Prof. Dr. Andreas Podelski, Marco Muñiz, Christian Herrera SS 2012

Theory I, Sheet 6

- The solutions should be submitted in English.
- JUST FOR FUN exercises are not mandatory.
- Your solutions should be delivered to the lockbox in building 051 floor 00, or right before the start of the tutorial (June 11, 4:00 p.m.).
- You are allowed to discuss your solutions with each other. Nevertheless, you are required to write down the answers in your own words.

Exercise 6.1 - Randomized Quicksort

Consider a variant of the randomized Quicksort algorithm, in which only l or r (leftmost,rightmost element) can be taken with probability p_l and p_r as pivot elements. Further, consider the set $n = \{n_1, n_2, \ldots, n_m\}$ where $n_i < n_j$ for $i < j$, $0 < i$ and $j \leq m$. Give 3 permutations π of n and 3 different assignments for p_l and p_r such that the running time $T(n) = \Theta(n^2)$.

Exercise 6.2 - Primality test

Consider the number $n = 1105$. Use the randomized primality test algorithm with $a = 7$ to determine if n is probably prime or not prime. Each recursive call and each intermediate value of the result should be provided.

Exercise 6.3 - RSA encryption

For an RSA encryption choose $p = 17, q = 23, e = 5$ and $d = 141$.

1. By using the public key, encrypt the decimal message $M = 12$.
2. Decrypt the message $M' = 53$.