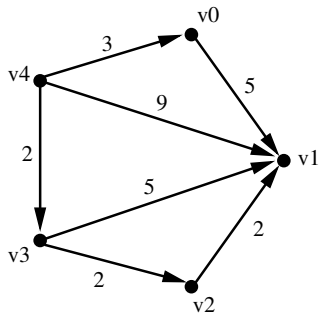
universität innsbruck

Discrete Structures/Mathematics WS 2019/2020 LVA 703070/703015

EXAM 3 September 25th, 2020, 9:00–10:45

This exam consists of three regular exercises (1–3) each worth 20 points. The time available is 1 hour and 45 minutes (105 minutes). The available points for each item are written in the margin. There are 60 points in total for the regular exercises. In addition, there is a bonus exercise (4∗) worth 17 points. You need at least 30 points to pass.

1 Let the graph G with nodes $\{v0, v1, v2, v3, v4\}$ be given by:



(a) For the nodes ordered as $v0, v1, v2, v3, v4$ in the matrices, we compute:

$$\begin{pmatrix} - & 5 & - & - & - \\ - & - & - & - & - \\ - & 2 & - & - & - \\ - & 5 & 2 & - & - \\ 3 & 9 & - & 2 & - \end{pmatrix} \xrightarrow{\text{Preprocessing}} A_0 = \left(\begin{array}{c|cccc} 0 & 5 & \infty & \infty & \infty \\ \hline \infty & 0 & \infty & \infty & \infty \\ \infty & 2 & 0 & \infty & \infty \\ \infty & 5 & 2 & 0 & \infty \\ 3 & 9 & \infty & 2 & 0 \end{array}\right) \rightarrow A_1 = \left(\begin{array}{c|cccc} 0 & 5 & \infty & \infty & \infty \\ \hline \infty & 0 & \infty & \infty & \infty \\ \infty & 2 & 0 & \infty & \infty \\ \infty & 5 & 2 & 0 & \infty \\ 3 & 8 & \infty & 2 & 0 \end{array}\right) \rightarrow A_2 = \left(\begin{array}{cc|ccc} 0 & 5 & \infty & \infty & \infty \\ \infty & 0 & \infty & \infty & \infty \\ \hline \infty & 2 & 0 & \infty & \infty \\ \infty & 5 & 2 & 0 & \infty \\ 3 & 8 & \infty & 2 & 0 \end{array}\right)$$

$$\rightarrow A_3 = \left(\begin{array}{cc|ccc} 0 & 5 & \infty & \infty & \infty \\ \infty & 0 & \infty & \infty & \infty \\ \hline \infty & 2 & 0 & \infty & \infty \\ \infty & 4 & 2 & 0 & \infty \\ 3 & 8 & \infty & 2 & 0 \end{array}\right) \rightarrow A_4 = \left(\begin{array}{cc|ccc} 0 & 5 & \infty & \infty & \infty \\ \infty & 0 & \infty & \infty & \infty \\ \hline \infty & 2 & 0 & \infty & \infty \\ \infty & 4 & 2 & 0 & \infty \\ \hline 3 & 6 & 4 & 2 & 0 \end{array}\right) \rightarrow A_5 = \begin{pmatrix} 0 & 5 & \infty & \infty & \infty \\ \infty & 0 & \infty & \infty & \infty \\ \infty & 2 & 0 & \infty & \infty \\ \infty & 4 & 2 & 0 & \infty \\ 3 & 6 & 4 & 2 & 0 \end{pmatrix} \xrightarrow{\text{Solution}} \begin{pmatrix} 0 & 5 & \infty & \infty & \infty \\ \infty & 0 & \infty & \infty & \infty \\ \infty & 2 & 0 & \infty & \infty \\ \infty & 4 & 2 & 0 & \infty \\ 3 & 6 & 4 & 2 & 0 \end{pmatrix}$$

Since the second column (paths to $v1$) of the last row (paths from $v4$) of the final matrix A_5 represents the length of the shortest path from $v4$ to $v1$, the answer is 6, the length of the path $(v4, v3, v2, v1)$.

(b) A topological sorting of the nodes of G is a listing $v_{i_0}, \ldots, v_{i_4}$ of the nodes in G such that if there is a path from v_{i_k} to v_{i_ℓ} in G, then $k \leq \ell$. Since we have edges $v4 \rightarrow v3 \rightarrow v2 \rightarrow v1$ in G, we must have that $v4$ precedes $v3$ precedes $v2$ precedes $v1$ in the topological sorting. Since we have edges $v4 \rightarrow v0 \rightarrow v1$, $v4$ must precede $v0$ which must precede $v1$. Combining both gives rise to the three topological sortings $v4, v0, v3, v2, v1$ and $v4, v3, v0, v2, v1$ and $v4, v3, v2, v0, v1$, obtained by inserting $v0$ somewhere between $v4$ and $v1$ in $v4, v3, v2, v1$.

