universität innsbruck

Discrete Structures/Mathematics WS 2020/2021 LVA 703069

EXAM 3 September 24th, 2021

This exam consists of <u>three</u> regular exercises (1–3) each worth 20 points, so 60 points in total. In addition, there are bonus exercises (1(e) and 2(d) worth 11 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, 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 name and m.**

The concrete solutions below are given for the Matrikelnr. 15658571, with solutions for other Martikelnrs. being analogous.

$\boxed{1}$ Consider the relation R on the set $D = \{1, 4, 5, 7, 9\}$ of digits, given by $i\ R\ j$ if i occurs strictly before j in your Matrikelnr.. For example, for the Matrikelnr. 15658571 we would obtain: $1\ R\ 1$, $1\ R\ 5$, $1\ R\ 7$, $5\ R\ 1$, $5\ R\ 5$, $5\ R\ 7$ and $7\ R\ 1$, with no other pair of elements of D being R-related. (Note that the questions below are about R for *your* Matrikelnr.).

[3] (a) Is R irreflexive? Explain your answer.

For R to be irreflexive it must hold that have that $d\ R\ d$ for no $d \in D$. Since $1\ R\ 1$ and $1 \in D$, we have that R is not irreflexive.

In general, R is irreflexive iff none of the digits in D occurs more than once in your Matrikelnr..

[3] (b) Is R well-founded? Explain your answer.

For R to be well-founded there should not be an infinite descending sequence $\ldots\ R\ d_2\ R\ d_1\ R\ d_0$ of elements $d_i \in D$. Well-foundedness does not hold here, since $1\ R\ 1$ and $1 \in D$ so setting $d_i = 1$ produces an infinite descending chain.

In general, R is well-founded iff R is irreflexive (so the answer to this item is the same as that to the previous item), with the only–if-direction being immediate and the if-direction following from that if no digit in D is repeated in D, then R is just the (well-founded) left-to-right order on the digits in D as they occur in m.

[7] (c) Compute the reflexive–transitive closure R^* of R. Illustrate the algorithm you use by giving (some of) the intermediate computation steps.

Enumerating the elements of D from small to large (left–right and top–down along the matrix), we obtain by Warshall's algorithm:

$$\begin{pmatrix} 1 & - & 1 & 1 & - \\ - & - & - & - & - \\ 1 & - & 1 & 1 & - \\ 1 & - & - & - & - \\ - & - & - & - & - \end{pmatrix} \xrightarrow{\textit{Preprocessing}} A_0 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \to A_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \to A_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

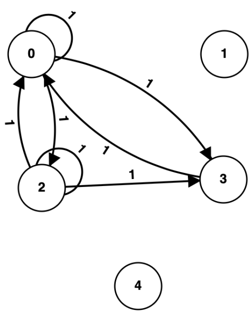
$$\to A_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \to A_4 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \to A_5 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{\textit{Solution}} \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

from which we read off that $i\ R^*\ j$ if $\mathit{Solution}_{ij} = 1$.

Note that although there are in principle 5 steps, the steps are simple or even trivial (since 4 and 9 do not occur in this Matrikelnr., the 3rd and 5th rows and columns only contain zeros; they could have simply been omitted from the computation).

[7] (d) Draw the directed graph G corresponding to R and compute for each pair of nodes in G the length of the shortest path (you may assume edges to have weight 1) from the first to the second. Illustrate the algorithm you use by giving (some of) the intermediate computation steps.

