h_2 = 0.215$ V a $h_3 = 0.196$ V. Rozdíl v počtu píků je přibližně 3 %.



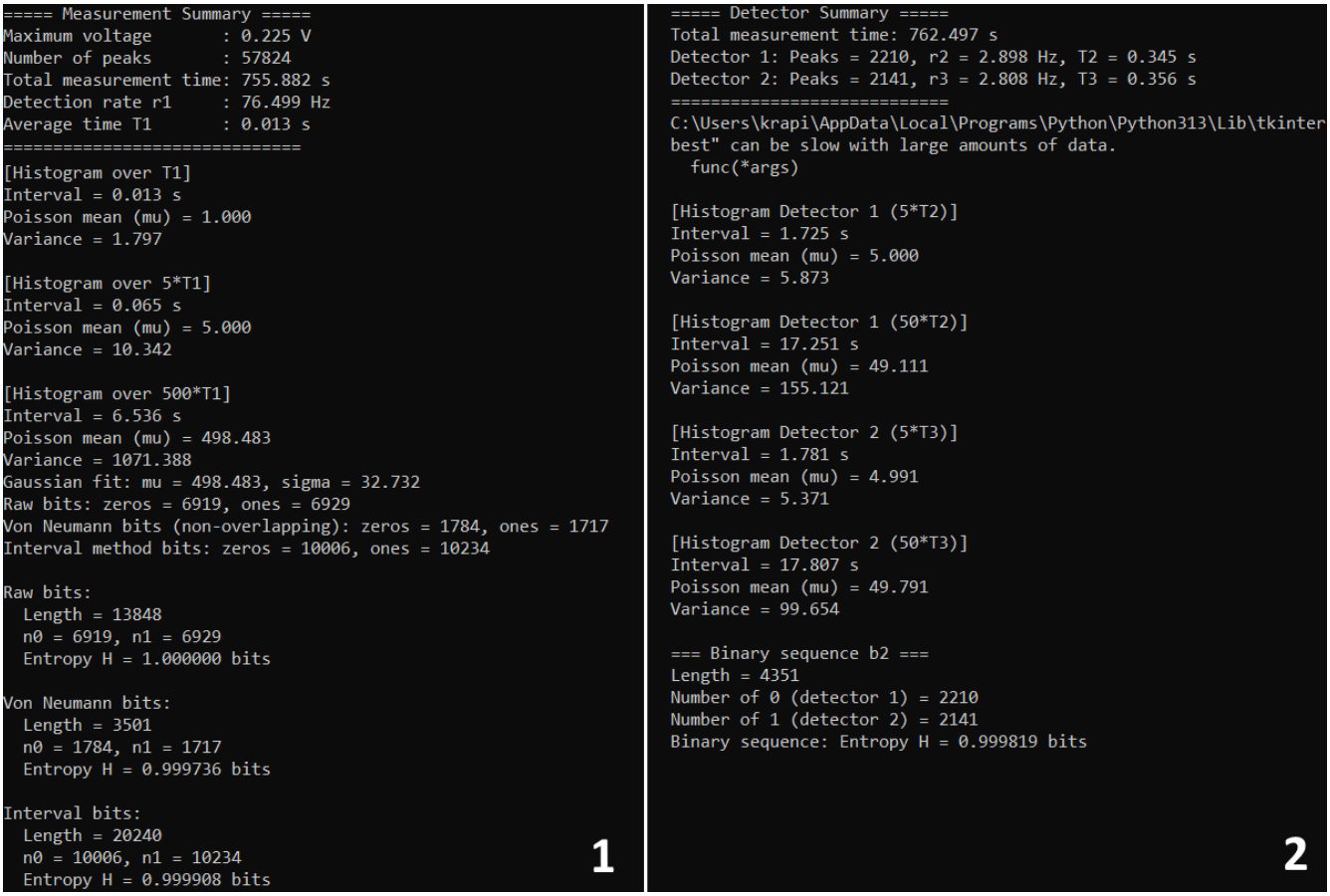
Obr. 4: Histogramy počtu detekcí na prvním jednofotonovém detektoru za doby a) $5T_2$, b) $50T_2$, a na druhém detektoru za doby c) $5T_3$, d) $50T_3$, kde $T_2 = 0.345$ s a $T_3 = 0.356$ s. Pro všechny histogramy byl proveden fit Poissonovým rozdělením.



Obr. 5: Histogramy pro jednotlivé binární řady: a) surové bity generované na scintilátoru, b) bity po použití John von Neumannova dekorelatoru, c) bity získané porovnáním signálů jednofotonových detektorů, d) bity získané intervalovou metodou.



Obr. 6: Autokorelační funkce pro binární řady pro: a) surové bity generované na scintilátoru, b) bity po použití John von Neumannova dekorelatoru, c) bity získané porovnáním signálů jednofotonových detektorů, d) bity získané intervalovou metodou.



Obr. 7: Pod číslem 1 jsou uvedeny výsledné hodnoty všech výpočtů pro scintilační detektor, pod číslem 2 pro jednofotonové detektory. Výpočty byly provedeny pomocí Pythonového kódu.