70-75
1997 年 7 月 重庆大学学报 (自然科学版) Vol. 20, №. 4
第 20 卷第 4 期 Journal of Chongqing University (Natural Science Edition) Jul. 1997

(3)

均匀分布随机数的一种综合评估法*

A Comprehensive Evaluation Method for Uniformly Distributed Random Numbers

蔡坤宝① 冯明志② V 0212.1
Cai Kunbao Feng Mingzhi
杨泽林③ 李盛才① 马登基①
Yang Zeling Li Shengcai Ma Dengji
(① 重庆大学电气工程系,重庆,630044; ② 重庆大学机械工程一系;
③ 重庆大学工程力学系; 第一作者 46 岁,男,副教授,硕士)

摘 要 描述了产生均匀分布的 $U(0,1)$ 随机数的数学原理,提出了均匀分布随机数的综合评估方法,对由软件产生的均匀分布序列的随机性能作出了评估,选出了若干能产生较佳随机性能的均匀分布随机序列的种子。

关键词 数学方法;随机数产生法 / 统计方法 综合评估
中国图书资料分类法分类号 O212.1

ABSTRACT Mathematical methods for generating uniformly distributed U(0,1) random numbers are described. A comprehensive evaluation method for uniformly distributed random numbers is presented. This method is used to evaluate the randomness of uniformly distributed random sequences generated by software. Some good seeds have been selected out that can be used to generate uniformly distributed random sequences with better performance.

KEYWORDS mathematical methods; generation of random numbers / statistical methods

0 引 言

随机数序列在科技工程领域中有着广泛的应用,例如生物系统辨识与控制,计算机模拟,随机抽样与决策和数值积分等。均匀分布的 $U(0,1)$ 随机数产生的数学方法及其软件实现是一个十分活跃的研究领域,其发展历程是统计性能良好的发生器取代性能极差而又泛滥于计算机系统的令人惊诧的过程[1]。在随机数产生方法的研究中,均匀分布的 $U(0,1)$ 随机数产生方法的研究当推首位,因为其它分布的随机数或随机过程的实现均可由均匀分布的随机数经相应的变换而获得。然而,欲在计算机上获得具有良好独立同分布性能的 $U(0,1)$ 随机数,并非易事。

* 收文日期 1996-09-12
重庆市中青年专家基金项目,国家自然科学基金的部分资助项目

1 数学方法与软件实现

至今，应用最为广泛的均匀分布随机数发生器，就是基于 Lehmer 于 1951 年首先提出的线性同余发生器[2]，简记为 LCGs(Linear congruential Generators). 随机非负整数序列 $s_1, s_2, \cdots$，由下列迭代公式递推而得：

$$s_i = (as_{i-1} + c) \mod m \qquad i = 1, 2, \cdots \tag{1}$$

其中可选择的整数参数有三：模 $m > 0$，乘数 $a(0 < a < m)$ 和增量 $c(0 \leqslant c < m)$. 称递推初始正整数 $s_0(0 < s_0 < m)$ 为种子。显然，s_i 可能的取值为 $0 \leqslant s_i \leqslant m - 1$.

若对任意的正整数 i 均有 $s_{i+p} = s_i$，则最小正整数 p 称为 LCG 的周期。在一个周期内 p 个模 m 的非负整数的取值是各不相同的，因此 LCG 的最大可能的周期必为 m. 将任一周期内的 p 点数据对 m 归一化，即令 $u_i = s_i/m$，遂可得分布于[0,1) 间的随机数序列，将所有的 p 点序列分为 k 段较短的子序列，称每一个子序列为一个流(stream). 此时，第一个流的种子即为 s_0，而其余流的种子即为前一个流的最后一点未经归一化的整数值。值得注意的是，由 LCG 产生的任一点数据完全依赖于三个参数和选定的种子，故所得的序列称为伪随机数(pseudo radom number) 序列，其随机性能取决于参数和种子的选择。

对式(1) 所示的 LCGs 的三个参数再加上约束条件：$c = 0$，m 是素数；a 是模 m 的原元素 (primitive element modulo m)，即参数 a 满足

$$a^i \mod m \neq 1 \qquad i = 1, \cdots, m - 2 \tag{2}$$

且由著名的 Fermat 定理可知

$$a^{m-1} \mod m = 1 \tag{3}$$

并将 a 称为模 m 的 $m - 1$ 阶原根(primitive root). 可以证明，由此获得的 LCGs 的周期是 $m - 1$，即为原根 a 模 m 的阶数。种子 s_0 可在 $1, \cdots, m - 1$ 这 $m - 1$ 个自然数内任意选取，在选定种子 s_0 的条件下所得的周期序列的任一周期内的 $m - 1$ 个数，就是 $m - 1$ 个自然数的一个随机排列，将 $m - 1$ 点数据对 m 归一化，即得欲求的伪随机数序列 $U(0,1)$. 这就是当今普遍采用的所谓的素数模乘法线性同余发生器(Prime Modulus Multiplicative LCGs)，简记为 PMMLCGs[2].

