第2章随机数的产生和检验

- **2.1** 随机数产生器
- **2.2** 均匀随机数的产生和检验
- **2.3** 非均匀随机数的产生
- **2.4** 随机向量的产生

2.1 随机数产生器

- 使用随机性

- 抛硬币
- 彩票
- 网络信息或信用卡信息需要通过安全确认，随机数就被用来形成加密密钥
- 随机数也可以用来**模拟**真实世界的现象。例如，经营自动取款机网络的银行设计的软件，常常通过随机时间随机取款机来模拟客户访问自己的帐户来测试软件的功能。
- 蒙特卡罗算法

2.1 随机数产生器

设随机变量X有分布函数$F(x)$，

$\{X_i, i=1,2,\ldots\}$独立同分布$F(x)$，

则$\{X_i, i=1,2,\ldots\}$的一次观测的数值 $\{x_i, i=1,2,\ldots\}$

称为分布$F(x)$的随机数序列， 简称**随机数**。

- 需要某种分布的随机数时，一般先生成**均匀分布**随机数，
- 然后由均匀分布随机数再转换得到**其它分布**的随机数。
- 产生均匀分布随机数的算法叫做**均匀分布随机数发生器**。

2.1 随机数产生器

- 均匀分布随机数发生器生成的是{0,1,…,M}或{1,2,…,M} 上离散取值的**离散均匀分布**，然后除以M或M+1变成[0,1]内的值当作连续型均匀分布随机数，
- 实际上是只取了有限个值。
- 因为取值个数有限， 根据算法可知序列一定在某个时间发生**重复**， 使得序列发生重复的间隔T叫做随机数发生器的周期。
- 好的随机数发生器可以保证M很大而且周期很长。

2.1 随机数产生器

- 随机数检验的意义

- 有意识地写上0和1组成的序列?
- 自然现象极有可能产生真正的随机数序列
- 无理数π给出的数字是否形成一个随机序列?

2.1 随机数产生器

- 平方取中法
- 假设我们想产生一个**8位数**的随机序列，
- 先给定一个初始值X_0，
- 下一个随机数X_1取自X_0^2的中间八位数。
- 例如， 给定$X_0 = 35385906$，
- 这时$X_0^2 = 1252162343440836$，
- 去掉其首尾各4位数，得到下一个数
- $X_1 = 16234344$。
- 这样重复做几次，就得到一系列数。

2.2 均匀随机数的产生和检验

2.2.1 线性同余发生器(LCG)

2.2.2 混合同余发生器

2.2.3 乘同余法

2.2.4 FSR发生器

2.2.5 组合发生器法

2.2.6 随机数的检验

2.2.1 线性同余发生器

- 定义 (同余)

  设i,j为整数，M为正整数，

  若j-i为M的倍数，

  则称i与j关于模M**同余**，记为 $i \equiv j(\mathrm{mod} M)$

  否则称i与j关于M不同余。

2.2.1 线性同余发生器

例5.1

$$11 \equiv 1 (\mathrm{mod}\ \mathit{10})$$
$$1 \equiv 11 (\mathrm{mod}\ \mathit{10})$$
$$-9 \equiv 1 (\mathrm{mod}\ \mathit{10})$$

2.2.1 线性同余发生器

- 同余性质：

1 对称性：$i \equiv j(\mathrm{mod}M) \Leftrightarrow j \equiv i(\mathrm{mod}M)$

2 传递性：若 $i \equiv j(\mathrm{mod}M), j \equiv k(\mathrm{mod}M)$

则 $i \equiv k(\mathrm{mod}M)$

3 若 $i_1 \equiv j_1(\mathrm{mod}M), i_2 \equiv j_2(\mathrm{mod}M)$

则 $i_1 \pm i_2 \equiv j_1 \pm j_2(\mathrm{mod}\ M)$

$i_1 i_2 \equiv j_1 j_2(\mathrm{mod}\ M)$

2.2.1 线性同余发生器

- 同余性质：

4 若 $ik \equiv jk(\mathrm{mod}M)$ (k为正整数)，
则

$$i \equiv j\left(\mathrm{mod}\,\frac{M}{gcd(M,k)}\right)$$

其中 gcd(M,k)表示M和k的最大公约数

2.2.1 线性同余发生器

- **线性同余随机数发生器**是利用求余运算的随机数发生器。 其递推公式为

$$x_n = (ax_{n-1} + c)(\text{mod } M),\ n = 1,2,\ldots$$

$$R_n = \frac{x_n}{M}$$

- 正整数M为除数
- 正整数a为乘数
- 非负整数c为增量

2.2.1 线性同余发生器

- 如果取c=0， 称为乘同余发生器
- 如果取c>0， 称为混合同余发生器

2.2.1 线性同余发生器

- 若存在正整数n和m使得 $x_n=x_m(m<n)$，则必有$x_{n+k}=x_{m+k}, k=0,1,2,\ldots,$
- 即$x_n, x_{n+1}, x_{n+2}, \cdots$ 重复了$x_m, x_{m+1}, x_{m+2}, \cdots$，称这样的n−m的最小值T为此**随机数发生器在初值x_0下的周期**。
- 由序列取值的有限性可见$T \le M$

2.2.1 线性同余发生器

例5.2 考虑线性同余发生器

$$x_n = 7x_{n-1} + 7(\text{mod } 10)$$

- 取初值x_0=7,
- 数列为: (7, 6, 9, 0, 7, 6, 9, 0, 7,…),
- 周期为T=4 < M=10。

2.2.1 线性同余发生器

例5.3 考虑线性同余发生器

$$x_n = 5x_{n-1} + 1(\text{mod } 10)$$

- 取初值x_0=1。
- 数列为: (1, 6, 1, 6, 1, …)
- 周期T=2

2.2.1 线性同余发生器

例5.4 考虑线性同余发生器

$$x_n = 5x_{n-1} + 1 \pmod 8$$

- 取初值x_0=1
- 数列为(1, 6, 7, 4, 5, 2, 3, 0, 1, 6, 7,…)
- 周期T=8=M达最大周期（**满周期**）。

2.2.2 混合同余发生器

- 线性同余发生器中c>0时称为**混合同余发生器**
- **定理5.1** (混合同余发生器达到满周期的一个充分条件)当下列三个条件都满足时，混合同余发生器可以达到满周期:

  1, c与M互素;

  2,对M的任一个素因子P，a-1被P整除;

  3, 如果4是M的因子，则a-1被4整除。

2.2.2 混合同余发生器

X_n的统计性质：

$$EX_n = \sum_{i=0}^{M-1} i \cdot \frac{1}{M} = (M-1)/2$$

$$\mathrm{Var}(X_n) = EX_n^2 - (EX_n)^2$$

$$= \sum_{i=0}^{M-1} i^2 \frac{1}{M} - \frac{(M-1)^2}{4} = \frac{1}{12}(M^2-1)$$

2.2.2 混合同余发生器

于是当M很大时，

R_n的统计性质

$$ER_n = \frac{1}{2} - \frac{1}{2M} \approx \frac{1}{2}$$

$$Var(R_n) = \frac{1}{12} - \frac{1}{12M^2} \approx \frac{1}{12}$$

- 说明M充分大时，生成的数列R_n很接近于均匀分布

- 满周期的混合同余发生器序列中前后两项自相关系数的近似公式

$$\rho(1) \approx \frac{1}{a} - \frac{6c}{aM}\left(1 - \frac{c}{M}\right)$$

- 应该选a值大(但a<M)

2.2.2 混合同余发生器

例5.5 Kobayashi提出了如下的满周期2^{31}的混合同余发生器

$$x_n = (314159269x_{n-1} + 453806245)(\mathrm{mod}\ 2^{31})$$

- 其周期较长，统计性质比较好

2.2.3 乘同余法

- 线性同余发生器中c=0时的生成方法称为**乘同余法**，或称积式发生器。
- 这时的递推公式为

$$x_n = a x_{n-1} (\bmod\ M),\ n = 1,2,\ldots$$

$$R_n = \frac{x_n}{M}$$

- 乘同余法能够达到的最大周期是M−1
- 每个x_n都只在{**1,2,…,M−1**}中取值。

2.2.3 乘同余法

- 定义5.2 (阶数) 设正整数a与正整数M互素，称满足 $a^V \equiv 1 \pmod{M}$

的最小正整数V为a对模M 的阶数(或次数)，简称为**a的阶数**。

Lemma 5.1 设a与M互素，初值x_0与M互素，则乘同余法的周期为a对模M的阶数V

2.2.3 乘同余法

- 当M充分大时可以类似得到

$$ER_n \approx \frac{1}{2}, \quad Var(R_n) \approx \frac{1}{12}.$$

为了使得前后两项的相关系数较小， 应取

- a较大且
- 使得a的二进制表示排列无规律。

2.2.3 乘同余法

例5.6 考虑如下乘同余发生器

$$
\begin{aligned}
x_n &= (8\alpha+5)x_{n-1}(\mathrm{mod}\ 2^L) \\
x_0 &= 4b+1
\end{aligned}
$$

再考虑如下的混合同余发生器

$$
\begin{aligned}
x_n^* &= \left((8\alpha+5)x_{n-1}^* + (2\alpha+1) \quad (\mathrm{mod}\ 2^{L-2}\right) \\
x_0^* &= b
\end{aligned}
$$

则 $x_n = 4x_n^* + 1, n = 0,1,2,\ldots$

2.2.4 FSR发生器

线性同余法

- 周期不可能超过2^L(L为整数型尾数的位数),

- 作为**多维**随机数相关性大
- 分布不均匀

- 基于Tausworthe(1965)文章的FSR方法是一种全新的做法， 对这些方面有改善。

2.2.4 FSR发生器

- FSR(Feedback Shift Register，反馈位移寄存器法)按照某种递推法则生成一系列二进制数

$\alpha_1, \alpha_2, \ldots, \alpha_k, \ldots$

- 其中 α_k 由前面的若干个 $\{\alpha_i\}$ 线性组合并求除以2的余数产生：

$$\alpha_k = (c_p\alpha_{k-p} + c_{p-1}\alpha_{k-p+1} + \cdots + c_1\alpha_{k-1}) (\mathrm{mod}\ 2),$$
$$k = 1,2, \ldots$$

线性组合系数 $\{c_i\}$ 只取0, 1，这样的递推可以利用程序语言中的整数二进制运算快速实现。

2.2.4 FSR发生器

给定初值$\left(\alpha_{-p+1}, \alpha_{-p+2}, \ldots, \alpha_0\right)$向前递推，

得到$\{\alpha_k, k=1,2,\ldots\}$序列后依次截取长度为L的二进制位组合成整数$x_n$，

取 $R_n = x_n/2^L$。

2.2.4 FSR发生器

- FSR算法中系数($c_1,c_2,\ldots,c_p$)如果仅有两个为1， 比如$c_p=c_{p-q}=1(1<q<p)$, 则算法变成

$$a_k = (a_{k-p} + a_{k-p+q}) \pmod 2$$

$$= \begin{cases} 0 & 若 a_{k-p} = a_{k-p+q} \\ 1 & 若 a_{k-p} \neq a_{k-p+q} \end{cases}$$