For the correspondence between nodes and digits given by $0 \mapsto 1$, $1 \mapsto 4$, $2 \mapsto 5$, $3 \mapsto 7$, $4 \mapsto 9$ we obtain the following graph and the result of Floyd's algorithm applied to it:



$$\begin{pmatrix} 1 & - & 1 & 1 & - \\ - & - & - & - & - \\ 1 & - & 1 & 1 & - \\ 1 & - & - & - & - \\ - & - & - & - & - \end{pmatrix} \xrightarrow{\textit{Preprocessing}} A_0 = \begin{pmatrix} 0 & \infty & 1 & 1 & \infty \\ \infty & 0 & \infty & \infty & \infty \\ 1 & \infty & 0 & 1 & \infty \\ 1 & \infty & \infty & 0 & \infty \\ \infty & \infty & \infty & \infty & 0 \end{pmatrix} \to A_1 = \begin{pmatrix} 0 & \infty & 1 & 1 & \infty \\ \infty & 0 & \infty & \infty & \infty \\ 1 & \infty & 0 & 1 & \infty \\ 1 & \infty & 2 & 0 & \infty \\ \infty & \infty & \infty & \infty & 0 \end{pmatrix} \to A_2 = \begin{pmatrix} 0 & \infty & 1 & 1 & \infty \\ \infty & 0 & \infty & \infty & \infty \\ 1 & \infty & 0 & 1 & \infty \\ 1 & \infty & 2 & 0 & \infty \\ \infty & \infty & \infty & \infty & 0 \end{pmatrix}$$

$$\to A_3 = \begin{pmatrix} 0 & \infty & 1 & 1 & \infty \\ \infty & 0 & \infty & \infty & \infty \\ 1 & \infty & 0 & 1 & \infty \\ 1 & \infty & 2 & 0 & \infty \\ \infty & \infty & \infty & \infty & 0 \end{pmatrix} \to A_4 = \begin{pmatrix} 0 & \infty & 1 & 1 & \infty \\ \infty & 0 & \infty & \infty & \infty \\ 1 & \infty & 0 & 1 & \infty \\ 1 & \infty & 2 & 0 & \infty \\ \infty & \infty & \infty & \infty & 0 \end{pmatrix} \to A_5 = \begin{pmatrix} 0 & \infty & 1 & 1 & \infty \\ \infty & 0 & \infty & \infty & \infty \\ 1 & \infty & 0 & 1 & \infty \\ 1 & \infty & 2 & 0 & \infty \\ \infty & \infty & \infty & \infty & 0 \end{pmatrix} \xrightarrow{\textit{Solution}} \begin{pmatrix} 0 & \infty & 1 & 1 & \infty \\ \infty & 0 & \infty & \infty & \infty \\ 1 & \infty & 0 & 1 & \infty \\ 1 & \infty & 2 & 0 & \infty \\ \infty & \infty & \infty & \infty & 0 \end{pmatrix}$$

from which we read off that the shortest path from i to j has length k if $\mathit{Solution}_{ij} = k$.

Note that this could also be used to answer other items; e.g. the graph having loops shows that R is neither irreflexive nor well-founded, and the reflexive–transitive closure R^* may be read off from the *Solution* by replacing all non-∞s by 1s.

[5] (e) (bonus) Does there exist a Martikelnr. for which the corresponding relation R would *not* be transitive? Argue why (not).

As we have seen above for the Matrikelnr. 15658571, the corresponding R is not transitive: we have $7\ R\ 1$ and $1\ R\ 5$ but not $7\ R\ 5$ (indeed, computing the reflexive–transitive closure was not trivial, it required one transitivity-step). In general, transitivity may fail due to a pattern like $\dots j \dots k \dots i \dots j \dots$ for a Matrikelnr., so that we have $i\ R\ j$ and $j\ R\ k$ but not (necessarily) $i\ R\ k$.

$\boxed{2}$ (a) For $k = m_7 + 2$, consider k-mergesort, the variation on mergesort that sorts a list ℓ of length greater than 1 by splitting it into k lists $\ell_1, \dots, \ell_k$ of equal lengths, recursively k-mergesorts $\ell_1, \dots, \ell_k$ to yield $s_1, \dots, s_k$,
[7] and then does a k-way merge of the $s_1, \dots, s_k$ to yield a sorted list s.

