MATH 414: STOCHASTIC SIMULATION

Rafiki's Notes

Rafael Barroso
Ingenierie Mathematique
École Polytechnique Fédérale de Lausanne
September 17, 2025

Contents

1 Pseudo Random Number Generators

In this section, we explore how random (you'll see that they're not so random) numbers are generated in our computers and how the programs designed for creating these numbers work.

Definition 1.1. A random number generatorn (RNG) is a procedure that produces an *infinite* stream of independent, identically distributed (i.i.d.) random variables $U_1, U_2, \ldots \sim \mu$ accoording to some *probability distribution* μ.

Recall that a probability dustribution is basically a fancy way of saying "how likely different things are to happen." Imagine you have a bag of Skittles, and you want to know the chances of grabbing each color. A probability distribution is like a chart or rulebook that says: 'Red has a 30% chance, green has 20%, purple is rare like a unicorn at 5%, etc.'

Remark 1.2. Note that an RNG is a *uniform* random number generator if μ is the *uniform distribution* in $(0, 1)$. Where the uniform distribution is the "everyone gets a fair share" version of probability. Every outcome has the same chance of happening.

Since all of the current RNG's are based on algorithms, they produce a *purely deterministic* (i.e. the outcome is already locked in once you know the rules) stream of variables $U_1, U_2, U_3, \ldots$ which 'look like' a stream of i.i.d. random variables. For this reason, algorithmic generators are called pseudo-random number generators.