

On generating a random number with a prescribed distribution function

Christoph Börgers
Department of Mathematics, Tufts University
December 2025

Intended readers: At roughly the level of a strong undergraduate mathematics major.

Specific prerequisites include: elementary probability theory, including a light understanding of *measure-theoretic* probability

Feedback: Feedback motivates me to write more of these. If you find this useful, or if you have comments or suggestions, or if you just want to say hello, I would very much enjoy hearing from you: cborgers@tufts.edu.

Contents

1	The question	1
2	The simplest special case	2
3	Pseudo-inverses of F	3
4	Any pseudo-inverse works for generating X	6
5	The left- and right-continuous pseudo-inverses	6
6	Evaluation of F_L^\dagger and F_R^\dagger by bisection	8
7	A numerical example	9

1 The question

Suppose $X \in \mathbb{R}$ is a random number. The *probability distribution function* of X is the function

$$F(x) = P(X \leq x), \quad x \in \mathbb{R}.$$

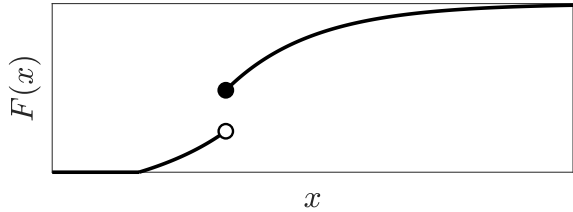
The function F encapsulates all there is to know about the statistics of X in a single function. That is, if X and Y are random numbers with the same probability distribution function, then they have the same distribution, i.e.,

$$\forall A \subseteq \mathbb{R} \text{ Borel-measurable} \quad P(X \in A) = P(Y \in A).$$

The function F has the following three properties.

1. F is continuous from the right,
2. $\lim_{x \rightarrow -\infty} F(x) = 0$ and $\lim_{x \rightarrow \infty} F(x) = 1$.
3. F is non-decreasing.

Here is an example:



All of this would be explained in a first undergraduate course on (calculus-based) probability. I am assuming that you know all of it.

Assumption from here on, for the remainder of this article: $F : \mathbb{R} \rightarrow [0, 1]$ is a function with properties 1–3.

Can you generate, in theory or even in practice (numerically), a random number X for which F is the distribution function? The answer is always yes, and these notes explain precisely why the answer is yes, and how to do it.

2 The simplest special case

First we assume that F has an inverse, or slightly more generally:

Assumption in this section: *There exist a and b with $-\infty \leq a < b \leq \infty$ so that*

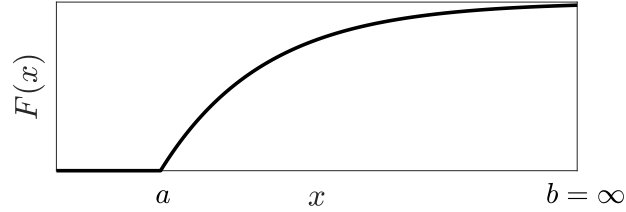
$$F : (a, b) \rightarrow (0, 1)$$

is a bijection. Equivalently: F is continuous, and it is strictly increasing as long as $0 < F(x) < 1$.

For example:

$$F(x) = \begin{cases} 0 & \text{if } x \leq 0, \\ 1 - e^{-x} & \text{if } x > 0. \end{cases} \tag{1}$$

In this case, $a = 0, b = \infty$.



This is the distribution function of an exponentially distributed random number $X > 0$ with mean 1.

Under these restrictive assumptions,

$$F^{-1} : (0,1) \rightarrow (a,b)$$

is well-defined, and if $U \in (0,1)$ has uniform distribution, then

$$X = F^{-1}(U)$$

has the distribution function X . To see this, let $x \in (a,b)$. Then

$$P(X \leq x) = P(F^{-1}(U) \leq x) = P(U \leq F(x)) = F(x).$$

Another way of saying this is that to construct X , we should simply solve

$$F(X) = U$$

for X , where $U \in (0,1)$ is uniformly distributed.

