Karlsruhe Institute of Technology

Stefan Walzer, Stefan Hermann
ITI Prof. Sanders
winter term 2025/2026

Exercise Sheet 2 – The Power of Randomness

Probability and Computing

Exercise 1 – Checking Polynomial Equations

Let $\mathbb{F}$ be a field, for example $\mathbb{F} = \mathbb{Q}$. Given is a polynomial equation, for example:

$$(x^3 + 2x^2 - 5x - 6)(x^2 + x - 20)(x - 6) \overset{?}{=} x^6 - 7x^3 + 25$$

(a) Argue: In the case that the example equation does *not* hold, there are at most 6 values of x for which both sides yield the same result.

(b) Describe a randomized algorithm that decides whether a polynomial equation holds or not. This algorithm may accept false polynomial equations as correct with a small probability. What can be said about this probability?

Exercise 2 – Checking Matrix Products[1]

Let $\mathbb{F}$ be a field, and $n \in \mathbb{N}$.

(a) Show: If $C, C' \in \mathbb{F}^{n \times n}$ are two different matrices and $v \in \{0,1\}^n$ is chosen uniformly at random, then $\Pr[C \cdot v \neq C' \cdot v] \geq \frac{1}{2}$.

(b) Describe an algorithm that, given $A, B, C \in \mathbb{F}^{n \times n}$, outputs a bit X with $X = 1$ if $A \cdot B = C$ and $\Pr[X = 1] \leq 1/2$ if $A \cdot B \neq C$. The algorithm should perform only $O(n^2)$ field operations.

Exercise 3 – Deterministic Evaluation of $\bar{\wedge}$-Trees

Let A be a deterministic algorithm that takes as input a bit vector $I \in \{0,1\}^n$ (with $n = 2^d$) and computes the value of the complete balanced $\bar{\wedge}$-tree whose leaves are labeled according to I. Show: There exists an input $I_A \in \{0,1\}^n$ such that A must inspect every leaf label.

[1] Known as Freivalds' Algorithm.