1　乱数生成アルゴリズム

乱数を生成するアルゴリズムにはいろいろな種類があります。その中で、最もよく用いられているアルゴリズムは、線形合同法と呼ばれるアルゴリズムです。線形合同法は、C 言語のライブラリ関数である rand() 乱数生成関数の実装において、生成の基礎となるアルゴリズムとして広く使われています。線形合同法のアルゴリズムは、非常に簡単です。乱数系列 $R_1, R_2, \ldots, R_i, R_{i+1}, \ldots$ において、下記の式により次の値を順に計算します。

$$R_{i+1} = (aR_i + c)\%m$$

ただし、a, c, m は、正の整数であり、%はモジュロ演算子 (剰余演算子)

通常 m は R_i のビット幅に依存して決定されます。例えば、R_i が 32 ビットの unsigned int 型であれば m を 2^{32} とすることができます。

m を小さくすると乱数の周期が短くなってしまい、同じならびが現れやすくなりますから、m は大きく取るほうが有利です。式の a と c は、乱数の性質に大きな影響を与えます。適切に選ぶと、周期が長くランダムな乱数系列を得ることができます。逆に不適切な選択をすると、乱数としての性質が失われます。

「ニューメリカルレシピ・イン・シー (日本語版)」技術評論社では、m を 2^{32} とする場合について

$$a = 1664525$$
$$c = 1013904223$$

を適切な値として例示しています。

プログラムには、線形合同法で行われるモジュロ演算が含まれていません。これは、gcc コンパイラでは unsigned int が 32 ビットで表現されていることを利用し、計算によって 32 ビットから桁あふれした値が捨てられていることで、2^{32} によるモジュロ計算を行ったのと同じ計算結果を得ているためです。

実行結果をみると、一見、ランダムな数値が順に出力されているように見えます。しかし、実は、これらの数値には、乱数らしからぬ規則性が潜んでいます。実は、出力は奇数と偶数が交互に並んでいます。出力された数値を 2 進数の最下位では、0 と 1 を交互に繰り返していることになります。このことは、線形合同法の欠陥のひとつです。

一般に線形合同法では、最下位桁だけでなく、下位の桁は上位の桁と比較して繰り返し周期が短く、ランダムさに欠けるという特徴があります。この特徴を考えると、線形合同法に基づく乱数の、特定のビット位置を取り出して乱数として利用することは避けるべきです。特に、繰り返しの周期の短い、下位の桁を取り出す操作はよくありません。

2 線形合同法による擬似乱数生成プログラム

```
0001: /*
0002: 擬似乱数生成プログラム
0003: 線形合同法による擬似乱数生成プログラムです
0004: 使い方  $./r（初期値）
0005: yukio sugawa
0006: 2012/4/14
0007: */
0008:
0009: #include <stdio.h>
0010: #include <stdlib.h>
0011:
0012: #define LIMIT 50
0013:
0014: int main(int argc, char *argv[])
0015: {
0016:   unsigned long r;
0017:   int      i;
0018:
0019:   if(argc < 2){
0020:     fprintf(stderr, "使い方  $./r（初期値）\n");
0021:     exit(1);
0022:   }
0023:   sscanf(argv[1], "%lu", &r);
0024:
0025:   for(i = 0; i < LIMIT; ++i){
0026:     r = 1664525L * r + 1013904223L;
0027:     printf("%lu\n", r);
0028:   }
0029:
0030:   return 0;
0031: }
```

3 「r」の操作方法

「r」の操作方法

./r 0「Enter」

上記の「./」は、Linux でのプログラムを実行する時の例です。
ウィンドウズでは、r.exe 0 「Enter」と入力してください。

4　実行結果

1013904223
1196435762
3519870697
2868466484
1649599747
2670642822
1476291629
2748932008
2180890343
2498801434
3421909937
3167820124
2636375307
3801544430
28987765
2210837584
3039689583
1338634754
1649346937
2768872580
2254235155
2326606934
1719328701
1061592568
53332215
1140036074
4224358465
2629538988
1946028059
573775550
1473591045

C による数値計算とシュミレーション　125 頁　小高智宏著　オーム社より