Analyse the (time) complexity $T(n)$ of k-mergesort, for n the length of the input-list. You may restrict your analysis to lists whose length is a power of k (so that in each recursive call all k parts indeed do have equal lengths), and you may assume that a k-way merge takes time linear in the length of the merged lists.

Given our Matrikelnr. $k = 9$, so we consider 9-mergesort. By the specification, the time-complexity expressed in term of the length n of the list, is then given by the recurrence $T(n) = 9 \cdot T(\frac{n}{9}) + n$ if n is a positive power of 9, and 1 otherwise. Since this recurrence is of the shape required by the master theorem for $a = b = 9$ and $s = 1$, and since we are in its second case since $a = b^s$, we obtain $T(n) \in \Theta(n \log n)$.

Note that in fact the result here is independent of k, i.e. of the Matrikelnr. (with the $\dots + 2$ in the definition of k guaranteeing that $a, b > 1$ even if the digit m_7 would be 0 or 1).

(b) Does there exist a natural number x such that $x \equiv m_2 \pmod{m_3 + 2}$ and
[7] $x \equiv m_4 \pmod{m_3 + 3}$? If so, compute such an x by applying Bézout's Lemma/the Chinese Remainder Theorem. If not, argue why not.

For the Matrikelnr. 15658571 the question becomes whether there exists a natural number x such that $x \equiv 5 \pmod 8$ and $x \equiv 5 \pmod 9$. This is obviously true for $x = 5$.

To compute this using the CRT, note that by the difference between 8 and 9 only being 1, we obtain a particularly simple instance of Bézout's lemma: $1 = -1 \cdot 8 + 1 \cdot 9$ and a ditto instance of the Chinese Remainder Theorem: $x = -1 \cdot 8 \cdot 5 + 1 \cdot 9 \cdot 5 = 5$, as desired.

In general, the computation is as simple as above, since for any number $n > 1$ (guaranteed by the $\dots + 2$ in the definition of the modulus), n and $n + 1$ are relatively prime (coprime) with difference 1.

(c) Do there exist sets A, B and C such that $\#(A \cup B \cup C) = 20$, $\#A = 10$,
[6] $\#B = 10$, $\#C = 10$, $\#(A \cap B) = m_5$, $\#(B \cap C) = m_6$, $\#(C \cap A) = m_7$ and $\#(A \cap B \cap C) = m_8$? Prove your answer.

[6] For this Matrikelnr. 15658571 the question becomes whether there are A, B and C such that $\#(A \cup B \cup C) = 20$, $\#A = 10$, $\#B = 10$, $\#C = 10$, $\#(A \cap B) = 8$, $\#(B \cap C) = 5$, $\#(C \cap A) = 7$ and $\#(A \cap B \cap C) = 1$?

By the inclusion–exclusion principle, if such sets were to exist, we should have $\#(A \cup B \cup C) = \#A + \#B + \#C + \#(A \cap B \cap C) - \#(A \cap B) - \#(B \cap C) - \#(C \cap A)$, i.e. $20 = 10 + 10 + 10 + 1 - 8 - 5 - 7$. Since $20 \neq 11$ we conclude no sets as desired exist.

In general, the question has a positive answer for a some Matrikelnr. iff $m_5 + m_6 + m_7 - m_8 = 10$ (inclusion–exclusion) and $m_5, m_6, m_7 \geq m_8$ (to ensure that the intersection of all three sets does not have more elements than the intersections of each pair of sets).

[6] (d) (bonus) Recall that for languages L_1, L_2 over Σ, L_1 is said to be *reducible* to L_2, denoted by $L_1 \leq L_2$, if there exists a computable $f : \Sigma^* \to \Sigma^*$ such that $x \in L_1 \Leftrightarrow f(x) \in L_2$.

Explain how the notion of reducibility is typically used to show languages are not recursive, and why the condition that f be *computable* cannot be omitted from the definition (of reducibility), without rendering it useless for that usage.

