NIST Statistical Test Suite

Výběr testů:

Pro otestování zadaných dat jsem vybral několik testů z baterie STS. Při výběru jsem se snažil vybrat takové testy u kterých jsem dobře chápal, co testují, abych mohl správně upravit parametry a vyhodnotit závěry testu.

Vybrané testy:

- Frequency – určuje poměr 0 a 1 v celém souboru
- BlockFrequency – určuje poměry 0 a 1 v jednotlivých blocích
- Runs – určuje, zda počet posloupností 0 a 1 je dostatečně náhodný
- LongestRun – testuje délku nejdeší posloupnosti 0, resp. 1
- Discrete Fourier Transform – testuje frekvenci 5% odchylek – zda tyto odchylky nejsou častější, než v 5% případů
- Rank – hodnocení hodností matic
- ApproximateEntropy – testuje frekvenci m-bitových vzorů, které se nachází v datech

K vybraným testům bylo nutné určit dodatečné parametry.

Dodatečné parametry:

Approximate Entropy Test	délka bloku	doporučená hodnota: 5	zvolená hodnota: 5
Block Frequency Test	délka bloku	doporučená hodnota: 128	zvolená hodnota: 1024

Postup:

Pomocí následujícího příkazu jsem vytvořil soubory, které obsahují vždy N-tý bit ze zadání.

```
cat 8mhz.bit | cut -c  1 | paste -s -d '' > "${data_dir}/bit_01.bit"
```

Jednotlivé sloupce jsem spojil a uložit tak do příslušných 16 souborů. Na těchto souborech jsem provedl statistické testy z baterie STS. Jako délku bitstreamu jsem zvolil **10 000** bitů, celkový počet bitstreamů tak vyšel **224**.
Vždy po proběhnutí testu jsem pro každý ze souborů analyzovat výstup uložený v souboru **finalAnalysisReport.txt** a dále výstupy z jednotlivých testů.

Je nutné si uvědomit, že se jedná pouze o statistický test, který může potvrdit, že zvolení zdroj dat není dostatečně náhodný. Nelze však tvrdit opak.

Výsledky:

Bit_01 – 6 ze 7 testů odmítlo vstupní data jako příliš závislá. Pouze test **Hodností matic** shledal vstup jako dostatečně náhodný – protože p-value vyšla okolo 0.039 – plus bylo přidáno upozornění.
Bit_02 – stejně jako v předchozím případě – 6/7 proti, pouze test **Hodností matic** prošel s upozorněním na p-value.
Bit_03 – stejně jako v předchozím případě – 6/7 proti, pouze test **Hodností matic** prošel s upozorněním na p-value.

Bit_04 – stejně jako v předchozím případě – 6/7 proti, pouze test **Hodností matic** prošel s upozorněním na p-value.
Bit_05 – stejně jako v předchozím případě – 6/7 proti, pouze test **Hodností matic** prošel s upozorněním na p-value.
Bit_06 – stejně jako v předchozím případě – 6/7 proti, pouze test **Hodností matic** prošel s upozorněním na p-value.
Bit_07 – stejně jako v předchozím případě – 6/7 proti, pouze test **Hodností matic** prošel s upozorněním na p-value.
Můžeme prohlásit, že testy správně zavrhly prvních 7 bitů, protože data jsou tvořena vždy pouze jednou konstatní sekvencí 0, či 1.
Bit_08 – je od pohledu rozvážený – tedy v části souboru převažují 0 a v jiné 1. 5/7 testů data odmítlo jako nekvalitní. Pouze test **Hodností matic** a test **Entropie** prošly.
Bit_09 – výsledek stejný jako pro bit 08
Bit_10 – 4/7 testů neprošly. Prošly pouze testy **Hodností matic**, **Entropie** a **FFT**. U testu **Entropie** bylo upozornění na p-value.
Bit_11 – Všech 7 testů prošlo, pouze u testu **Entropie** a **Hodnosti matic** bylo upozornění na p-value.
Bit_12 – Všech 7 testů prošlo, pouze u testu **Entropie** a **Hodnosti matic** bylo upozornění na p-value.
Bit_13 – Všech 7 testů prošlo, pouze u testu **Entropie** bylo upozornění na p-value.
Bit_14 – Všech 7 testů prošlo, pouze u testu **Entropie** a **Hodnosti matic** bylo upozornění na p-value.
Bit_15 – Všech 7 testů prošlo, pouze u testu **Entropie** bylo upozornění na p-value.
Bit_16 – 6 ze 7 testů odmítlo vstupní data jako příliš závislá. Pouze test **Hodností matic** shledal vstup jako dostatečně náhodný – protože p-value vyšla okolo 0.039 – plus bylo přidáno upozornění.

Barevně označené bity jsou nejkvalitnější.

Okometricky souhlasím s výsledky provedených testů. Očividně rozvážené posloupnosti byly odmítnuty. Ostatní vypadají poměrně spolehlivě.