综述：产生伪随机数的若干新方法*1)

杨自强　魏公毅

(中国科学院计算数学与科学工程计算研究所)
(北京应用物理与计算数学研究所计算物理实验室)

A REVIEW ON SOME NEW METHODS TO GENERATE RANDOM NUMBERS

Yang Ziqiang　Wei Gongyi
(*Institute of Computational Mathematics and Scientific/Engineering Computing, Chinese Academy of Sciences, Beijing*)
(*Laboratory of Computational Physics, Institute of Applied Physics & Computational Mathematics, Beijing*)

Abstract

In the present paper, we give a review of pseudo-random number generators. The new methods and theory appearing in 1990's will be focused. This paper concerns with almost all kinds of generators such as the linear, nonlinear and inversive congruential methods, Fibonacci and Tausworthe (or feedback shift register) sequences, add-with-carry and subtract-with-borrow methods, multiple prime generator and chaotic mapping, as well as the theory of combination of generators.

Key words: Monte, Carlo method, random number, Combined random number generator

产生随机数是 Monte-Carlo 方法的基础. 本文简要综述有关方法，重点是近年来国际上热门的一些新方法与评论，包括作者们的一些工作. 除了线性同余法外，还将涉及非线性同余法， Fibonacci, Tausworthe 序列，进位加 — 借位减发生器法，以及乘子和增量也在递推中变化的复合素数发生器和基于混沌映射产生随机数的方法. 除此之外，也介绍组合发生器，特别是介绍用于证明组合发生器优于单个发生器的一些理论结果，基于这些理论可实际地构造优良的随机数发生器. 在本文中，我们也注意收集和指出某些发生器在应用中可能存在的一些问题.

本文所讨论的随机数,只涉及传统 Monte-Carlo 方法中使用的伪随机数 (pseudo-random number). 至于近几年在数学金融的超高维积分 (维数高达千维) 计算中十分有效的拟 Monte-Carlo 方法所使用的拟随机数 (quasi-random number) 将在另文讨论.

* 2000 年 4 月 30 日收到.
1) 计算物理实验室基金试点项目资助.

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

§ 1. 线性同余序列的长周期相关与稀疏网格结构

1.1. 线性同余法与乘子的选取

线性同余法历史悠久，因其算法简单，至今仍被广泛使用. 其递推式为

$$X_{i+1} = aX_i + c \mod M, \quad i = 0, 1, \cdots, \tag{1.1}$$

式中参数 a, c 和 M 分别称为乘子、增量和模. 如果这些参数和种子 (初值) X_0 都指定，序列也就确定下来了. 通常取

$$r_i = X_i/M, \quad i = 0, 1, \cdots \tag{1.2}$$

作为区间 $(0,1)$ 上均匀分布 $U(0,1)$ 的随机数. 线性同余法中一个最重要的特例是 $c = 0$, 这时也称乘同余法. 给定 M 后，其余参数的选取应保证序列 $\{X_i\}$ 有最大的周期. 例如，若 M 为素数，则 a 应为 M 的原根. 判断原根的一个易于操作的准则 (见 Knuth, 1981) 是：对 $M-1$ 的任一素因子 q 都有 $a^{(M-1)/q} \neq 1 \mod M$

平方根准则与 Euclidean 商. 显然，参数的选取还应保证序列有较好的统计品质. 历史上，常用平方根准则指导乘子 a 的选取，这时 a 在 $\sqrt{M}$ 附近取值，例如

$$X_{i+1} = 16807X_i \mod (2^{31} - 1) \tag{1.3}$$

就是一个十分著名的随机数发生器. 这样做的主要考虑是便于计算机上实现, 另外是受 Greenberger (1961) 的一步顺序相关估计式的影响. 根据该式，若 $a \simeq \sqrt{M}$, 则 (X_i, X_{i+1}) 有较小的相关. 但是有些作者对平方根准则有异议，例如可见 Dieter (1971), Knuth (1981) 等人的论著. 此外 Fishman-Moore (1986) 根据理论和经验检验得到的 5 个最好乘子 (当 $M = 2^{31} - 1$ 时) 也与平方根准则不符. 特别是 Dieter (1971) 给出了 (X_i, X_{i+s}) 的可精确计算的分布. 他使用一个与一步顺序相关有紧密关系的偏差准则 (discrepancy, 其含义见 2.1 节) 使选 a 简化为选取与 b (若 M 是 2 的幂，则 $b = M/4$; 若 M 是素数，则 $b = M$) 具有最小 Euclidean 商的 a. 所谓 Euclidean 商是指辗转相除法所得的商 q_i 的和 $\sum_{i=0}^{n} |q_i|$. 各 q_i 的定义如下：

$$a = q_0 b - a_1, \quad b = q_1 a_1 - a_2, \quad a_1 = q_2 a_2 - a_3, \cdots, a_{n-1} = q_n a_n, \tag{1.4}$$

式中 $|b| > |a_1| > |a_2| > \cdots > |a_{n-1}| > |a_n| = 1$, 且各步的 a_i 取最小值.

易知当 $a \simeq \sqrt{M}$ 时有 $|q_1| \simeq \sqrt{M}$, 从而其 Euclidean 商不会是最小的一个.

1.2. 线性同余序列的长周期相关

为说明线性同余序列的长周期相关现象，先看一个简单例子：

$$X_{i+1} = 15X_i \mod 19, \qquad X_0 = 1. \tag{1.5}$$

此发生器产生周期为 18 的如下序列

$\{X_i\}$: 1, 15, 16, 12, 9, 2, 11, 13, 5, 18, 4, 3, 7, 10, 17, 8, 6, 14, 1.

为容易看出此序列的前半段与后半段强相关，今写出与它相关系数为 -1 的另一序列

$\{19 - X_i\}$: 18, 4, 3, 7, 10, 17, 8, 6, 14, 1, 15, 16, 12, 9, 2, 11, 13, 5, 18

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

显然，后者只是前者前后两半段位置的互易．换句话说，线性同余发生器 (1.5) 所得的序列其前后两半段是强相关的．

Matteis-Pagnutti (1988, 1990) 已从理论上证明了所有线性和非线性同余序列都存在长周期相关现象．在平行计算中，我们应特别警惕和回避这种现象．如果几个并行处理器分别使用同一个同余序列的不同段落，分割时应避开具有强相关的分点．

1.3. 线性同余序列的稀疏网格结构与谱检验

线性同余序列的最大缺陷是高维不均匀性．当把相继的 t 个随机数 $(X_{i+1}, X_{i+2}, \cdots, X_{i+t})$ 看作是 t 维空间上的一个点的座标时，这些点只散布在 t 维空间中的少数几个超平面上，并形成稀疏网格结构，二维情形可见 6.4 节的图 6.2．均匀随机数是产生其它分布随机变数的基础．用具有稀疏网格结构的线性同余序列产生其它分布随机变数时也可能会出现一些不应有的问题 (见 Bratley 等，1987)．例如两个独立的均匀随机数 (r_i, r_{i+1}) 可经 Box-Muller (1958) 变换得到一对独立的正态分布随机变数 (y_i, z_i)

$$\begin{cases} y_i = \cos(2\pi r_{i+1})\sqrt{-2\ln r_i}, \\ z_i = \sin(2\pi r_{i+1})\sqrt{-2\ln r_i}. \end{cases} \tag{1.6}$$