2.2.5 组合发生器法

例5.10 Wichmann和Hill（1982）设计了如下的线性组合发生器。

利用三个16位运算的素数模乘同余发生器:

$$
\begin{aligned}
U_n &= 171U_{n-1} \pmod{30269} \\
V_n &= 172V_{n-1} \pmod{30307} \\
W_n &= 170W_{n-1} \pmod{30323}
\end{aligned}
$$

作线性组合并求余:

$$R_n = (U_n/30269 + V_n/30307 + W_n/30323) \pmod 1$$

2.2.5 组合发生器法

例5.11 MacLaren和Marsaglia(1965)

- 组合两个同余发生器，一个用来“搅乱”次序。
- 设有两个同余发生器A和B。
- 用A产生m个随机数(如m=128)， 存放在数组$T=(t_1,t_2,\ldots,t_m)$.
- 需要产生x_n时，从B中生成一个随机下标$j\in\{1,2,\ldots,m\}$， 取$x_n=t_j$， 但从A再生成一个新随机数y代替T中的t_j, 如此重复。
- 这样组合可以增强随机性，加大周期(可超过2L)。 也可以只使用一个发生器，用x_{n-1}来选择下标。

2.2.6 随机数的检验

- **理论检验**

  不必产生任何随机数

- **经验检验**

  以发生器产生的均匀随机数列为基础的

  1，参数检验

  2，均匀性检验

  3，独立性检验

  4，组合规律检验

2.2.6 随机数的检验

1 对随机数列$\{R_n, n = 1,2,\ldots,N\}$
计算

$$\bar{R} = \frac{1}{N}\sum_{n=1}^{N} R_n,\ \overline{R^2} = \frac{1}{N}\sum_{n=1}^{N} R_n^2,\ S^2 = \frac{1}{N}\sum_{n=1}^{N}\left(R_n - \frac{1}{2}\right)^2$$

则N→∞时 $\bar{R}, \overline{R^2}$ 和S^2均渐近服从正态分布，可以用Z检验法检验这三个统计量与理论期望值的偏离程度。

Z检验法

在原假设$H_0: E\bar{R}=\frac{1}{2}$下，$u_1=\frac{\bar{R}-\frac{1}{2}}{\sqrt{\frac{1}{12N}}}\sim N(0,1)$

在原假设$H_0: E\bar{R}^2=\frac{1}{3}$下，$u_2=\frac{\bar{R}^2-\frac{1}{3}}{\sqrt{\frac{4}{45N}}}\sim N(0,1)$

在原假设$H_0: ES^2=\frac{1}{12}$下，$u_3=\frac{S^2-\frac{1}{12}}{\sqrt{\frac{1}{180N}}}\sim N(0,1)$

2.2.6 随机数的检验

2 把[0,1]等分成k段，用拟合优度卡方检验法检验 $\{R_n, n = 1,2,\ldots,N\}$

落在每一段的取值概率是否近似为1/k。

2.2.6 随机数的检验

3 用Kolmogorov-Smirnov检验法进行拟合优度检验， 看 $\{R_n, n = 1,2,\ldots,N\}$ 是否与U[0,1]分布相符。

2.2.6 随机数的检验

4 把 $\{R_n, n = 1,2,\ldots,N\}$

每d个组合在一起成为R^d向量， 把超立方体$[0,1]^d$每一维均分为k份，得到k^d个子集， 用卡方检验法检验组合得到的R^d向量落在每个子集的概率是否近似为k^{-d} 。

2.2.6 随机数的检验

5 把 $\{R_n, n = 1,2,\ldots,N\}$ 看作时间序列样本，计算其样本自相关函数列

$$\{\hat{\rho}_j, j = 1,2,\ldots\}$$

在 $\{R_n, n = 1,2,\ldots,N\}$ 独立同分布情况下

$$\{\sqrt{N}\hat{\rho}_j, j = 1,2,\ldots,N\}$$

应该渐近服从独立的标准正态分布， 可以据此进行白噪声检验。

2.2.6 随机数的检验

6 把 $\{R_n, n = 1,2,\dots,N\}$ 离散化为

$$y_n = floor(kR_n), n = 1,2,\dots,N$$

令 $\xi_n = y_n, \eta_n = y_{n+b}$

其中b为正整数, n=1,2,..., N-b,

用列联表检验法检验 ξ_n, η_n 的独立性。

2.2.6 随机数的检验

7 游程检验

- 把序列 $\{R_n, n = 1,2, \dots, N\}$ 按顺序切分为不同段，
- 每一段中的数值都是递增的，这样的一段叫做一个上升游程，
- 如(0.8555), (0.108, 0.226), (0.108, 0.226),(0.055, 0.545, 0.642, 0.870) ,... 。

2.2.6 随机数的检验

7 游程检验

- 在相邻的两个上升游程中前一个游程的最后一个值大于后一个游程的第一个值。
- 在 $\{R_n, n = 1,2,\dots,N\}$ 独立同分布条件下游程长度的理论分布可以得知，
- 然后可以比较实际游程长度与独立同分布条件下期望长度

2.2.6 随机数的检验

8 扑克检验

- 把 $\{R_n, n = 1,2,\ldots,N\}$ 离散化为

$$y_n = floor(kR_n), n = 1,2,\ldots,N$$

- 然后每连续的8个作为一组， 计数每组内不同数字的个数（1-8个）。
- 在R_n同均匀分布条件下每组内不同数字个数的理论分布概率可以计算出来，
- 然后用卡方检验法检验实际观测与理论概率是否相符。

2.2.6 随机数的检验

9 配套检验

- { R_n }离散化为 $y_n = floor(kR_n)$ (k为正整数), n=1,2,…, N,
- 然后顺序抽取 $\{y_n, n = 1,2, \ldots, N\}$
- 直到{y_n}的可能取值{0,1,…,k-1}都出现过为止，
- 记录需要抽取的{y_n}的个数L， 反复抽取并记录配齐数字需要抽取的值的个数l_j, j=1,2,…

2.2.6 随机数的检验

9 配套检验

- 在{ R_n }独立同U(0,1)分布条件下这样的L分布可以得到，
- 可以计算{l_j}的平均值并用渐近正态分布检验观测均值与理论均值的差异大小，
- 或直接用卡方检验法比较{l_j}的样本频数与理论期望值。

2.2.6 随机数的检验

10 正负连检验

令$y_n = R_n - \frac{1}{2}$

把连续的$\{y_n\}$的负值分为一段， 每段叫做一个“连”， 连长L的分布概率为

$$P(L=k)=2^{-k}, k=1,2,\ldots$$

可以用卡方检验法检验L的分布；

总连数T满足 $ET=\frac{n+1}{2}, Var(T)=\frac{n-1}{4}$

可以用Z检验法检验T的值与理论期望的差距。

2.2.6 随机数的检验

11 升降连检验

- 计算 $y_n = R_n - R_{n-1}, n = 2,3,\dots,N$
- 把连续的正值的$\{y_n\}$分为一段叫做一个上升连，
- 把连续的负值的$\{y_n\}$分为一段叫做一个下降连，
- 可以用卡方检验法比较连的长度与 $\{R_n\}$独立同分布假设下的理论分布，
- 或用Z检验法比较总连数与理论期望值的差距。

2.3 非均匀随机数的产生

2.3.1 逆变换法

2.3.2 用逆变换法生成离散型随机数

2.3.3 用逆变换法生成连续型随机数

2.3.4 利用变换生成随机数

2.3.5 舍选法

2.3.6 复合法

2.3.1 逆变换法(The Inverse Transform Method)

定理6.1 X为**连续型**随机变量，取值于区间(a,b)(可包括$\pm\infty$和端点), X的密度在(a,b)上取正值，X的分布函数为F(x)，$U \sim$ U(0,1)，

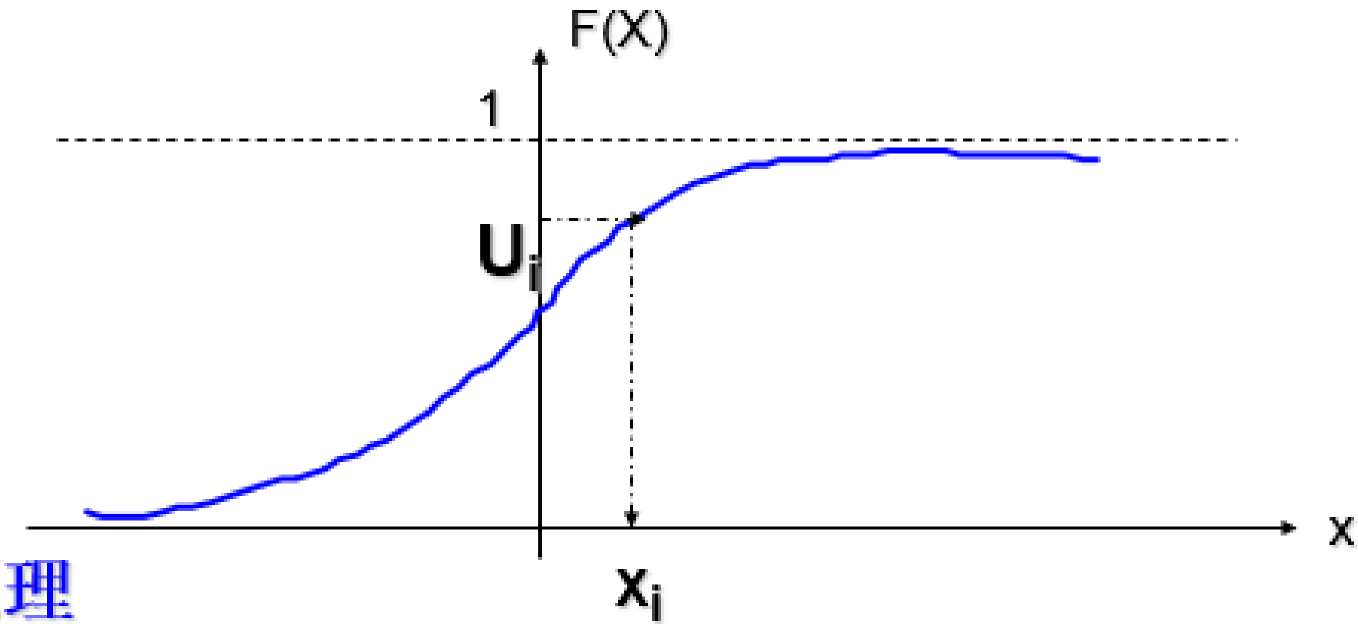
则$Y = F^{-1}(U) \sim F(\cdot)$。

定理6.2 设X为**离散型**随机变量, 取值于集合$\{a_1, a_2, \ldots\}$($a_1 < a_2 < \cdots$)，F(x)为X的分布函数，$U \sim$ U(0,1)， 根据U的值定义随机变量Y为

$$Y = \quad a_i \text{ 当且仅当 } F(a_{i-1}) < U \leq F(a_i),\ i = 1,2, \ldots$$

(定义$F(a_0) = 0$) 则$Y \sim F(y)$

2.3.1 逆变换法



原理

纵坐标表示累计分布值，范围[0,1)。利用随机数发生器产生[0,1)间均匀分布的随机数，相当于在纵坐标上随机地找到一个点U_i，从这一点利用反函数就可以求得该分布在这一点上的随机变量X_i。

2.3.2 用逆变换法生成离散型随机数

模拟分布列为：

$$p_1 = 0.20, p_2 = 0.15, p_3 = 0.25, p_4 = 0.40$$

的随机变量X(其中$P_j = P\{X = j\}$)

法1 (自然顺序)

- 如果U ≤ 0.20,则令X = 1且停止
- 如果U ≤ 0.35=0.2+0.15,则令X = 2且停止
- 如果U ≤ 0.60=0.2+0.15+0.25,则令X = 3且停止
- 否则令X = 4.

