1982年 第2卷 第4期
Vol.2, No.4, 1982

数学研究与评论
JOURNAL OF MATHEMATICAL RESEARCH & EXPOSITION

研究伪随机数序列独立性的均匀偏度法*

裴鹿成

(中国科学院原子能研究所)

§1 引 言

由具有在[0,1]上均匀分布的总体中产生的简单子样称为随机数序列，其中的每一样本称为随机数.所谓伪随机数序列,一般是指用数学递推公式所产生的随机数序列. 如最常见的乘同余方法，它所产生的伪随机数序列 $\{\xi_n\}_1^N$ 就是对给定的正整数M和小于M的任意正整数初值 β_1，用如下递推公式确定的[1]：

$$\xi_n=\frac{\beta_n}{M}, \qquad \beta_{n+1}\equiv a\beta_n \ (mod M), \tag{1}$$

其中 a 是参数.

如何确定产生伪随机数序列的递推公式及其中的初值和参数?一般来说有两个准则,一个是尽量使它在产生伪随机数时所需的费用小；另一个是尽量使它所产生的伪随机数序列能较好地具备在[0,1]上均匀且相互独立的性质. 作为前者的表现形式主要是如何确定递推公式，而作为后者的表现形式则主要是如何确定递推公式中的初值和参数. 二者比较起来，很明显，后一问题的解决要比前一问题的解决困难得多，而且，更为重要的是，确定产生伪随机数序列的递推公式是好，还是不好，有赖于是否能确定出好的初值和参数，换句话说，后一问题不解决，要想解决前一问题是根本不可能的.

对于确定的伪随机数序列 $\{\xi_n\}_1^N$，为确定它是否较好地具备了均匀且相互独立的性质，一般的方法是用统计检验的方法来确定. 然而，统计检验方法只能研究某一确定的伪随机数序列，而不能很好地研究伪随机数序列对产生它的方法中的初值和参数的依赖关系，因此，为了从理论上能较好地确定出理想的初值和参数，有必要用解析的方法来研究伪随机数序列的均匀性和独立性.

用解析方法研究伪随机数序列均匀性和独立性的一般办法是，用若干量对伪随机数序列的均匀性和独立性进行标志，并且认为，这些标志量越靠近零相应的性质满足得越好. 对于均匀性问题,只用均匀偏度这样一个量标志已足够[2].对于相互独立性问题，要比均匀

* 1981 年 8 月 26 日收到.

性问题复杂得多，常用多个量进行标志．本文的目的在于研究给出这样的标志量，它不仅可以很好地标志伪随机数序列的独立性，而且还可以将其他所有标志量统一在这一标志量中．

§2 研究伪随机数序列独立性的历史回顾

对于伪随机数序列 $\{\xi_n\}_1^N$，1960年，Coveyou首先提出了用相邻两个伪随机数的相关系数来标志伪随机数序列的独立情况[3]，这是用解析方法研究伪随机数序列独立性的第一个工作．1961年，Greenberger指出了Coveyou工作中的问题，给出了相邻两个伪随机数的相关系数的确切表达式[4]：

$$\rho^{(0,1)}=\frac{\frac{1}{N}\sum_{n=1}^{N}\xi_n\xi_{n+1}-\left(\frac{1}{N}\sum_{n=1}^{N}\xi_n\right)^2}{\frac{1}{N}\sum_{n=1}^{N}\xi_n^2-\left(\frac{1}{N}\sum_{n=1}^{N}\xi_n\right)^2} \tag{2}$$

其中N为伪随机数序列的周期，亦即对于任意的正整数 i，$\xi_{N+i}=\xi_i$．

1964年，Jansson推广了Greenberger的工作，讨论了间距为 δ 的两个伪随机数的相关系数：

$$\rho^{(0,\delta)}=\frac{\frac{1}{N}\sum_{n=1}^{N}\xi_n\xi_{n+\delta}-\left(\frac{1}{N}\sum_{n=1}^{N}\xi_n\right)^2}{\frac{1}{N}\sum_{n=1}^{N}\xi_n^2-\left(\frac{1}{N}\sum_{n=1}^{N}\xi_n\right)^2} \tag{3}$$