(c) We define $r(n, v)$ by recursion on its first argument as $\{v\}$ if $n = 0$ and as $\bigcup_{(v,w)\in G} r(n-1, w)$ otherwise. The function is well-defined because the first argument $n-1$ in the recursive call in the rhs is strictly less than the first argument n in the lhs, and the less-than order on natural number is well-founded, so the recursion always terminates in the base case $n = 0$. We evaluate $r(2, v4) = r(1, v0) \cup r(1, v1) \cup r(1, v3) = (r(0, v1)) \cup (\emptyset) \cup (r(0, v1) \cup (r(0, v2)) = \{v1, v2\}$.

2 (a) Using fast exponentiation and modular arithmetic we compute $15^{14} \equiv 2^{14} = 4^7 = 4 \cdot 16^3 \equiv 4 \cdot 3^3 = 12 \cdot 3^2 \equiv 4 \pmod{13}$. If $2 \cdot x = 14$, then $15 \cdot x \equiv 2 \cdot x \equiv 1 \pmod{13}$, so we may take $x = 7$ as the inverse of 15 modulo 13. This may be verified by computing $7{\cdot}15 = 105 = 8{\cdot}13{+}1 \equiv 1 \pmod{13}$.

(b) Intuitively, a pair (n, m) can be thought of as the fraction $\frac{n}{m}$. Then R relates fractions representing the same rational number, which we already 'know' to be an equivalence relation. We verify it. That is, we verify that R is reflexive, symmetric, and transitive. Reflexivity holds since $n \cdot m = n \cdot m$, symmetry since $n \cdot m' = n' \cdot m$ iff $n' \cdot m = n \cdot m'$, and transitivity follows from that if $n \cdot m' = n' \cdot m$ and $n' \cdot m'' = n'' \cdot m'$, then $n \cdot m' \cdot m'' = n' \cdot m \cdot m'' = n'' \cdot m \cdot m'$ hence $n \cdot m'' = n'' \cdot m$ by cancelling m' on both ends.

Two pairs R-related to $(3, 5)$ are, for example, $(6, 10)$ and $(9, 15)$; indeed the fractions $\frac{6}{10}$ and $\frac{9}{15}$ both simplify to the fraction $\frac{3}{5}$.

(c) Computing an inverse p' of p modulo q is trivial, since $9 \equiv 1 \pmod{8}$ so is self-inverse; i.e. we may take $p' = 1$. Using this inverse we may compute, using the RSA-version of the Chinese Remainder Theorem, directly that $x = 7 + 9 \cdot (1 \cdot (6 - 7) \mod 8) = 70$. One easily verifies that $70 \equiv 7 \pmod{9}$, and $70 \equiv 6 \pmod{8}$, as desired.

(d) Consider a TM U that given an input first checks that it is of shape $M\#x$ and if not rejects, and if it is simulates running M on x as follows while keeping track of the configurations the TM M has been in, where a configuration comprises the contents of the first 9 symbols on the tape, the position of the head, and the state the TM M is in: U accepts as soon as M would move to the 10th symbol on the tape. Otherwise if the move would lead to a configuration already encountered before, then U rejects (since M would cycle). Otherwise, the configuration is stored and the simulation continues. Since there are only finitely many distinct configurations (because of keeping track only of 9 symbols on the tape, not the whole tape), eventually the simulation halts (accepts or rejects).

[20] 3 Determine whether the following statements are true or false. Every correct answer is worth 2 points. For every wrong answer 1 point is subtracted, provided the total number of points is non-negative.

statement	
	No. For instance, taking $A = \mathbb{N}$ and $B = \{a\}$, the function mapping a to 0 and n to $n + 1$ is an injection from $\mathbb{N} \cup \{a\}$ into $\mathbb{N}$.

Yes. Since reflexivity and transitivity hold by assumption, it suffices to show symmetry. Suppose $a\ R\ b$. By reflexivity then also $a\ R\ a$, hence by the assumption $b\ R\ a$, as desired.

Yes. We have to show that for all $b \in A$, $a \leq b$ (a is least) iff for no $b \in A$, $b < a$ (a is minimal). For the if-direction, we have for an arbitrary b that $a \leq b$ or $b \leq a$ by totality of $\leq$. Since $b < a$ does not hold by assumption, we conclude the former, i.e. $a \leq b$, must hold. For the only–if-direction, for an arbitrary b we cannot have $b < a$ since then the assumption that $a \leq b$ combined with transitivity would yield $b < b$ contradicting irreflexivity of $<$.

No. R is symmetric since $|x-y| = |y-x|$, but R is not transitive, for instance $0\ R\ 4$ and $4\ R\ 8$ but not $0\ R\ 8$.

