平成 12 年度卒業研究		
入学年度　平成 9 年度	学籍番号　09117925	氏名　　後藤 嘉洋
論文題目　ウェーブレット変換を用いた擬似乱数系列の評価法		中野研究室

1　はじめに

擬似乱数系列は暗号等に使用され，統計的一様性を満たしていなければならない．よって，本稿では擬似乱数系列の時間的変化について調べるため，時間周波数解析を行なうことができるウェーブレット変換を用いての評価方法を提案し，考察を行なう．

2　ウェーブレット変換

ウェーブレット変換は，さざ波状の関数 (ウェーブレット) を基底関数とする変換である．また，局所性を持っており，時間周波数変換に用いられる．ウェーブレットには様々な種類が存在するが，多重解像度解析に用いられる直交ウェーブレットの中で最も理論解析しやすいものは図 1の $haar$である．

離散ウェーブレット変換は，離散数列を用いることで簡単に求めることができ，図 2のように分解して解析を行なう．一般に，jレベルのスケーリング係数 $s_k^{(j)}$から，$j+1$ レベルのスケーリング係数 $s_k^{(j+1)}$とウェーブレット係数 $w_k^{(j+1)}$が導出できる．なお，ウェーブレット係数は個々のスケールにおける信号特性とエネルギーを表している．

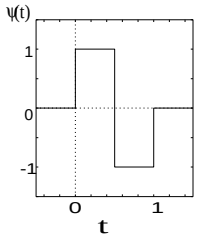

図 1: $haar$のウェーブレット

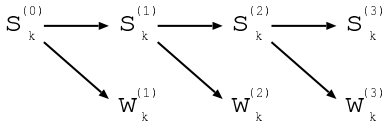

図 2: スケーリング係数の精度の低いレベルへの分解

3　評価対象とする擬似乱数生成器

非線形フィードバック型無周期擬似乱数生成器のレジスタ長は，固定ではなく，生成した擬似乱数系列長に従って逐次長くなる．また，非線形変換への入力ビット数を m 個とし，レジスタの相対的な位置を参照している．これを方式 1 とする．方式 1 では，$m+1$ ステップ毎に参照位置が変わらないという現象が起こる．そこで，このビットを取り除くよう改良した方式を方式 2 とする．また，位置を参照する際，線形合同法によって，入力値が変化する確率の偏りが生じないように改良したものを，方式 3 としている．

4　スペクトル密度

擬似乱数系列の性質が時間とともに変化していくかどうかの評価尺度として，スペクトル密度の傾きを調べた．系列長は 16384 とし，全体を 8 分割してそれぞれの傾きを算出した．表 1がその結果である．傾きの算出にあたってはまず，各レベルでウェーブレット係数を求め，次に，その 2 乗平均をパワーと考えた．理論的にはどのレベルでも同じパワーを持っているので，傾きが 0 になるはずであるが，方式 1 は明らかに大きい値を示している．これは大きなランレングスが発生していることが起因していると考えられる．

表 1: スペクトル密度の傾き

区間	方式 1	方式 2	方式 3
1〜2048	-0.562	-0.067	-0.036
2049〜4096	-0.675	-0.041	-0.013
4097〜6144	-0.612	-0.081	0.048
6145〜8192	-0.695	-0.063	-0.003
8193〜10240	-0.707	-0.086	-0.019
10241〜12288	-0.781	0.003	0.008
12289〜14336	-0.702	-0.006	0.038
14337〜16384	-0.794	-0.083	-0.025

5　提案する評価法

本節では，ウェーブレット係数の理論値と実験値を用いた評価法を提案する．スペクトル密度の傾きは，それぞれのレベルでウェーブレット係数の 2 乗平均から求めていた．理想的擬似乱数のウェーブレット係数の平均値は 0 なので，2 乗平均は分散を求めていることに等しい．よってそれぞれのレベルで，分散を評価尺度とすることができる．

すべてのレベルにおけるウェーブレット係数の分散は 1 である．よって，良い擬似乱数生成器であれば，そこから推定される母分散の範囲の中に，理論的な分散の値である 1 が当然入るはずである．そこで，擬似乱数系列から標本をとり，信頼度を 95%として母分散を推定する．すべてのレベルで母分散の信頼区間の中に 1 が入っていなければ，擬似乱数系列として適さないと判断できる．

表 2は各レベルにおける母分散の信頼区間を表したものである．表 2より，方式 1 と方式 2 は範囲内に 1 が入っていないレベルが存在している．一方，方式 3 はどのレベルでも 1 が入っており，同じような範囲を推移している．よって本評価法では，方式 3 が擬似乱数系列として最も適していると言える．

表 2: 母分散の推定区間

level	方式 1	方式 2	方式 3
1	0.892〜1.217	0.847〜1.144	0.852〜1.151
2	0.754〜1.020	0.856〜1.158	0.883〜1.193
3	0.830〜1.120	0.863〜1.165	0.864〜1.168
4	1.052〜1.422	1.048〜1.415	0.857〜1.158
5	1.119〜1.512	0.939〜1.269	0.859〜1.160

6　まとめ

本稿では，ウェーブレット変換を用いた擬似乱数系列の評価法を提案した．実際に，数種類の擬似乱数系列に対して評価を行なった．

参考文献

[1] 丹羽，“非線形フィードバック型無周期擬似乱数生成器に関する研究”，2000