主张用多种间距的相关系数标志伪随机数序列的独立情况[5]．

进入七十年代后，除继续用上述顺序相关法研究伪随机数序列的独立性外[6][7]，1971年，Dieter提出了用对分布法研究伪随机数序列的独立性．引入符号

$$\eta(\cdot)=\begin{cases}1, & \text{当条件}\cdot\text{满足时},\\ 0, & \text{当条件}\cdot\text{不满足时},\end{cases} \tag{4}$$

所谓对分布法就是对于给定的 $0\leqslant x_1<x_2\leqslant 1$ 和 $0\leqslant y_1<y_2\leqslant 1$，用

$$\Delta_{PD}^{(0;1)}(x_1,x_2,y_1,y_2)=\frac{1}{N}\sum_{n=1}^{N}\eta(x_1\leqslant\xi_n<x_2,y_1\leqslant\xi_{n+1}<y_2)-(x_2-x_1)(y_2-y_1), \tag{5}$$

标志伪随机数序列的独立情况[8]．

1972年，Dieter进一步提出了用三排列法研究伪随机数序列的独立性．所谓三排列法就是用

$$\Delta_{TP}^{(0;1,2)}=\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<\xi_{n+1}<\xi_{n+2})-\frac{1}{6}, \tag{6}$$

标志伪随机数序列的独立情况[9]．

除了上述各种标志方法外，1974年，作者还提出了一种用独立偏度来研究伪随机数序列独立性的方法．所谓独立偏度法就是用

$$\Delta_{ID}^{(0;1)}=\sup_{0\leqslant x,\,y\leqslant 1}\left|\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x,\xi_{n+1}<y)\right.$$

$$-\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_{n+1}<y)\Bigg|, \tag{7}$$

标志伪随机数序列的独立情况[2]。

§3　标志伪随机数序列独立性的均匀偏度法

根据随机数的定义，随机数具有一个非常重要的性质：对于任意自然数S，由S个随机数所组成的点$(\xi_n,\xi_{n+1},\cdots,\xi_{n+s-1})$在$S$维超正方体$G_s$上均匀分布；反之，如果某随机变数序列$\{\xi_n\}_1^N$，对于任意自然数$S\leqslant N$，由$S$个元素所组成的$(\xi_n,\xi_{n+1},\cdots,\xi_{n+s-1})$在$G_s$上均匀分布，则随机变数序列$\{\xi_n\}_1^N$具有在$[0,1]$上均匀且相互独立的性质。由此可以看出，对于给定的伪随机数序列$\{\xi_n\}_1^N$，用$(\xi_n,\xi_{n+1},\cdots,\xi_{n+s-1})$，$n=1,2,\cdots,N$，是否在$G_s$上均匀来标志伪随机数序列的相互独立性是很合适的。

对于确定的伪随机数序列$\{\xi_n\}_1^N$和S个互不相同的非负整数$i_1,i_2,\cdots,i_s$，如果令

$$\Delta_s^{(i_1,i_2,\cdots,i_s)}=\sup_{0\leqslant x_1,x_2,\cdots,x_s\leqslant 1}\Bigg|\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_{n+i_1}<x_1,\xi_{n+i_2}<x_2,\cdots,\xi_{n+i_s}<x_s)-x_1x_2\cdots x_s\Bigg|, \tag{8}$$

则$\Delta_s^{(i_1,i_2,\cdots,i_s)}$恰好表示点$(\xi_{n+i_1},\xi_{n+i_2},\cdots,\xi_{n+i_s})$，$n=1,2,\cdots,N$，在$G_s$上与均匀分布偏离程度，简称$\Delta_s^{(i_1,i_2,\cdots,i_s)}$为$S$维均匀偏度。标志伪随机数序列独立性的均匀偏度法就是用$\Delta_s^{(i_1,i_2,\cdots,i_s)}$进行标志，它的值越小伪随机数序列的独立性越好。下面将主要讨论$(i_1,i_2,\cdots,i_s)=(0,1,\cdots,s-1)$情况，并简单地记$\Delta_s^{(0,1,\cdots,s-1)}$为$\Delta_s$。