但如果 r_i 来自同余序列，则点 (y_i, z_i) 只落在一条螺线上，这时 y_i 与 z_i 就不是独立的了．

自从发现高维稀疏网格现象之后，人们在构造线性同余发生器时，自然要考虑参数的选择应使网格尽可能不那么稀疏．这导致了一系列度量和检验网格稀疏程度的准则出现．例如相邻平行超平面之间最大距离，平行超平面的最小数目，点间距，Discrepancy, 和 Lattice 检验等．这些检验都属于理论检验，只要给定参数 M, a, 便可进行检验而不必实际产生具体的序列．基于相邻平行超平面之间最大距离的检验亦称谱检验．该距离越大，发生器越差．设乘同余发生器为 $X_{i+1} = aX_i \bmod M$, 则谱检验计算归结为求解极值

$$\nu_t = \min\{\sqrt{X_1^2 + X_2^2 + \cdots + X_t^2} \ \Big| X_1 + aX_2 + \cdots + a^{t-1}X_t = 0 \bmod M\}, \tag{1.7}$$

式中 ν_t 称为该发生器的 t 维精度，而 $d_t(M, a) = 1/\nu_t$ 便是相邻平行超平面之间的最大距离．人们已经找到了上述极值问题的可行算法 (至少对 $t \le 10$ 是如此)，也找到了最大距离的下限 (对于给定的 M 值而言)．实践中人们还发现谱检验与该类的其它方法有很强的相关性 (Fishman-Moore, 1986)，因此谱检验成为这类方法中最为流行而且也是最为重要的一个 (Knuth, 1981)．

§ 2. 逆同余与非线性同余发生器

80 年代末开始，许多学者讨论称之为 逆同余 的一类新发生器．这是非线性同余类中最有前途的一种．Niederreiter (1992) 的书是这方面最好的入门．我们的介绍将从一般的非线性同余发生器入手．

2.1. 一般的非线性同余发生器

记 $Z_M = \{0, 1, \cdots, M-1\}$, 这是一个 M 阶有限域．同余发生器有如下形式：

$$X_{i+1} = f(X_i) \mod M, \quad i = 0, 1, \cdots, \tag{2.1}$$

$$r_i = X_i/M, \quad i = 0, 1, \cdots, \tag{2.2}$$

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

式中 $X_i \in Z_M$, 而 f 是 Z_M 上的一个整值函数. 若 $f(X_i) = aX_i + c$, 则 (2.1) 就是前节定义的线性同余发生器. 在非线性同余发生器中 f 通常是 Z_M 上的一个排列多项式, 这时有 $\{f(0), f(1), \cdots, f(M-1)\} = Z_M$. 多项式 f 的阶 d ($< M$) 在理论分析中至关重要.

定义 2.1. 令 Z_M^s 为 Z_M 上的 s 维向量空间, $X_0, X_1, \cdots$ 是模为素数 M 的一个同余序列. 对于给定的 $s \geq 1$, 若向量 $\mathbf{X}_n - \mathbf{X}_0$, $n = 1, 2, \cdots$ 张成 Z_M^s, 则称该序列通过 s 维网格检验. 此处

$$\mathbf{X}_n = (X_n, X_{n+1}, \cdot, X_{n+s-1}) \in Z_M^s \quad n = 0, 1, \cdots. \tag{2.3}$$

定理 2.1. 当且仅当 $s \leq d$, 模为 M 的非线性同余发生器通过 s 维网格检验.

上述定理由 Eichenauer-Grothe-Lehn (1988) 给出证明. 也可参考 Niederreiter (1992).

偏差(discrepancy) $D_N^{(s)}$ 可理解为 N 个 s 维点落入 $[0,1)^s$ 的所有形如 $\prod_{i=1}^{s}[u_i, v_i)$ 的子区间的实际频率与理论频率之差的上确界.

定理 2.2. 对于素数模 M 的非线性同余发生器, 其偏差

$$D_M^{(s)} \leq 1 - (1 - \frac{1}{M})^s + (d-1)M^{-1/2}\Big(\frac{4}{\pi^2}\log M + 1.72\Big)^s, \quad 2 \leq s \leq d. \tag{2.4}$$

2.2. 逆同余发生器

逆同余发生器是非线性同余类中目前研究得最多, 并且也是最有前途的一种.

(1) 几个逆同余发生器

对于 $c \in Z_M$ (M 为素数), 定义 $c\bar{c} = 1 \bmod M$ 且 $\bar{c} \in Z_M$ (若 $c = 0$, 定义 $\bar{c} = 0$). 这时称 $\bar{c}$ 为 c 关于模 M 的乘法逆. 下面是逆同余发生器的递推式 (常数 $a, b \in Z_M$):

$$X_{i+1} = (a\overline{X_i} + b) \mod M, \quad i = 0, 1, \cdots. \tag{2.5}$$

定理 2.3. 模为 M 的逆同余发生器对于所有的 $s \leq \frac{1}{2}(M+1)$ 都通过 s 维网格检验.

定理 2.4. 对于素数模 M 的逆同余发生器, 其偏差

$$D_M^{(s)} \leq 1 - \Big(1 - \frac{1}{M}\Big)^s + \Big(\frac{2s-2}{M^{1/2}} + \frac{s-1}{M}\Big)\Big(\frac{4}{\pi^2}\log M + 1.72\Big)^s, \quad s \geq 2. \tag{2.6}$$

Eichenauer-Grothe (1992) 给出一个新的逆同余发生器. 对于整数 a, b, w, x (x 为奇数),

$$f(2^k x) = 2^k a x^{-1} + b \mod 2^w. \tag{2.7}$$

这是模为 2 的幂的发生器. 他们还给出如下两个定理:

定理 2.5. 当且仅当 $a = 1 \bmod 4$ and $b = 1 \bmod 2$, 逆同余发生器 (2.7) 有最大的周期长度 2^w.

定理 2.6. 令 $M = 2^w$, 则有最大周期长度的任一逆同余发生器 (2.7) 的偏差满足

$$D_M^{(2)} < \frac{8}{7}(6 + 5\sqrt{2})M^{-1/2}\Big(\frac{1}{\pi^2}\log M + \frac{3}{5}\Big)^2 + 2M^{-1}. \tag{2.8}$$

对 t 附加某些条件后, 偏差的下界满足

$$D_M^{(2)} > \frac{t}{2(\pi+2)}M^{-1/2}. \tag{2.9}$$

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

此外 Eichenauer (1993) 还给出另一个新的逆同余发生器：对于整数 $a,b\in Z_M$ (模 M 为素数，且 $a\neq 0$)

$$X_i=\overline{ai+b},\quad i\geq 0 \tag{2.10}$$

Eichenauer 指出此发生器甚至比标准型 (2.5) 有更好的结构和统计独立性.

(2) 逆同余发生器的基本算法

对于逆同余发生器，最关键的问题是给出 $c\in Z_M$ 后如何有效地计算 $\bar{c}$. 算法之一是基于如下事实：对于所有的 $c\in Z_M$ (M 为素数), $\bar{c}=c^{M-2} \bmod M$, 而 c^{M-2} 又可以通过标准的平方乘法技术 (只有 $O(\log M)$ 个乘法) 算出. 例如要计算 c^{137}. 这时首先把 137 用二进制表示得 10001001; 然后分别算出 $d_k=c^{2^k}\bmod M$, $k=0,1,2,\cdots 7$; 最后得 $c^{137}=d_0*d_3*d_7$.

