

自主課題研究概要

擬似乱数の検定

3年 311 水上直紀 2011/2/17 担当教員 藤崎礼志

調査方法

線形合同法を用いて2つ、C言語のrand関数、メルセンヌ・ツイスタと以下の4つの乱数を生成し検定法を試してみる。

A $Y_{n+1} = ((2^{18} + 1)Y_n + 1) \bmod 2^{35}$ $Y_0 = 31415$

B $Y_{n+1} = (16807 \times Y_n) \bmod 2^{147483647}$ $Y_0 = 31415$

C C言語 初期値 31415

D メルセンヌ・ツイスタ 初期値 0x123, 0x234, 0x345, 0x456

検定法は、連の検定、最大値検定、系列相関検定である。

結果

相関係数検定	合格回数	合格率 (%)
A	885	88.588589
B	999	100
C	999	100
D	999	100

最大値検定	合格率(%)	検定量	合否
A	0	21.82	不可
B	91.3	0.1665	可
C	91.2	0.2167	可
D	91.8	0.4678	可

連の検定	検定量	合否
A	6075	不可
B	5.258	可
C	0.745	不可
D	3.814	可

考察

以上の結果では、AとCはもとかくとして乱数の質が良くないとされる線形合同法と良いとされるメルセンヌ・ツイスタの差はわからなかった。理由としては検定に使った乱数列が短く、周期の長さがあるものを検出できなかったと考えられる。