ETH Zürich, D-INFK
HS 2020, 4. November 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Solution 7

7.1 Countability

i) The set of all Java programs is countable. Every Java program can be seen as a finite binary sequence. That is, there is an injection from the set of all Java programs to the set $\{0,1\}^*$ of finite binary sequences. By Theorem 3.16, this set is countable.

ii) This set is uncountable. Let S denote the set of all equivalence relations on $\mathbb{N}$. We give an injection $f : \mathcal{P}(\mathbb{N} \setminus \{0\}) \to S$. The claim follows, since $\mathcal{P}(\mathbb{N} \setminus \{0\})$ is uncountable (the elements of $\mathcal{P}(\mathbb{N} \setminus \{0\})$ correspond to semi-infinite binary sequences, which are uncountable by Theorem 3.21).

To define the injection $f : \mathcal{P}(\mathbb{N} \setminus \{0\}) \to S$, consider an $A \in \mathcal{P}(\mathbb{N} \setminus \{0\})$. We partition $\mathbb{N}$ into $A \cup \{0\}$ and $\mathbb{N} \setminus (A \cup \{0\})$ and define the equivalence relation $f(A)$ such that two numbers are $f(A)$-related if they are in the same set of the partition. Clearly, f is injective, since for two different sets A and A', the equivalence classes of 0 are different for the relations $f(A)$ and $f(A')$ and hence $f(A) \neq f(A')$.

7.2 The Diagonalization Argument

a) Let $\beta_{i,j}$ be the j-th bit in α_i. In the lecture, α was defined as $\alpha \stackrel{\text{def}}{=} \overline{\beta_{0,0}},\ \overline{\beta_{1,1}},\ \overline{\beta_{2,2}},\ \ldots$ A second sequence α' can be defined as $\alpha' \stackrel{\text{def}}{=} \beta_{0,0},\ \overline{\beta_{0,1}},\ \overline{\beta_{1,2}},\ \overline{\beta_{2,3}},\ \ldots$. For any i, α' disagrees with α_i on the bit $i+1$. Moreover, it disagrees with α on the first bit. Note that there are many possible solutions (see Subtask b)).

b) The set L is uncountable. Indeed, we have $L \cup \{\alpha_0, \alpha_1, \ldots\} = \{0,1\}^\infty$, and if L was countable, then we would have a contradiction with Theorem 3.21 (since $\{0,1\}^\infty$ is uncountable).

7.3 More Countability

For any $b \in \{0,1\}^\infty$, let b_i for $i \in \mathbb{N}$ denote the i-th bit of b, and define the function $f_b : \mathbb{N} \to \{0,1\}$ by

$$f_b(3i) = b_i,\ f_b(3i+1) = 0,\ \text{and}\ f_b(3i+2) = 1.$$

We define the function $g : \{0,1\}^\infty \to S$ by $g(b) = f_b$. It is easy to verify that $f_b \in S$ for any $b \in \{0,1\}^\infty$: for any $i \in \mathbb{N}$ we have $f_b(3i) = f_b(3i+1)$ or $f_b(3i) = f_b(3i+2)$, as well as $f_b(3i+1) = f_b(3(i+1)+1)$ and $f_b(3i+2) = f_b(3(i+1)+2)$.

We show that g is injective: Let $b, b' \in \{0,1\}^\infty$ be arbitrary and assume $b \neq b'$. This implies that $b_i \neq b'_i$ for some $i \in \mathbb{N}$. Since $f_b(3i) = b_i$ and $f_{b'}(3i) = b'_i$ we have $f_b(3i) \neq f_{b'}(3i)$. Hence, $g(b) = f_b \neq f_{b'} = g(b')$.

As g is injective, we have $\{0,1\}^\infty \preceq S$. Since $\{0,1\}^\infty$ is uncountable by Theorem 3.21, S is uncountable as well.

7.4 The Hunt for the Red October

At any time t we can fire a torpedo to position $s = x \cdot t + y$ for some x and y. The submarine sinks if its speed and the starting position happened to be x and y. Thus, at any time t we can make a guess about x and y and sink the submarine based on that guess. We now have to systematically check all the pairs $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

Hence, we need a surjective function $f : \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}$ that will assign to a time t a pair (x, y). (Surjectivity guarantees that every (x, y) will be tested at some time t'.) Since $\mathbb{Z} \times \mathbb{Z}$ is countable (by Example 3.64 and Corollary 3.18), there exists an injective function $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$. We can now define f as

$$f(n) := \begin{cases} (a,b) & \textbf{if} \quad \exists (a,b) \;\; g((a,b)) = n \\ (0,0) & \textbf{otherwise} \end{cases}$$

By the injectivity of g, we have $\{(a,b)\} = g^{-1}(\{g((a,b))\})$ for all $(a,b) \in \mathbb{Z} \times \mathbb{Z}$. Also, for any (a,b) there exists an $n \in \mathbb{N}$ such that $g((a,b)) = n$ and, therefore, there exists an $n \in \mathbb{N}$ such that $f(n) = (a,b)$. Hence, f is surjective and we will eventually sink the submarine.

