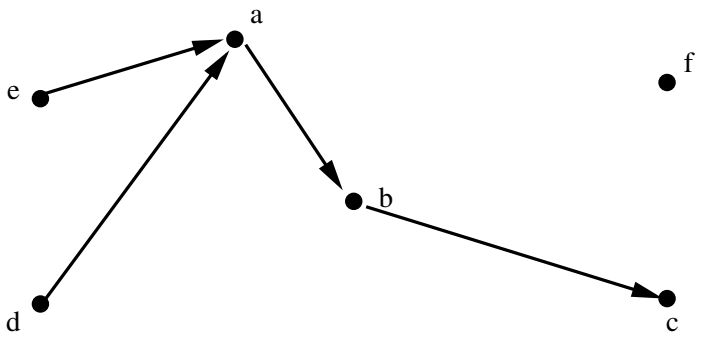
universität innsbruck

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

EXAM 2 | February 28th, 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 are bonus exercises (4∗, 5∗) each worth 15 points. You need at least 30 points to pass.

1 Let the Hasse diagram of the partial order $\leq$ on $\{a, b, c, d, e, f\}$ be given by the dag G:



so that, e.g., $a \leq c$ but not $c \leq a$.

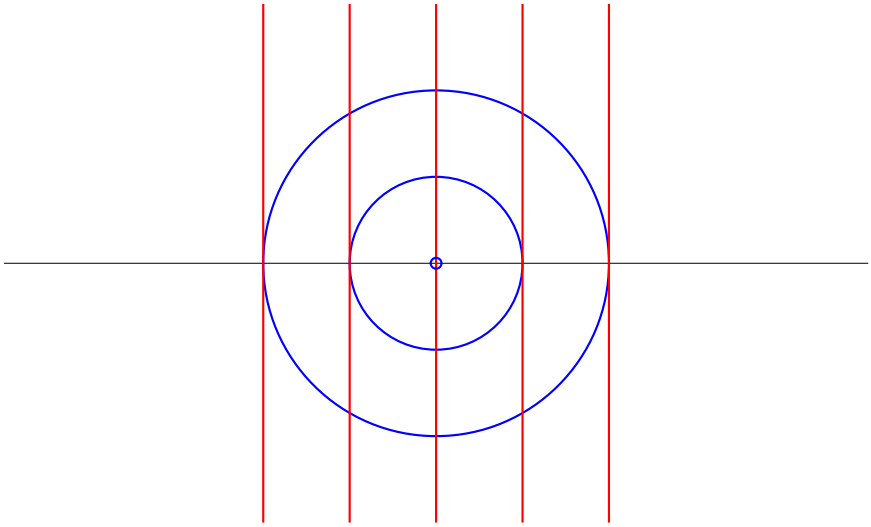
(a) $\{(e,e),(e,a),(e,b),(e,c),(d,d),(d,a),(d,b),(d,c),(a,a),(a,b),(a,c),(b,b),(b,c),(c,c),(f,f)\}$, obtained by relating v to w if there is a (possibly empty) path from v to w in G.

(b) (e,d,a,b,c,f), (d,e,a,b,c,f), (f,e,d,a,b,c), obtained by arbitrarily ordering d and e, before (a,b,c) (as each depends on the one before), and then inserting f somewhere (as that is independent).

(c) $r(v) = \{v\} \cup \bigcup_{(v,w)\in G} r(w)$. This specification is well-defined since G is a dag, hence the edge relation (and its converse) are well-founded. $r(e) = \{e\} \cup r(a) = \{e\} \cup \{a\} \cup r(b) = \{e,a\} \cup \{b\} \cup r(c) = \{e,a,b\} \cup \{c\} = \{e,a,b,c\}$.

2 (a) Using fast exponentiation and modular arithmetic we compute $13^{14} \equiv ((-2)^2)^7 = 4^7 = 4 \cdot (4^2)^3 \equiv 4 \cdot 1^3 = 4 \pmod{15}$. Using $13 \equiv -1 \pmod{14}$ and $-1 \cdot -1 = 1$, we see 13 is its own inverse modulo 14. This may be verified by computing $13 \cdot 13 = 169 = 12 \cdot 14 + 1 \equiv 1 \pmod{14}$.