第二个算法是对 c 和 M 的 Euclidean 算法 (即辗转相除法). 其流程如下：

```
Set b(0)=M,  b(1)=c,  a(0)=0,  a(1)=1,  i=1.
While b(i)>0 do:
   Set b(i+1)=b(i-1) (mod b(i)).
   Set a(i+1)=a(i-1)-[b(i-1)/b(i)]*a(i).
   Set i=i+1.
Set c_inv=b(i-1)*a(i-1) (mod M).
```

上述算法 (见 Eichenauer, 1992) 仅需 $O(\log M)$ 步便会得到结果.

(3) 逆同余发生器的优缺点

逆同余发生器的主要优点在于能克服高维网格结构. 例如模为 $M=2^{31}-1$ 的逆同余发生器可以通过直至 2^{30} 维的网格检验. 而线性同余发生器要保证 10 维以内近似最优的网格结构都有困难 (请参考 Fishman-Moore, 1986).

然而逆同余发生器的周期不比线性同余发生器的长， Matteis-Pagnutti (1990) 也从理论上证明了所有逆同余序列也都象线性同余序列那样存在长周期相关现象. 另外，从应用上看，逆同余发生器的速度明显慢于线性同余. 对于后者， James (1990) 曾指出，考虑效率在早年是十分重要的，但从目前要计算的类型来看，产生随机数所占的时间和内存相对地越来越不重要了，并且几乎可以被忽略. 因此这不应该成为应用中的大问题.

§ 3. 对于经典 FIBONACCI 与 TAUSWORTHE 序列的非议

3.1. 经典 Fibonacci 与延迟 Fibonacci 序列

历史上曾使用 Fibonacci 序列产生随机数，其递推式为

$$X_{i+1}=(X_i+X_{i-1}) \bmod M,\quad i=1,2,\cdots. \tag{3.1}$$

例如 $M=100$, $X_0=1$, $X_1=1$, 则有序列

$$1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 44,\ 33,\ 77,\ 10,\ 87,\ \cdots,$$

此发生器没有乘法运算，产生速度快，但存在着致命的缺点.

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

投掷骰子游戏的模拟例子. 如果用 Fibonacci 序列产生随机数, 并以相邻的三个数的大小顺序决定骰子点数. 譬如

$$X_{i-1} < X_i < X_{i+1} \text{ 对应 1 点}, \quad X_{i-1} < X_{i+1} < X_i \text{ 对应 2 点},$$
$$X_i < X_{i-1} < X_{i+1} \text{ 对应 3 点}, \quad X_i < X_{i+1} < X_{i-1} \text{ 对应 4 点},$$
$$X_{i+1} < X_{i-1} < X_i \text{ 对应 5 点}, \quad X_{i+1} < X_i < X_{i-1} \text{ 对应 6 点}.$$

那么人们会惊讶地发现, 无论模拟多少次, 都不会出现 2 或 4 点. 原因是 Fibonacci 序列存在着令人不能容忍的不居中现象, 即由前两个数得到的第三个数要不是同时大于就是同时小于前二者而永不居中 (见 Dieter, 1982). 此序列的另一个缺点是显著的序列相关, 即取小值的数后面出现也取小值的趋势. 所有这些都是一个真正的随机数序列不应有的特性. Knuth (1981) 戏称现今对 Fibonacci 发生器的兴趣只是它能产生很出色的 "坏例子".

对经典 Fibonacci 序列的简单改进是延迟 Fibonacci 序列, 这时使用序列中更前面的数去产生新数. 例如

$$X_{i+1} = (X_i + X_{i-p}) \mod M, \quad i = p, p+1, \cdots, \tag{3.2}$$

$$X_i = (X_{i-q} + X_{i-p}) \mod M, \quad i = p, p+1, \cdots. \tag{3.3}$$

对于延迟 Fibonacci 序列, 本文的第 4.2 节还将涉及.

3.2. Tausworthe 序列

Tausworthe 序列发生器亦称移位寄存器序列发生器. 这本是随机产生 0,1 二进制位的方法. 它基于本原多项式与模 2 运算 (亦称异运算, 记作 XOR 或 $\oplus$). 例如本原三项式为 $x^p + x^q + 1$, 则有对应的移位寄存器序列发生器为

$$X_i = (X_{i-p} + X_{i-(p-q)}) \mod 2, \quad i = p, p+1, \cdots \tag{3.4}$$

或

$$X_i = X_{i-p} \oplus X_{i-(p-q)}, \quad i = p, p+1, \cdots. \tag{3.5}$$

Tausworthe (1965) 指出, 若把上述的相继 k 个随机二进制位看作是 k 位二进制小数

$$0.X_{i+1}X_{i+2}\cdots X_{i+k},$$

则此数可看作是区间 (0,1) 上的均匀随机数. 人们称此序列为 Tausworthe 序列.

但有不少人对此持异议. Knuth (1981) 指出, "某些人因为相信二进制位发生器技术可被用于产生整字长小数的随机数而落入陷井. $\cdots$ 因为实际上这是十分差劲的随机数虽然这些二进制位都是十分随机的." 其后 Marsaglia (1985) 也指出: "使用位方式的 XOR 运算的移位寄存器序列只得到十分坏的随机数发生器." 还有 Press 等人 (1986, p.213) 和 Bratly 等人 (1987, p.202) 也在他们的著作中直接或间接地重复 Knuth (1981) 的上述警告. 另一方面, Tezuka-L'Ecuyer (1991) 还用图形显示指出, 在线性同余序列中出现的高维稀疏网格结构也在 Tausworthe 序列中出现. 从他们的图形可以看出, 二维网格线虽不象线性同余那样平行规整, 但规则的波纹状明显可见.

可是有不少人忽视 (或未知) 上述警告, 贪图 Tausworthe 序列容易获得巨大的周期长度和理想的速度, 而在他们的工作中仍然大量地使用 Tausworthe 序列. 直至 Ferrenberg 等人

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

(1992) 报告了他们在统计物理学的著名 Ising 模型的 Monte Carlo 模拟中，因 Tausworthe 序列内的微妙相关而得到完全错误的结果，这才引起更多人的注意和讨论. 稍后 Grassberger (1993) 也发现了在统计物理学的另一著名模型 (三维自回避行走 SAW) 的 Monte Carlo 模拟也因 Tausworthe 序列而出现类似的问题. 他非议说："这个发现支持了 Press 等人 (1986) 的看法，也就是使用 XOR 运算的移位寄存器发生器是最坏的随机数发生器之一，今后永远不要再用".

§ 4. 进位加和借位减发生器

Marsaglia-Zaman (1991) 提出了一类新随机数发生器，包括进位加 (add-with-carry, 简记为 AWC) 和借位减 (Subtract-with-borrow, 简记为 SWB). 它们的产生速度甚至比常用的线性同余法还快，但却有令人吃惊的长周期. 其后 Tezuka-L'Ecuyer-Couture (1993) 发表文章，对这类方法 (通称为 AWC/SWB) 的本质，与线性同余的关系，以及有关的统计特性作了更明晰的揭示. 下面的介绍主要来自这两篇文章.

