universität innsbruck

Discrete Structures/Mathematics WS 2020/2021 LVA 703069

EXAM 1 January 27th, 2021

This exam consists of three regular exercises (1–3) each worth 20 points, so 60 points in total. In addition, there are bonus exercises (1(f),2(d),3(d) worth 16 points in total). The available points for each item are written in the margin. You need at least 30 points to pass. Always explain your answer. In particular, for yes/no questions the correct answer is worth 1 point with the remaining points for the explanation. The time available is 1 hour and 45 minutes (105 minutes).

Throughout this exam, let the words f and l be your first respectively last name written (in lowercase, omitting diacritics) over the alphabet $\Sigma = \{\mathtt{a}, ..., \mathtt{z}\}$, and let m be your Matrikelnr. having 8 digits $m_1m_2m_3m_4m_5m_6m_7m_8$ with $0 \leq m_i \leq 9$. **Start each document handed in with (writing down) your f, l, and m.**

1 Consider the relation $<$ on words over the alphabet Σ defined by:

$$v < w \text{ if } (\ell(v) \leq \ell(w) \text{ and } v <_{lex} w)$$

where $\ell(w)$ denotes the length of the word w as usual.

[4] (a) Is $f < l$ true? Is $l < f$ true? Explain your answers, basing yourself on the definition of $<$.

[4] (b) Draw the Hasse diagram of the relation $<$ restricted to the 6 words $\mathtt{a}$, $\mathtt{z}$, $\mathtt{a}^{20}$, $\mathtt{z}^{20}$, f, and l.

[4] (c) Describe the goal of topological sorting and do a topological sort of the same 6 words as in the previous item with respect to the relation $<$. Give the set of minimal elements at each stage of the topological sorting process.

[4] (d) Is the relation $<$ total? Give a justification (in case of yes) or a counter-example (in case of no).

[4] (e) Is the relation $<$ well-founded? Give a justification or a counter-example.

[5] (f) (bonus) Let the language L over $\{0, 1\}$ consist of the empty word ϵ and the words that are created by adding a 0 as a prefix and a 1 as a suffix for any word in L. For example, the word $0011 \in L$ but $101 \notin L$. Specify a well-founded relation on the words in L and prove by well-founded induction using that relation, that words in L contain the same number of the zeros and ones.

2 (a) Determine whether $f_i \in \mathrm{O}(n^4)$ for $i \in \{1, 2\}$, where the functions $f_i : \mathbb{N} \to \mathbb{N}$ are described by the following properties:

[6] • $f_1(n) = 8n^{m_8} + n^2 + m_7$;

[6] • f_2 is an increasing function satisfying $f_2(n) = 8f_2(\frac{1}{2}n) + m_8$ for $n = 2^k$ with k a positive natural number and $f_2(1) = 1$;

Base your answers on the definition of O, give intermediate steps, and mention results (from the lecture) used. However, simple convergences, e.g. of $\frac{1}{n^i}$ for positive i, or divergences can be used without proof.

(b) Let A and B be arbitrary sets, such that there exists no bijection between [4] A and B. Do total functions $g : A \to B$ and $g' : B \to A$ exist such that both g and g' are injective? Explain your answer.

(c) Suppose A, B, C are finite sets such that $\#(A \cup B \cup C) \neq \#A + \#B + \#C$. [4] Argue whether or not there then exists some a that is an element of (at least) two of A, B, C. If so, give a proof. If not, give a counterexample.

(d) (bonus) When is a language recursively enumerable? Determine for each of the following two languages (over some appropriate finite alphabet) [6] whether it is recursively enumerable or not, explaining why (not):

• $L_1 = \{M\#x \mid \text{Turing Machine } M \text{ halts on } x \text{ within } \ell(M) \text{ steps}\}$, where ℓ is the length function as usual.

• $L_2 = \sim(HP \cup MP)$, i.e. the complement of the union of the halting and membership problems.

3 (a) Let $k = 3m_3m_6$ in decimal notation (so $300 \leq k \leq 399$).

Determine *all* $0 \leq x \leq k$ that satisfy the 3 congruences:

$$\begin{aligned} x &\equiv 0 \pmod 5 \\ x &\equiv 6 \pmod 7 \\ x &\equiv 3 \pmod 4 \end{aligned}$$

[10] by application(s) of the Chinese Remainder Theorem, and check that your solutions for x satisfy the congruences. Give all computation steps and explain how you conclude that your solutions are the only ones.

(b) Let $k = 1m_2$ in decimal notation (so $10 \leq k \leq 19$).

Determine what value n in an RSA public key (e, n) should have *at least*, to allow for the faithful encryption of all words of *exactly* k symbols over [5] the alphabet Σ (which comprises 26 symbols). To that end, determine how many such words there are, and propose an encoding/decoding of such words as numbers. (Encryption being faithful means that decrypting after encryption yields the original.)

(c) Let $k = m$ in decimal notation (so $0 \leq k < 10^8$).

Compute $2^k \mod 101$ by hand, giving each computation step and ex- [5] plaining the reasoning steps used. (You may use a calculator/computer program to verify your result, but your computation/reasoning by hand is what is asked for. You may, but need not, use $2^{10} \equiv 14 \mod 101$.)

(d) (bonus) Determine *all* solutions $0 \leq x \leq k$ after adjoining the congru- [5] ence $x \equiv 1 \pmod 2$ to the ones in item a). Explain these are *all*.