For instance, if F is given by eq. (1), we solve

$$1 - e^{-X} = U$$

for X , obtaining

$$X = \ln \frac{1}{1-U}.$$

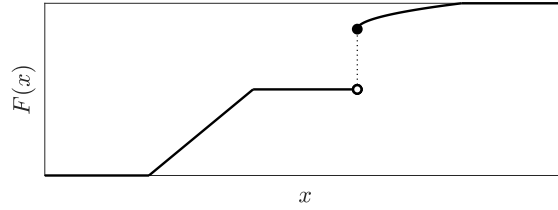
Of course, when $U \in (0,1)$ is uniformly distributed, so is $V = 1 - U$, so we can also say

$$X = \ln \frac{1}{V},$$

where $V \in (0,1)$ is uniformly distributed. This is the well-known, standard way of generating an exponentially distributed random number with mean 1.

3 Pseudo-inverses of F

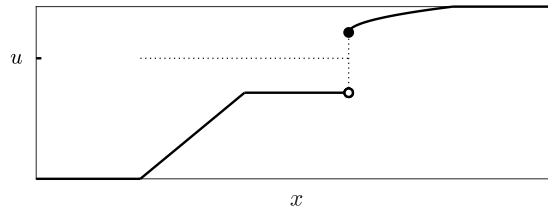
In general, there are two possible complications: F may have plateaus, and F may have jump discontinuities. Here is an example that has one plateau and one jump discontinuity:



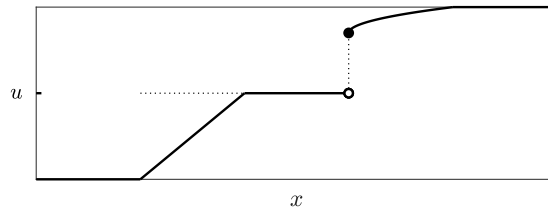
So given $u \in (0, 1)$, the equation

$$F(x) = u$$

may have no solutions:



or it may have infinitely many solutions:



Definition. We call $u \in (0, 1)$ a plateau value of F if there are at least two values $x_1 < x_2$ with $F(x_1) = F(x_2) = u$ (and therefore $F(x) = u$ for $x \in (x_1, x_2)$ as well).

Lemma. The set of plateau values of F is finite or countably infinite.

Proof. Let \mathcal{P} denote the set of plateau values of F . So $u \in \mathcal{P}$ if and only if there exists a whole interval I of positive length so that $F(x) = u$ if $x \in I$. For each $u \in \mathcal{P}$ denote by $\psi(u)$ a rational number with

$$F(\psi(u)) = u.$$

Then ψ is a mapping from \mathcal{P} into \mathbb{Q} , and clearly it is strictly increasing and therefore injective. This implies that \mathcal{P} is at most countably infinite. \square

Lemma. *The set of discontinuities of F is finite or countably infinite.*

Proof. Let \mathcal{D} denote the set of discontinuities of F . So if $x_0 \in \mathcal{D}$, then $\lim_{x \rightarrow x_0^-} F(x) < \lim_{x \rightarrow x_0^+} F(x)$. For each $x_0 \in \mathcal{D}$, denote by $\varphi(x_0)$ a *rational* number with

$$\lim_{x \rightarrow x_0^-} F(x) < \varphi(x_0) < \lim_{x \rightarrow x_0^+} F(x).$$

Then φ is a mapping from \mathcal{D} into \mathbb{Q} , and clearly it is strictly increasing and therefore injective. This implies that \mathcal{D} is at most countably infinite. \square

Definition. *As throughout this article, make the assumptions of Section 1 on F . A function*

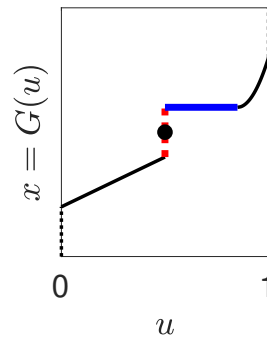
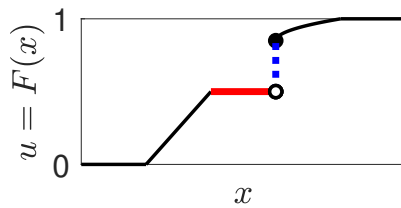
$$G: (0, 1) \rightarrow \mathbb{R}$$

is called a pseudo-inverse of F if it has the following properties.