在计算机上实现 PMMLCGs 必须精心考虑整数和浮点数的表达范围。至今应用最为成功的 PMMLCG 的素数模取为 $m = 2^{31} - 1$，而乘数取为 $a = 630\ 360\ 016$. 笔者应用文献[3]中实现 PMMLCG 的方法编制了一个完整的软件。系统缺省种子设定为 1 973 272 912，将该系统缺省种子可以产生的一个周期内的 $m - 1$ 点数据，分成 21 474 个相互独立的长度为 100 000 的流，第一个流的种子为系统缺省种子，从第二个流起，第 $k(k = 2 \sim 21\ 474)$ 个流的种子就是第 $k - 1$ 个流的最后一点归一化前的数据。由该软件可产生长度不大于 100 000 的均匀分布于(0,1) 间的随机数序列 $u_1, \cdots, u_n$.

2 经验检验方法

用计算机软件产生的随机数序列只可能是伪随机数序列,以上已说明,作为流的每一个序列的随机性能取决于参数和种子的选择。若欲产生的序列的长度小于一个流的长度,则序列的随机性能还与长度相关,故对产生的每一个序列必须进行均匀性和独立性检验,并称其为经验检验或局部检验。

2.1 独立性检验

采用两类共三种检验方法[4]。第一类为 RUNS 检验,包含两种方法:RUN-UP 和 RUN-DOWN. 两种检验均取零假设 H_0:代表被检验序列的分布是独立的。检验的基本步骤是:记录被检验序列中的六类单调升子序列(RUN-UP)或单调降子序列(RUN-DOWN)的个数,构造自由度为 6 的 χ^2 检验统计量,取检验水平 $\alpha = 0.10$ 并作判断。第二类检验用顺序相关(SC)法直接计算顺序相关系数(SCC),以此评估被检验序列中 u_{j+1} 对 u_j 的依赖关系,若 SCC 的绝对值越小则序列的独立性越好。

2.2 均匀性检验

采用 χ^2 拟合优度检验和 K-C(Колмогоров-Смирнов)检验[5] 偏重于对序列进行均匀分布的假设检验,两种检验均取零假设 H_0:代表被检验的序列服从均匀分布 $U(0,1)$,检验水平取 $\alpha = 0.10$. 笔者认为,若将易于查得的 χ^2 拟合优度检验公式中的观察频率和理论频率均对子区间宽度取归一化,则可推知:χ^2 检验统计量是:评估从被检验序列估计而得到的概率密度函数曲线与假设的理论概率密度函数曲线接近程度的一个判据。K-C 检验的实质是:评估从被检验序列估计而得的概率分布曲线与假设的理论概率分布曲线的接近程度。事实上,若被检验的序列为 $X_i(i = 1,\cdots,n)$,则其估计的概率分布函数定义为

$$F_n(x) = \frac{\text{number of } X_i s \leqslant x}{n} \tag{4}$$

即 $F_n(x)$ 是右连续阶梯型函数,且有

$$F_n(X_{(i)}) = i/n \qquad i = 1,\cdots,n \tag{5}$$

其中 $X_{(i)}$ 为顺序统计量。设被拟合的理论概率分布曲线为 $\hat{F}(x)$,则 K-C检验统计量 D_n 定义为

$$D_n = \sup_x \{|F_n(x) - \hat{F}_n(x)|\}$$

且应该按下式计算

$$D_n = \max\left\{\max_{1\leqslant i\leqslant n}\left[\frac{i}{n} - \hat{F}(X_{(i)})\right], \max_{1\leqslant i\leqslant n}\left[\hat{F}(X_{(i)}) - \frac{i-1}{n}\right]\right\} \tag{6}$$

显然,D_n 就是估计而得的概率分布曲线在 n 个离散点上的左右极限处,与连续的理论概率分布曲线的最大绝对偏差。易知 K-C 检验法与区间的划分无关,且优于 χ^2 拟合优度检验法,两种检验的拟合优度具有互补性,故两者的联合应用必将收到更好的检验效果。

3 检验结果

笔者提出了统计平均意义下的综合评估法，充分利用五种检验统计量提供的信息，对产生的随机序列的性能作出客观的评估，以便于产生满足应用要求的随机序列。综合评估法的检验方法和具体步骤如后续的式(8)，(9) 和(10) 所示。

