L-044

NIST SP800-22 を用いた RPG の検定
NIST SP800-22 Test for RPG

岡田芳明† 金子敏信† 五十嵐保隆†
Yoshiaki Okada Toshinobu Kaneko Yasutaka Igarashi

1. まえがき

RPG(Random Pulse Generator)は有限会社RPGテクニクスによって開発された、放射性原子を用いた物理乱数生成器で、8bit ごとに乱数を生成する。本稿では乱数評価ツールである NIST SP800-22 を用いてその試作版について乱数性の評価を行った。

2. 乱数生成方法

RPG は原子の放射性がポアソン分布に従うことを利用した物理乱数生成器である。RPG における単位時間当たりの平均発生パルス数は 800pal/s である。

放射性原子にはα線を発生するアメリシウム Am（原子番号 95、半減期 432.2 年）が使用されている。アメリシウムから放出されたα線は半導体 Si に衝突し、Si のポテンシャルエネルギーを超えるので、電子が飛び出す。この電子を PIN ダイオードで検出し、アンプにより電気的パルスに変換・増幅されて計測される。このパルスに変換・増幅するまでの部分をα - RPG と呼ぶ。

α - RPG を並列に 8 個用意し各々を 1bit に対応させる。パルスが発生する度に bit が反転するように、8 個のフリップフロップにより状態を記憶し、それらの状態をある瞬間にサンプリングする事により、8bit ごとに乱数を生成する。

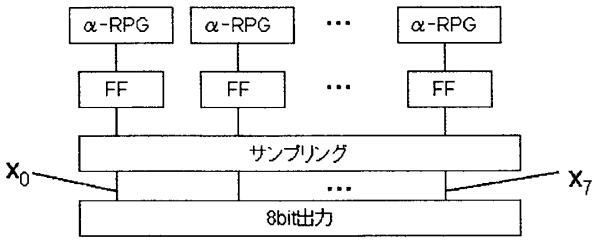

図 1 RPG のブロック図

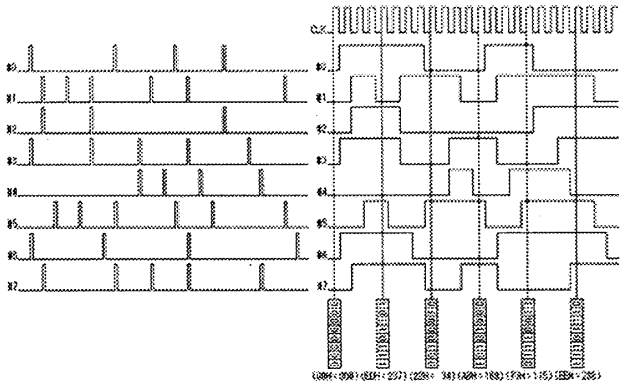

図 2 タイミングチャート図

3. 検定について

3.1 検定の種類

NIST SP800-22(Version1.8)は米国商務省標準技術局 NIST(National Institute for Standards and Technology)で公開されている、15 種類の検定からなる乱数の統計試験ツールである。NIST SP800-22 は,0 と 1 からなる乱数列を対象としており、複数の乱数列を検定する事で乱数生成器の評価が行える点が特徴である。各検定における入力パラメータ、乱数長(1,000,000bit)及び標本数(1,000 本)は全て NIST 推奨値を用いた。

3.2 検定結果

今回サンプリング周波数が 4096Hz 及び 1024Hz において発生させた乱数についての検定を行った。

サンプリング周波数 4096Hz

合格項目

検定番号④ブロック単位の最長連検定⑤2 値行列ランク検定⑩線形複雑度検定⑭ランダム偏差検定⑮種々のランダム偏差検定

不合格項目

検定番号①頻度検定②ブロック単位の頻度検定③連の検定⑥離散フーリエ変換検定⑦重なりのないテンプレート適合

†東京理科大学理工学部

検定⑧重なりのあるテンプレート適合検定⑨Maurer のユニバーサル統計検定⑪系列検定⑫近似エントロピー検定⑬累積和検定

サンプリング周波数 1024Hz

検定番号②ブロック単位の頻度検定以外全ての検定に合格

4. 考察

今回サンプリング周波数を 4096Hz から 1024Hz に下げることにより、乱数の偏りの改善が見られたが、ブロック単位の頻度検定にて不合格という結果となった。