- (a) *If $u \in (0, 1)$ and there exists exactly one $x \in \mathbb{R}$ with $F(x) = u$, then $G(u) = x$.*
- (b) *If $u \in (0, 1)$ is a plateau value, so there exist multiple $x \in \mathbb{R}$ with $F(x) = u$, then $G(u)$ is any value in the closed interval*

$$[\min \{x \in \mathbb{R} : F(x) = u\}, \sup \{x \in \mathbb{R} : F(x) = u\}]. \quad (2)$$

- (c) *If $u \in (0, 1)$ and there exist no $x \in \mathbb{R}$ with $F(x) = u$, then $G(u)$ is the smallest value x with $F(x) > u$.*



Plateaus of F become discontinuities of G , and discontinuities of F become plateaus of G . Any pseudo-inverse G is non-decreasing.

Note that the “min” in (2) is really a “min” and not an “inf”, since F is continuous from the right. The “sup” in (2) is a “max” only if F is left-continuous, and therefore continuous, at $\sup \{x \in \mathbb{R} : F(x) = u\}$.

4 Any pseudo-inverse works for generating X

Proposition. Let $G: (0,1) \rightarrow \mathbb{R}$ be any pseudo-inverse of F . Let $U \in (0,1)$ be uniformly distributed. Then $X = G(U)$ has the distribution function F .

Proof. Let $u \in (0,1)$ and assume that u isn't a plateau value. I will prove:

$$G(u) \leq x \Leftrightarrow u \leq F(x). \quad (3)$$

To show this, first assume that there is exactly one x_0 with $F(x_0) = u$. Then $F(x) < u$ for $x < x_0$, $F(x) > u$ for $x > x_0$, and $G(u) = x_0$. Therefore

$$G(u) \leq x \Leftrightarrow x_0 \leq x \Leftrightarrow F(x_0) \leq F(x) \Leftrightarrow u \leq F(x).$$

Second, assume that $F(x) = u$ has no solution. Then there exists an x_0 so that F is discontinuous at x_0 , and

$$u \in \left[\lim_{x \rightarrow x_0^-} F(x), F(x_0) \right).$$

Then $G(u) = x_0$, and

$$G(u) \leq x \Leftrightarrow x_0 \leq x \Leftrightarrow u < F(x) \Leftrightarrow u \leq F(x).$$

(The last equivalence holds simply because $F(x) = u$ does not hold for any x .)

If $U \in (0,1)$ is uniformly distributed, and $X = G(U)$ for some pseudo-inverse G of F , then

$$P(X \leq x) = P(G(U) \leq x) =$$

$$P(G(U) \leq x \text{ and } U \text{ is not a plateau value}) + P(G(U) \leq x \text{ and } U \text{ is a plateau value}) =$$

$$P(U \leq F(x) \text{ and } U \text{ is not a plateau value}) = P(U \leq F(x)) = F(x)$$

because U is a plateau value with probability zero. □

5 The left- and right-continuous pseudo-inverses

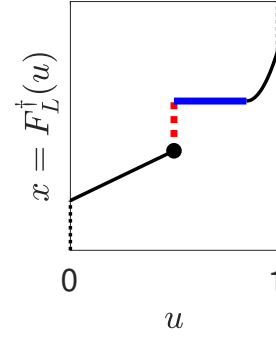
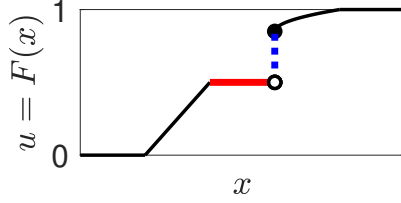
Let $u \in (0,1)$ be a plateau value of F . If G is a pseudo-inverse of F , then $G(u)$ can be any value in the interval

$$[\min \{x \in \mathbb{R} : F(x) = u\}, \sup \{x \in \mathbb{R} : F(x) = u\}].$$

