Random Number Generation

P. Neidhardt

February 24, 2013

Abstract

This is an approximate translation. Some mathematical terms need to be corrected.

1 Random number generators

1.1 Maximal period

Problem situation: a random number generator (RNG) is an application from $\mathbb{N}$ to $\mathbb{N}^{\mathbb{N}}$, *i.e.* given an integer it will return an integer sequence.

In computer science, numbers have an upper bound. RNG are often defined by a recursive linear congruential sequence:

$$u_{n+1} = (a \cdot u_n + b) \bmod m$$

Here, m is the upper bound. The sequence is periodic. If the period is less than m, then the sequence values will not match all values between 0 and $m - 1$.

Definition A RNG is said to be of *maximal period* if all values of the target interval are met by the sequence.

Property

$$\text{The period is maximal if and only if } \begin{cases} (1)\ \gcd(b, m) = 1 \\ (2)\ \text{For all prime } p \text{ dividing } m, \text{ we have } a \bmod p = 1 \\ (3)\ \text{If 4 divides } m, \text{ then } a \bmod 4 = 1 \end{cases}$$

Proof

Relation (1) Let's assume the period is maximal. The sequence can be solved:

$$u_{n+1} = a \cdot u_n + b$$

Fixed point:

$$l = a \cdot l + b \Rightarrow l = \frac{b}{1-a}$$

$$u_{n+1} - l = a \cdot (u_n - l)$$

$$u_n = a^n \cdot (u_0 - l) + l$$

The modulus does not change anything. Hence

$$\boxed{u_n = a^n \cdot (u_0 - l) + l \bmod m}$$

Changing the indices this is equivalent to using a sequence where the first term would be 0.

$$u_n = l \cdot (1 - a^n) \bmod m$$

Since the period is maximal, we have $k \in [0; m-1]$ so that $u_k = 1$, *i.e.*

$$u_k = 1 = l \cdot (1 - a^k) \bmod m$$

$$1 = \frac{b}{1-a} \cdot (1 - a^k) + A \cdot m$$

with A an integer.

$$\boxed{1 = b \cdot \sum_{i=0}^{k-1} a^i + A \cdot m}$$

From Bézout's identity we can state that b and m are coprime.

Relation (2) I got from an unknown source that first we have to prove if the period is maximal for m, then it is maximal for p dividing m. Hence

$$u_{n+1} = (a \cdot u_n + b) \bmod p$$

would be of maximal period too.

N.B.: if $a = 1$, then

$$u_{n+1} = (u_n + b) \bmod p$$

And the period is effectively maximal if and only if m and b are coprime.

Relation (3) According to relation (2) which is supposed proven,

$$4 \text{ divise } m \Rightarrow a \bmod 4 = 1 \text{ ou } a \bmod 4 = -1$$

If $a \bmod 4 = -1$, then

$$u_{n+2} = -(-u_n + b) + b \bmod m = u_n$$

The period is not maximal, so necessarily we have $a \bmod 4 = 1$.