法2 (P_j从大到小排序)

- 如果U $\leq$ 0.40,则令X=4且停止
- 如果U $\leq$ 0.65,则令X=3且停止
- 如果U $\leq$ 0.85,则令X =1且停止
- 否则令X=2.

2.3.2 用逆变换法生成离散型随机数

例6.1 (离散均匀分布)

如果随机变量X在{1,2,…,m }中取值且

$$P(X=i)=\frac{1}{m}, i=1,2,\dots,m$$

则称X服从**离散均匀分布**

由于$X=j \quad \left(\text{if} \quad \frac{j-1}{m}<U\le\frac{j}{m}\right)$

即$X=j \quad (\text{if} \quad j-1<mU\le j)$

则$X=Int(mU)+1$

其中Int(x)表示取整，不大于x的最大整数

2.3.2 用逆变换法生成离散型随机数

例6.3 (无放回抽样) 生成（1,2,3，…，n）的一个随机排列。

生成随机排列的**步骤**:

- 步骤1:设$P_1, P_2, ... P_n$是1,2,...,n的任一排列
- 步骤2:令k=n.
- 步骤3:生成一随机数U,并设I=Int(kU)+1.
- 步骤4:交换P_I和P_k.
- 步骤5:令k=k-1,如果k>1,则转至步骤3.
- 步骤6:$P_1, P_2, ... P_n$为所求的随机排列.

2.3.2 用逆变换法生成离散型随机数

例6.4 (几何分布随机数)

设随机变量X表示在成功概率为p(0<p<1)的独立重复试验中首次成功所需的试验次数，则X的概率分布为

$$P(X=k)=pq^{k-1}, k=1,2,\ldots,\ (q=1-p)$$

称X服从几何分布，记为

$$X\sim Geom(p)$$

2.3.2 用逆变换法生成离散型随机数

例6.4 (几何分布随机数)

分布函数 $F(k) = 1 - q^k,\ k = 1,2,\ldots$

令 $U \sim U(0,1)$

生成X的方法为当且仅当 $1 - q^{k-1} < U \leq 1 - q^k$

时取X=k， k=1,2, ...。

此条件等价于 $q^k \leq 1 - U < q^{k-1}$

2.3.2 用逆变换法生成离散型随机数

例6.4 (几何分布随机数)

$$
\begin{aligned}
X &= \min\{k: q^k \le 1 - U\} \\
&= \min\{k: k\log(q) \le \log(1-U)\} \\
&= \min\left\{k: k \ge \frac{\log(1-U)}{\log(q)}\right\} \\
&= ceil\left(\frac{\log(1-U)}{\log(q)}\right)
\end{aligned}
$$

在没有指定底数时，log默认使用自然对数。 注意到1-U也是服从U(0,1)分布的，所以只要取

$$X = ceil\left(\frac{\ln(U)}{\ln(q)}\right)$$

2.3.2 用逆变换法生成离散型随机数

例6.5 (生成独立试验序列)

产生$X_1,X_2,\ldots,X_N$ iid **b(1,p)**， 即

$$P(X_i = 1) = p = 1 - P(X_i = 0),\ i = 1,2,\ldots,N$$

法1： 设$(U_1,U_2,\ldots,U_N)$ iid U(0,1),

则当$U_i \le p$时取$X_i=1$,

当$U_i > p$时取$X_i=0$

可以构造独立试验序列$(X_1,X_2,\ldots,X_N)$

2.3.2 用逆变换法生成离散型随机数

例6.5 (生成独立试验序列)

产生$X_1,X_2,\dots,X_N$ iid **b(1,p)**，即

$$P(X_i = 1) = p = 1 - P(X_i = 0), \ i = 1,2,\dots,N$$

法2：用几何分布当p比较小时

- 生成首次成功时间，则在成功之前的试验都是失败，
- 然后再生成下次成功时间，两次成功之间的试验为失败，
- 一直到凑够N次试验为止。

2.3.2 用逆变换法生成离散型随机数

例6.5 (生成独立试验序列)

```
rbernoulli.geom <- function(size=1, prob=0.1){
 x <- numeric(size)
 k <- 0
 while(k <= size){
   T <- rgeom(1, prob=prob)
   if(T > 1){
     x[(k+1):(min(c(k+T-1, size)))] <- 0
   }
   if(k+T <= size) x[k+T] <- 1
   k <- k+T
 }
   x
}
```

2.3.2 用逆变换法生成离散型随机数

例6.6 (二项分布随机数)

设p为成功的概率, 做n次的独立重复试验，X为n次试验中成功的次数， 则

$$p_k = P(X = k) = \binom{n}{k} p^k (1-p)^{n-k},$$

$$k = 0,1,\dots,n \, (0 < p < 1)$$

称X服从二项分布，记为X~B(n,p)

2.3.2 用逆变换法生成离散型随机数

例6.6 (二项分布随机数)

设法用定理6.2构造二项分布随机数。

二项分布取值概率有如下递推式:

$$p_{k+1} = \frac{n-k}{k+1}\frac{p}{1-p}p_k,\ k = 0,1,\dots,n-1$$

故利用定理6.2构造二项分布随机数时， 可以递推计算

$$F(k+1) = F(k) + p_{k+1} = F(k) + \frac{n-k}{k+1}\frac{p}{1-p}p_k,\ k = 0,1,\dots,n-1$$

2.3.2 用逆变换法生成离散型随机数

例6.6 (二项分布随机数)

步骤1:生成一个随机数U.

步骤2:$c=p/(1-p), i=0, a=(1-p)^n, F=a$.

步骤3:如果$U<F$,令$X=i$并停止.

步骤4:$a=(c(n-i)/(i+1)a, F=F+a, i=i+1$.

步骤5:转至步骤3.

当np较大时，令$K=\text{floor}(np)$，应先判断要生成的随机变量X是小于等于K还是大于K。先计算出$F(K)$。

1. 当$U \le F(K)$时，X取值小于等于K，这时可依次判断X是否应取$K, K-1, \ldots, 0$，在这个过程中可以反向递推计算各个$F(k)$的值。
2. 当$U > F(K)$时，X取值大于K，这时可依次判断X是否应取$K+1, K+2, \ldots, n$，在这个过程中可以递推计算各个F(k)的值。

2.3.2 用逆变换法生成离散型随机数

例6.7 (泊松分布随机数)

设离散型随机变量X分布为

$$p_k = P(X = k) = e^{-\lambda}\frac{\lambda^k}{k!}, k = 0,1,2,\ldots(\lambda > 0)$$

称X服从泊松分布，记为X~ Poisson(λ)

2.3.2 用逆变换法生成离散型随机数

例6.7 (泊松分布随机数)

$$p_{k+1} = \frac{\lambda}{k+1} p_k, \; k = 0,1,2,\ldots$$

用定理6.2构造泊松随机数时， 可以递推计算

$$F(k+1) = F(k) + p_{k+1} = F(k) + \frac{\lambda}{k+1} p_k, \; k = 0,1,2,\ldots$$

2.3.2 用逆变换法生成离散型随机数

例6.7 (泊松分布随机数)

步骤1:生成一个随机数U.

步骤2:$i=0, p=e^{-\lambda}, F=p$.

步骤3:如果$U<F$,取$X=i$且停止.

步骤4:$p=\lambda p/(i+1), F=F+p, i=i+1$.

步骤5:转向步骤3.

如果λ比较大，令$K =$ Į→╗(λ),

先递推计算出$F(K)$和$F(K+1)$，然后判断$F(K) < U \leq F(K+1)$是否成立，

1. 如果成立就令$X = K + 1$;
2. 如果$U \leq F(K)$则依次判断是否应取X为$K, K-1, \ldots, 0$，在这个过程中可以反向递推计算各$F(k)$；
3. 如果$U > F(K+1)$则依次判断是否应取X为$K+2, K+3, \ldots$，这个过程中仍然用递推计算各$F(k)$。

2.3.3 用逆变换法生成连续型随机数

- 对于反函数F^{-1}容易计算的情形， 逆变换法是最方便的。
- **例** 产生[a,b]上均匀分布的随机数。
- 如果U服从标准均匀分布U(0,1),
- 则$X=a+(b-a)U$服从U(a,b)

