並列計算のための乱数生成法

2002MM091 高井 宏和
指導教員　伏見 正則

1　はじめに

最近では，様々な問題の解決の手段としてシミュレーションが多く用いられるようになった．シミュレーションとは不確実な出来事の仮の結果として乱数を用いた値を代入し問題に対する仮の結果を計算するものである．シミュレーションは実際の結果とほぼ同じ結果が得られるため様々な分野の研究で利用されている．しかし，データ数が膨大であったり計算が複雑であったりすると 1 つのコンピュータで解くことができない．この問題を解決するには処理速度の速い計算機を使うという方法があるが，速度の速い計算機ほど高価になるので実用的ではない．そこで考え出されたのが処理速度はそれほど速くない安価な複数の計算機を接続して，1 つの大きなコンピュータのように使うという方法である．この方法を「並列計算」という．ここで問題となるのが並列計算でシミュレーションのときに使う乱数である．このときに用いる乱数には様々な観点から見た乱数の質が問題となる．詳細はこの後の章で述べるが，評価基準としては計算時間，一様性，乱数と乱数の間の相関が挙げられる．本研究では，計算時間，一様性について過去の研究で保証されている乱数発生方法を使うことでこの項目の調査を省略し，乱数と乱数の間の相関を調べる研究を進めていく．

2　乱数評価基準

2.1　発生にかかる時間

まず 1 つ目の評価基準として発生にかかる時間を考える．本研究では研究が進んでいる発生方法を用いるので，もし発生に長い時間がかかるならばシミュレーションには向かないという程度の基準とする．

2.2　一様性

2 つ目は乱数として最も大切なことである一様性について考える．乱数の一様性の検定についてはいくつか方法があるが，本研究ではこの一様性については，すでに研究が進んでおりある程度の一様性が保証された発生法を使うこととする．

2.3　乱数と乱数の間の相関

計算方法は以下の式 (1) に乱数列を代入して関数の値を調べる．この関数はある乱数列 $< x_n >$ と，その位相を τ だけずらした乱数列 $< x_{n+\tau} >$ の相関を調べるものである．関数中の x_n は n 番目の乱数，N は相関を調べる乱数の個数，$\overline{x}$ は乱数列の一周期の平均値である．

$$P_{xx}(\tau) = \frac{1}{N}\sum_{n=0}^{N-1}(x_n - \overline{x})(x_{n+\tau} - \overline{x}) \qquad (1)$$

自己相関の大きさを測る指標として関数 $P_{xx}(\tau)$ を考えたが，この値では，はっきりと相関の大きさを比べることはできないので $P_{xx}(\tau)$ を $P_{xx}(0)$ で割った値，つまり，

$$r(\tau) = \frac{P_{xx}(\tau)}{P_{xx}(0)} \qquad (2)$$

この $r(\tau)$ の値を考える．τ を横軸にとり，$r_{xx}(\tau)$ を縦軸にとり，少しづつ τ を大きくしていき τ が大きくなると $r_{xx}(\tau)$(相関係数) がどのような値をとるのかをグラフに点をプロットして調べる．

3　線形合同法と並列計算

3.1　線形合同法 [1][2]

一様乱数の生成法として最も一般的で古くから使われてきたのは，1948 年頃レーマー (Lehmer) によって提案された線形合同法である．この方法は、以下のような漸化式

$$X_n = aX_{n-1} + c \pmod m \qquad (3)$$

を用いて負でない整数列 $< X_n >$ を生成させるものである．区間 [0,1) 上の実数型乱数が必要なときは，$x_n = X_n/m$ を使う．上式の a は乗数，m は法と呼ばれ，ともに正の整数である．また c は加数といい，$c = 0$ の場合は乗算型合同法，$c \neq 0$ の場合は混合型合同法と区別される．本研究では乗算型合同法を扱うこととする．

3.2　並列計算の方法

線形合同法で発生させた乱数を用いて，並列計算によるシミュレーションを行う際には注意点がある．異なる計算機で乱数列の同じ部分を使うことは，シミュレーションの解を実際の解に近づけるためには避けるべきである．よって，それぞれの計算機に乱数列を割り当てるときは十分に位相差のある乱数列を割り当てなければならない．しかし位相差のある乱数列を，いくつかの計算機に割り振るためにはそれぞれの計算機で使う乱数の初期値を求める必要がある．乱数をどんどん発生させていけば，いつかは求めたい初期値を求めることができるが，かなりの時間がかかってしまうからである．よって線形合同法による乱数発生の性質を利用して途中の乱数 (2 台目以降の計算機で使う乱数列の初期値) を求めることとした．これが付録のプログラムである．このプログラムでは，以下のような性質を用いて計算を行っている，

線形合同法は，X_0 を初期値，a を乗数，m を法とすると

$$X_n = aX_{n-1} \pmod m \qquad (4)$$

という計算により乱数を発生させるので，この式を変形すると第 n 項は初期値 X_0 を用いて，

$$X_n = a * X_{n-1} \pmod m \qquad (5)$$

$$= a * aX_{n-2} \pmod m \quad (6)$$
$$= a^2 * aX_{n-3} \pmod m \quad (7)$$
$$\vdots$$
$$= a^{n-1} * X_0 \pmod m \quad (8)$$