If $L_1 \leq L_2$ and L_1 is not recursive then L_2 is not recursive either. So typically to show that a language L_2 is not recursive, one tries to come up with a language L_1 that is

- already known to be non-recursive, e.g. the HP or the MP;
- is easily/conveniently reducible to L_2.

The condition that the reduction f be computable cannot be omitted, since otherwise we could show HP to be recursive by defining f to map $x \in HP$ to 0 and $x \notin HP$ to 1. Technically, if $L_1 \leq L_2$ and L_2 is decided by a Turing Machine M_2 but we do not know whether f is computable, it need not be possible to construct a Turing Machine M_1 deciding L_1 (if f is computable, say by TM F, then such an M_1 *can* be constructed by composing F and M_2).

$\boxed{3}$ Determine for each of the following statements whether they are true or not. (Recall from above that a correct yes/no answer gives 1 point; the remaining 3 points are for the explanation.)

[4] (a) Let $k = m_8 + 2$ and suppose p is a natural number relatively prime to k such that $k^{p-1} \not\equiv 1 \pmod{p}$. Then p is not a prime number.

This is true by (the contrapositive) of Fermat's Little Theorem. (The value of k is in fact not relevant for this, only k and p being relatively prime is.)

[4] (b) Every undirected connected multigraph having exactly 4 edges e_3, e_4, e_5, e_6, with respective weights m_3, m_4, m_5, m_6 (where the m_i are taken from your Matrikelnr.), has a *unique* minimum spanning tree.

For this Matrikelnr. 15658571 the edges have weights $6, 5, 8, 5$. Putting the edges in a straight line except for e_4 and e_6 being parallel, gives *two* distinct minimum spanning trees (containing e_3 and e_5, and either e_4 or e_6).

In general, the statement is true iff there are no duplicate weights: If there are no duplicates then Kruskal's MST algorithm is deterministic, yielding a unique MST. Otherwise, we can build a multigraph as above having parallel edges of the same weight giving rise to more then one MST.

[4] (c) For all finite sets A, B, C and D with respective cardinalities m_4, m_5+1, m_6 and m_7 (where the m_i are taken from your Matrikelnr.), the cardinality of the set $A^B \times (C \cup D)$ can be computed as $m_4^{m_5+1} \cdot (m_6 + m_7)$.

For this Matrikelnr. 15658571 the respective cardinalites are $5, 9, 5, 7$. If make C have a non-empty intersection with D, then the cardinality of $C \cup D$ is smaller than $m_6 + m_7$, and the computation given fails.

In general, the computation works ('by accident') iff there cannot be non-empty intersections between C and D, i.e. iff at least one of m_6 and m_7 is 0.

[4] (d) If removing an edge from an undirected (and unweighted) graph G results in G', then we have for their diameters $d(G) \leq d(G')$.

Here the *diameter* $d(G)$ of a graph G is the maximum of the distances of all pairs of vertices in G, where for vertices v and w their *distance* $d(v, w)$ is defined as usual as the length of the shortest path in G between v and w (∞ if no such path exists; thus, $d(G) = \infty$ iff G is not connected).

This is true since the set of paths between two given vertices of G' are a subset of those in G, hence distances can only increase.

[4] (e) Let k be the number $m_1m_2m_3m_4m_5m_6m_7m_88$ in decimal notation, i.e. your Matrikelnr. followed by an 8. Then k is not a square.

This is seen to be true by modulo arithmetic. For every $0 \leq d \leq 9$, we have $d^2 \not\equiv 8 \pmod{10}$ as one may check by distinguishing (the 10) cases. Since every natural number n can be written uniquely as $m \cdot 10 + d$ for some $0 \leq d \leq 9$ and $n^2 \equiv d^2 \pmod{10}$, we conclude.

Note that this reasoning does not depend in fact on the Matrikelnr..