7.5 The Greatest Common Divisor

Let $a, b, u, v \in \mathbb{Z} \setminus \{0\}$ be such that $ua + vb = 1$ and let $d = \gcd(a,b)$. By the definition of $\gcd$, we have $d \mid a$ and $d \mid b$. That is, there exist $k, l \in \mathbb{Z}$ such that $a = kd$ and $b = ld$.

Hence, $1 = ua + vb = ukd + vld = (uk + vl)d$. Thus, $d \mid 1$.

Since 1 is the only positive divisor of 1, it follows that $d = 1$.

7.6 Congruences

a) Take arbitrary $m, n \in \mathbb{N}$. By Lemma 4.14 we have

$$123^m - 33^n \equiv_{10} 3^m - 3^n.$$

Assume without loss of generality that $m \leq n$. If $m \equiv_4 n$, then there exists a $k \in \mathbb{N}$, such that $n - m = 4k$ and by Lemma 4.14, we have:

$$\begin{aligned} 3^m - 3^n &\equiv_{10} 3^m(1 - 3^{n-m}) \equiv_{10} 3^m(1 - 3^{4k}) \equiv_{10} 3^m(1 - 9^{2k}) \\ &\equiv_{10} 3^m(1 - (-1)^{2k}) \equiv_{10} 3^m(1 - 1^k) \equiv_{10} 3^m \cdot 0 \equiv_{10} 0. \end{aligned}$$

b) Take any $a, b, c, d, m \in \mathbb{Z}$, such that $m > 0$. Assume that $a \equiv_m b$ and $c \equiv_m d$. Then, there exist $s, t \in \mathbb{Z}$ such that $a - b = ms$ and $c - d = mt$. It follows that

$$ac = (ms + b)(mt + d) = m^2st + msd + mtb + bd = m(mst + sd + tb) + bd.$$

Therefore, $m \mid ac - bd$, so $ac \equiv_m bd$.

c) Consider all possible remainders $R_{11}(n^5 + 7)$ and $R_{11}(m^2)$ when $m, n \in \mathbb{Z}$. By Corollary 4.17, we have $R_{11}(n^5 + 7) = R_{11}((R_{11}(n))^5 + 7)$ and $R_{11}(m^2) = R_{11}((R_{11}(m))^2)$. By trying all ten possibilities for $R_{11}(n)$ and, respectively, for $R_{11}(m)$, we get that $R_{11}(n^5 + 7) \in \{6, 7, 8\}$ and $R_{11}(m^2) \in \{0, 1, 3, 4, 5, 9\}$. Since these sets are disjoint, $n^5 + 7$ cannot be equal to m^2.

7.7 Modular Arithmetic

a) Take any even $n \geq 0$ and let $k \in \mathbb{N}$ be such that $n = 2k$. By Corollary 4.17, we have $R_7(13^n+6) = R_7(R_7(13)^n+6) = R_7(R_7(-1)^n+6) = R_7((-1)^n+6) = R_7((-1)^{2k}+6) = R_7(7) = 0$. Hence, $7 \mid 13^n + 6$.

b) Let $a, e, m, n \in \mathbb{N} \setminus \{0\}$ and assume that $R_m(a^e) = 1$. By Theorem 4.1, there exists a $q \in \mathbb{N}$, such that $n = qe + R_e(n)$. Therefore,

$$\begin{aligned}
R_m(a^n) &= R_m\left(a^{qe+R_e(n)}\right) \\
&= R_m\left((a^e)^q \cdot a^{R_e(n)}\right) \\
&= R_m\left((R_m(a^e))^q \cdot R_m\left(a^{R_e(n)}\right)\right) && \text{(Corollary 4.17)} \\
&= R_m\left(1^q \cdot R_m\left(a^{R_e(n)}\right)\right) && (R_m(a^e) = 1) \\
&= R_m\left(R_m(1)^q \cdot R_m\left(a^{R_e(n)}\right)\right) \\
&= R_m\left(a^{R_e(n)}\right). && \text{(Corollary 4.17)}
\end{aligned}$$

c) By Subtask b), $R_{13}(4^{2020}) = R_{13}(4^{R_6(2020)}) = R_{13}(4^4)$. Now we have $4^4 \equiv_{13} 16^2 \equiv_{13} 3^2 \equiv_{13} 9$.