3.1 五种检验

长度为 4 096 点的 100 个被检验序列中，第 $k(k=1\sim100)$ 个序列取自第 k 个流的前面部分。χ^2 检验中，[0,1] 区间等分为 13 个子区间，故 χ^2 检验统计量的自由度为 12. 每一种检验所得的 15 个最佳序列的检验统计量数值依序列于表 1 中，而每一种检验所得的随机性能最差者列于最后一行。前 15 个 SCC 的绝对值均小于 5%，顺序相关不显著。对于 K-C 检验，若

$$\left(\sqrt{n}+0.12+\frac{0.11}{n}\right)D_n > c_{1-\alpha}\Big|^{\alpha=0.1}=1.224 \tag{7}$$

则应该拒绝假设 H_0. 上式不等号左侧的表达式称为调整的 K-C 检验统计量(adjusted K-C test statistics)，n 是被检验序列的长度，α 为检验水平，表 1 中列出的即为该统计量的数值，前 15 个显然比临界值 1.224 小得多。对于其余的 3 列数据易于从 χ^2 分布百分点表作出推断，总之，表 1 中列出的最佳序列的统计量数值(|SCC| 不在此例) 均比检验水平 $\alpha=0.1$ 时的临界值小得多，故接受假设 H_0，而最后一行序列均拒绝假设 H_0.

表 1　检验统计量数值

均匀性				独立性					
流	chi	流	K-C	流	RUN-DOWN	流	RUN-UP	流	|SCC|
17	4.212 7	2	0.433 4	92	0.793 4	1	1.150 8	91	0.000 2
59	4.846 2	38	0.492 3	44	1.105 1	7	1.632 6	37	0.000 5
23	4.979 5	93	0.508 0	36	1.257 3	31	1.670 7	25	0.000 5
100	5.430 2	24	0.508 4	47	1.279 6	11	1.731 0	97	0.000 7
47	5.481 0	87	0.519 7	98	1.298 9	99	1.917 8	4	0.000 8
67	5.709 5	64	0.530 0	62	1.720 6	91	1.934 2	31	0.001 3
74	5.963 4	63	0.544 9	77	1.728 0	50	1.976 6	61	0.001 3
93	6.515 6	51	0.547 3	91	1.807 3	16	1.980 7	39	0.001 8
79	6.775 9	37	0.565 7	42	1.917 3	74	2.155 7	18	0.001 8
39	7.118 7	28	0.566 9	31	1.965 9	39	2.172 7	85	0.002 3
57	7.455 1	69	0.583 7	64	1.968 0	43	2.188 6	44	0.002 6
71	7.582 0	21	0.589 7	1	2.177 3	32	2.272 1	72	0.002 9
5	7.664 6	92	0.590 7	49	2.202 2	41	2.283 7	95	0.003 6
9	7.772 5	18	0.593 0	45	2.226 8	62	2.366 9	33	0.003 8
87	7.952 5	59	0.598 0	54	2.4272	64	2.6508	73	0.004 3
44	29.354 5	19	1.852 2	38	21.653 8	37	16.626 7	79	0.038 8

3.2 均匀性与独立

用下式评估第 i 个序列分布的独立性

$$\left.\begin{aligned} id(i) &= [du(i) + fi \times |SCC(i)|] \times 0.5 \\ du(i) &= 0.5 \times [rd(i) + ru(i)] \\ fi &= \text{mean}[du] / \text{mean}[|SCC|] = 436.234\ 2 \end{aligned}\right\} \quad (i = 1, \cdots, 100) \tag{8}$$

其中,rd 和 ru 分别表示 RUN-DOWN 和 RUN-UP 的检验统计量数值;mean 代表取样本均值;id 为分布的独立性相对指标。

用下式评估第 i 个序列分布的均匀性

$$\left.\begin{aligned} uni(i) &= 0.5 \times [chi(i) + fu \times kc(i)] \\ fu &= \text{mean}[chi] / \text{mean}[kc] = 14.628\ 3 \end{aligned}\right\} \quad (i = 1, \cdots, 100) \tag{9}$$

其中 chi 和 kc 分别代表 X^2 和 K-C 检验统计量数值,两者对均匀分布性相对指标 uni 的贡献在统计平均意义下是等同的。

3.3 均匀独立同分布性能

用下式评估第 i 个序列的均匀独立同分布性能

$$\left.\begin{aligned} T(i) &= 0.5 \times [uni(i) + fi \times id(i)] \\ ft &= \text{mean}[uni] / \text{mean}[id] = 2.264\ 8 \end{aligned}\right\} \quad (i = 1, \cdots, 100) \tag{10}$$