2.3.3 用逆变换法生成连续型随机数

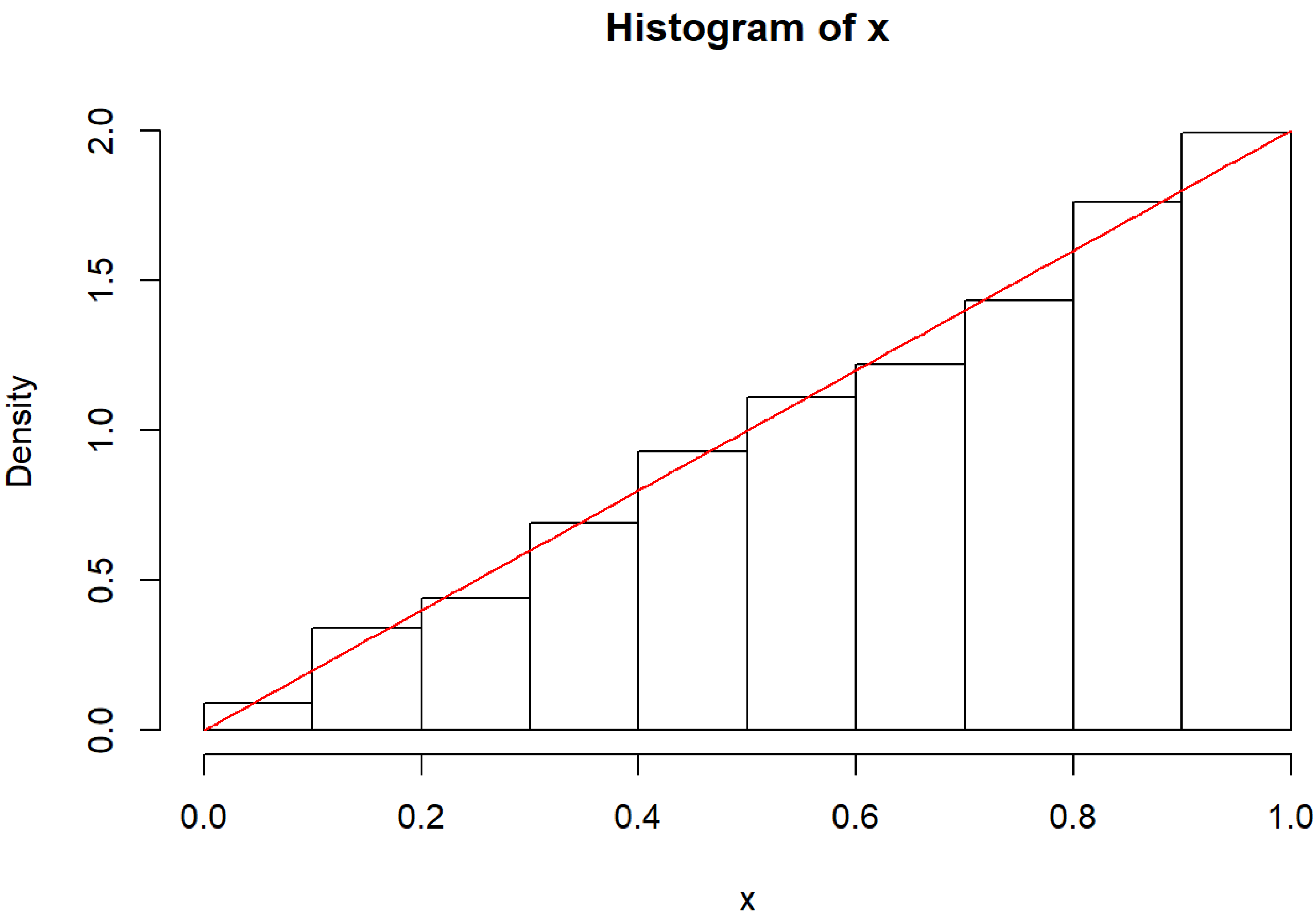
例6.8 (右三角形分布)

Beta(2,1)分布的分布密度和分布函数分别为

$$p(x) = \quad 2x, x \in [0,1] \quad F(x) = \quad x^2, x \in [0,1]$$

- 密度函数为三角形
- 若U~U(0,1)，则$X = \sqrt{U}$

为**Beta(2,1)**随机数


Histogram of x
Density
x
0.0
0.5
1.0
1.5
2.0
0.0
0.2
0.4
0.6
0.8
1.0

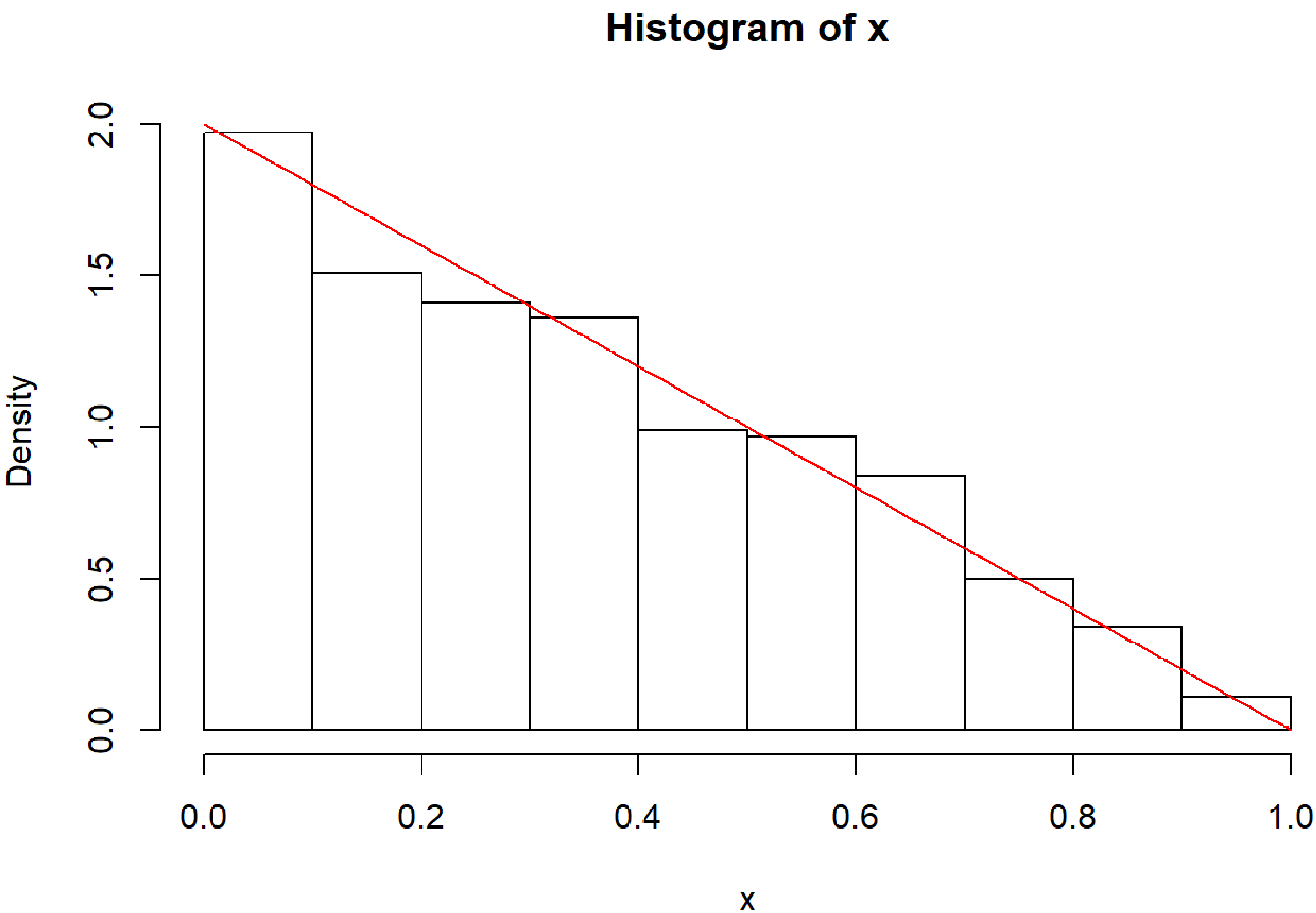
2.3.3 用逆变换法生成连续型随机数

例6.8 (左三角形分布)

Beta(1,2)分布的分布密度和分布函数分别为

$$p(x) = 2(1-x), x \in [0,1] \quad F(x) = 1-(1-x)^2, x \in [0,1]$$

- 密度函数为三角形
- 若U~U(0,1)， 则 $X = 1 - \sqrt{1-U}$ 为Beta(1,2)随机数
- 因为U与1−U同分布所以 $X = 1 - \sqrt{U}$ 也是Beta(1,2)随机数。



Histogram of x
Density
x
0.0
0.5
1.0
1.5
2.0
0.0
0.2
0.4
0.6
0.8
1.0

2.3.3 用逆变换法生成连续型随机数

例6.9 (指数分布随机数)

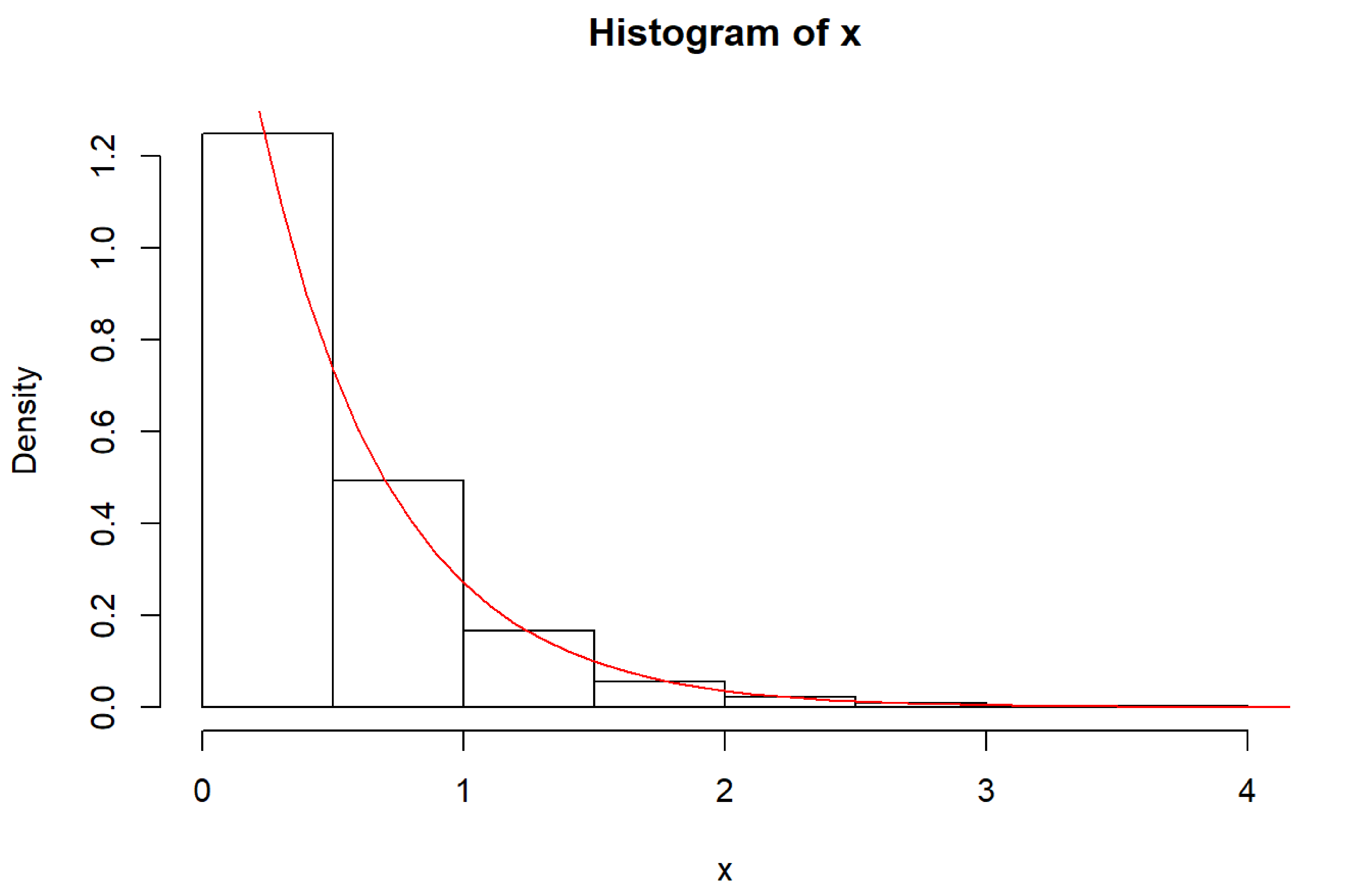
服从指数分布Exp(λ) (λ>0)的随机变量X的分布密度和分布函数分别为

$$p(x) = \lambda e^{-\lambda x},\ x > 0$$
$$F(x) = 1 - e^{-\lambda x},\ x > 0.$$

反函数为

$$F^{-1}(u) = -\lambda^{-1}\log(1-u)$$

- 以U~U(0,1)时$X=-\lambda^{-1}\log(1-U)$服从Exp(λ)