4.1. 基本概念

设 b, p, q 为正整数，此处 b 称为基，$p > q$ 称为延迟. 进位加发生器的递推式是

$$X_i = (X_{i-q} + X_{i-p} + c_{i-1}) \mod b, \quad i = p, p+1, \cdots, \tag{4.1}$$

$$c_i = \begin{cases} 1, & \text{若 } X_{i-q} + X_{i-p} + c_{i-1} \geq b, \\ 0, & \text{若 } X_{i-q} + X_{i-p} + c_{i-1} < b, \end{cases} \tag{4.2}$$

式中 c_i 称为进位. 递推初值 (集合) 由 $(X_0, X_1, \cdots, X_{p-1})$ 和 c_{p-1} 构成. 值得注意的是这里没有乘法运算，加之 mod b 运算不超过一个减法运算，所以有很高的效率. 它的最大 (全) 周期 $b^p + b^q - 2$ 可以是个巨大的值，达到此全周期的条件是 $M = b^p + b^q - 1$ 为素数，且 b 是 M 的一个本原根 (定义见 1.1 节). 例如取 $b \simeq 2^{31}$, $p \simeq 20$, 如果它们符合条件，这时 (全) 周期近似 2^{620}. 此值之大已超过现今实际应用的需要.

为产生 $U(0,1)$ 随机数序列 $\{r_i\}$, 可取 $k \leq p$ 个相继的 X_i 产生一个 r_i (James, 1990)

$$r_i = \sum_{j=1}^{k} X_{ki-j+1} b^{-j}. \tag{4.3}$$

若 k 与 $M-1$ 互素，则 $\{r_i\}$ 与 $\{X_i\}$ 有相同的周期. 对于我们的精度要求而言，如果 b 已足够大，则可取 $k = 1$, 这时 (4.3) 简化为 $r_i = X_i/b$; 否则令 $k > 1$. 此处的 $\{r_i\}$ 是类比着 3.2 节的 Tausworthe 序列构造的. 但 Tausworthe 序列中 r_i 由模 2 (即 $b = 2$) 的移位寄存器序列产生. 而这里却是有进位运算，并且 b 可以不是 2.

进位加发生器有一个变形，称之为补进位加发生器 (complementary AWC) 其递推式是

$$X_i = (-X_{i-q} - X_{i-p} - c_{i-1} - 1) \mod b, \quad i = p, p+1, \cdots, \tag{4.4}$$

式中 c_i 的定义同前，而使 X_i 取正值的 mod b 实际上是 $+b$ 或 $+2b$.

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

借位减发生器也有两种形式，其一是

$$X_i = (X_{i-q} - X_{i-p} - c_{i-1}) \mod b, \quad i = p, p+1, \cdots \tag{4.5}$$

$$c_i = \begin{cases} 1, & \text{若 } X_{i-q} - X_{i-p} - c_{i-1} < 0, \\ 0, & \text{若 } X_{i-q} - X_{i-p} - c_{i-1} \geq 0. \end{cases} \tag{4.6}$$

其二是

$$X_i = (X_{i-p} - X_{i-q} - c_{i-1}) \mod b, \quad i = p, p+1, \cdots, \tag{4.7}$$

$$c_i = \begin{cases} 1, & \text{若 } X_{i-p} - X_{i-q} - c_{i-1} < 0, \\ 0, & \text{若 } X_{i-p} - X_{i-q} - c_{i-1} \geq 0, \end{cases} \tag{4.8}$$

式中 c_i 称为借位.

上面提到的四种 AWC/SWB 发生器，每一种的最大 (满) 周期都是 $M-1$, 而达到此周期的条件是 M 为素数，且 b 是 M 的一个本原根. 但每个发生器的 M 值是不同的，详见表 4.1. Marsaglia-Zaman (1991) 对借位减发生器 SWB-I 推荐了参数 (b, p, q) 的几组具体值，并列出了相应的周期. 表 4.2 是其中的一部分.

表 4.1. 进位加和借位减发生器的 M 值

发生器	M 值 (最大周期是 $M-1$)
进位加 (AWC)	$b^p + b^q - 1$
补进位加 (AWC-c)	$b^p + b^q + 1$
借位减 -I (SWB-I)	$b^p - b^q + 1$
借位减 -II (SWB-II)	$b^p - b^q - 1$

表 4.2. 借位减发生器 $X_i = (X_{i-q} - X_{i-p} - c_{i-1}) \mod b$ 参数的几组推荐值

基 (b)	延迟 (p)	延迟 (q)	周期	种子数目与类型
2	847	240	$2^{846} - 2^{239} \simeq 10^{255}$	847 bits
2	1751	472	$2^{1750} - 2^{471} \simeq 10^{527}$	1751 bits
$2^{32} - 5$	43	22	$b^{43} - b^{22} \simeq 10^{414}$	43 个 32-bit 整数
2^{31}	48	8	$\frac{1}{105}(2^{1487} - 2^{247}) \simeq 10^{445}$	48 个 31-bit 整数
2^{24}	39	25	$\frac{1}{21}(2^{931} - 2^{595}) \simeq 10^{279}$	39 个实数

4.2. 进一步讨论

在全部 AWC/SWB 发生器中，可以证明 $\{X_i\}$ 在直至 p 维内的均匀性. AWC/SWB 方法可以看作是 Knuth (1981) 中讨论过的加法和减法发生器的微小改进 (另外加法和减法发生器又属于更为一般的延迟 Fibonacci 发生器，见 3.1 节), 但是除了 AWC/SWB 之外，其它方法没有进位和借位 (即 $c_i = 0$, $\forall i$). 然而就周期而言两者却有天渊之别. 若令 $b = 2^e$, 后者的周期长为 $(2^p - 1)2^{e-1} \simeq 2^{e+p-1}$, 它远比 AWC/SWB 的 $b^p + b^q - 2 \simeq 2^{ep}$ 小得多，除非 $e = 1, 2$ 等小值.

Tezuka-L'Ecuyer-Couture (1993) 的文章分析了由 AWC/SWB 产生的序列 $\{r_i\}$ 结构，证明了如下定理:

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

定理 4.1. 若 b 为 AWC/SWB 的基，M 的定义如表 4.1, r_i 与 k 如 (4.3) 所示，此外

$$Y_i = b^{k(M-2)}Y_{i-1} \mod M, \qquad w_i = Y_i/M, \tag{4.9}$$

且 AWC/SWB 的初值 $X_{i-p+1}, \cdots, X_i, c_i$ 与 Y_i 状态对应，则

$$r_i = b^{-k}[b^k w_i]. \tag{4.10}$$

关于 "状态对应" 的含义，请参考 Tezuka-L'Ecuyer-Couture (1993) 的文章. 上述定理表明，AWC/SWB 产生的序列 $\{r_i\}$ 本质上等价于线性同余序列 (4.9), 而 (4.10) 进一步说明了等价是指线性同余序列中的前 b^k 位与 AWC/SWB 序列 $\{r_i\}$ 相同，或者说它们近似相等 (精度是 b^{-k}).

由表 4.1–4.2 可知，在 AWC/SWB 中，M 可以取非常巨大的值 (譬如 2^{1000}), 把它用作为等价的线性同余发生器的模 M 时，后者在程序上实际上是无法实现的. 现在根据上述定理，可把 AWC/SWB 方法理解为线性同余发生器中当模 M 有巨值时的一种极其巧妙的算法，但这样却带来了不超过 b^{-k} 的 "截断误差".