众所周知，相关系数为零与相互独立是两个不同的概念，相互独立则相关系数一定为零，相关系数为零则不一定相互独立。因此，用相关系数来标志伪随机数序列的独立情况并不是一种好方法。为了说明这一问题，作者曾找到过这样一个伪随机数序列$\{\xi_n\}_1^N$，它的均匀性情况是不能再改善的，相关系数由下式给出

$$\rho^{(0,1)}=\frac{3\left(1-\frac{4}{N}\right)}{2\left(1-\frac{1}{N^2}\right)}\cdot\frac{1}{N}, \tag{9}$$

当N较大时是一个非常靠近零的量，可是由它所组成的点(ξ_n,ξ_{n+1})，$n=1,2,\cdots,N$，却只能落在G_2中的三根直线上[2]，就是说，该伪随机数序列的独立性却很差。与此情况不同，对于均匀偏度法来说，这种现象是一定不会出现的。至于其他方法，如对分布法、三排列法和独立偏度法等，同均匀偏度法比较都明显地存在着这样或那样的缺点，在这里就不再一一说明了。

§4　顺序相关法与二维均匀偏度法

对于任意的伪随机数序列$\{\xi_n\}_1^N$，根据如下明显等式

$$\frac{1}{N}\sum_{n=1}^{N}\xi_n\xi_{n+1}=1-2\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx$$

$$+\int_0^1\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x,\xi_{n+1}<y)dxdy,$$

$$\frac{1}{N}\sum_{n=1}^{N}\xi_n=1-\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx,$$

$$\frac{1}{N}\sum_{n=1}^{N}\xi_n^2=1-2\int_0^1 x\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx, \tag{10}$$

和 $\rho^{(0,1)}$ 的定义 (2)，立即得到

$$\rho^{(0,1)}=\frac{\int_0^1\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x,\xi_{n+1}<y)dxdy-\left[\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx\right]^2}{\int_0^1 2(1-x)\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx-\left[\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx\right]^2}. \tag{11}$$

又由于

$$\left|\int_0^1\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x,\xi_{n+1}<y)dxdy-\left[\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx\right]^2\right|$$

$$\leqslant\left|\int_0^1\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x,\xi_{n+1}<y)dxdy-\int_0^1\int_0^1 xydxdy\right|$$

$$+\left|\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx+\int_0^1 xdx\right|\cdot\left|\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx-\int_0^1 xdx\right|$$

$$\leqslant\Delta_2+\Delta_1+\Delta_1^2,$$

$$\left|\frac{1}{12}-\left\{\int_0^1 2(1-x)\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx-\left[\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx\right]^2\right\}\right|$$

$$\leqslant\left|\int_0^1 2(1-x)xdx-\int_0^1 2(1-x)\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx\right|$$

$$+\left|\left[\int_0^1 xdx\right]^2-\left[\int_0^1\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)dx\right]^2\right|\leqslant 2\Delta_1+\Delta_1^2, \tag{12}$$

代入到 (11) 式中立即得到

$$|\rho^{(0,1)}|\leqslant\frac{\Delta_2+\Delta_1+\Delta_1^2}{\frac{1}{12}-2\Delta_1-\Delta_1^2}\leqslant 24\Delta_2+12\Delta_2^2. \tag{13}$$

上述结果表明，相关系数 $\rho^{(0,1)}$ 是否靠近零被二维均匀偏度 Δ_2 是否靠近零所完全确定，换句话说，顺序相关法可由二维均匀偏度法所完全替代.

§5 对分布法与二维均匀偏度法

对于任意的伪随机数序列 $\{\xi_n\}_1^N$，根据如下明显等式

$$\frac{1}{N}\sum_{n=1}^{N}\eta(x_1\leqslant\xi_n<x_2,\ y_1\leqslant\xi_{n+1}<y_2)-(x_2-x_1)(y_2-y_1)$$
$$=\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x_2,\ \xi_{n+1}<y_2)-x_2y_2-\left[\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x_1,\ \xi_{n+1}<y_2)-x_1y_2\right]$$
$$-\left[\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x_2,\ \xi_{n+1}<y_1)-x_2y_1\right]+\left[\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x_1,\ \xi_{n+1}<y_1)-x_1y_1\right],\quad(14)$$