If we choose

$$G(u) = \min \{x \in \mathbb{R} : F(x) = u\}$$

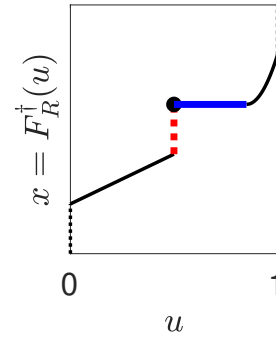
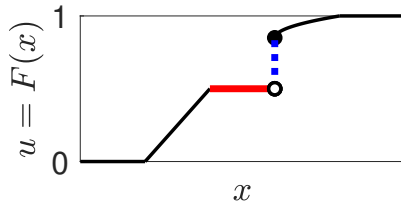
for any plateau value u of F , the function G becomes continuous from the left. We denote the left-continuous pseudo-inverse by F_L^\dagger .



If we choose

$$G(u) = \sup \{x \in \mathbb{R} : F(x) = u\}$$

for any plateau value u of F , then G becomes continuous from the right. We denote this pseudo-inverse by F_R^\dagger .



Both F_L^\dagger and F_R^\dagger have appealing, compact descriptions:

Proposition. For all $u \in (0, 1)$,

$$F_L^\dagger(u) = \min \{x \in \mathbb{R} : F(x) \geq u\}.$$

and

$$F_R^\dagger(u) = \sup \{x \in \mathbb{R} : F(x) \leq u\}.$$

Proof. Let $u \in (0, 1)$ be such that there exists exactly one $x_0 \in \mathbb{R}$ with $F(x_0) = u$. Then

$$F_L^\dagger(u) = F_R^\dagger(u) = x_0.$$

We have $F(x) > u$ for $x > x_0$, and $F(x) < u$ for $x < x_0$. Therefore

$$\min \{x \in \mathbb{R} : F(x) \geq u\} = \sup \{x \in \mathbb{R} : F(x) \leq u\} = x_0.$$

Let $u \in (0, 1)$ be a plateau value of F . Then

$$F_L^\dagger(u) = \min \{x \in \mathbb{R} : F(x) = u\} = \min \{x \in \mathbb{R} : F(x) \geq u\}$$

and

$$F_R^\dagger(u) = \sup\{x \in \mathbb{R} : F(x) = u\} = \sup\{x \in \mathbb{R} : F(x) \leq u\}.$$

Let $u \in (0, 1)$ be a value outside the range of F . There then exists an $x_0 \in \mathbb{R}$ so that

$$\lim_{x \rightarrow x_0^-} F(x) \leq u < F(x_0),$$

and

$$F_L^\dagger(u) = F_R^\dagger(u) = x_0.$$

We have $F(x) > u$ for $x \geq x_0$, and $F(x) < u$ for $x < x_0$. Therefore

$$\min\{x \in \mathbb{R} : F(x) \geq u\} = \sup\{x \in \mathbb{R} : F(x) \leq u\} = x_0.$$

□

6 Evaluation of F_L^\dagger and F_R^\dagger by bisection

Proposition. Let $u \in (0, 1)$. Let $x_\ell^{(0)}$ and $x_r^{(0)}$ be numbers with $F(x_\ell^{(0)}) < u$ and $F(x_r^{(0)}) > u$. For $k = 1, 2, \dots$, define

$$x_m^{(k)} = \frac{x_\ell^{(k-1)} + x_r^{(k-1)}}{2}.$$

(a) If

$$F(x_m^{(k)}) < u, \tag{4}$$

define $x_\ell^{(k)} = x_m^{(k)}$ and $x_r^{(k)} = x_r^{(k-1)}$, otherwise $x_r^{(k)} = x_m^{(k)}$ and $x_\ell^{(k)} = x_\ell^{(k-1)}$. Then

$$\lim_{k \rightarrow \infty} x_\ell^{(k)} = \lim_{k \rightarrow \infty} x_m^{(k)} = \lim_{k \rightarrow \infty} x_r^{(k)} = F_L^\dagger(u). \tag{5}$$

(b) If we replace " $<$ " by " \leq " in (4), the limit in (5) becomes $F_R^\dagger(u)$.

