第二章　伪随机数的产生

一. 伪随机数产生的意义

1. 随机数的产生是进行随机优化的第一步也是最重要的一步，随机优化算法运行过程中需要大量随机数
2. 传统手工方法：抽签，掷骰子，抽牌，摇号等，无法满足产生大量随机数的需求
3. 伪随机数方法：利用计算机通过某些数学公式计算而产生，从数学意义上说不是随机的，但只要通过随机数的一系列统计检验，就可以作为随机数来使用

一. 伪随机数产生的意义

4. 伪随机数的产生过程

- 确定一个数学模型或某种规则
- 规定几个初始值
- 按照上述模型产生第一个随机数
- 用产生的上一个随机数作为新的初值，按照相同的步骤产生下一个随机数，重复之，得到一个伪随机数序列

一. 伪随机数产生的意义

5. 一个良好的伪随机数产生器应具有的特性

- 数列中每个数出现的频率应相等或近似相等，即分布均匀
- 数列中任意一数都不能由其他数推出，即独立性
- 产生的数列要有足够长的周期，即不可预测性
- 产生数列的速度要快，占用计算机的内存要尽可能的少

二. 产生U(0, 1)的乘同余法

1. 均匀随机数是产生其他随机数的基础
2. 乘同余法
   - 计算公式

$$S_{k+1} = (A \cdot S_k) \bmod (M)$$

式中A表示整数常数， **mod**表示取模运算， M表示较大的整数

   - 如何确定A和M的值，以保证产生的随机数周期最长？

数论理论可以证明：当$M = 2^L (L > 2)$时，若$A = 8k \pm 3$或者$A = 4k + 1$，且S_0为奇数时，可以获得的最长随机数序列长度为2^{L-2}。

二. 产生U(0, 1)的乘同余法

3. 计算举例

令$M=2^4=16$

I. 若$A=3$且$S_0=1$时，则

$S_1=(A\cdot S_0)\bmod(M)=(3\times 1)\bmod(16)=3$；

$S_2=(3\times 3)\bmod(16)=(9)\bmod(16)=9$；

$S_3=(3\times 9)\bmod(16)=(27)\bmod(16)=11$；

$S_4=(3\times 11)\bmod(16)=(33)\bmod(16)=1$

…

于是可以产生一个周期为4的随机整数序列：

$$S=\{1,3,9,11,1,\ldots\}$$

二. 产生U(0, 1)的乘同余法

3. 计算举例

令$M = 2^4 = 16$

II. 若$A = 5$且$S_0 = 1$时，则

$S_1 = (A \cdot S_0) \bmod (M) = (5 \times 1) \bmod (16) = 5$;

$S_2 = (5 \times 5) \bmod (16) = (25) \bmod (16) = 9$;

$S_3 = (5 \times 9) \bmod (16) = (45) \bmod (16) = 13$;

$S_4 = (5 \times 13) \bmod (16) = (65) \bmod (16) = 1$;

…

于是可以产生周期为4的随机整数序列：

$$S = \{1, 5, 9, 13, 1, \ldots\}$$

二. 产生U(0, 1)的乘同余法

3. 计算举例

令$M = 2^4 = 16$

III. 若$A = 3$且$S_0 = 2$时，则

$S_1 = (A \cdot S_0) \bmod (M) = (3 \times 2) \bmod (16) = 6$;

$S_2 = (3 \times 6) \bmod (16) = (18) \bmod (16) = 2$;

…

于是可以产生一个周期为2的随机整数序列：

$$S = \{2, 6, 2, \ldots\}$$

二. 产生U(0, 1)的乘同余法

3. 计算举例

若想产生U(0,1)，则令$\boldsymbol{\xi_i = S_i/M}$即可

I. $\boldsymbol{A = 3}, S_0 = 1$	$\xi = \{\frac{1}{16}, \frac{3}{16}, \frac{9}{16}, \frac{11}{16}, \dots\}$
II. $\boldsymbol{A = 5}, S_0 = 1$	$\xi = \{\frac{1}{16}, \frac{5}{16}, \frac{9}{16}, \frac{13}{16}, \dots\}$
III. $\boldsymbol{A = 3}, S_0 = 2$	$\xi = \{\frac{2}{16}, \frac{6}{16}, \dots\}$