因为所有线性同余序列都有高维稀疏网格结构，所以与之近似等价的 AWC/SWB 序列也有近似的高维稀疏网格结构. 在 t 维空间中，其相邻平行超平面间的距离大于 $b^{-k}\sqrt{t}$ (见 1.3 节). 根据 Tezuka-L'Ecuyer-Couture (1993) 的模拟结论：AWC/SWB 发生器当 $k = 1$ 时，其 p 维以上的网格结构很坏. 所以它们不应单独使用，而应与有良好理论特性的其它类型发生器适当组合后使用. 关于组合发生器的理论，本文将在第 6 节介绍.

§ 5. 关于复合素数和混沌映射产生随机数

5.1. 乘子和增量在递推中变化的复合素数随机数发生器 MPRNG

Hass (1987) 给出一个复合素数随机数发生器 (简记为 MPRNG), 其最大特点是在递推中乘子和增量不断变化. Hass 用一个 Fortran 程序来刻划他的 MPRNG:

```
cccc         initialize seed variable
      ia = 971
      ic1 = 11113
      ic2 = 104322
      irn = 4181
cccc         generate 5000 numbers
      do 10 i=1,5000
        ia = ia + 7
        ic1 = ic1 + 1907
        ic2 = ic2 + 73939
        if (ia .ge. 9973) ia = ia - 9871
        if (ic1 .ge. 99991) ic1 = ic1 - 89989
        if (ic2 .ge. 224729) ic2 = ic2 - 96233
        irn = (mod((irn*ia+ic1+ic2), 100000))/10
  10  continue
```

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

这是一个可在 32-bit 的计算机上运行的程序. 其中 ia 为乘子, $ic1$, $ic2$ 是两个增量, irn 是不大于 10000 的随机数, 周期为 $9871 \times 89989 \times 96233$ (约合 85.5×10^{12}). 如果嫌 irn 太短, 可把相邻两个连接起来. Hass 的文章虽不算短, 但主要是介绍对 MPRNG 进行的各种 (经验) 检验. 没有涉及多少理论方面的探讨. 可能是因为 MPRNG 在递推中乘子和增量不断变化, 很难作理论分析. 但正是乘子和增量在递推中不断变化这一点确实与众不同, 这才令人感到兴趣.

5.2. 关于混沌映射产生随机数的一个注

An (1996) 曾经研究了混沌映射 (chaotic mapping) 产生随机数的方法, 该文使用如下的递推式:

$$y_{i+1} = \begin{cases} (3/2)y_i + 1/4, & \text{若 } 0 \le y_i < 1/2, \\ (1/2)y_i - 1/4, & \text{若 } 1/2 \le y_i < 1. \end{cases} \tag{5.1}$$

并指出此递推式可产生周期为无穷的序列, 其经验分布的极限分布为

$$F(y) = (Ln(y + 1/2) + Ln2)/Ln3. \tag{5.2}$$

根据产生随机数中的熟知理论, 若随机变量 η 的分布函数为 $F(y)$, 则 $\xi = F(\eta)$ 有 $U(0,1)$ 分布. 于是由

$$x_i = (Ln(y_i + 1/2) + Ln2)/Ln3 \tag{5.3}$$

得到的序列 $\{x_i\}$ 可看作是有 $U(0,1)$ 分布的随机数列. 因序列 $\{y_i\}$ 是无限不循环的, 所以上述方法可以产生周期为无限的 $U(0,1)$ 分布的随机数列.

此处我们指出: 上述 An (1996) 的混沌映射方法等价于如下的线性同余发生器

$$x_{i+1} = ax_i + c \bmod 1, \quad i = 0, 1, \cdots, \tag{5.4}$$

式中 $a = 1$, 且

$$c = Ln(3/2)/Ln3 = 1 - Ln2/Ln3 = 0.369070246\cdots. \tag{5.5}$$

其证明不难给出. 首先设 $y_i < 1/2$, 这时 $y_{i+1} = (3/2)y_i + 1/4$, 由 (5.3) 有

$$x_{i+1} - x_i = Ln\Big(\frac{(3/2)y_i + 3/4}{y_i + 1/2}\Big)/Ln3 = Ln(3/2)/Ln3 = c.$$

其次设 $y_i \ge 1/2$, 这时 $y_{i+1} = (1/2)y_i - 1/4$,

$$x_{i+1} - x_i = Ln\Big(\frac{(1/2)y_i + 1/4}{y_i + 1/2}\Big)/Ln3 = Ln(1/2)/Ln3 = Ln(3/2)/Ln3 - 1 = c - 1.$$

理论上, c 的位数是无穷不循环的, 所以序列 $\{x_i\}$ 的周期理论上也是无限的. 但是在实际应用中, c 只能取有限位, 从而所得的序列不可能无穷长而不循环. 总之, An (1996) 的随机数发生器在实际应用中就是一个线性同余发生器, 而且其乘子 $a = 1$. 显然, 这种发生器的统计品质不可能优于两个参数 (a, c) 都经过精心设计的某些线性同余发生器.

§ 6. 组合发生器及有关的理论结果

6.1. 组合发生器

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

几个线性同余发生器的组合也可以得到一个新的发生器. 例如有 m 个乘同余发生器

$$X_{i+1}^{(j)} = a^{(j)} X_i^{(j)} \mod M^{(j)}, \quad i = 0, 1, \cdots, \quad j = 1, 2, \cdots, m, \tag{6.1}$$

式中诸模 $M^{(j)}$ 为互异素数, 且不失一般性, 设 $M^{(1)}$ 为诸 $M^{(j)}$ 中的最大者, 按惯例, 乘子 $a^{(j)}$ 为模 $M^{(j)}$ 的原根. 令 $c^{(1)}, c^{(2)}, \cdots, c^{(m)}$ 为 m 个任意非零整数, 并定义

$$U_i = \sum_{j=1}^{m} \frac{c^{(j)} X_i^{(j)}}{M^{(j)}}, \qquad i = 0, 1, \cdots, \tag{6.2}$$

$$V_i = \Big(\sum_{j=1}^{m} c^{(j)} X_i^{(j)} \Big) \mod M^{(1)}, \qquad i = 0, 1, \cdots, \tag{6.3}$$

则

$$u_i = U_i \bmod 1, \quad \text{和} \quad v_i = \frac{V_i}{M^{(1)}}, \quad i = 0, 1, \cdots \tag{6.4}$$

都可看作是 $U(0,1)$ 随机数. 当然, 组合的对象不限于线性同余类, 前面提到的几个不同类型发生器都可以出现在同一个组合中, 但至今只有线性同余类的组合获得较深刻的理论成果.

从历史上看, 70 年代已有人提出组合发生器, 例如见 Nance-Overstreet (1978) 和 Brown-Solomon (1979). 最著名的组合发生器可能归功于 Wichmann-Hill (1982), 他们用 m=3 得到好的结果. 进入 90 年代, Deng-George (1990) 对组合发生器给出了严格的理论分析, 杨自强, 张正军 (1993) 又把 Deng-George 的结果稍加拓广. 这些工作主要是针对形式 (6.2) 的组合开展的. L'Ecuyer (1988) 提出了形式 (6.3) 的组合并研究了该发生器在高维空间的均匀性. 同时针对这两类组合的最重要的理论工作归功于 L'Ecuyer-Tezuka (1991).