Proof. It is straightforward to see that

$$\lim_{k \rightarrow \infty} x_\ell^{(k)} = \lim_{k \rightarrow \infty} x_m^{(k)} = \lim_{k \rightarrow \infty} x_r^{(k)},$$

and that $F(x_\ell^{(k)}) \leq u$ and $F(x_r^{(k)}) \geq u$ for all k . This implies the assertion for all $u \in (0, 1)$ that are not plateau values of F .

If $u \in (0, 1)$ is a plateau value, then in (a), $F(x_\ell^{(k)}) < u$ and $F(x_r^{(k)}) \geq u$ for all k , and this implies

$$\lim_{k \rightarrow \infty} x_\ell^{(k)} = \lim_{k \rightarrow \infty} x_m^{(k)} = \lim_{k \rightarrow \infty} x_r^{(k)} = \min\{x \in \mathbb{R} : F(x) = u\} = F_L^\dagger(u).$$

In (b), $F(x_\ell^{(k)}) \leq u$ and $F(x_r^{(k)}) > u$ for all k , and this implies

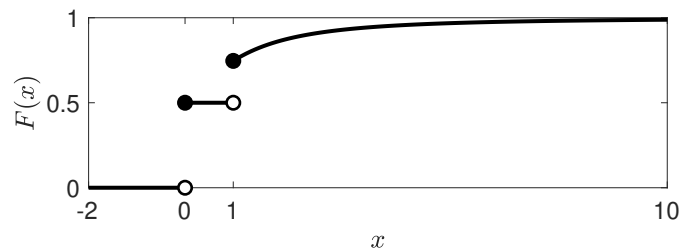
$$\lim_{k \rightarrow \infty} x_\ell^{(k)} = \lim_{k \rightarrow \infty} x_m^{(k)} = \lim_{k \rightarrow \infty} x_r^{(k)} = \sup\{x \in \mathbb{R} : F(x) = u\} = F_R^\dagger(u).$$

□

7 A numerical example

I will consider the example

$$F(x) = \begin{cases} 0 & \text{if } x < 0, \\ 0.5 & \text{if } 0 \leq x < 1, \\ 1 - ((2 + x^{3/2}) \ln(2 + x))^{-1} & \text{if } x \geq 1. \end{cases}$$



Here is a piece of Matlab code that samples from this distribution:

```
F=@(x) (x>=0 && x<1)*0.5+ ...
    (x>=1)*(1-((2+x^(3/2))*log(2+x))^(-1));
U=rand(1,1);
x_l=-1; x_r=10;
while F(x_r)<=U
    x_r=2*x_r;
end
while x_r-x_l>10^(-12)
    x_m=(x_l+x_r)/2;
    if F(x_m)<U
        x_l=x_m;
    else
        x_r=x_m;
    end
end
X=(x_l+x_r)/2
```

This code computes $F_L^\dagger(U)$, where $U \in (0, 1)$ is uniformly distributed. If the line

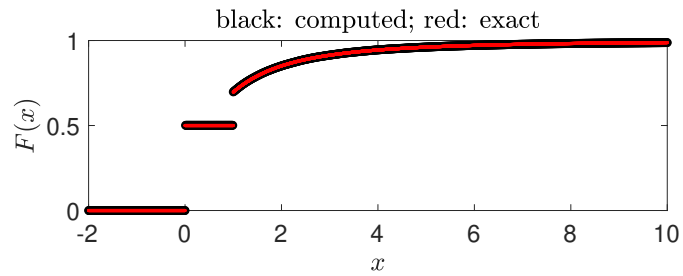
```
if F(x_m)<U
```

were replaced by

if $F(x_m) \leq U$

then $F_R^\dagger(U)$ would be computed. It makes no difference *unless* U happens to be 0.5, which has probability zero. In that case, $F_L^\dagger(0.5) = 0$, but $F_R^\dagger(0.5) = 1$.

To make sure that I've implemented it all correctly, I sampled X a hundred thousand times, and then plotted the graph of F (red) and the distribution function estimated based on the samples (black):



This picture looks the same regardless of whether F_L^\dagger or F_R^\dagger is used, since U is never exactly 0.5.