ショット雑音を発振器に印加した乱数発生装置

◎渡会　哲也*，斉藤　義明**，堀　潤一**

*新潟大学大学院自然科学研究科，**新潟大学工学部福祉人間工学科

1．はじめに

乱数は，社会現象や物理現象の数値シミュレーションや情報保護のための暗号化技術に広く利用されており，周期性のない一様乱数を生成する方法が切望されている．これまで，ショット雑音や，ガンマ線等を用いた物理乱数発生装置の開発が試みられてきたが，乱数生成速度が遅い，大規模の装置を必要とするなどの問題がある[1]-[2]．

本研究では，ダイオードのショット雑音を発振器に印加することで，発振器の発振周波数をランダムに変化させて，その出力から乱数を生成することを試みた．また，本装置の高速化の可能性について検討した．また，生成された数値データが乱数とみなせるかどうかを，統計学的検定法を用いて評価した．

2．乱数生成法

発振回路の発振周波数は次の式で与えられる．

$$f = 1/2\pi\sqrt{LC} \qquad (1)$$

発振回路に可変容量ダイオードをつなぎ，そこに増幅整形したショット雑音を印加することで，式(1)の C の値を雑音に依存して変化させれば，周波数が不規則に変化する発振出力を得ることができる．本研究では，この出力を利用して乱数を生成することを試みた．

乱数生成の流れを図 1 に示す．ダイオードに直流電圧を加えてショット雑音を発生させ，その振幅を 0V から 10V 程度の範囲まで増幅整形し，発振回路に入力する．発振回路の出力を A/D 変換器を介してディジタル化し，パーソナルコンピュータに取り込む．ディジタル化したデータを，0，1 の 2 進数データに変換した後，8 ビットごとに 10 進数に変換して乱数として出力する．

3．乱数の評価

発振周波数 200kHz の発振回路に雑音を印加して，発振周波数の+1%までの範囲で発振周波数を不規則に変化させる．その出力をサンプリング周波数 50Hz でディジタル化し，8 ビット数値データを 1 万個生成し，頻度検定，連の検定を用いて評価を行った．結果を表 1 に示す．

高速化の可能性について検討するため，発振周波数を 400kHz，800kHz，1.5MHz，2.5MHz と変化させ，数値データを取得した．生成された数値データに対して検定を行い，各発振周波数においてのサンプリング周波数の上限を調べた．結果を図 2 に示す．

4．まとめ

ショット雑音を印加した乱数発生装置を開発し，生成された数値データに対して統計学的検定法を用いて評価を行った．表 1 より，本装置で生成した数値データが乱数とみなせることを示した．図 2 より，発振周波数を高くすることで，乱数生成速度が向上することを示した．

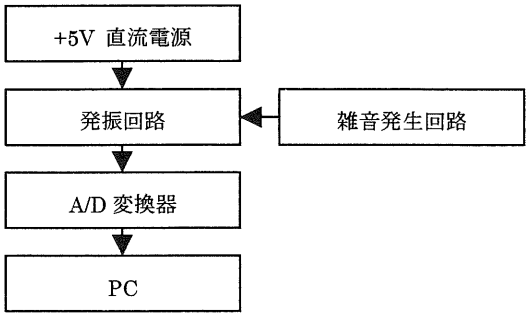

図 1　乱数生成の流れ

表 1 検定結果

検定法	検定値	有意水準 5％の棄却閾値
頻度検定	249.933	293.248
連の検定	0.158	9.488

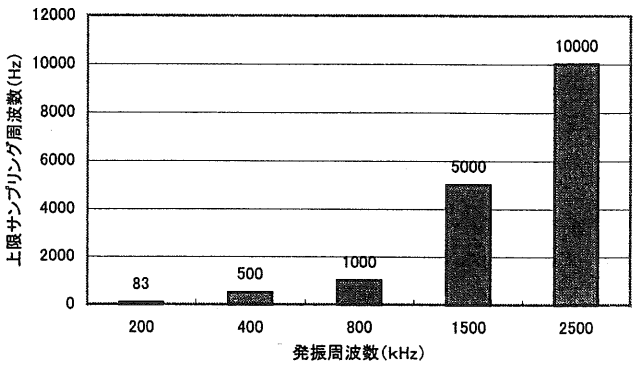

図 2 発振周波数と乱数生成速度

参考文献

[1]　仁木直人，“パーソナルコンピュータのための物理乱数発生器”，統計数理研究所彙報，vol.31，no.1，pp.33-49，1983.

[2]　岸本俊祐，福江万寿夫，“ダイオードノイズを利用した物理乱数の発生とその評価”，信学論，vol.J82-A，no.11，pp.1704-1709，Nov.1999.