6.2. 关于组合发生器的若干重要理论成果

下面两个定理最早来自 Deng-George (1990), 这里的叙述来自杨自强, 张正军 (1993) 的稍有拓广的形式:

定理 6.1. 设 $X^{(1)}, X^{(2)}, \cdots, X^{(m)}$ 是区间 $(0,1)$ 上的独立随机变量, $c_1, c_2, \cdots, c_m$ 是常数, 又设 $X = \Big(\sum_{j=1}^{m} c_j X^{(j)} \Big) \mod 1$, 若 $X^{(1)} \sim U(0,1)$ 且 c_1 是整数, 则 $X \sim U(0,1)$.

注: $X^{(2)}, X^{(3)}, \cdots, X^{(m)}$ 可以不是 $U(0,1)$, 且 $c_2, c_3, \cdots, c_m$ 也可以不是整数.

定理 6.2. 设 $X^{(1)}, X^{(2)}, \cdots, X^{(m)}$ 是区间 $(0,1)$ 上的独立随机变量, 其密度函数分别为 $f_1(x_1), f_2(x_2), \cdots, f_m(x_m)$, 又设 $c_1, c_2, \cdots, c_m$ 是整数, $X = \Big(\sum_{j=1}^{m} c_j X^{(j)} \Big) \mod 1$, X 的密度函数记为 $f(x)$, 若 $|f_j(x_j) - 1| \le \epsilon_j$, $j = 1, 2, \cdots, m$, 则 $|f(x) - 1| \le \prod_{j=1}^{m} \epsilon_j$. 进而有

$$X \xrightarrow{p} U(0,1), \quad \text{若} \quad \prod_{j=1}^{m} \epsilon_j \longrightarrow 0. \tag{6.5}$$

上述定理 6.2 意味着几个独立且近似均匀的随机变量的线性组合也是一个近似均匀的随机变量, 但其分布比组成它的任一个变量更接近 $U(0,1)$.

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

L'Ecuyer-Tezuka (1991) 证明了组合 (6.2) 和 (6.3) 分别等价和近似等价一个关联 LCG. 记

$$M = \prod_{j=1}^{m} M^{(j)}, \tag{6.6}$$

$$n^{(j)} = \Big(\frac{M}{M^{(j)}}\Big)^{M^{(j)}-2} \mod M^{(j)}, \quad j = 1, 2, \cdots, m, \tag{6.7}$$

$$a = \Big(\sum_{j=1}^{m} \frac{a^{(j)} n^{(j)} M}{M^{(j)}}\Big) \mod M, \tag{6.8}$$

并定义如下的一个关联 LCG

$$Z_{i+1} = aZ_i \mod M, \quad i = 0, 1, \cdots. \tag{6.9}$$

定理 6.3. 若 $Z_0/M = u_0$, 则 $Z_i/M = u_i$ 对所有 $i \geq 0$ 成立.

定理 6.4. 若 $Z_0/M = u_0$, 则

$$v_i = (U_i + \varepsilon_i) \mod 1, \tag{6.10}$$

此处 ε_i 是一个依赖于 $M^{(j)}$ 与 $c^{(j)}$ 的偏差 (详见 L'Ecuyer-Tezuka, 1991).

基于这两个定理, 研究线性同余组合发生器的统计性质可简化 (或近似简化) 为形如 (6.9) 的一个关联 LCG.

6.3. 组合发生器的周期

假设被组合的诸序列 $\{X_i^{(j)}\}$ 的周期为 $\mathrm{Period}(X_i^{(j)})$, $j = 1, 2, \cdots, m$, 它们两两互素, 且 $\mathrm{Period}(X_i^{(j)})$ 与 $c^{(j)}$ 互素, 这时组合发生器的周期是组合它的 m 个序列周期的最小公倍数 (lcm), 即

$$\mathrm{Period}(r_i) = \mathrm{lcm}\Big(\mathrm{Period}(X_i^{(1)}), \mathrm{Period}(X_i^{(2)}), \cdots, \mathrm{Period}(X_i^{(m)})\Big). \tag{6.11}$$

如果被组合的是乘同余发生器, 且每个 $M^{(j)}$ 都是 2 的幂, 则 $\mathrm{Period}(X_i^{(j)})$ 也是 2 的幂, 当诸 $\mathrm{Period}(X_i^{(j)})$ 中仅有一个最大者, 则

$$\mathrm{Period}(r_i) = \max_j\{\mathrm{Period}(X_i^{(j)})\}.$$

为了得到更长的周期, 通常令所有模 $M^{(j)}$ 为互异的素数. 这时组合发生器的最大周期是

$$\begin{aligned} \mathrm{Period}(r_i) &= \mathrm{lcm}\Big((M^{(1)}-1), (M^{(2)}-1), \cdots, (M^{(m)}-1)\Big) \\ &= (M^{(1)}-1)(M^{(2)}-1)\cdots(M^{(m)}-1)/cf \\ &\leq (M^{(1)}-1)(M^{(2)}-1)\cdots(M^{(m)}-1)/2^{m-1}. \end{aligned} \tag{6.12}$$

事实上, 上式的 $cf = \prod_j f_j^{k_j - 1}$, 其中 f_j 是出现在 $k_j > 1$ 个 $(M^{(j)} - 1)$ 值内的公因子. 当 $M^{(j)}$ 是个大素数时, $(M^{(j)} - 1)$ 是个偶数, 于是 $cf \geq 2^{m-1}$. 容易明白, 如果 $(M^{(j)} - 1) = 2p_j$, $j = 1, 2, \cdots, m$, 且 p_j 全是素数, 则组合发生器达到其最大周期.

6.4. 线性同余组合发生器的统计性质和网格结构

根据 6.2 节的定理, 组合发生器优于组成它的任一个发生器, 但是线性同余组合发生器本质上等价 (或近似等价) 于另一个线性同余发生器 (即单个的关联 LCG). 因此对于线性同

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

余组合发生器的统计性质的研究可简化 (或近似简化) 为对单个的关联 LCG 的研究. 从这个意义上说, 线性同余组合发生器也具有 (或近似具有) 高维网格结构的特征. 不过根据关联 LCG 的定义 (6.6)-(6.9), 它可以具有极为巨大的模 $M = \prod_{j=1}^{m} M^{(j)}$, 又根据谱检验理论 (见 1.3 节), 只要适当选取关联 LCG 的乘子 a (它由被组合的模 $M^{(j)}$ 和乘子 $a^{(j)}$ 决定, 见 (6.8)) 其网格将会足够地稠密. 并满足实际应用的需要. 另一方面, 还可以借助定理 6.4 选取较大的偏差 ε_i 以扰乱规则的网格.

