

1 Gaussian Random Number Generator

Given U_1 and U_2 belong $[-1, 1]$, the following is to find out random variables that are Gaussian distributed.

1.1 Principle

1) Start from an cdf of joint Gaussian random variable x and y

$$\begin{aligned} & \int \int \exp(-1/2x^2)\exp(-1/2y^2)dx dy \\ &= \int d\theta \int r \exp(-r^2/2) dr \\ &= \int pdf(\theta) * \int pdf(r) \end{aligned}$$

So if we are able to find r and θ , then by taking $x = r \cos \theta$, $y = r \sin \theta$, we get x and y

2) To find θ is easy as we can take $\theta = 2\pi U_2$

3) Suppose $R = \sqrt{-2\ln U_1}$

The cdf of R is

$$\begin{aligned} & P(R \leq r) \\ &= P(\sqrt{-2\ln U_1} \leq r) \\ &= P(U_1 \geq \exp(-1/2r^2)) \\ &= \int_{\exp(-1/2r^2)}^1 du_1 \\ &= 1 - \exp(-1/2r^2) \end{aligned}$$

So the pdf = $r \exp(-1/2r^2)$

4) Therefore

$$\begin{aligned} X &= \sqrt{-2\ln U_1} \cos(2\pi U_2) \\ Y &= \sqrt{-2\ln U_1} \sin(2\pi U_2) \end{aligned}$$

1.2 Efficient way of evaluating cos and sin function

In most computers, evaluating cos and sine is not quite straightforward, so the above method is not practical to use. So the following alternative avoids evaluating sine and cos functions directly.

1) We generate new random variable $S = U_1^2 + U_2^2$, then the cumulative probability of S when $S \leq 1$ is the ratio of the area of the circle with radius $r = \sqrt{S}$

to the area of the circle with radius 1.

$$\begin{aligned} \text{Prob}(S < s, s \leq 1) &= \frac{\pi r^2}{\pi} \\ &= s \end{aligned}$$

So pdf of s is 1, it is uniform distribution in $[0, 1]$.

2) So if we confine $S < 1$, by taking S that satisfies only $U_1^2 + U_2^2 < 1$, then throwing away others, then S is uniform in $(0, 1)$, which corresponds r in $(0, 1)$. Then a.4) becomes

$$\begin{aligned} X &= \sqrt{-2\ln S} \cos(2\pi S) = \sqrt{-2\ln S} U_1 / \sqrt{S} \\ Y &= \sqrt{-2\ln S} \sin(2\pi S) = \sqrt{-2\ln S} U_2 / \sqrt{S} \end{aligned}$$

1.3 Final algorithm

- 1) Generate two uniform random variables U_1, U_2 y belongs to $[-1, 1]$
- 2) If $U_1^2 + U_2^2 \geq 1$, throw away and regenerate.
- 3) Return

$$\begin{aligned} U_1 &* \sqrt{-2\log(U_1^2 + U_2^2)/(U_1^2 + U_2^2)} \\ U_2 &* \sqrt{-2\log(U_1^2 + U_2^2)/(U_1^2 + U_2^2)} \end{aligned}$$

2 Poisson Random Number Generator

2.1 Inverse Transform Sampling

The probability integral transform states that if X is a continuous random variable with cumulative distribution function F_X , then the random variable $Y = F_X(X)$ has a uniform distribution on $[0, 1]$. The inverse probability integral transform is just the inverse of this: specifically, if Y has a uniform distribution on $[0, 1]$ and if X has a cumulative distribution F_X , then the random variable $F_X^{-1}(Y)$ has the same distribution as X .

Proof:

If random variable X has cumulative distribution function $F_X(X)$, and if we define random variable $Y = F_X(X)$, then $Y \in [0, 1]$, and the cumulative distri-

bution function of Y is

$$\begin{aligned}
 &P(Y < y) \\
 &=P(F_X(X) < y) \\
 &=P(X < F_X^{-1}(y)) \\
 &=F_X(F_X^{-1}(y)) \\
 &=y
 \end{aligned}$$

So $P(Y < y) = y$ and $Y \in [0, 1]$. This means Y has uniform distribution.

Correspondingly, the reverse direction holds as well. Suppose Y is a uniform random variable on $(0, 1)$ and F is a cumulative distribution function, then the random variable $X = F^{-1}(Y)$ has a cumulative distribution function of the following

$$\begin{aligned}
 &P(X < x) \\
 &=P(F^{-1}(Y) \leq x) \\
 &=P(Y \leq F(x)) \\
 &=F(x)
 \end{aligned}$$

The last line is based on the definition of cumulative distribution function.

2.2 Generating Possion Random Number

Based on the inverse transform method above, we can generate a Possion random variable by: first generate uniform random variable $U \in [0, 1]$, then find X where $F(X) = u$. Since Possion random variable is discrete, we would like to find largest X where $F(X) \leq u$, meaning $X = F^{-1}(u) = \inf\{x | F(x) < u\}$.

Algorithm generating Possion random variable with parameter λ

$p = \exp(-\lambda)$

$F = p$

$N = 0$ generate $U \in Unif[0, 1]$

while ($U > F$)

$N = N + 1$

$p = p\lambda/N$, because $P(N = k + 1) = P(N = k)\theta/(k + 1)$

$F = F + p$

return N