CS724: Topics in Algorithms
Problem Set 1

Prof. Dan A. Simovici

Problem 1:

Prove that if $m, n \in \mathbb{N}$ we have $\equiv_n \subseteq \equiv_m$ if and only if m evenly divides n.

Solution 1:

If m is a divisor of n we have $n = km$. Thus, if $p - q$ is divisible by n, it is also divisible by m, hence $p \equiv_m q$.
Conversely, suppose that $\equiv_n \subseteq \equiv_m$. Since $(0, n) \in \equiv_n$, it follows that $(0, n) \in \equiv m$, which means that $n = n - 0 = km$. Thus, m evenly divides n.

Problem 2:

Let $p_1, p_2, p_3, \ldots$ be the sequence of prime numbers $2, 3, 5, \cdots$. Define the function $f : \mathbf{Seq}(\mathbb{N}) \longrightarrow \mathbb{N}$ by $f(n_1, \ldots, n_k) = p_1^{n_1} \cdots p_k^{n_k}$. Prove that $f(n_1, \ldots, n_k) = f(m_1, \ldots, m_k)$ implies $(n_1, \ldots, n_k) = (m_1, \ldots, m_k)$.

Solution 2: Suppose that $f(n_1, \ldots, n_k) = f(m_1, \ldots, m_k)$, that is,

$$p_1^{n_1} \cdots p_k^{n_k} = p_1^{m_1} \cdots p_k^{m_k}.$$

Note that this implies $p_i^{n_i} | p_i^{m_i}$ and $p_i^{m_i} | p_i^{n_i}$, or $n_i \leqslant m_i$ and $m_i \leqslant n_i$. Thus, $n_i = m_i$ for $1 \leqslant i \leqslant k$.

Problem 3:

Let $\mathcal{C}$ be a collection of subsets of a set S such that $\bigcup \mathcal{C} = S$. Define the relation $\rho_{\mathcal{C}}$ on S by

$$\rho_{\mathcal{C}} = \{(x, y) \in S \times S \mid |x \in C \text{ if and only if } y \in C \text{ for every } C \in \mathcal{C}\}.$$

Prove that, for every collection $\mathcal{C}$, the relation $\rho_{\mathcal{C}}$ is an equivalence. What changes if the condition $\bigcup \mathcal{C} = S$ is not satisfied?

Solution 3:

$\rho_{\mathcal{C}}$ is clearly reflexive because for each $x \in S$ there exists $C \in \mathcal{C}$ such that $x \in C$. Suppose that $(x, y) \in \rho_{\mathcal{C}}$. Then, we have $x \in C$ if and only if $y \in C$ hence $(y, x) \in \rho$. Thus, $\rho_{\mathcal{C}}$ is symmetric. If $(x, y), (y, z) \in \rho_{\mathcal{C}}$ $x \in C$ if and only if $y \in C$ and $y \in C$ if and only if $z \in C$ for any $C \in \mathcal{C}$. Thus, $(x, z) \in \rho_{\mathcal{C}}$, hence ρ is a transitive relation.

Problem 4

Let S and T be two finite sets such that $|S| = m$ and $|T| = n$.

- Prove that the set of functions $S \longrightarrow T$ contains n^m elements.
- Prove that the set of partial functions $S \rightsquigarrow T$ contains $(n+1)^m$ elements.

Solution 4

A function $f : S \longrightarrow T$ can be represented by an array having m locations corresponding to the elements $x_1, \ldots, x_n$ of the set S. If we write in the box that corresponds to x_i the value of $f(x_i)$ we have n choices for each of the boxes. Such an array corresponds to a function $f : S \longrightarrow T$, so we have n^m functions.

$f(x_1)$	$f(x_2)$	$\cdots$		$f(x_m)$
x_1	x_2			x_m

A partial function can be represented by a similar array. If $f(x_i)$ is defined, we write the value $f(x_i)$ in the box; if not, we write $\uparrow$. Thus, there are $n+1$ choices for each box, and the total number of partial functions is $(n+1)^m$.

Problem 5

Let $\mathcal{C}$ be a nonempty collection of nonempty subsets of a set S. Prove that $\mathcal{C}$ is a partition of S if and only if every element $a \in S$ belongs to exactly one member of the collection $\mathcal{C}$.

Solution 5

Let A, B be two sets in $\mathcal{C}$. Note that if $x \in A \cap B$, then $x \in A$ and $x \in B$, and this violates the description of $\mathcal{C}$. Thus, any two sets in $\mathcal{C}$ are disjoint. Since every $a \in S$ belongs to a set of $\mathcal{C}$, the union of these sets equals S, hence $\mathcal{C}$ is a partition.

Things to remember when you do homework:

- write neatly, using latex;
- use clear and correct English;
- do not use the expression "it is easy to see"; fully justify your statements.