(b) Both R and S relate (x,y) to (x',y') if their images for some function are the same, namely $f(x,y) = x^2 + y^2$ respectively $g(x,y) = x^2$. All relations defined in this way (via equality of some function on the values) inherit the properties of $=$. In particular, they are equivalence relations. Drawing the equivalence classes of R in blue and those of S in red yields:



where the R-equivalence classes are circles with radius 0, 1, and 2, and the S-equivalence classes are (pairs of) vertical lines through $(0,0)$, $(-1,0)$ and $(1,0)$, and $(-2,0)$ and $(2,0)$.

(c) We see that we have an instance of the Master theorem with $a = 5$, $b = 2$, $c = 2$, and $s = 2$. Since $a = 5 > 4 = b^s$, we are in the first case, hence $T(n) \in \Theta(n^{\log 5})$. 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 $n^{\log 5}$.

(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 of that shape, simulates running M on x as follows. U rejects as soon as M moves to the left. U accepts if M stays at the same position and then cycles (reaching the same state with the same symbol; there are only finitely many such pairs so that can be detected), or if it reaches the end of x, as detected by finding a blank, and then moves right twice into the same state (again that can be detected). Since then the same behaviour (without moving to the left) will repeat itself, this is correct.

Since either of the two cases must eventually apply by the pigeon hole principle, U is a total TM. From the description it is clear that $L(U) = L$.

[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

Yes. By Schröder–Bernstein, there is then a bijection between A and a proper subset of A (namely B), so A cannot be finite. An countably infinite subset can be constructed explicitly as follows: Let $a \in A - B$. Let $a_i = f^i(a)$. We claim that all a_i are distinct, which we prove by showing that for all n, all a_i with $i \leq n$ are distinct, by induction on n. The case $n = 0$ is trivial. In case $n > 0$, the IH yields that all a_i with $i < n$ are distinct, hence it suffices to show that these are also distinct from a_n. For a_0 this follows from that $a_0 = a \in A - B$ and $a_n \in B$. Otherwise $a_i = f(a_{i-1}) \neq f(a_{n-1}) = a_n$ by injectivity of f as the IH yields $a_{i-1} \neq a_{n-1}$.

No. For instance, if $a \; R \; b$ and $a \; R \; c$, then the latter does relate b to c, but the former doesn't.

No. For instance, 0 is the least element of the less-than-or-equal relation $\leq$ on the non-negative real numbers, but $\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1$ is an infinite descending chain.

Yes. For instance, $\mathbb{N}$ being countable, each of its subsets is countable as well, but there are uncountably many of them (as was shown by diagonalisation).

Yes. Since f is specified recursively, to check that $f = g$, it suffices to check that the latter satisfies the specification of the former, by substitution. For $n = 0$ and $n = 1$, this is trivial. For $n \geq 2$ we compute

$$\begin{aligned} g(n) &= \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}} \\ &= 2 \cdot \frac{(1+\sqrt{2})^{n-1} - (1-\sqrt{2})^{n-1}}{2\sqrt{2}} + \frac{(1+\sqrt{2})^{n-2} - (1-\sqrt{2})^{n-2}}{2\sqrt{2}} \\ &= 2 \cdot g(n-1) + g(n-2) \end{aligned}$$

which follows from $(1+\sqrt{2})^2 = 3 + 2 \cdot \sqrt{2} = 2 \cdot (1+\sqrt{2})^1 + (1+\sqrt{2})^0$ and $(1-\sqrt{2})^2 = 3 - 2 \cdot \sqrt{2} = 2 \cdot (1-\sqrt{2})^1 + (1-\sqrt{2})^0$. (This is the Pell sequence.)

