合同法乱数

伏見　正則　東京大学

1. 合同法

2つの正整数 M, a, および1つの非負整数 c を適当に選び，漸化式

(1) $X_n = aX_{n-1} + c \pmod{M}$

を用いて数列 $\{X_n\}$ を生成する方法を**線形合同法**あるいは単に**合同法**と呼ぶ．これは約40年前に Lehmer によって提案された方法であるが，今日でもなお大型計算機からパーソナル・コンピュータまで，手軽な乱数発生法として広く使われている．2進法の計算機では，M は 2^l (l は正整数) とすることが多いが，$2^l \pm 1$ や大きな素数を選ぶこともある．a, c の選び方については，きわめて多数の研究が行なわれてきたが，その結果は Knuth [2] にまとめられている．

式 (1) からただちにわかる合同法乱数列の特徴は，

①周期がM以下である

②1周期の間に同一の数が現われることはない

の2点である．①は，使用する計算機の整数演算の桁数によって周期が制約されることを意味する．現在計算機メーカから提供されている“標準的な”乱数発生プログラムの場合の周期は，32ビットの大型機では $2^{30} \fallingdotseq 10^{10}$，16ビットのパーソナル・コンピュータでは $2^{15} \fallingdotseq 26$ 万程度のものが多いようである．②については，次節で詳しく述べる．

2. 多次元疎結晶構造

②の特徴がもつ意味を簡単な例で見てみよう．$M=16$, $a=5$, $c=1$, $X_0=1$ とすると，(1) 式によって発生される数列の1周期分は，$\{1, 6, 15, \cdots, 3, 0\}$ となり，15以下のすべての非負整数がちょうど1回ずつ現われる．この数列のあい続く2個の要素を座標成分とする点列 $\{P_n (X_n, X_{n+1}); n=0, 1, 2, \cdots\}$ をプロットすると図1の(1)のようになる．プロットされた点の脇の数字は n の値を示す．点列全体がこのような“**結晶構造**”をなす理由は次のとおりである．点 P_0 が $(x, y)=(1, 6)$ にくると，②の性質により，それ以降の点は直線 $x=1$ および $y=6$ の上にはけっしてこない．次の点 P_1 は $(x, y)=(6, 15)$ にくるので，それ以後は直線 $x=6$ および $y=15$ の上には点がのらない．以下同様であり，結局 $M^2=256$ 個の格子点のうち，規則的に並んだ16点以外には点 P_n がこないことになる．

表 1　合同法乱数によって生成される k 次元空間内の点をすべて含む超平面の枚数の上界

M	$k=$ 3	4	5	6	7	8	9	10
2^{16}	73	35	23	19	19	15	14	13
2^{24}	465	141	72	47	36	30	26	23
2^{32}	2,953	566	220	120	80	60	48	41
2^{35}	5,907	952	333	170	108	78	61	51
2^{36}	7,442	1,133	383	191	119	85	66	54
2^{48}	119,086	9,065	2,021	766	391	240	167	126

整数の演算を有限桁の精度で行なう以上，生成される点列が結晶構造をなすのは当然であるが，その構造が疎であるところが問題であり，高次元空間になるほど，点列の密度が疎になる．そこで，この性質は**多次元疎結晶構造**と呼ばれている．k 次元の場合には，点列は高々 $(k!M)^{1/k}$ 枚の等間隔に並んだ平行な $(k-1)$ 次元超平面の上にのってしまうことが知られている．**表1**は，この枚数の上界を示したものである．実際の枚数は，この上界よりかなり少なくなることが多いことに注意する必要がある．

3. スペクトル検定

k 次元空間内の点列が平行な超平面上に並んでしまうことは避けられないにしても，これらの超平面の間隔が小さければ，実用上はさほど支障がないであろうと考えられる．簡単な例を示すと，**図1**の (2)～(4) の中では，(1) が比較的好ましいであろう．このような観点から，与えられた乗数 a の良さを判定するためのアルゴリズムが提案されており，スペクトル検定と呼ばれている．この検定法の詳細および検定結果の例については [2] を参照するとよい．