注意二维均匀偏度的定义，立即得到，对于任意给定的 $0\leqslant x_1<x_2\leqslant 1$ 和 $0\leqslant y_1<y_2\leqslant 1$，有如下不等式成立

$$|\Delta_{PD}^{(0;\,1)}(x_1,x_2,y_1,y_2)|\leqslant 4\Delta_2.\quad(15)$$

上述结果表明，对分布标志 $\Delta_{PD}^{(0;\,1)}(x_1,x_2,y_1,y_2)$ 是否靠近零被二维均匀偏度 Δ_2 是否靠近零所完全确定，而不管其中参数如何，换句话说，对分布法可由二维均匀偏度法所完全替代。

§6　三排列法和三维均匀偏度法

对于任意的伪随机数序列 $\{\xi_n\}_1^N$ 和任意的正整数 I，由于

$$\left|\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<\xi_{n+1}<\xi_{n+2})-\frac{1}{6}\right|\leqslant\left|\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<\xi_{n+1}<\xi_{n+2})\right.$$
$$-\sum_{i=1}^{I}\sum_{j=i+1}^{I}\frac{1}{N}\sum_{n=1}^{N}\eta\left(\frac{i-1}{I}\leqslant\xi_n<\frac{i}{I},\ \frac{j-1}{I}\leqslant\xi_{n+1}<\frac{j}{I},\ \frac{j}{I}\leqslant\xi_{n+2}\right)\Bigg|$$
$$+\left|\sum_{i=1}^{I}\sum_{j=i+1}^{I}\frac{1}{N}\sum_{n=1}^{N}\eta\left(\frac{i-1}{I}\leqslant\xi_n<\frac{i}{I},\ \frac{j-1}{I}\leqslant\xi_{n+1}<\frac{j}{I},\ \frac{j}{I}\leqslant\xi_{n+2}\right)-\frac{1}{6}\right|$$
$$\leqslant\sum_{i=1}^{I}\frac{1}{N}\sum_{n=1}^{N}\eta\left(\frac{i-1}{I}\leqslant\xi_n<\frac{i}{I},\ \frac{i-1}{I}\leqslant\xi_{n+1}<\frac{i}{I},\ \frac{i-1}{I}\leqslant\xi_{n+2}\right)$$
$$+\sum_{i=1}^{I}\frac{1}{N}\sum_{n=1}^{N}\eta\left(\xi_n<\frac{i-1}{I},\ \frac{i-1}{I}\leqslant\xi_{n+1}<\frac{i}{I},\ \frac{i-1}{I}\leqslant\xi_{n+2}<\frac{i}{I}\right)$$
$$+\left|\sum_{i=1}^{I}\sum_{j=i+1}^{I}\frac{1}{N}\sum_{n=1}^{N}\eta\left(\frac{i-1}{I}\leqslant\xi_n<\frac{i}{I},\ \frac{j-1}{I}\leqslant\xi_{n+1}<\frac{j}{I},\ \frac{j}{I}\leqslant\xi_{n+2}\right)-\frac{1}{6}\right|,\quad(16)$$

因此，若采用上节中得到不等式（15）时的类似方法，则可以进一步得到

$$\left|\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<\xi_{n+1}<\xi_{n+2})-\frac{1}{6}\right|$$
$$\leqslant\sum_{i=1}^{I}\left(\frac{1}{I^2}\,\frac{I-i+1}{I}+8\Delta_3\right)+\sum_{i=1}^{I}\left(\frac{1}{I^2}\,\frac{i-1}{I}+4\Delta_3\right)$$
$$+\left|\sum_{i=1}^{I}\sum_{j=i+1}^{I}\frac{1}{I^2}\,\frac{I-j}{I}-\frac{1}{6}\right|+\sum_{i=1}^{I}\sum_{j=i+1}^{I}8\Delta_3$$
$$=\frac{3}{2I}-\frac{1}{3I^2}+8I\Delta_3+4I^2\Delta_3,\quad(17)$$

取 $I\cong(3/16)^{1/3}\cdot\Delta_3^{-1/3}$，最后得到

$$|\Delta_{TP}^{(0;\,1,\,2)}|\leqslant\frac{3}{2}18^{\frac{1}{3}}\Delta_3^{\frac{1}{3}}+\frac{14}{9}12^{\frac{1}{3}}\Delta_3^{\frac{2}{3}}. \tag{18}$$

上述结果表明，三排列标志 $\Delta_{TP}^{(0;\,1,\,2)}$ 是否靠近零被三维均匀偏度 Δ_3 是否靠近零所完全确定，换句话说，三排列法可由三维均匀偏度法所完全替代.