No. $\frac{\mathrm{lcm}(2^5 \cdot 17^2 \cdot 4, 7)}{\gcd(2^8 \cdot 17^3 \cdot 49, 2^6 \cdot 17^2)} = \frac{2^7 \cdot 7^1 \cdot 17^2}{2^6 \cdot 17^2} = 2 \cdot 7 = 14 \neq 34$.

Yes. By the pigeon hole principle, using that there are no persons more than 150 years old.

Yes. This is Fermat's Little Theorem.

Yes. We are looking for an A having cardinality n such that $n = n^n$. This is satisfied when $n = 1$, i.e. when A is a singleton, e.g. $A = \{a\}$.

No. Consider a DFA having two states p and q having only transitions from the states to themselves.

4∗ (a) We show both sets of equivalence classes to be equinumerous to the set of non-negative real numbers, from which we conclude as the latter is known to be uncountable. Using f as defined above the function $r \mapsto \{(x, y) \mid f(x, y) = r\}$ is seen to be a bijection: it is surjective by the R-equivalence classes being defined via the function f, and it is injective since none of the images is the empty set as $f(\sqrt{r}, 0) = r$, for every non-negative real number r. The same reasoning applies to g and S.

(b) To compute an inverse p' of p modulo q note that $15 \equiv 2 \pmod{13}$ from which we

immediately see that we may take $p' = 7$. Alternatively, since the gcd of 15 and 13 is 1, we may compute p' using Bézout's lemma and the gcd algorithm:

$$\begin{aligned} 15 &= 1 \cdot 15 + 0 \cdot 13 \\ 13 &= 0 \cdot 15 + 1 \cdot 13 \\ 2 &= 1 \cdot 15 - 1 \cdot 13 \\ 1 &= -6 \cdot 15 + 7 \cdot 13 \end{aligned}$$

computing modulo 13 the right-hand side simplifies to $-6 \cdot 15 \equiv 7 \cdot 15$, so we see that $1 \equiv 7 \cdot 15 \pmod{13}$, as before. Using this inverse we may compute, using the RSA-version of the Chinese Remainder Theorem, directly that $x = 4 + 15 \cdot (7 \cdot (5 - 4) \bmod 13) = 109$. One easily verifies that $109 \equiv 4 \pmod{15}$, and $109 \equiv 5 \pmod{13}$, as desired.

5∗ Consider the following specification of M on $\mathbb{N}$ (the natural numbers including 0): $M(n) = M(M(n + 11))$ if $n \leq 100$ and $n - 10$ otherwise.

(a)

$$\begin{aligned} M(99) &= M(M(110)) && \text{since } 99 \leq 100 \\ &= M(100) && \text{since } 110 > 100 \\ &= M(M(111)) && \text{since } 100 \leq 100 \\ &= M(101) && \text{since } 111 > 100 \\ &= 91 && \text{since } 101 > 100 \end{aligned}$$

(b) M is McCarthy's 91 function. The results of evaluating the function are given by $M(n) = 91$ for all natural numbers $n \leq 101$, and $M(n) = n - 10$ for $n > 101$.

To show that M specifies a function $\mathbb{N} \to \mathbb{N}$, we have to show that for every natural number n, there exists a unique natural number $M(n)$ satisfying the specification. This we prove by well-founded induction on $f(n)$ ordered by $\leq$, with $f(n) = 101 - n$ where $-$ is monus, i.e. yielding a natural number. We distinguish cases on whether or not $n > 100$. If $n > 100$, then $M(n) = n - 10$ by the second case of the specification, so we conclude (using that $M(101) = 101 - 10 = 91$). If $n \leq 100$, then $M(n) = M(M(n+11))$ by the first case of the specification, and we further distinguish cases on whether or not $n \geq 90$. If $n < 91$, then the IH yields $M(n + 11) = 91$ (since $f(n + 11) < f(n)$), so $M(n) = M(M(n + 11)) = M(91) = 91$ by another application of the IH (as $f(91) < f(n)$). If $n \geq 91$, then $M(n + 11) = n + 1$ by the second case of the specification, so $M(n) = M(M(n + 11)) = M(n + 1) = 91$ by another application of the IH (as $f(n + 1) < f(n)$).