超平面の間隔の逆数 ν_k のことを Knuth は k 次元精度と呼んでいる．この精度をもつ合同法乱数列によって生成される k 次元点列は，その座標成分を上位 $\log_2 \nu_k$ ビットまでの分解能で見れば，ほぼ一様に分布しているものと見なすことができる．乱数列に要求される精度は

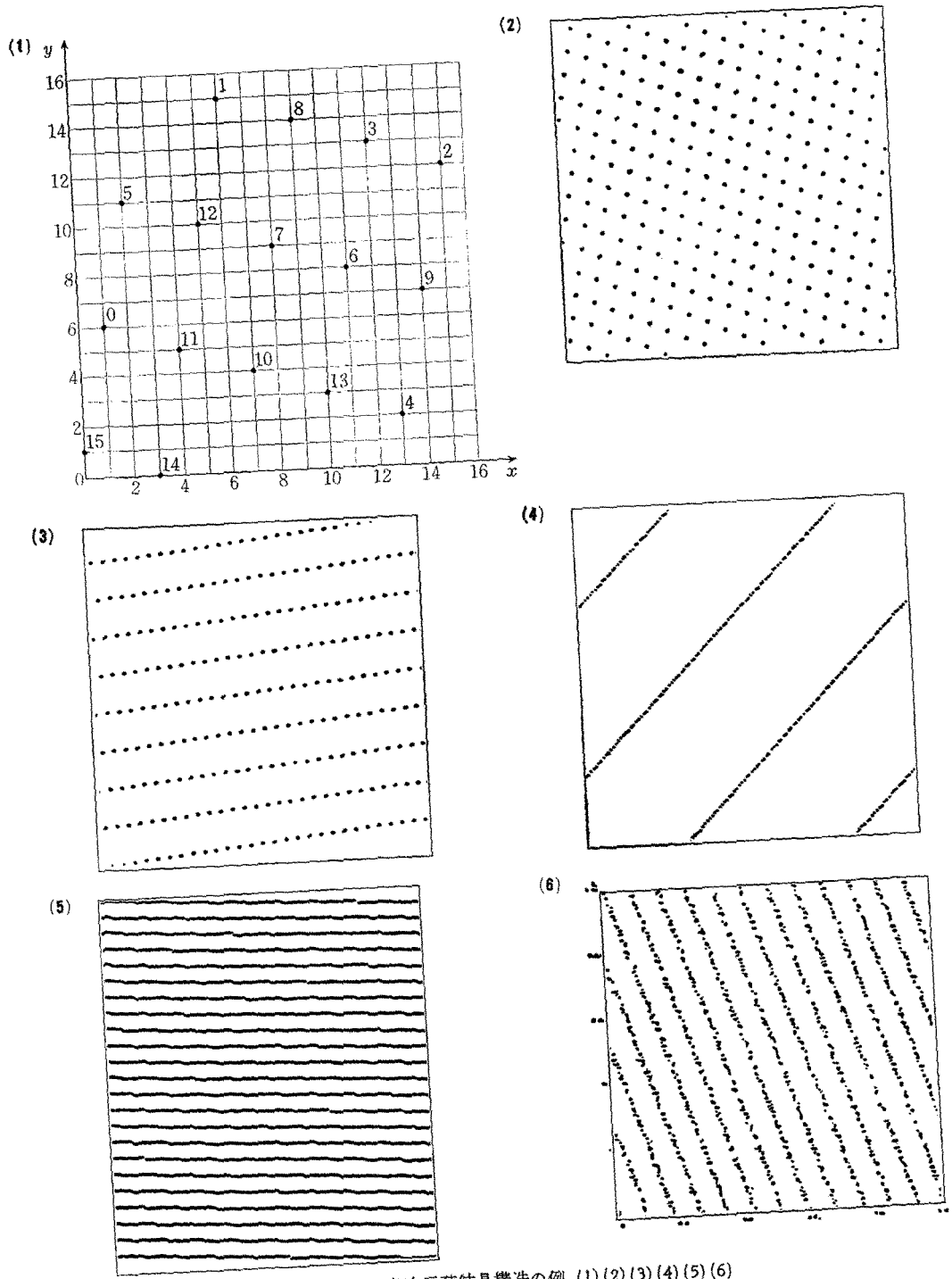

図 1　多次元疎結晶構造の例 (1) (2) (3) (4) (5) (6)

(1) $M=16$, $a=5$, $c=1$. (2) $M=256$, $a=45$, $c=1$. (3) $M=256$, $a=57$, $c=1$. (4) $M=256$, $a=129$, $c=51$. (5) あるパーソナル・コンピュータの BASIC の乱数の 2 次元結晶構造. (6) あるパーソナル・コンピュータの BASIC の乱数の 4 次元結晶構造を 2 次元平面に射影したもの.

