UNIVERSITÉ Grenoble Alpes — Master of Science in Informatics at Grenoble — Grenoble INP ensimag

UE Mathematics for Computer Science

Homework, November 2016

Write on your homework:
I understand what plagiarism entails and I declare that this report is my own, original work.
Name, date and signature.

- The firm deadline is Monday December 19 midnight (before Tuesday).
- The homework should be 4 pages (one for each generator and proof) in the pdf format (scanned manuscripts in pdf are allowed)
- the filename should be FamilyName-Mosig-MfCS-HW2.pdf
- send with your official mail () at Jean-Marc.Vincent@imag.fr with the subject
  `[MOSIG1:MfCS] Homework2 FamilyName`

Passwords

The problem is to build random generators of passwords. We have to guarantee that all possible passwords have the same probability of occurence (uniformity property), so that a generated password will be difficult to predict. To avoid too simple passwords, the generator should verify some given constrains, (at least one figure, more than 3 vowels,...) We suppose given a set of characters (letters and figures) :

$$\mathcal{C} = \{a, b, \cdots, z, 0, 1, \cdots, 9\}.$$

A password is a sequence of n characters in $\mathcal{C}$, for simplicity we choose $n = 8$. For the following constrains, **design a generation algorithm** and provide a **proof of uniformity** :

1. no restrictions on the password;
2. contains two or three figures;
3. not two consecutive figures;
4. only $n = 5$ figures (in $\{0, 1, \cdots, 9\}$) satisfying the sum equals 25.

For all the homework, we suppose given a random generator **Random** (), a sequence of calls to **Random** () is modeled by a sequence of independent random variables uniformly distributed on $[0, 1[$.