§7 独立偏度法与二维均匀偏度法

对于任意的伪随机数序列 $\{\xi_n\}_1^N$，由于有如下结果

$$\begin{aligned}\Delta_{ID}^{(0;\,1)}\leqslant&\sup_{0\leqslant x,\,y\leqslant1}\left|\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x,\xi_{n+1}<y)-x\cdot y\right|\\&+\sup_{0\leqslant x,\,y\leqslant1}\left|\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_{n+1}<y)-\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)y\right|\\&+\sup_{0\leqslant x,\,y\leqslant1}\left|\frac{1}{N}\sum_{n=1}^{N}\eta(\xi_n<x)y-x\cdot y\right|\leqslant\Delta_2+2\Delta_1\leqslant3\Delta_2,\end{aligned} \tag{19}$$

因此，同其他标志量的情况完全相类似，独立偏度标志 $\Delta_{ID}^{(0;\,1)}$ 是否靠近零被二维均匀偏度 Δ_2 是否靠近零所完全确定，换句话说，独立偏度法可由二维均匀偏度法所完全替代.

§8 乘同余法的三维均匀偏度

根据以上结果，为了给出顺序相关法中的 $\rho^{(0,\,1)}$，对分布法中的 $\Delta_{PD}^{(0;\,1)}(x_1,x_2,y_1,y_2)$、三排列法中的 $\Delta_{TP}^{(0;\,1,\,2)}$ 和独立偏度法中的 $\Delta_{ID}^{(0;\,1)}$ 的估计，只须给出二维均匀偏度 Δ_2 和三维均匀偏度 Δ_3 的估计. 关于乘同余法的二维均匀偏度的估计，作者在给出独立偏度法的同时已经给出[2]，下面给出乘同余法的三维均匀偏度估计的结果.

将伪随机数序列 $\{\xi_n\}_1^N$ 按由小到大重新排列：$\xi_1'\leqslant\xi_2'\leqslant\cdots\leqslant\xi_N'$，如果 $\xi_{n+1}'-\xi_n'=1/N$，对于所有的 $n=1,2,\cdots,N-1$ 成立，则称该伪随机数序列是等分布的（对于乘同余法，只要其中的初值和参数选得合适，就可使由它所产生的伪随机数序列是等分布的[2]）. 有了了等分布定义后，便可进一步给出乘同余法的三维均匀偏度估计的结果如下：

对于乘同余法（1），如果它所产生的伪随机数序列 $\{\xi_n\}_1^N$ 是等分布的，则它的三维均匀偏度一定满足

$$\Delta_3\leqslant\frac{2}{a}+\frac{a^2}{N}+\frac{1}{a^2}+\frac{2a}{N}+\frac{1}{N}. \tag{20}$$

为了证明以上结果，只须证明 $a^2<N$ 时不等式（20）是正确的，因为 $a^2\geqslant N$ 时不等式（20）的正确性是明显的. 下面分两步进行证明：

第一步证明，对于任意的 $0\leqslant x,y,z\leqslant1$，有一点而且只有一点 $(\xi_n,\xi_{n+1},\xi_{n+2})$ 属于区域 $G=(x,x+1/a]\times(y,y+1/a]\times(z,z+a^2/N]$，当 $x+1/a>1$ 时，约定 $(x,x+1/a]=(0,\{x+1/a\}]+(x,1]$，其中 $\{\cdot\}$ 表示取其中数 $\cdot$ 的小数部分，其他二变数的约定完全相类似.