もちろん個々の問題によって異なり，絶対的な基準というものはありえないが，Knuth はごく大まかな基準として $\log_2 \nu_k \geq 30/k$ $(2 \leq k \leq 6)$ を挙げている．この規準に合格するためには，M は 2^{30} 程度以上に選ぶ必要がある．パーソナル・コンピュータの BASIC の関数として提供されている RND の内部の整数演算は 16～24 ビット程度の桁数で行なっているものが多いようであり，桁数不足であるといえよう．図1の (5), (6) は，市販されている（または，いた）ものの中で，特に悪いものの例である，

4. その他の乱数発生法

合同法乱数の多次元疎結晶構造は，1周期中に同一の数が現われないという性質に由来するものであり，この性質は漸化式 (1) の次数が1であることから生ずるものである．そこで，高次の漸化式を用いる方法もいろいろ提案されているが，それらの理論的性質については，未だよくわかっていないことが多い．（M系列にもとづく方法については，ある程度の解明はされている．これについては，たとえば [1] を参照されたい．）

参 考 文 献

[1] 伏見正則：擬似乱数は信用出来るか．日本OR学会第16回シンポジウム「シミュレーション」予稿集，1986, pp. 38–49.

[2] Knuth, D. E.: *The Art of Computer Programming*, Vol.2: *Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading, Mass., 1981.（渋谷政昭(訳)：準数値算法/乱数，サイエンス社，1981.）

Lanchester の法則

岸　尚　防衛大学校

性能・装備が伯仲する赤軍の戦艦5隻と青軍の戦艦3隻とが洋上で相見えたとする．3隻は5隻に比べ数の上でいささか劣ってはいるが，結果はどうだろうか？

1921年のワシントン軍縮条約でわが国の主力艦はアメリカの6割と決まり，海軍の内外に危機感が拡がったが彼らの絶望は3隻の戦艦は5隻の前に鎧袖一触という認識のゆえであった．それは赤軍の5隻は1隻を失うのみで青軍のすべてを屠り去ることを予言する N 自乗法則にもとづいていた．

N 自乗法則なるものを提案したのは F.W. Lanchester である．Lanchester は英国人．自動車産業の揺籃期に育ち，数々のすぐれた自動車を設計・製作した．自動車技術者でありながら飛行機の研究に対する夢やみ難く，独力の研究は翼揚力理論にその名を残すことになる．彼はまた飛行機の軍事利用にも関心を示した．1916年1冊の本を著し，その1章を交戦の数学モデルにあてた．Lanchester の交戦モデルや，これと類似の Fiske モデルはいち早くわが国に伝えられ，京都大学教授野満隆治がこれに興味を抱いて海軍軍人を啓蒙したようである．軍縮論議の基礎をなす重要なセオリーとなった N 自乗法則は今日では Lanchester の2次法則と呼ばれている．

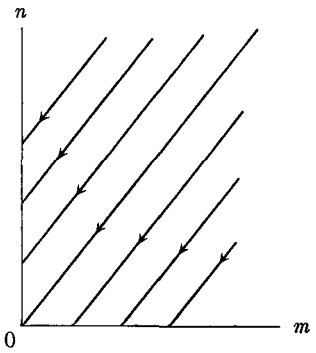

図1　1次法則

交戦の間にどのように損耗が発生するかを描写するモデルには精疎さまざまのものが案出されてきたが，古典的でありながら捨てがたい存在が Lanchester の2つのモデルである．

1. 1次法則

赤軍の兵力数を適当な単位で測って m，青軍のそれを n で表わす．両軍に発生する損耗が微分方程式

$$\begin{cases} dm/dt = -A \\ dn/dt = -B \end{cases}$$