Yes. Since g is specified recursively, to verify the claim it suffices to check that the former satisfies the specification of the latter, by substitution. For $n = 0$ and $n = 1$, this is trivial. For $n \geq 2$ we compute $2^{f(n)} = 2^{f(n-2)+f(n-1)} = 2^{f(n-2)} \cdot 2^{f(n-1)}$.

Yes. $\frac{\mathrm{lcm}(5^2 \cdot 17^2 \cdot 25, 7 \cdot 5^4)}{\gcd(5^7 \cdot 17^3 \cdot 49, 5^4 \cdot 17^2)} = \frac{5^4 \cdot 7^1 \cdot 17^2}{5^4 \cdot 17^2} = 7$.

Yes. The if-direction follows from that $R \subseteq R^+$, by definition of R^+ as the least relation *extending* R that is transitive: if there were an infinite descending chain $\ldots\ R\ x_2\ R\ x_1$ then there also would be an infinite descending chain $\ldots\ R^+\ x_2\ R^+\ x_1$ contradicting the assumed well-foundedness of R^+.
The only–if-direction follows from that if $x\ R^+\ x'$, then for some n there are $x^1, \ldots, x^n$ such that $x = x^1\ R\ \ldots\ R\ x^n = x'$, by definition of R^+ as the *least* relation extending R that is *transitive*: if there were an infinite descending chain $\ldots\ R^+\ x_2\ R^+\ x_1$ then there also would be an infinite descending chain $\ldots\ldots\ R \ldots R\ x_2 = x_1^{n_1}\ R \ldots R\ x_1^1 = x_1$ contradicting the assumed well-foundedness of R.

Yes. Considering these numbers modulo 7, we know by the Pigeon Hole Principle that at least two of them must be in the same equivalence class as there are more than 7 numbers in the list. The difference of two numbers in the same equivalence class is divisible by 7; formally, $x - y \equiv 0 \pmod 7$ iff $x \equiv y \pmod 7$. (Note that the PHP only yields that there must be such numbers, but does not give a concrete pair. A procedure for finding such a pair of numbers is to successively compute for each number in the list its remainder when dividing by 7. Proceeding from the left we find that both 98430 and 28451 have remainder 3, and indeed for their difference we have $98430 - 28451 = 69979 = 7 \cdot 9997$.)

Yes. Since N is finite, by the PHP there must be some $n \in N$ that occurs twice in the sequence s, say $s_k = n = s_{k+\ell}$ for some k and $\ell > 0$. Since f is a function, it follows that $s_{k+1} = f(s_k) = f(s_{k+\ell}) = s_{k+\ell+1}$ and more generally/by induction that $s_i = s_{\ell+i}$ for all $i \geq k$. (Note that the PHP only yields that there must be such a repetition, but does not give concrete values for k and ℓ. To find such numbers various algorithms exists, one particularly nice one being the so-called tortoise and hare algorithm 'due' to Floyd.)

No. The former is countable (is equinumerous to $\mathbb{N}$) but the latter is not (is equinumerous to $\mathbb{R}$)

4∗ (a) Transitivity may fail. For instance, we have $(1,2)\ R_0\ (0,0)$ and $(0,0)\ R_0\ (2,3)$ but not $(1,2)\ R_0\ (2,3)$. Transitivity fails for R_0 because of 'division by zero'; multiplying different numbers by 0 yields 0. Formally, the cancellation law saying that if $n \cdot m = n \cdot k$ then $m = k$, used in our reasoning above, fails if n is allowed to be 0.

(b) We see that we have an instance of the Master theorem with $a = 5$, $b = 2$, $c = 2$, and $s = 3$. Since $a = 5 < 8 = b^s$, we are in the third case, hence $T(n) \in \Theta(n^3)$. That is, the complexity function T of algorithm A is asymptotically bounded both from below and above by a constant (not necessarily the same) times n^3. As a consequence, since $\Theta = \Omega \cap O$, also $T(n) \in \Omega(n^3)$, i.e. the complexity function T of algorithm A is asymptotically bounded from below by a constant times n^3.

(c) Suppose there is a shortest path from v to w having $k \geq n$ edges. Since $k \geq n$ and the graph has only n nodes, the path must contain a cycle, say the path has weight x and the cycle has weight y. By the assumption that the path is the *shortest* path from v to w, both $y \geq 0$ (otherwise repeating it would give a shorter path contradicting that we had a shortest path), and $y \leq 0$ (otherwise omitting it would give a shorter path contradicting that we had a shortest path). Hence $y = 0$ and omitting the cycle gives another shortest path (i.e. one still having weight x) having fewer edges. Since we may repeat this as long as there are more than n edges on a path, we will obtain a shortest path having fewer than n edges.