首先证明有一点 $(\xi_n,\xi_{n+1},\xi_{n+2})$ 属于区域 G. 对于任意的整数 i，j，根据等分布假设，一定存在这样的 $0<\theta\leqslant1$ 和 ξ_n，使得

$$\xi_n=\left\{\frac{i}{a}+\frac{j}{a^2}+\frac{z}{a^2}+\frac{\theta}{N}\right\}. \tag{21}$$

选取 i 和 j 依次满足如下两个不等式

$$ax-\frac{j}{a}-\frac{z}{a}-\frac{a}{N}\theta<i\leqslant ax-\frac{j}{a}-\frac{z}{a}-\frac{a}{N}\theta+1,$$

$$ay-z-\frac{a^2}{N}\theta<j\leqslant ay-z-\frac{a^2}{N}\theta+1, \tag{22}$$

则容易验证，由此所确定的点 $(\xi_n,\xi_{n+1},\xi_{n+2})$ 属于G．

下面证明，不可能有另一个点 $(\xi'_n,\xi'_{n+1},\xi'_{n+2})$ 也属于G．假若不然，即假设 $\xi'_n\neq\xi_n$，$(\xi'_n,\xi'_{n+1},\xi'_{n+2})$ 属于G．则由于 $0\leqslant\xi'_{n+2}-\xi_{n+2}<a^2/N$，立即可以得出 $0\leqslant\xi'_n-\xi_n<1/N$，根据等分布假设，只能是 $\xi'_n-\xi_n=0$，与 $\xi'_n\neq\xi_n$ 相矛盾．

第二步证明不等式（20）是正确的．对于任意的 $0\leqslant x,y,z\leqslant 1$，根据第一步证明，可以直接得到如下不等式

$$\begin{aligned}&\left|\frac{1}{N}\sum_{n=1}^{N}\eta\left(\xi_n<\frac{[ax]}{a},\xi_{n+1}<\frac{[ay]}{a},\xi_{n+2}<\frac{a^2}{N}\left[\frac{N}{a^2}z\right]\right)-x\cdot y\cdot z\right|\\&=\left|\frac{1}{N}\sum_{n=1}^{N}\eta\left(\xi_n<\frac{[ax]}{a},\xi_{n+1}<\frac{[ay]}{a},\xi_{n+2}<\frac{a^2}{N}\left[\frac{N}{a^2}z\right]\right)\right.\\&\left.-\left(\frac{[ax]}{a}+\frac{\{ax\}}{a}\right)\left(\frac{[ay]}{a}+\frac{\{ay\}}{a}\right)\left(\frac{a^2}{N}\left[\frac{N}{a^2}z\right]+\frac{a^2}{N}\left\{\frac{N}{a^2}z\right\}\right)\right|\\&\leqslant\frac{2}{a}+\frac{a^2}{N}+\frac{1}{a^2}+\frac{2a}{N}+\frac{1}{N},\end{aligned} \tag{23}$$

其中 $[\cdot]$ 表示取其中数 $\cdot$ 的整数部分．完全相类似地，还有如下不等式

$$\begin{aligned}&\left|\frac{1}{N}\sum_{n=1}^{N}\eta\left(\xi_n<\frac{[ax]}{a}+\frac{1}{a},\xi_{n+1}<\frac{[ay]}{a}+\frac{1}{a},\xi_{n+2}<\frac{a^2}{N}\left[\frac{N}{a^2}z\right]\right.\right.\\&\left.\left.+\frac{a^2}{N}\right)-x\cdot y\cdot z\right|\leqslant\frac{2}{a}+\frac{a^2}{N}+\frac{1}{a^2}+\frac{2a}{N}+\frac{1}{N}.\end{aligned} \tag{24}$$

于是，根据三维均匀偏度的定义，注意不等式（23）、（24）和如下明显不等式

$$\begin{aligned}&\frac{1}{N}\sum_{n=1}^{N}\eta\left(\xi_n<\frac{[ax]}{a},\xi_{n+1}<\frac{[ay]}{a},\xi_{n+2}<\frac{a^2}{N}\left[\frac{N}{a^2}z\right]\right)\\&\leqslant\frac{1}{N}\sum_{n=1}^{N}\eta\left(\xi_n<x,\xi_{n+1}<y,\xi_{n+2}<z\right)\leqslant\frac{1}{N}\sum_{n=1}^{N}\eta\left(\xi_n<\frac{[ax]}{a}\right.\\&\left.+\frac{1}{a},\xi_{n+1}<\frac{[ay]}{a}+\frac{1}{a},\xi_{n+2}<\frac{a^2}{N}\left[\frac{N}{a^2}z\right]+\frac{a^2}{N}\right),\end{aligned} \tag{25}$$