Histogram of x
Density
0.0
0.2
0.4
0.6
0.8
1.0
1.2
0
1
2
3
4
x

2.3.3 用逆变换法生成连续型随机数

例6.10 (利用指数分布随机数产生泊松随机数)

- N(t)为到时刻t为止到来的事件个数(t>=0),
- 如果两个事件到来之间的间隔都服从独立的Exp(λ)分布，则称N(t)为**泊松过程**

- N=N(1)称为服从参数为λ的**泊松分布**。

2.3.3用逆变换法生成连续型随机数

例6.10 (利用指数分布随机数产生泊松随机数)

若U_1, U_2 ,…是独立的U(0,1)随机变量列，
X_1, X_2 ,…是独立的Exp(λ)随机变量列，
则

$$N = \max\{n: \sum_{i=1}^{n} X_i \le 1\}$$

$$N = \max\{n: -\lambda^{-1} \sum_{i=1}^{n} \ln U_i \le 1\}$$
$$= \max\{n: U_1 U_2 \ldots U_n \ge e^{-\lambda}\}$$

2.3.3 用逆变换法生成连续型随机数

例6.10 (利用指数分布随机数产生泊松随机数)

- 生成泊松随机数：
- 相继生成均匀随机数，
- 直至其连乘积小于$e^{-\lambda}$,
- 则取n为使用的均匀随机数个数减1， 即

$$N = \min\{n : U_1 U_2 \ldots U_n < e^{-\lambda}\} - 1$$

2.3.4 利用变换生成随机数

定理6.3 设随机变量X有密度p(x)，Y=g(X)是X的函数， 函数g(.)有反函数$x = g^{-1}(y) = h(y)$, h(y)有一阶连续导数，则Y有密度

$$f(y) = p(h(y)) \cdot |h'(y)|$$

2.3.4 利用变换生成随机数

定理6.4 设随机向量(X,Y)具有联合密度函数p(x,y)，令

$$\begin{cases} u = g_1(x,y) \\ v = g_2(x,y) \end{cases}$$

设(u,v) = (g_1(x,y), g_2(x,y))的反变换存在唯一， 记为

$$\begin{cases} x = h_1(u,v) \\ y = h_2(u,v) \end{cases}$$

设h_1, h_2的一阶偏导数存在，反变换的Jacobi行列式

$$J = \begin{vmatrix} \frac{\partial x}{\partial u} & \frac{\partial x}{\partial v} \\ \frac{\partial y}{\partial u} & \frac{\partial y}{\partial v} \end{vmatrix} \neq 0$$

- 则随机向量(U,V)的联合密度为

$$f(u,v) = p(h_1(u,v), h_2(u,v)) \cdot |J|$$

2.3.4 利用变换生成随机数

有些分布之间有已知的关系，可以利用这样的关系产生随机数。如:

- 二项分布B(n, p)是n个伯努利分布b(1,p)之和，可以产生n个伯努利分布b(1,p)随机数求和得到二项分布随机数。
- 如果U服从标准均匀分布U(0,1), 则$X = a + (b - a)U$服从U(a, b)。
- 如果Z服从标准正态分布，则可以用$X = \mu + \sigma Z$服从N(μ, σ^2)分布。
- 如果Z服从标准指数分布Exp(1), 则$X = \lambda^{-1}Z$服从指数分布Exp(λ)。
- 如果Z服从标准伽马分布Gamma(α,1), 则$X = \lambda^{-1}Z$服从伽马分布Gamma(α, λ)。

2.3.4 利用变换生成随机数

定理6.5 设U_1, U_2独立且都服从U(0,1),

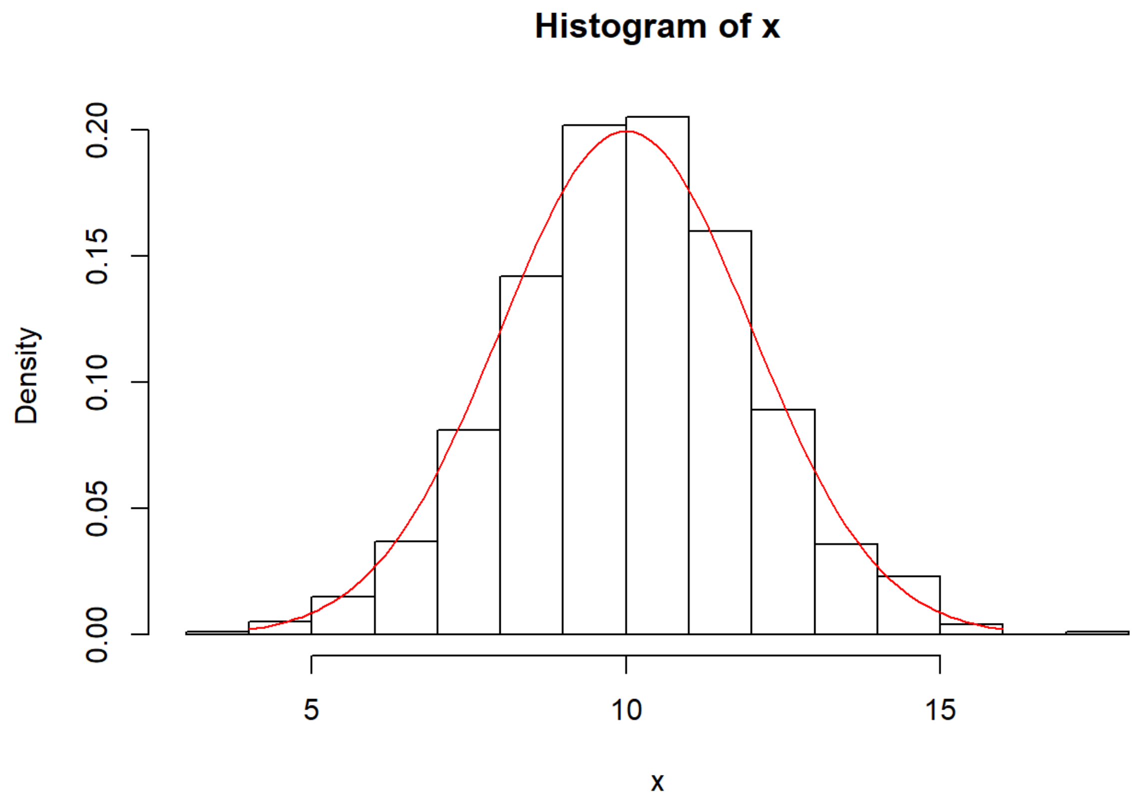
$$X = \sqrt{-2\ln U_1}\cos(2\pi U_2),$$
$$Y = \sqrt{-2\ln U_1}\sin(2\pi U_2).$$

则X, Y独立且都服从标准正态分布。

- 叫做**Box-Muller变换**。

2.3.4 利用变换生成随机数

Box-Muller变换。



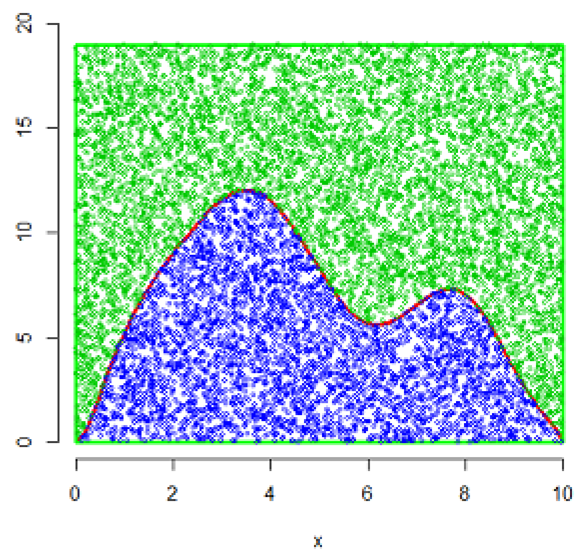
2.3.5 舍选法(The Acceptance-Rejection Method)

设随机变量Z的分布函数很难求反函数$F^{-1}(u)$。
若Z取值于有限区间[a,b]且密度函数$p(x)$有上界M

$$p(x) \le M, \forall x \in [a,b]$$

则可以用如下算法生成Z的随机数:

舍选法I
until($Y \le p(X)$){
从U(0,1)抽取U_1, U_2
取$X \leftarrow a + (b-a) * U_1$, $Y \leftarrow M * U_2$
}
输出$Z \leftarrow X$



