Heads and tails, summer 2015

PROF. DR. JOACHIM VON ZUR GATHEN AND DR. DANIEL LOEBENBERGER

9. Exercise sheet
Hand in solutions until Sunday, 21 June 2015, 23:59:59

Exercise 9.1 (Filling a gap). (3 points)

When creating a square root findet from an lsb-postdictor, we used the following fact without a proof: 3

$$[\frac{x}{2}]_N = \frac{[x]_N + \mathrm{lsb}([x]_N)N}{2}$$

Prove it.

Exercise 9.2 (Continuing the experiments). (17 points)

Goal of this task is to modify your implementations of the generators, such that initializing computations are not measured while running the generators. 17

(i) If not already done, exclude parameter generation from your timing experiments.

(ii) Now measure how long it takes to generate the first 10, 100, 1000, etc. Bytes of output. When does the process stabilize?

(iii) Generate 512 kB of data from the corresponding generators, after their runtime behavior had stabilized.

(iv) Assemble your new findings in a beautiful table.