便可得到不等式（20）．

结果（20）表明，为使由乘同余法所产生的伪随机数序列较为理想，从三维均匀偏度法考虑，最好选取 $a\cong N^{1/3}$．与此情况不完全相同，顺序相关法或独立偏度法所得到的结论却是最好选取 $a\cong N^{1/2}$[2][4]，看来两者之间是矛盾的，其实并不矛盾，因为三维均匀

偏度法考虑的是三维情况，而顺序相关法或独立偏度法所考虑的只是二维情况，前者可以兼顾后者，而后者却根本没有考虑前者.

产生伪随机数的另一个常见的方法是混合同余法[10]，对于由该方法所产生的伪随机数序列的二维均匀偏度的估计，作者在另一工作中已经给出[2]，至于它的三维均匀偏度的估计，有同（20）式完全相类似的结果.

§9 结 束 语

关于顺序相关法，前面我们已经指出过，Jansson 曾经建议用 $\rho^{(0,\delta)}$ 标志伪随机数序列的独立情况. 对于这一问题有同（13）式相类似的结果如下：

$$|\rho^{(0,\delta)}| \leqslant 24\Delta_2^{(0,\delta)} + 12(\Delta_2^{(0,\delta)})^2. \tag{26}$$

关于三排列法，Dieter 也曾经建议用 $\xi_n, \xi_{n+1}, \xi_{n+2}$ 的各种组合形式的三排列标志来研究伪随机数序列的独立性. 对于这一问题有同顺序相关法完全相类似的结果. 例如，对于排列：$\xi_{n+2}, \xi_{n+1}, \xi_n$，同（18）式相当的结果是

$$|\Delta_{T_P}^{(2,1,0)}| \leqslant \frac{3}{2} 18^{1/3} (\Delta_3^{(2,1,0)})^{1/3} + \frac{14}{9} 12^{1/3} (\Delta_3^{(2,1,0)})^{2/3}. \tag{27}$$

采用类似于上述 Jansson 和 Dieter 的方法，对伪随机数序列进行任意组合，也可给出相应的对分布标志量和独立偏度标志量，对于这些标志量自然有与（26）式和（27）式完全相当的结果.

参 考 文 献

[1] Lehmer, D. H. Ann. Comp. Lab. Harvard Univ., 26, 141 (1951).
[2] 裴鹿成，张孝泽，蒙特卡罗方法及其在粒子输运问题中的应用，科学出版社，1980.
[3] Coveyou, R. R. J. Assoc. comp. Mach., 7, 72 (1960).
[4] Greenberger, M. Math. Comp., 15, 383 (1961).
[5] Jansson, B. BIT MR* 29* 2934, 4, 6(1964).
[6] Dieter, U. and Ahrens, J. Numer. Math., 16, 101 (1971).
[7] Dieter, U. *Applications of number theory to numerical analysis*, (Ed. S. K. Zaremba) Press New York London 1972, 287.
[8] Dieter, U. Math. Comp., 25, 855 (1971).
[9] Dieter, U. J. Res. Nat. Bur. of standerds, 76B (1972).
[10] Rotenberg, A. J. Assoc. Comp. Mach., 7, 75 (1960).

An Uniform Departureness Method for Studying Independence of Pseudorandom Sequence

By Pei Lu-cheng (裴鹿成)

Abstract

In this paper, an uniform departureness method for studying the independence of the pseudorandom sequence is developed. This method can mark the independence of the pseudorandom sequence better than existing serial correlation method, pairs distribution method, triplets permutation method, and independent departureness method. The more impotant result is that the uniform departureness method is in fact a mark method of integrating with aforesaid all other methods. The three-dimensional uniform departureness of the pseudorandom sequence generated by the multiplicative congruential method is specifically given.