2.3.5 舍选法I

定理6.6 舍选法I产生的Z密度为p(x)，算法所需的**迭代次数**是均值为M(b−a)的几何分布随机变量。

2.3.5 舍选法

例6.12 (用舍选法生成Beta(2,4)随机数) 用舍选法产生Beta(2,4)的随机数，密度为

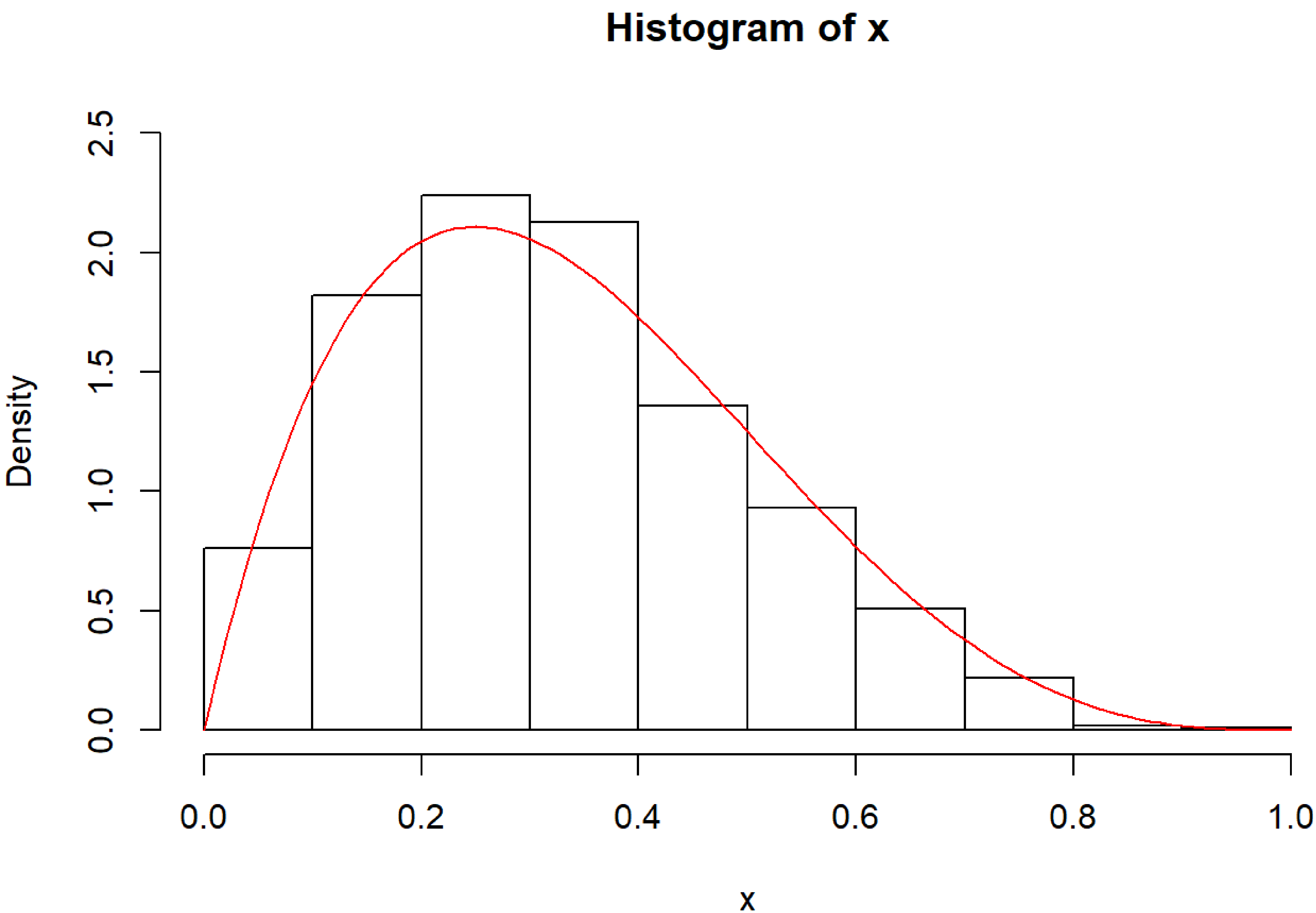
$$p(x) = 20x(1-x)^3,\ 0 < x < 1.$$

可以用舍选法I， 这时

$$M = \max_{0 \le x \le 1} p(x) = p(\frac{1}{4}) = \frac{135}{64},$$

平均迭代次数为$\frac{135}{64} \approx 2.1$。

$$
\begin{aligned}
& until(Y \le p(X) = 20x(1-x)^3)\{ \\
& \qquad \text{从}U(0,1)\text{抽取}U_1, U_2 \\
& \qquad \text{取}X \leftarrow U_1,\ Y \leftarrow \frac{135}{64} * U_2 \\
& \} \\
& \text{输出}Z \leftarrow X
\end{aligned}
$$


Histogram of x
Density
x
0.0
0.5
1.0
1.5
2.0
2.5
0.0
0.2
0.4
0.6
0.8
1.0

2.3.5 舍选法I

- **舍选法I的优点：** 只要随机变量在有限区间取值且密度函数有界就可以使用这种方法
- **舍选法I缺点**：
- 首先，X的取值范围必须有界；
- 其次，X的密度p(x)必须有界；
- 第三， 当算法中X取到p(x)值很小的位置时，被拒绝的概率很大, X被接受的概率实际是曲线p(x)下的面积和整个矩形面积之比， 当p(x)高低变化很大时这个比例很低， 算法效率很差。

2.3.5 舍选法II

- 为解决第一个和第二个问题， 抽取X时从一个一般密度g(x)抽取， 称这密度为“**试投密度**”要求g(x)的随机数容易生成。
- 为解决第三个问题， 使得g(x)形状与p(x)相像
  即p(x)大时相应g(x)也大，
  p(x)小时相应g(x)也小
  目标密度小的地方尝试抽取X也少

2.3.5 舍选法II

目标密度(要生成随机数的密度)*p*(x)可能本身是未知的， 只知道 $\tilde{p}(x) = ap(x)$

其中a为未知常数。

要求存在常数c使得

$$\frac{\tilde{p}(x)}{g(x)} \le c, \forall x$$

如果 $\tilde{p}(x)$ 在接近 $\pm\infty$ 处有定义， 需要满足

$$\tilde{p}(x) = O(g(x))(x \to \pm\infty)$$

选取试投密度*g*(.)时上述常数c越小越好

2.3.5 舍选法II

舍选法II
until $\left(Y \leq \frac{\tilde{p}(X)}{(cg(X))}\right)\{$
从$g(x)$抽取X
从U(0,1)抽取Y
$\}$
输出$Z \leftarrow X$

2.3.5 舍选法II

定理6.7 舍选法II产生的Z密度为p(x)，算法所需的迭代次数是均值为c/a的几何分布随机变量。

2.3.5 舍选法

例6.13 (用舍选法生成Gamma(3/2,1)随机数) 生成Gamma($\frac{3}{2}$, 1)的随机数Z，密度为

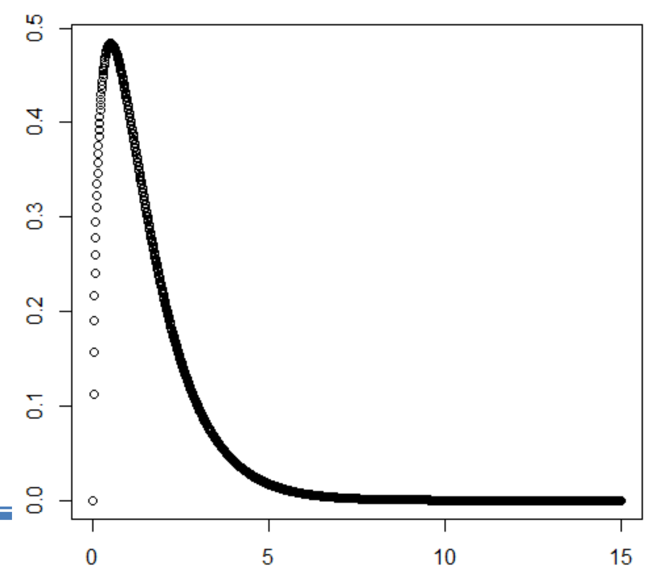
$$p(x) = \frac{1}{\Gamma(\frac{3}{2})} x^{\frac{1}{2}} e^{-x}, \ x > 0$$

其中$\Gamma(\frac{3}{2}) = \frac{\sqrt{\pi}}{2}$。

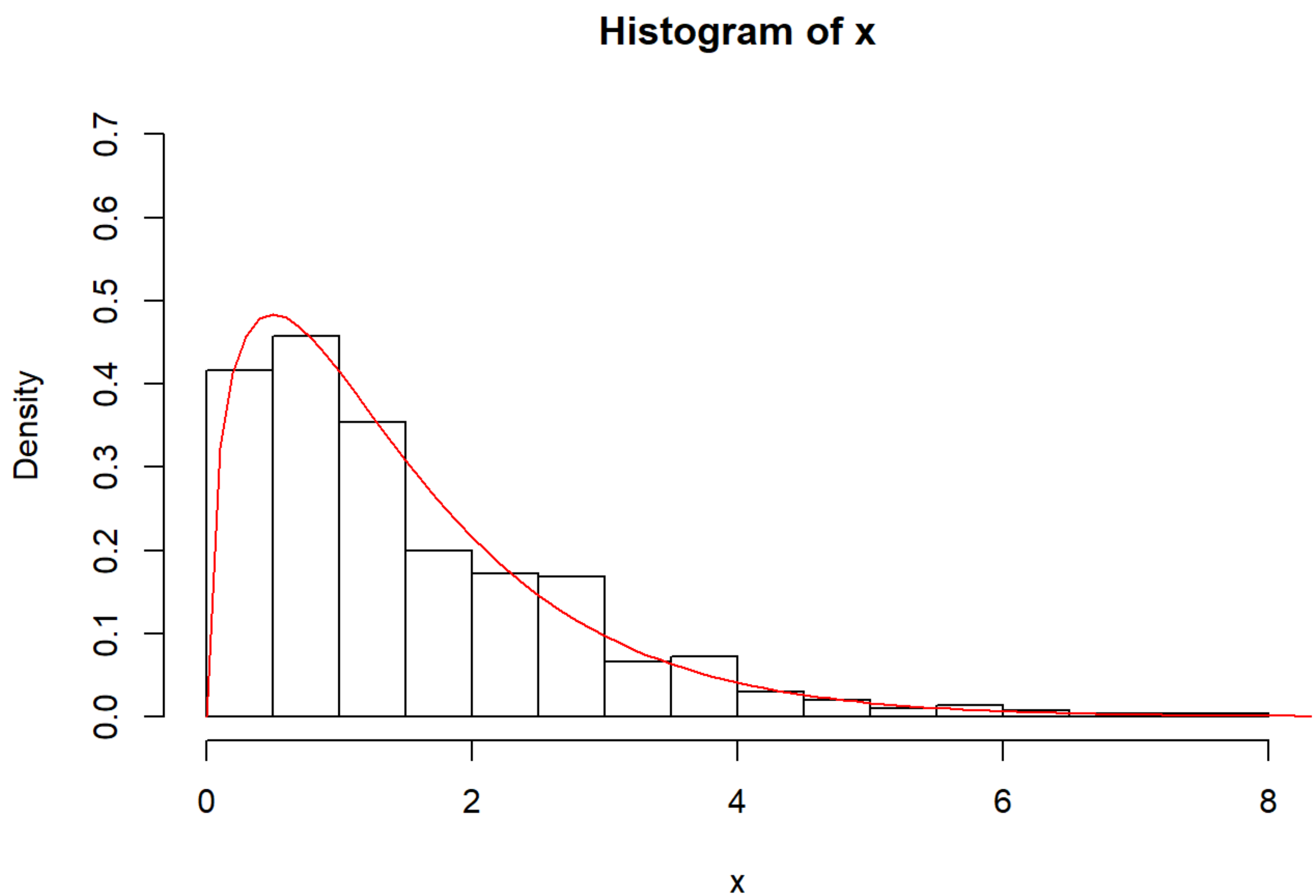
用舍选法II。$p(x)$形状在尾部与指数分布相近，且$EZ = \frac{3}{2}$，所以使用期望为$\frac{3}{2}$的指数分布作为试投密度$g(x) = \frac{2}{3} e^{-\frac{2}{3}x}$，求常数$c$使得$\sup(p(x)/g(x)) \leq c$。用微分法求得$p(x)/g(x)$最大值点$\frac{3}{2}$，最大值为$c = \frac{3\sqrt{3}}{\sqrt{2\pi e}}$，这时

$$\frac{p(x)}{cg(x)} = \sqrt{\frac{2e}{3}} x^{\frac{1}{2}} e^{-\frac{1}{3}x},$$

平均迭代次数为 $c = \frac{3\sqrt{3}}{\sqrt{2\pi e}} \approx 1.257.$



2.3.5 舍选法



2.3.5 舍选法

例6.15 (用舍选法生成正态随机数) 如果$X \sim \mathrm{N}(0,1)$则$Y=\mu+\sigma X \sim \mathrm{N}(\mu,\sigma^2)$，所以只要产生N(0,1)随机数Z。