となることを利用して，途中の項を計算する．具体的には，$a^{n-1} * X_0 \pmod m$ の中の $a^{n-1} \pmod m$ を先に計算する．

実際の計算の際は，この値に初期値 X_0 をかけて，m で割った余りを 2 台目以降の計算機で使う乱数の初期値とする．このプログラムの工夫として，a^{n-1} の式中の $n-1$ の値を 2 のべき乗にすることにより乗算と剰余算を用いて速く計算が可能となる．

4 3 項 GFSR 法と並列計算

4.1 3 項 GFSR 法 [1][2]

M 系列に基づく方法の中で計算機での計算が，容易で高速に実行できる乱数発生法として GFSR 法がある．この発生法の演算は漸化式であるが，和を求める部分が排他的論理和であり，計算機内での演算では早く演算が行われるので，乱数発生速度は速くなることが期待できる．ただ，この方法を用いるときは初期値の設定に注意が必要である．それは初期値が 1 個ではないということである．この発生方法の初期値は X_0 から X_{p-1} までの p 個であり，これら p 個の中からいくつかを選んで排他的論理和により演算を行う．この p 個は，線形合同法により乱数列を生成するのだが，本研究では $a = 69069, m = 4294967296$ の乗算型線形合同法により p 個の初期値を発生させている．GFSR 法にはいくつか種類があるので，本研究ではその中の 3 項 GFSR 法を扱うこととする．この方法は以下のような演算で乱数を発生させている．

$$X_n = X_{n-p} \bigoplus X_{n-q} \quad (0 < q < p) \quad (9)$$

4.2 並列計算の方法

3 項 GFSR 法により発生させた乱数を用いて並列計算のシミュレーションを行うときには，先にも述べたように (9) 式のような 3 項 GFSR 法の場合には p 個の初期値を持つので，これら p 個の初期値を全て 2 台目以降の計算機に振り分けなければならない

3 項 GFSR 法の場合も線形合同法の場合と同じで，並列計算の際には初期値を用いてかなり後の p 個の初期値乱数列を早く出力したい．そこで 3 項 GFSR 法の乱数発生式は，k を自然数として，

$$X_n = X_{n-2^k*p} \bigoplus X_{n-2^k*q} \quad (0 < q < p) \quad (10)$$

と変形することができるので，これを利用してすばやく n 項目から $n+p$ 項目までの p 個を出力できる．これらの初期値列を用いて 2 台目以降の計算機による計算を実行できる．

5 実行結果と考察

実行結果として各発生方法とも初期値を変えて 5 パターンずつ，位相差と相関係数の関係をプロットしたものが下の図 1，図 2 である．初期値を変えて 5 回相関係数を計算しグラフにプロットした．このグラフから見て位相差が 0 のときの相関係数を 1 とすると位相差があるときの相関係数は十分小さいので 2 つの発生方法とも相関は，ほとんど無いと結論できる．位相差をさらに大きくしても相関係数の値は変わらなかったので相関は無いといってよい．よって乱数列を重ならないように選べばシミュレーションを行うのに支障は無いことがわかった．

今後の課題として，いろいろな定数の値を変更したり，異なった乱数発生法の間の相関を調べるとさらに深い研究になったと思われる．

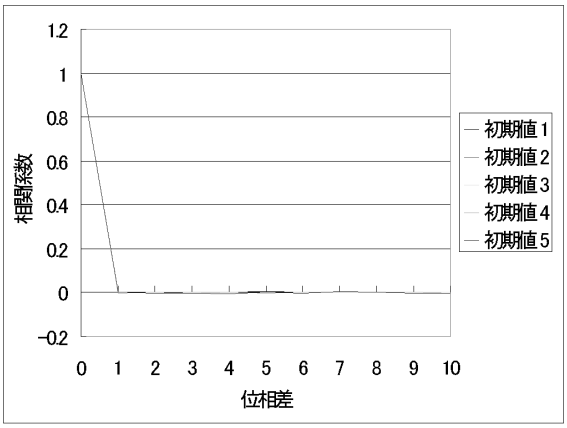

図 1　線形合同法相関係数
$(a = 2100005341, m = 2147483647, N = 300000)$

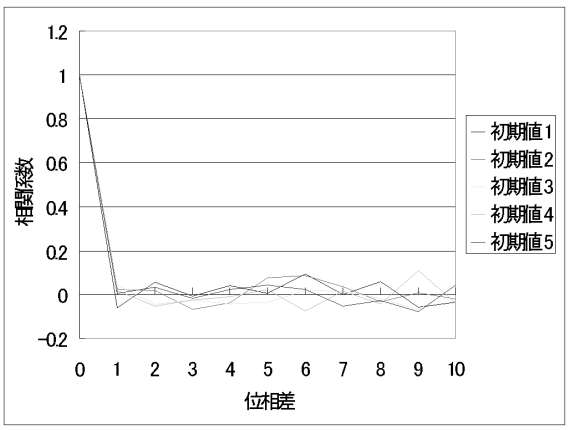

図 2　3 項 GFSR 法相関係数
$(p = 489, q = 521, N = 300000)$

参考文献

[1] 伏見正則：乱数，東京大学出版会，1989.
[2] 伏見正則：確率的方法とシミュレーション，岩波書店，1994.