Heads and Tails, summer 2009

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

11. Exercise sheet
Hand in solutions until Sunday, 12 July 2009, 24:00h.

Exercise 11.1 (Blum-Blum-Shub Generator). (17+12 points)

Let $N := 1333$ and $x_0 := 101$. We consider the set $S \subseteq \mathbb{Z}_{1333}^\times$ of squares modulo 1333, and the set T of numbers a modulo 1333 with $\left(\frac{a}{1333}\right) = 1$, which are not squares.

(i) How many elements do S and T have? $\boxed{1}$

(ii) Determine the sets S and T by giving an algorithm to find them. $\boxed{2}$

(iii) Verify (using a programming language of your choice), that squaring modulo 1333 is a bijection $S \to S$. $\boxed{2}$

(iv) Verify (using a programming language of your choice), that the function $x \mapsto x^2 \bmod 1333$ is a bijection $T \to S$. $\boxed{+2}$

Let p, q be the smallest prime numbers with $p \geq 2^9$ or $q \geq 2^{11}$ and $p \equiv q \equiv 3 \bmod 4$. Let $N := p \cdot q$ and $x_0 = 100\,001$.

(v) Implement the Blum-Blum-Shub-Generator in a programming language of your choice. [$x_i \leftarrow x_{i-1}^2 \operatorname{rem} N$, $z_i \leftarrow x_i \operatorname{rem} 2$.] $\boxed{5}$

(vi) Compute the first 50 bits with the generator. $\boxed{2}$

Carry out a few statistical tests:

(vii) What is the probability of possible pairs (z_{2i}, z_{2i-1}) for $i = 1..2^{13}$? Compare with the theoretical values. $\boxed{2}$

(viii) What is the mean value and the standard deviation for 2^{13} bits. Compare with the theoretical values for a "real" random generator. $\boxed{3}$

(ix) Repeat the last statistical analysis, but this time, combine two bits to one number: $Z_i = z_{2i} \cdot 2 + z_{2i-1}$. [This is how to get the theoretical values: If X, Y are independent random bits, then the expected value of $Z = 2X + Y$ can easily be determined as: $E(Z) = 2E(X) + E(Y) = 2 \cdot \frac{1}{2} + \frac{1}{2}$. Considering $X^2 = X$, obviously $E(X^2) = E(X)$ holds thus we can easily compute $E(Z^2) = E(4X^2 + 4XY + Y^2) = 2 + 1 + \frac{1}{2} = 3\frac{1}{2}$. Now the variance is $V(Z) := E((Z - EZ)^2) = E(Z^2) - (E(Z))^2 = 3\frac{1}{2} - (\frac{3}{2})^2 = \frac{5}{4}$.] $\boxed{+3}$

(x) Plot 1 000 points (u, v), where the binary representation of u and v are 10 bits out of the produced series of bits each. Can any regularities be seen in the picture? Compare with a simple linear Kongruenzgenerator: $x_i \leftarrow 313x_{i-1} \operatorname{rem} 2053$, $z_i \leftarrow x_i \operatorname{rem} 1024$, where each value gives a coordinate u or v. $\boxed{+4}$

(xi) Interpret your results! $\boxed{+3}$