用舍选法II，标准正态分布密度在尾部正比于$e^{-\frac{1}{2}x^2}$，用标准指数分布密度来作为试投密度(可以像例6.14那样证明在指数分布中 参数为1的指数分布是最优的)。

因为指数分布是非负的，所以先产生$|Z|$的随机数，易见$|Z|$的密度函数为

$$p(x)=\sqrt{\frac{2}{\pi}}e^{-\frac{1}{2}x^2},\ x>0$$

取$g(x)=e^{-x}, x>0$,

$$h(x)=\frac{p(x)}{g(x)}=\sqrt{\frac{2}{\pi}}e^{x-\frac{1}{2}x^2},\ x>0$$

为使$h(x)$最大只要使$x-\frac{1}{2}x^2$最大，所以$h(x)$最大值点为$x_0=1$，取

$$c=h(1)=\sqrt{\frac{2e}{\pi}},\quad \frac{p(x)}{cg(x)}=e^{-\frac{1}{2}(x-1)^2},$$

产生$|Z|$随机数后只需要以各自$\frac{1}{2}$的概率加上正负号。算法迭代次数为$c=\sqrt{\frac{2e}{\pi}}\approx 1.32$。

2.3.5 舍选法

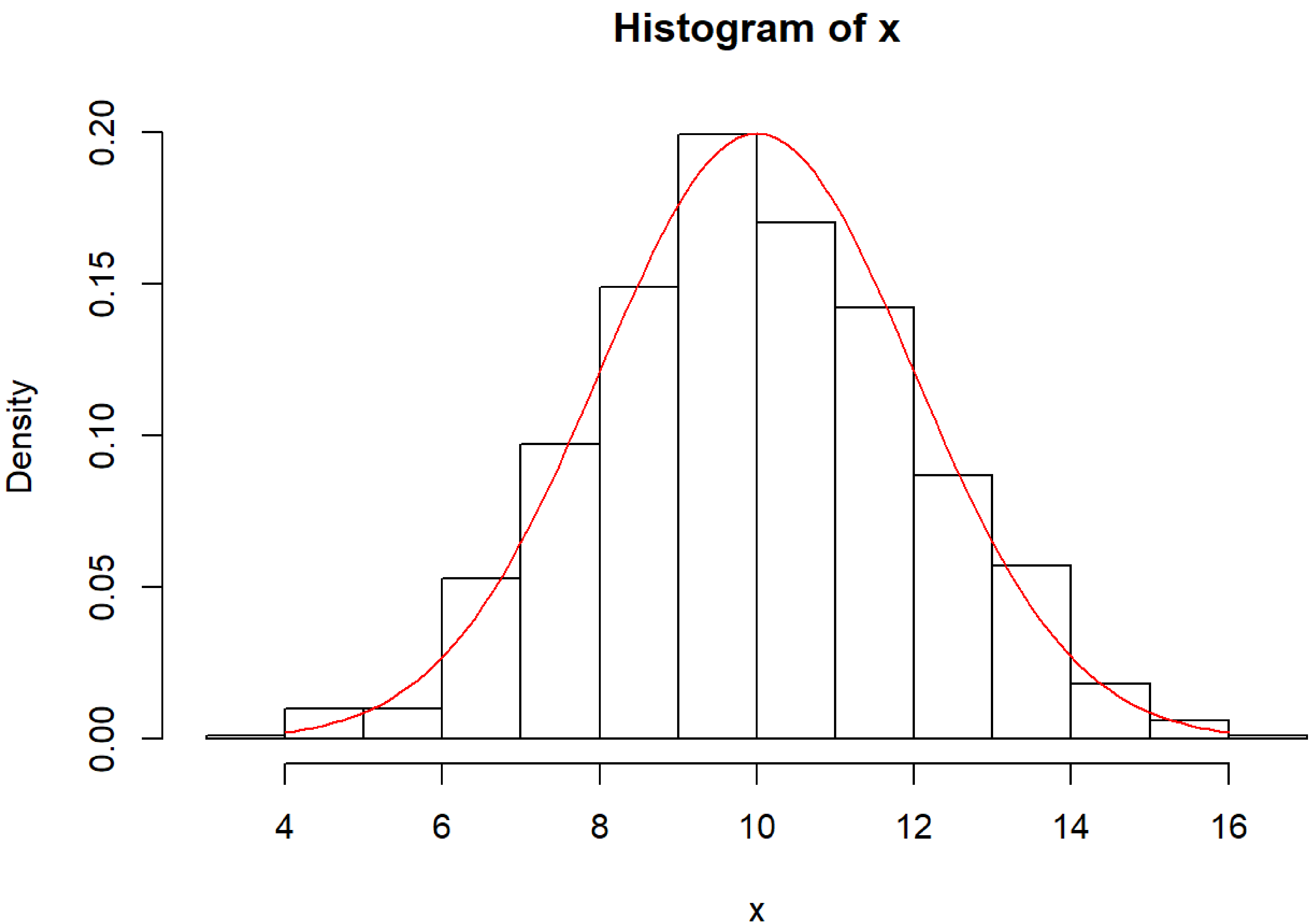
生成Z的算法:

- 步骤1:生成参数为1的指数随机变量X.
- 步骤2:生成一个均匀随机数Y.
- 步骤3:如果$Y \geq e^{-\frac{1}{2}(x-1)^2}$,则

  {生成均匀随机数U_2;

  若U_2<0.5，则令Z=X.否则,令Z=-X}

  否则,转至步骤1.


Histogram of x
Density
0.00
0.05
0.10
0.15
0.20
4
6
8
10
12
14
16
x

2.3.5 舍选法

例6.16 (用舍选法和Box-Muller变换生成正态随机数)

设U_1, U_2是两个标准均匀分布随机数, 令

$$V_1 = 2U_1 - 1$$

$$V_2 = 2U_2 - 1$$

则(V_1, V_2)在在中心为原点、面积为4的正方形中均匀分布

进一步，令

$$V_1^2 + V_2^2 \leq 1.$$

此时，(V_1, V_2)在此圆内均匀分布

2.3.5 舍选法

例6.16 (用舍选法和Box-Muller变换生成正态随机数)

若记R和Θ为点(V_1, V_2)的极坐标,

则 R与Θ是独立的,且

R^2在(0,1)上均匀分布；Θ在(0,2π)上均匀分布,

$$sin\Theta = \frac{V_2}{R} = \frac{V_2}{\sqrt{V_1^2 + V_2^2}}$$

$$cos\Theta = \frac{V_1}{R} = \frac{V_1}{\sqrt{V_1^2 + V_2^2}}$$

2.3.5 舍选法

例6.16 (用舍选法和Box-Muller变换生成正态随机数)

一对独立的标准正态随机变量可以如下生成:

生成一个随机数U后,令

$$X = \sqrt{-2\ln U}\,\frac{V_1}{\sqrt{V_1^2 + V_2^2}}$$

$$Y = \sqrt{-2\ln U}\,\frac{V_2}{\sqrt{V_1^2 + V_2^2}}$$

2.3.5 舍选法

例6.16 (用舍选法和Box-Muller变换生成正态随机数)

令$S = R^2 = V_1^2 + V_2^2$，则

$$X = \sqrt{-2\ln S}\frac{V_1}{\sqrt{S}} = V_1\sqrt{\frac{-2\ln S}{S}}$$

$$Y = \sqrt{-2\ln S}\frac{V_2}{\sqrt{S}} = V_2\sqrt{\frac{-2\ln S}{S}}$$

是独立的标准正态随机变量,其中(V_1, V_2)是中心在原点半径为1的圆内的随机点,且$S = V_1^2 + V_2^2$

2.3.5 舍选法

例6.16 (用舍选法和Box-Muller变换生成正态随机数)

- 产生一对独立的标准正态随机变量的**极坐标算法步骤**:

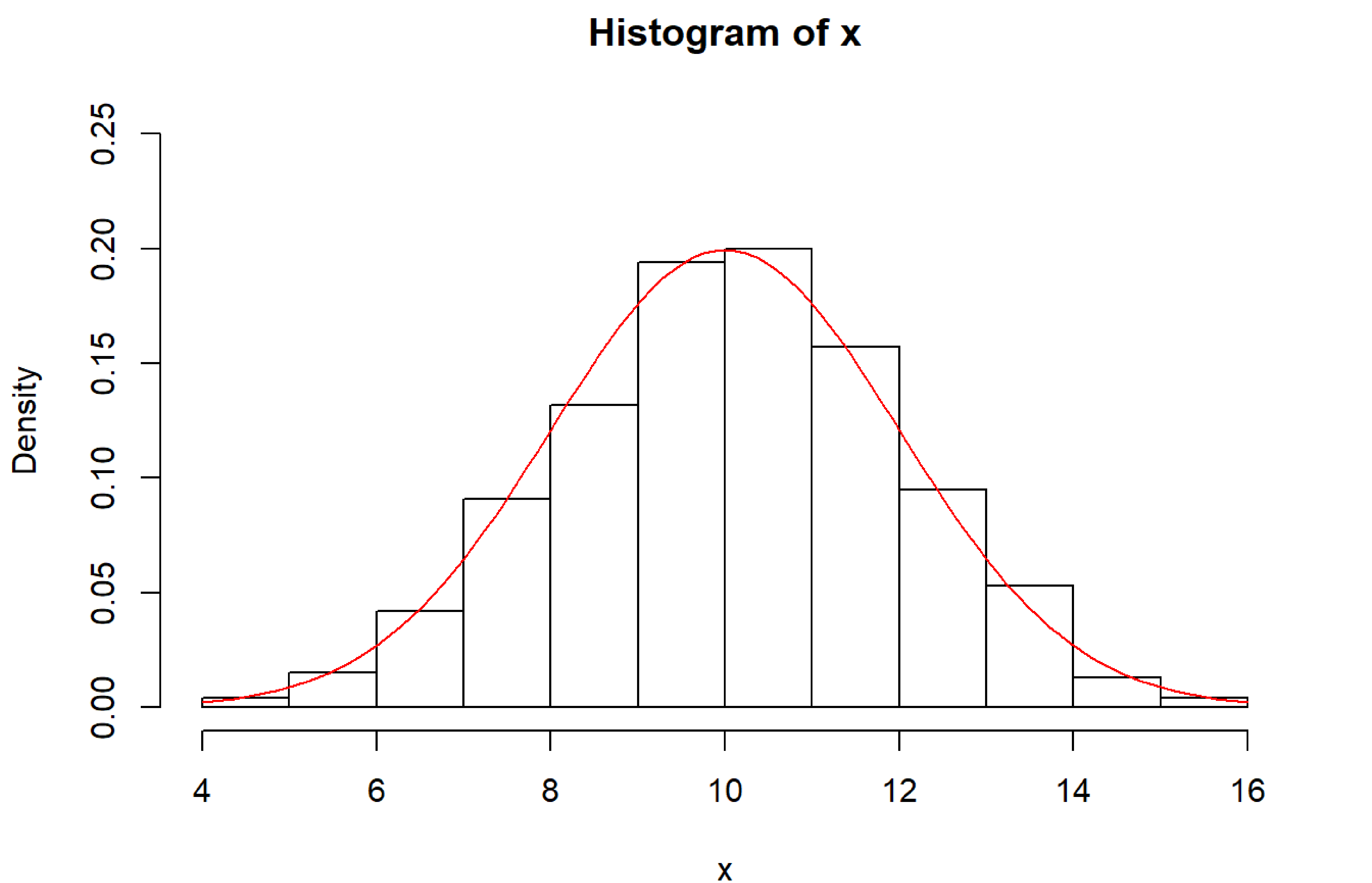
步骤1: 生成随机数U_1, U_2

步骤2: 令$V_1 = 2U_1 - 1. V_2 = 2U_2 - 1, S = V_1^2 + V_2^2.$

步骤3: 如果S>1,则转至步骤1.

步骤4: 产生独立的标准正态随机变量:

$$X = \sqrt{\frac{-2\ln S}{S}} V_1, \quad Y = \sqrt{\frac{-2\ln S}{S}} V_2$$



Histogram of x
Density
0.00
0.05
0.10
0.15
0.20
0.25
4
6
8
10
12
14
16
x

2.3.6 复合法

设离散型随机变量I的概率分布为

$$P(I=i)=\alpha_i \quad i=1,2,\ldots,m$$

若随机变量$Z_1, Z_2, \ldots, Z_m$都是离散型随机变量，定义随机变量X的值为

$$X=\begin{cases} Z_1, & \text{当}I=1, \\ Z_2, & \text{当}I=2, \\ \cdots & \cdots\cdots \\ Z_m, & \text{当}I=m \end{cases}$$

则X是离散型随机变量，且

$$P(X=x)=\sum_{i=1}^{m}P(X=x\mid I=i)P(I=i)=\sum_{i=1}^{m}\alpha_i P(Z_i=x)$$

- 1生成I的样本， 2根据I的值生成Z_I的样本， 结果就是X的样本

2.3.6 复合法

例6.18 设离散型随机变量X的分布为

$$P(X=k)=\begin{cases}0.05, & k=1,2,3,4,5\\ 0.15, & k=6,7,8,9,10\end{cases}$$

- 随机变量I分布为

P(I=1)=0.25, P(I=2)=0.75

- 随机变量Z_1服从1,2,3,4,5上的离散均匀分布，
- 随机变量Z_2服从6,7,8,9,10上的离散均匀分布，
- X的分布为I=1时取Z_1, I=2时取Z_2。

2.3.6 复合法

例6.18 设离散型随机变量X的分布为

$$P(X=k)=\begin{cases}0.05, & k=1,2,3,4,5\\ 0.15, & k=6,7,8,9,10\end{cases}$$

```
function randmix(n)
    local xs, u1, u2
    xs = zeros(n)
    for i=1:n
        u1, u2 = rand(2)
        if u1 < 0.75
            xs[i] = ceil(Int, 5*u2) + 5
        else
            xs[i] = ceil(Int, 5*u2)
        end
    end

    return xs
end
```

2.3.6 复合法

- 若随机变量Z_1, Z_2, …, Z_m都是连续型随机变量，密度函数分别为

$$p_1(z), p_2(z), \dots, p_m(z)$$

- 则X的分布函数为

$$F(x) = P(X \le x) = \sum_{i=1}^{m} P(X \le x | I = i) P(I = i)$$

$$= \sum_{i=1}^{m} \alpha_i P(Z_i \le x)$$

- 于是X有分布密度 $p(x) = F'(x) = \sum_{i=1}^{m} \alpha_i p_i(x)$

- 可以先生成I， 然后根据的值生成Z_I作为X。

2.3.6 复合法

例6.19 (梯形分布)

对0<a<1，考虑梯形密度

$$p_1(x) = a + 2(1-a)x,\ 0 < x < 1,$$

或

$$p_2(x) = 2 - a - 2(1-a)x,\ 0 < x < 1$$

因为分布函数为

$$F_1(x) = ax + (1-a)x^2,\ 0 < x < 1$$

或

$$F_2(x) = (2-a)x - (1-a)x^2,\ 0 < x < 1$$

2.3.6 复合法

例6.19 (梯形分布)

分布函数反函数为

$$F_1^{-1}(u) = \frac{-a + \sqrt{a^2 + 4(1-a)u}}{2(1-a)}, \quad 0 < u < 1$$

或

$$F_2^{-1}(u) = \frac{2 - a - \sqrt{(2-a)^2 - 4(1-a)u}}{2(1-a)}, \quad 0 < u < 1$$

可以用逆变换法获得$p_1(x)$和$p_2(x)$的随机数

2.3.6 复合法

例6.19 (梯形分布)

下面给出复合法生成$p_1(x)$随机数的做法。

- $p_1(x)$下的区域可以分解为一个面积等于a的矩形和一个面积等于1−a的三角形， 令

$$g_1(x) = \quad 1,\ 0 < x < 1,$$
$$g_2(x) = \quad 2x,\ 0 < x < 1,$$

$$p_1(x) = \quad a \cdot g_1(x) + \quad (1-a) \cdot g_2(x),\ 0 < x < 1$$

- 可见$p_1(x)$是由一个均匀分布和一个三角形分布复合而成。

2.4 随机向量的产生

- 条件分布法
- 多项分布随机数
- 多元正态分布模拟

2.4 随机向量的产生

➢ 条件分布法

设随机向量$X = (X_1, X_2, \ldots, X_r)$

X的分布密度或分布概率为 $p(X_1, X_2, \ldots, X_r)$

p可以分解为：

$$p(x_1, x_2, \ldots, x_r) = p(x_1)p(x_2|x_1)p(x_3|x_1, x_2)\cdots p(x_r|x_1, x_2, \ldots, x_{r-1})$$

2.4 随机向量的产生

- **条件分布法步骤：**
- 首先生成X_1
- 由已知的X_1的值服从条件分布$p(X_2|X_1)$产生X_2
- 再从已知的X_1, X_2的值从条件分布$p(x_3|X_1, X_2)$产生x_3
- 如此重复直到产生x_r

2.4 随机向量的产生

> 多项分布

- 进行了n次独立重复试验Y_1, Y_2, …, Y_n,
- 每次的试验结果Y_i在1,2,…,r中取值,

  $P(Y_i=j)=p_j$, $j=1,2,\ldots,r$; $i=1,2,\ldots,n$。

令X_j为这n次试验中结果j的个数$(j=1,2,\ldots,r)$,

称$X = (X_1, X_2,\ldots, X_r)$服从**多项分布**,

- 其联合概率函数为

$$P(X_j = x_j, j = 1, 2, \ldots, r) = \frac{n!}{x_1!x_2!\ldots x_r!} p_1^{x_1} p_2^{x_2} \ldots p_r^{x_r}$$

其中 $\sum_{j=1}^{r} x_j = n$

2.4 随机向量的产生

➢ 产生多项分布随机数

- 当r和n相比很大时， 模拟产生

$Y_i, i = 1,2, \dots, n$然后从$\{Y_i\}$中计数得到$(X_1, X_2, \dots, X_r)$。

- 当r与n相比较小时，

使用条件分布逐个地产生$X_1, X_2, \dots, X_r$。

2.4 随机向量的产生

➢ 使用条件分布产生多项分布随机数

- X_1表示n次重复试验中结果1的出现次数， 以结果1作为成功，其它结果作为失败， 显然$X_1 \sim \mathrm{B}(n, p_1)$。
- 产生X_1的值x_1后，n次试验剩余的$n - x_1$次试验结果只有$2,3,\ldots,r$可取， 于是在$X_1 = x_1$条件下结果2的出现概率是

$$P(Y_i = 2|Y_i \neq 1) = \frac{P(Y_i = 2)}{\sum_{k=2}^{r} P\,(Y_i = k)} = \frac{p_2}{1 - p_1}$$

剩下的$n - x_1$次试验中结果2的出现次数服从$\mathrm{B}\left(n - x_1, \frac{p_2}{1-p_1}\right)$分布， 从这个条件分布产生$X_2 = x_2$。

2.4 随机向量的产生

➢ 使用条件分布产生多项分布随机数

- 类似地， 剩下的$n-x_1-x_2$次试验中结果3的出现次数服从 $\mathrm{B}\left(n-x_1-x_2,\frac{p_3}{1-p_1-p_2}\right)$分布，从这个条件分布中抽取$X_3=x_3$，

- 如此重复可以产生多项分布**X**的随机数$(x_1,x_2,\ldots,x_r)$。

2.4 随机向量的产生

➢ 多元正态分布

- 设随机向量$X=(X_1,X_2,\ldots,X_p)^T$服从$N(\boldsymbol{\mu},\Sigma)$

- 联合密度函数为

$$p(\mathbf{x})=(2\pi)^{-\frac{p}{2}}|\Sigma|^{-\frac{1}{2}}\exp\left\{-\frac{1}{2}(\mathbf{x}-\boldsymbol{\mu})^T\Sigma^{-1}(\mathbf{x}-\boldsymbol{\mu})\right\}$$

$$\mathbf{x}\in R^p$$

2.4 随机向量的产生

➢ 多元正态分布随机数的产生

- 正定矩阵Σ有Cholesky分解$\Sigma = CC^T$， 其中C为下三角矩阵。
- 设$\mathbf{Z} = \left(Z_1, Z_2, \dots, Z_p\right)^T$服从p元标准正态分布N$(\mathbf{0}, I)$($I$表示单位阵)，
- 则$\mathbf{X} = \boldsymbol{\mu} + C\mathbf{Z}$服从N$(\boldsymbol{\mu}, \Sigma)$分布。

2.4 随机向量的产生