其中 T 为总体随机性能相对指标。

表 2 相对指标

	最佳序列										最差序列
流	91	31	25	18	41	39	44	3	32	33	38
id	0.970 4	1.183 4	1.832 8	2.348 3	2.361 8	2.369 6	2.554 1	2.696 1	2.724 3	2.867 6	12.486 3
流	59	93	47	17	87	2	38	57	39	37	96
uni	6.797 3	6.973 8	7.276 2	7.414 1	7.782 3	7.815 0	7.8298	8.159 8	8.294 6	8.306 3	23.914 5
流	39	91	31	2	18	23	41	67	71	59	19
T	6.830 7	7.088 3	7.607 2	7.808 8	7.808 9	7.957 1	8.217 3	8.246 8	8.485 9	8.498 2	21.848 5

各相对指标的数值越小,则其相应的随机机性能越好。按式(8),(9)和(10)对 100 个序列评估所得的最佳序列(各 10 个)和最差序列(各 1 个)列于表 2 中。

3.4 图形表示

由若干序列估计而得的三个函数,即概率密度函数(PDF),概率分布(distribution)函数和归一化的自协方差(NCOV)函数的三种图形示于附图中,现结合上述两表加以说明:

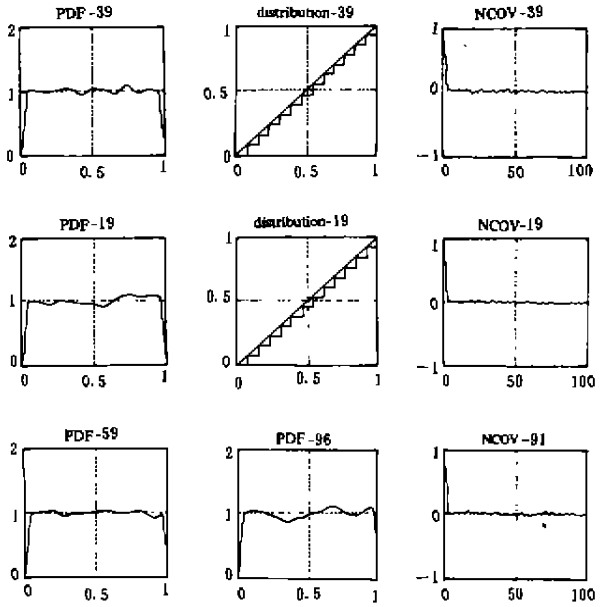
1) 序列 39 的三种图形与该序列的总体随机性能最佳相符合;

2) 总体最差序列 19 的概率密度和分布函数图形与序列 39 的对应图形有明显的差异;

3) 均匀分布性能最差序列 96 的 PDF 曲线起伏最大;

4) 序列 59 的 PDF 曲线较平坦,与该序列在表 1 的 chi 栏中的排序相符合;

5) 三幅 NCOV 图形的曲线幅值很小(不用考虑原点处),与顺序相关系数的数量级相近,在图形上看不出明显的差异,故序列的独立性差异的判别应该偏重相对指标。



附 图　三种函数图形

从图形分析易知，综合评估法对序列的随机性能的评估十分客观，效果极佳，并且方法简单明了。若按表 2 所提供的流号(对应种子)即可产生长度为 4 096 的较佳的随机序列。显然，综合评估法易于应用于产生其它长度的随机序列中去。

4 结　论

为用软件产生均匀独立同分布随机数提供了选择良好种子的方法。表 2 所提供的流号(对应种子)便于直接应用，对于产生长度为 4 096 点的其它流号的随机数序列，可依据样本均值的无偏性，用本文三个参数 fi，fu 和 ft，以及五种检验统计量数值，计算其对应的相对指标，并与表 2 的相对指标对照，或许可产生性能更佳的序列。

参 考 文 献

1　Park K P, Miller K W. Random Number Generators: Good Ones Are Hard to Find. communications of the ACM, 1988, 31(10), 1192～1201

2　L' Ecuyer P. Efficient and Portable Combined Random Number Generators. Communications of the ACM, 1988, 31(6), 742～774

3　Marse K, Roberts S D. Implementing a Portable FORTRAN Uniform(0,1) Generator. simulation, 1983, 41, 135～139

4　Kunth D E. The Art of Computer Programming. Massachusetts: Addison-Wesley Reading, 1969. 1～155

5　Stephens M A. EDF Statistics for Goodness-Fit and Some Comparisions. J Am Statist Assoc, 1974, 69, 730～737