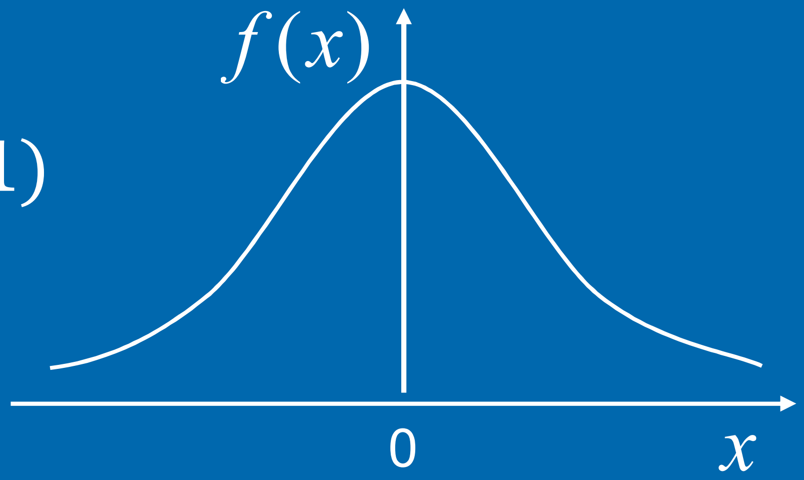
二. 产生U(0, 1)的乘同余法

4. 混合同余法

- 公式：$\boldsymbol{S_{k+1} = (A \cdot S_k + C) \bmod (M)}$
- 参数取值：$\boldsymbol{M = 2^L}$，$\boldsymbol{A = 4k + 1}$，C与M互为质数，则可以获得最长的随机数序列长度为$\boldsymbol{2^L}$
- 上例中，若$M = 16$，$A = 5$，$C = 3$，$\boldsymbol{S_0 = 1}$，则产生的随机整数序列？

三. 正态分布N(0, 1)的产生

$\boldsymbol{X \in N(0,1)}$



$$f(x) = \frac{1}{\sqrt{2\pi}} e^{\frac{x^2}{2}} \qquad F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{\frac{t^2}{2}} dt$$

三. 正态分布N(0, 1)的产生

基本原理：若$\boldsymbol{Y_1, Y_2, \dots, Y_n}$是独立同分布，均值和方差分别为$\boldsymbol{\mu}$和$\boldsymbol{\sigma^2}$，且$n$较大，则$\boldsymbol{X} = Y_1 + Y_2 + \cdots + Y_n$近似于正态分布，且满足$\boldsymbol{\mu_x = \mu_1 + \mu_2 + \cdots + \mu_n = n\mu}$及$\boldsymbol{\sigma_x^2 = \sigma_1^2 + \sigma_2^2 + \cdots + \sigma_n^2 = n\sigma^2}$，即$\boldsymbol{x \in N(n\mu, n\sigma^2)}$。

三. 正态分布N(0, 1)的产生

于是正态分布可以由多个**U(0,1)**来近似

对于$\boldsymbol{Y} \in \boldsymbol{U}(\mathbf{0}, \mathbf{1})$来说，有

$$\boldsymbol{\mu_y} = \frac{\mathbf{1}}{\mathbf{2}}$$

且

$$\boldsymbol{\sigma_y^2} = \boldsymbol{E}\left(\boldsymbol{Y}^2\right) - \left(\boldsymbol{E}(\boldsymbol{Y})\right)^2 = \int_{-\infty}^{+\infty} \boldsymbol{f}(\boldsymbol{y})\boldsymbol{d}\boldsymbol{y} - \left(\frac{\mathbf{1}}{\mathbf{2}}\right)^2$$

$$= \int_0^1 \boldsymbol{y}^2 \boldsymbol{d}\boldsymbol{y} - \frac{\mathbf{1}}{\mathbf{4}} = \frac{\boldsymbol{y}^3}{\mathbf{3}}\Big|_0^1 - \frac{\mathbf{1}}{\mathbf{4}} = \frac{\mathbf{1}}{\mathbf{12}}$$

三. 正态分布N(0, 1)的产生

令$z=\frac{x-\mu_x}{\sigma_x}$，则$z\in N(0,1)$

$$z=\frac{\sum y_i-\mu_x}{\sigma_x}=\frac{\sum y_i-n\mu_y}{\sqrt{n\sigma_y^2}}=\frac{\sum y_i-\frac{n}{2}}{\sqrt{{}^{n}\!/_{12}}}$$

三. 正态分布N(0, 1)的产生

一般n取12，则

$$z=\sum_{i=1}^{12} y_i-6\in N(0,1)$$

若想产生服从一般正态分布$N(\mu,\sigma^2)$的随机数x，则只需产生$z\in N(0,1)$，再按公式$x=\mu+\sigma z$，即可获得$x\in N(\mu,\sigma^2)$

四. 逆变法与其它分布随机数的产生

基本原理：设$\boldsymbol{Y}$是$(\mathbf{0},\mathbf{1})$上均匀分布随机变量，$\boldsymbol{F}$为任意一个连续分布函数，定义随机变量$\boldsymbol{X}=\boldsymbol{F}^{-\mathbf{1}}(\boldsymbol{Y})$，则$\boldsymbol{X}$具有分布函数$\boldsymbol{F}$。