今時刻 t における、1 つのフリップフロップの状態値を x(t)、T をサンプリング間隔とする。フリップフロップによってパルスが発生する度に bit 値を反転するので、

x(t)が x(t+T)で反転する確率 = 時間区間[t,T]でα - RPG より奇数個のパルスが出る確率となる。

単位時間当たりの平均発生パルス数は 800pal/sなので、サンプリング周波数 4096Hzの時、1 サンプリング間隔当たり平均 $\lambda = \frac{800}{4096} = 0.1953$ パルスが発生する。1 サンプリング間隔に奇数個のパルスが出る確率はポアソン分布から次式で求まる。

$$\sum_{k=0}^{\infty} \frac{e^{-\lambda}\lambda^{2k+1}}{(2k+1)!} = e^{-\lambda}\mathrm{Sinh}\,\lambda$$

上式より計算すると、状態値が反転する確率は 0.1617 となる。サンプリング周波数 1024Hzの時も同様に計算すると、

1 サンプリング間隔当たり平均 $\lambda = \frac{800}{1024} = 0.7813$ パルスが発生し、状態値が反転する確率は 0.3952 となる。

状態値が反転する確率が 0.5 となる事が理想であるが、乱数検定において、これらの誤差が 100 万 bit(乱数長)分に影響を与えるので検定に不合格となったと考えられる。

ここで 1 サンプリング間隔の平均パルス発生数λと誤差εとの関係を求めると次式のようになる。

$$e^{-\lambda}\mathrm{Sinh}\,\lambda = 0.5 + \varepsilon$$

$$\therefore \quad \varepsilon = -0.5\,e^{-2\lambda}$$

1 サンプリング間隔の平均パルス発生数λと誤差εの関係をグラフ化したものを以下に示す。

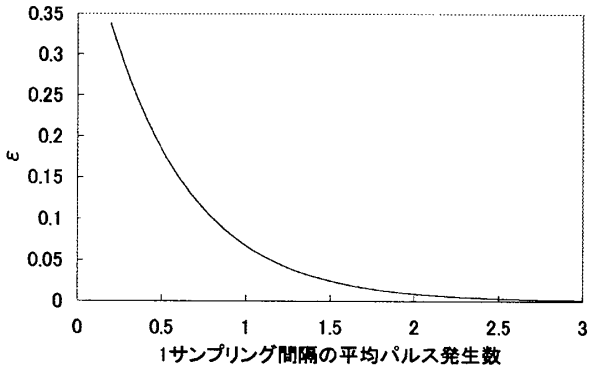

図 3 εとλの関係

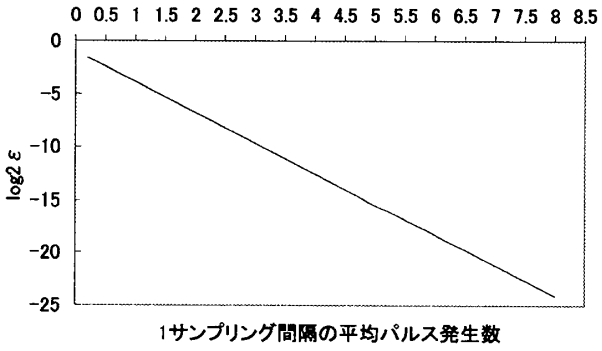

図 4 $\log_2\varepsilon$ とλの関係

100 万bitで考えた場合に十分小さいと考えられる誤差を仮に $2^{-10}(\frac{1}{1024})$～$2^{-20}(\frac{1}{1048576})$だとすると、グラフからサンプリング周波数を 256Hz～120Hz当たりに変更することで乱数の偏りを修正できると考えられる。

参考文献

[1] NIST Special Publication 800-22,"A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" (http://csrc.nist.gov/rng/SP800-22b.pdf)

[2] 吉沢康和、井上光、宮武修「物理乱数の特徴と算術乱数の欠点-良質の乱数を求めて-」農業技術短期大学誌 第 32 巻(1998)