Anna Ruthishauser
Andrea Scheidegger

Handout Aufgabe 3 – Erzeugung von Zufallszahlen

Ausgangslage:

Rekursive Folge $x_{n+1} = (a \cdot x_n + b) \bmod m$

$a, b, m \in R$, $a, b \geq 0$ und $m > 0$ (m kann nicht null sein, weil Division durch 0 nicht definiert ist)

mod -> entspricht dem Rest einer Division

(Bsp. 7mod3 = 1 heisst so viel wie 7/3 = 2 Rest 1, 8mod3 = 2, 12mod20 = 12)

Lösung der Aufgabe:

Teilaufgabe a)

Die Zufallszahl x_{n+1} kann nicht negativ sein, weil die Konstanten a, b und m nicht negativ sind und bei einer Division keine negativen Reste entstehen.

$0 \leq x_{n+1}$

Weiter kann die Zufallszahl x_{n+1} nicht gleich m oder grösser m sein, da sonst nicht vollständig dividiert wurde. Der Rest kann nicht grösser/gleich dem Divisor sein.

$x_{n+1} < m$

Die Folgenglieder liegen alle im Intervall [0,m)

Teilaufgabe b)

Kriterien für eine brauchbare Folge von Zufallszahlen/einen brauchbaren Parametersatz
-lange Periode (soll lange gehen bis sich eine Zufallszahl wiederholt)
-kein wiederholendes Zahlenmuster

I) $a = 17$, $b = 1$, $m = 307$, $x_0 = 0$ und $n \leq 10000$

$x_{n+1} = (17 \cdot x_n + 1) \bmod 307$

$x_0 = 0$

$x_1 = (17 \cdot 0 + 1) \bmod 307 = 1$

$x_2 = (17 \cdot 1 + 1) \bmod 307 = 18$

$x_3 = (17 \cdot 18 + 1) \bmod 307 = 0$

$x_4 = (17 \cdot 0 + 1) \bmod 307 = 1$

$x_5 = (17 \cdot 1 + 1) \bmod 307 = 18$

II) $a = 2$, $b = 0$, $m = 10000$, $x_0 = 1$ und $n \leq 13$

$x_{n+1} = (2 \cdot x_n + 0) \bmod 10000$

$x_0 = 1$

$x_1 = (2 \cdot 1 + 0) \bmod 10000 = 2$

$x_2 = (2 \cdot 2 + 0) \bmod 10000 = 4$

$x_3 = (2 \cdot 4 + 0) \bmod 10000 = 8$

$x_4 = (2 \cdot 8 + 0) \bmod 10000 = 16$

$x_5 = (2 \cdot 16 + 0) \bmod 10000 = 32$

III) $a = 2$, $b = 0$, $m = 10000$, $x_0 = 1$ und $n \leq 10^6$

$x_0 = 1$

$x_1 = 2$

$x_2 = 4$

$x_3 = 8$

$x_4 = 16$

$x_5 = 32$

IV) $a = 0.9$, $b = 0$, $m = 10000$, $x_0 = 5$ und $n \leq 10^6$

$x_0 = 5$

$x_1 = 4.5$

$x_2 = 4.05$

$x_3 = 3.645$

$x_4 = 3.2805$

$x_5 = 2.95245$

V) $a = 1$, $b = 1$, $m = 10000$, $x_0 = 2$ und $n \leq 1000$

$x_0 = 2$

$x_1 = 3$

$x_2 = 4$

$x_3 = 5$

$x_4 = 6$

$x_5 = 7$

Beurteilung der Parametersätze

I) unbrauchbar, weil sehr kurze Periode (beginnt nach drei Folgenglieder sich zu wiederholen)

II) unbrauchbar, weil sehr kurze Periode (13 Folgenglieder) und erkennbares Zahlenmuster (Potenzen von zwei)

III) unbrauchbar, gleicher Parametersatz wie II, aber mit längerer Periode

IV) unbrauchbar, Zahlenmuster (Multiplikation von 0.9)

V) unbrauchbar, Zahlenmuster (alle natürlichen Zahlen beginnend bei zwei)