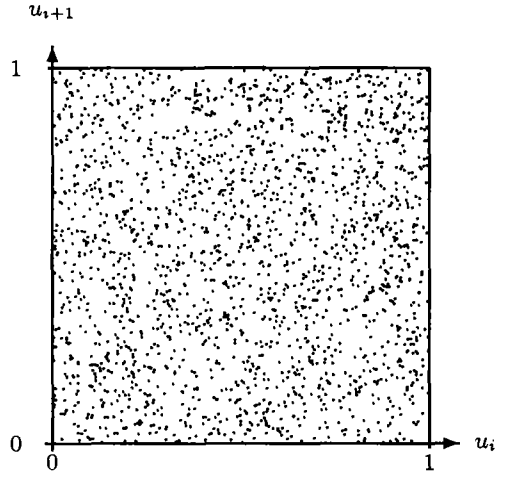

图 6.1a 组合发生器之一

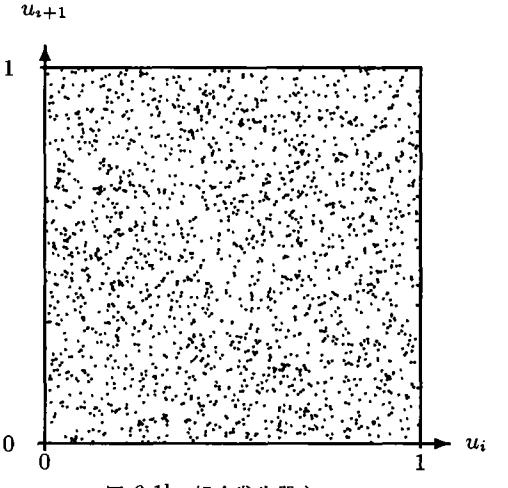

图 6.1b 组合发生器之二

下面, 让我们看一些例子. 图 6.1a 和图 6.1b 显示了两个组合发生器的二维相继点 (u_i, u_{i+1}), 这些组合发生器是本文作者们精心设计的, 每个都由四个乘同余组合而成, 组合后的周期超过 2^{100}. 但是为了便于观察, 每个图只包括 2000 个点. 从这两个图来看, 似乎看不到网格结构. L'Ecuyer (1988) 也给出过类似的图, 并有同样的结论.

为了容易看到理论分析指出的线性同余组合发生器的网格结构, 今使用两个特别小的素数来构造具有形式 (6.2) 和 (6.3) 的组合发生器:

$$X_{i+1} = 15X_i \bmod 19, \qquad X_0 = 1, \qquad x_i = X_i/19,$$

$$Y_{i+1} = 14Y_i \bmod 17, \qquad Y_0 = 1, \qquad y_i = Y_i/17,$$

$$u_i = (X_i/19 + Y_i/17) \bmod 1, \quad \text{和} \quad u_i = (X_i/19 + 3Y_i/17) \bmod 1,$$

$$V_i = (X_i + Y_i) \bmod 19, \quad v_i = V_i/19, \quad \text{和} \quad V_i = (X_i + 3Y_i) \bmod 19, \quad v_i = V_i/19.$$

图 6.2 的六个小图分别显示了它们的二维相继点 (x_i, x_{i+1}) 的网格结构, 其中前两个小图对应于组合前的单个 LCG, 网格非常稀疏. 图 6.2c 和 6.2d 对应于形式 (6.2) 的组合, 从图中可以看出, 组合后的网格结构不象单个发生器那样整齐但仍清晰可见, 不过组合后的网格确实不那么稀疏了. 值得注意的是, 因关联 LCG 的模不是素数, 其周期远小于 M, 故每个图都缺失许多点, 但当把两图叠加时, 没有缺失点, 网格更为规则.