四. 逆变法与其它分布随机数的产生

证明：

$$F_X(a)=P\{X\le a\}=P\left\{F^{-1}(Y)\le a\right\}=P\{Y\le F(a)\}$$

这里$Y\in U(0,1)$，有

$$f(y)=1,\quad F(y)=P\{Y\le y\}=\int_{-\infty}^{y}f(y)dy=y$$

故

$$F_X(a)=F(a)$$

得证。

四. 逆变法与其它分布随机数的产生

逆变法的步骤：

I. 已知 $F(x)$，或由$f(x)$求 $F(x)$，即 $F(x) = \int_{-\infty}^{x} f(x)dx$，令$y = F(x)$

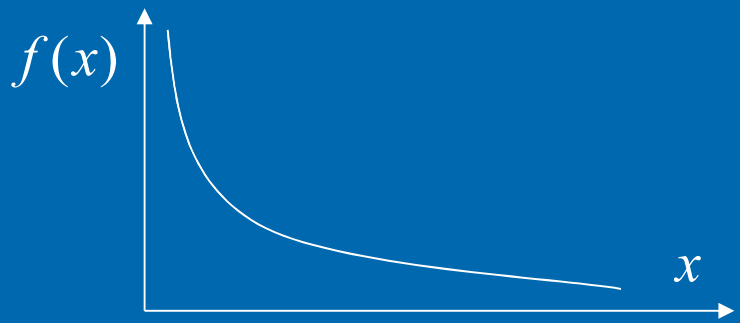
II. 推导$x = F^{-1}(y)$

III. 产生$y \in U(0,1)$

IV. 用$x = F^{-1}(y)$得到$x_0, x_1, x_2, \dots, x_{i-1}, x_i$

四. 逆变法与其它分布随机数的产生

举例：负指数分布的产生



负指数函数的密度函数：

$$f(x) = \lambda e^{-\lambda x} (x \geq 0)$$

四. 逆变法与其它分布随机数的产生

推导过程：

① $F(x)=\int_0^x \lambda e^{-\lambda x}dx=-\frac{\lambda}{\lambda}e^{-\lambda x}\Big|_0^x=1-e^{-\lambda x}$

令$y=F(x)$

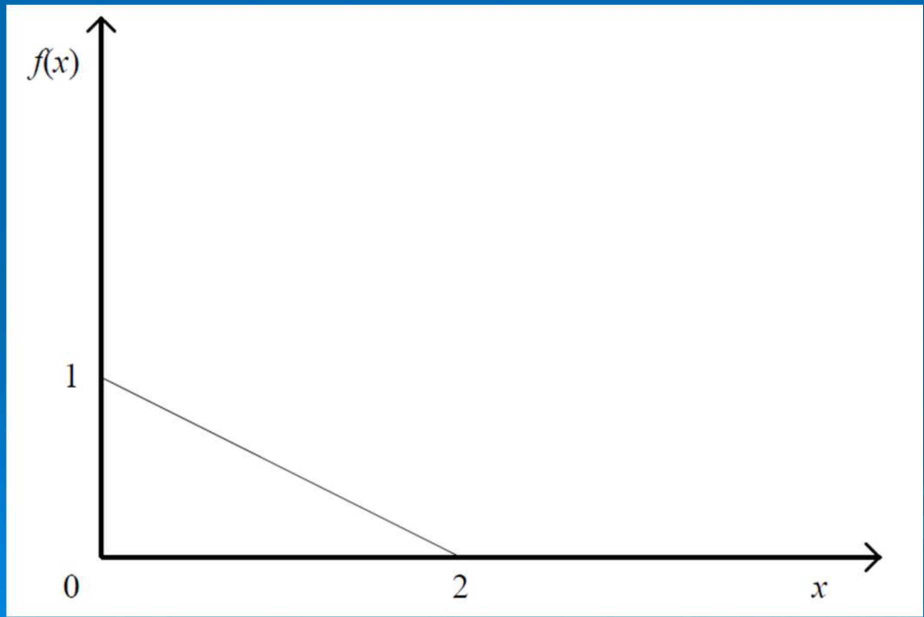
② $F^{-1}(y)=-\frac{1}{\lambda}\ln(1-y)$， $u=1-y$

③ 产生$y\in U(0,1)$，则$u\in U(0,1)$

④ $F^{-1}(y)=-\frac{1}{\lambda}\ln u$，即$x=-\frac{1}{\lambda}\ln u$

四. 逆变法与其它分布随机数的产生

思考：某随机变量的概率密度函数$f(x)$如下图所示，利用逆变法产生符合该分布的伪随机数。



思考题

若某离散随机变量X的概率分布函数为：

$$P\{X=0\}=p，\quad P\{X=1\}=1-p$$

则如何产生符合该分布的伪随机数？

若X的概率分布函数为：

$$P\{X=x_i\}=p_i，\quad i=1,2,\ldots,n-1$$

$$P\{X=x_n\}=1-\sum_{i=1}^{n-1}p_i$$

则如何产生符合该分布的伪随机数？