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

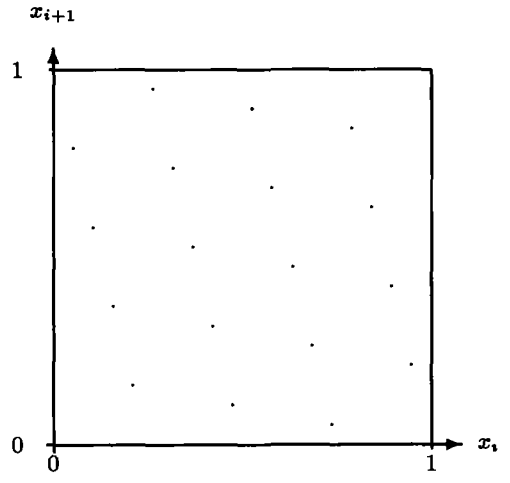

图 6.2a $X_{i+1} = 15X_i \bmod 19$

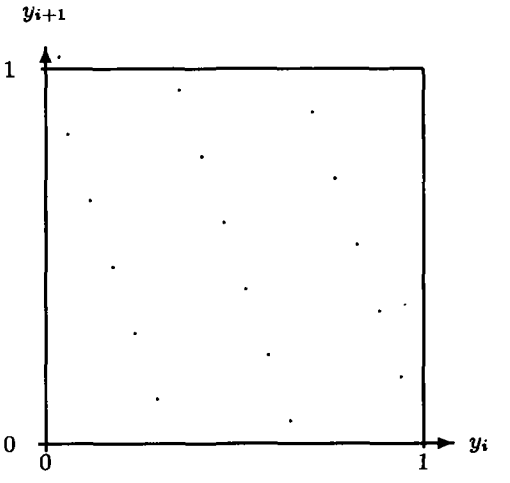

图 6.2b $Y_{i+1} = 14Y_i \bmod 17$

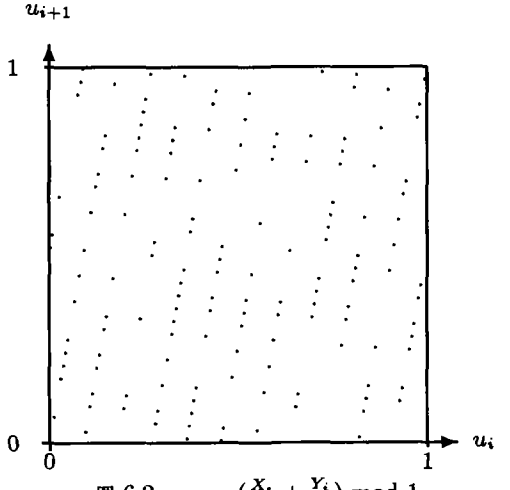

图 6.2c $u_i = (\frac{X_i}{19} + \frac{Y_i}{17}) \bmod 1$

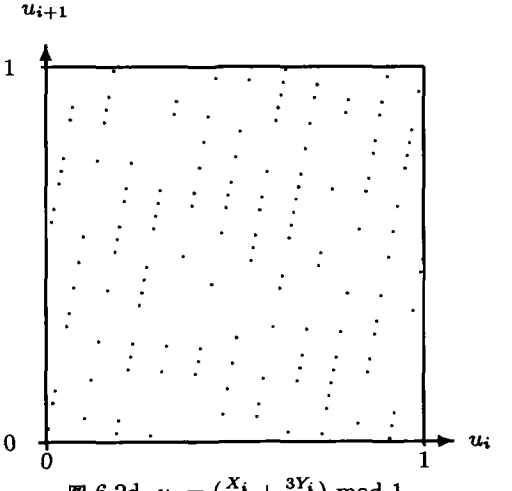

图 6.2d $u_i = (\frac{X_i}{19} + \frac{3Y_i}{17}) \bmod 1$

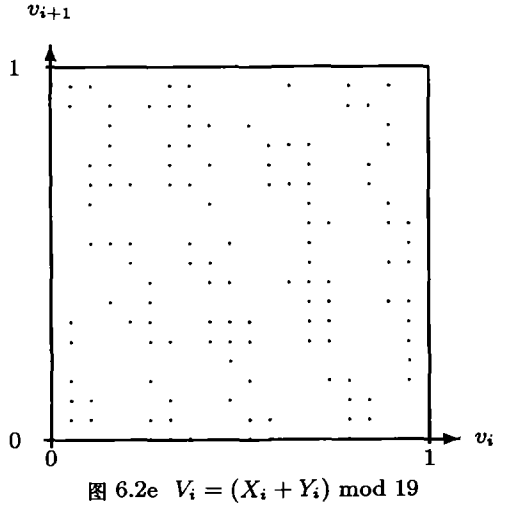

图 6.2e $V_i = (X_i + Y_i) \bmod 19$

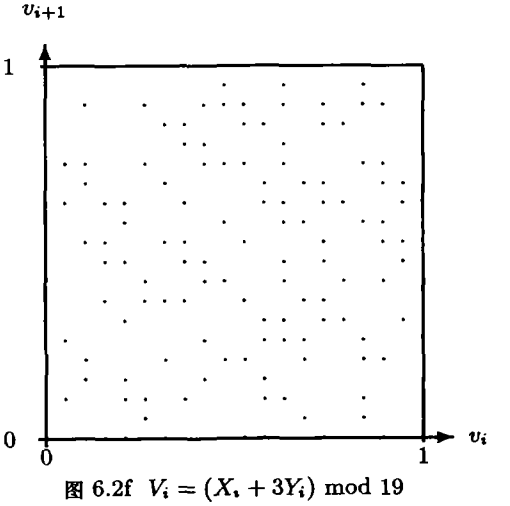

图 6.2f $V_i = (X_i + 3Y_i) \bmod 19$

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

图 6.2e 和 6.2f 对应于形式 (6.3) 的组合，其网格结构同样不那么稀疏，与前面的组合相比，其网格现象更不容易被察觉，特别是最后一个图，因有较大的偏差 ε_i 从而扰乱了规则的网格.

6.5. 关于 $(M^{(j)},\ a^{(j)})$ 数值表

为了构造优良的组合线性同余发生器，对于不同的组合数 $(m = 2, 3, 4)$，我们都给出了若干组 $(M^{(j)},\ a^{(j)})$ 值. 它们是根据定理 6.3, 6.4 和谱检验理论 (见 1.3 节)，并使用高精度运算系统 (中间结果精度超过 120 位十进制数) 获得的，其相应的序列周期分别超过 2^{30m}. 在选出这些优良组合时，我们经历了繁重的寻优计算和多种局部随机性检验. 限于篇幅这里不再详述，有兴趣的读者可与我们联系.

参 考 文 献

[1] 杨自强，张正军，乘同余法和组合随机数发生器的若干结果，第二届全国仿真方法与建模学术会议论文集 (SCSI 中国会员办公室编) (1993), 131–137.

[2] An, Hongzhi, *A Note on Chaotic Maps and Time Series*, in P.M. Robinson and M. Rosenblatt (editors), Lecture Notes III, Statistics 115, Athens Conference on Applied Probability and Time Series (Vol. II: Time Series Analysis in Memory of E.J. Hannan). Springer-Verlag (1996), 15-26.

[3] Box, G.E.P, and Muller, M.E., A Note on the Generation of Random Normal deviates, *Ann. Math. Statist.*, **29** (1958), 610.

[4] Bratley, P., Bennett, L.F., Schrage, L.E., *A Guide to Simulation*, 2nd ed. Springer-Verlag (1987).

[5] Brown, M., and Solomom, H., On Combining Pseudorandom Number Generators, *Ann. Math. Statist.*, **7** (1979), 691–695.

[6] Deng, L.Y., George, E.O., Generation of Uniform Variate from Several Nearly Uniformly Distributed Variables, *Comm. Statist. Simu.*, **19** (1990), 145–154.

[7] Dieter, U., Pseudo-Random Number: the Exact Distribution of Pairs, *Mathematics of Computation*, **25** (1971), 855–883.

[8] Eichenauer, J., Grothe, H., Leh, J., Marsaglia's lattice test and non-linear congruential pseudo random number generators, *Metrika*, **35** (1988), 241–250.

[9] Eichenauer-Herrmann, J., Grothe, H., A new inversive congruential pseudorandom number generator with power of two modulus. *ACM Transactions on Modeling and Computer Simulation*, **2** : 1 (1992), 1–11.

[10] Eichenauer-Herrmann, J., Statistical independence of a new class of inversive congruential pseudorandom numbers. *Mathematics of Computation*, **60** :201 (1993), 375–384.

[11] Ferrenberg, A.M., Landau, D.P., Wong, Y.J., Monte Carlo Simulations: Hidden Errors from "Good" Random Number Generators, *Physical review letters*, **69** :23 (1992), 3382–3384.

[12] Fishman, G.S., Moore, L.R., An Exhaustive Analysis of Multiplicative Congruential Random Number Generators with Modulus $2^{31} - 1$. *SIAM J. Sci. Statist. Comput.*, **7** (1986), 24–45.

[13] Grassberger, P., On Correlations in "Good" Random Number Generators, *Phys. Lett.*, **A 181** (1993), 43–46.

[14] Hass, A., The Multiple Prime Random Number Generator, *ACM Transactions on Mathematical Solfware*, **13** :4 (1987), 368–381.

[15] James, F., A review of pseudorandom number generators, *Comp. Physics Commun.*, **60** :4 (1990), 329–344.

[16] Knuth, D.E., *The Art of Computer Programming*, Vol.2, 2nd ed. Addison Wesley, (1981).

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

[17] L'Ecuyer, P., Efficient and Portable Combined Random Number Generators, *Communications of ACM*, **31** :6 (1988), 742–749,774.

[18] L'Ecuyer, P. and Tezuka, S., Structural Properties for Two Classes of Combined Random Number Generators, *Mathematics of Computation*, **57** :196 (1991), 735–746.

[19] Marsaglia, G., Random Numbers Fall Mainly in the Planes, *Proc. Nat. Acad. Sci.*, **61** :1 (1968), 25–28.

[20] Marsaglia, G., A Current View of Random Number Generators, in: *Computer Science and Statistics: The Interface*, Vol. 16 ed. L. Billadr, Elsevier, (1985).

[21] Marsaglia, G., Zaman, A., A New Class of Random Numbers Generators, *Ann. Appl. Prob.*, **1** :3 (1991), 462–480.

[22] Matteis, A.D., Pagnutti, S., Parallelization of Random Number Generators and Long-Range Correlations, *Numerische Mathematik*, **53** (1988), 595–608.

[23] Matteis, A.D., Pagnutti, S., Long-Range Correlation in Linear and Non-Linear Random Number Generation, *Parallel Computing*, **14** (1990), 207–210.

[24] Nance, B.E., Overstreet, C., Some Experimental Observation on the Behaviour of Composite Random Number Generators, *Oper. Res.*, **26** :5 (1978), 915–935.

[25] Niederreiter, H., *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, Pennsylvania, (1992).

[26] Tausworthe, R.C., Random Numbers Generated by Linear Recurrence Modulo Two, *Math. Comput.*, **19** (1965), 201–209.

[27] Tezuka, S., Lattice Structure of Pseudorandom Sequences from Shift Register Generators, *Proceedings of the 1990 Winter Simulation Conference*, IEEE Press, (1990).

[28] Tezuka, S. and L'Ecuyer, P., Efficient and Portable Combined Tausworthe Random Number Generators, *ACM Transactions on Modeling and Computer Simulation*, **1** :2 (1991), 99–112.

[29] Tezuka, S., L'Ecuyer, P., Couture, R., On the Lattice Structure of the Add-With-Carry and Subtract-With-Borrow Random Number Generators, *ACM Transactions on Modeling and Computer Simulation*, **3** :4 (1993), 315–333.

[30] Wichmann, B.A., Hill, I.D., An Efficient and Portable Pseudo-Random Number Generator, *Appl. Statist.*, **31** (1982), 188–190.

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net