T-79.148 **Spring 2002**
Introduction to Theoretical Computer Science
Tutorial 2, 5-7 February
Problems

Homework problems:

1. Let $\Sigma = \{a, b\}$. Give some examples of strings from each of the following languages:
   (a) $\{w \in \Sigma^* \mid w$ contains a substring aba, but no substring $bab\}$;
   (b) $\{w \in \Sigma^* \mid w = w^R\}$;
   (c) $\{w \in \Sigma^* \mid \exists u, v \in \Sigma^*$ s.t. $w = uvuv\}$;
   (d) $\{w \in \Sigma^* \mid \exists u \in \Sigma^*$ s.t. $ww = uuu\}$.

2. The *reversal* of a string $w \in \Sigma^*$, denoted w^R, is defined inductively by the rules:
   (i) $\varepsilon^R = \varepsilon$;
   (ii) if $w = ua$, where $u \in \Sigma^*$ and $a \in \Sigma$, then $w^R = au^R$.

   It was proved in class (cf. also Lewis & Papadimitriou, p. 43) that for any strings $u, v \in \Sigma^*$ it is the case that $(uv)^R = v^R u^R$. Prove in a similar manner, by induction based on the above definition of reversal, the following facts:
   (a) $(w^R)^R = w$;
   (b) $(w^k)^R = (w^R)^k$, for any $k \geq 0$.

3. Let A be a countably infinite set and $B \subseteq A$. Prove that B must be either finite or countably infinite.

Demonstration problems:

4. Show that any alphabet Σ with at least two symbols is comparable to the binary alphabet $\Gamma = \{0, 1\}$, in the sense that strings over Σ can be easily encoded into strings over Γ and vice versa. How much can the length of a string change in your encoding? (I.e., if the length of a string $w \in \Sigma^*$ is $|w| = n$ symbols, what is the length of the corresponding string $w' \in \Gamma^*$?) Could you design a similar encoding if the target alphabet consisted of only *one* symbol, e.g. $\Gamma = \{1\}$?

5. Prove that the Cartesian product $\mathbb{N} \times \mathbb{N}$ is countably infinite. (*Hint:* Think of the pairs $(m, n) \in \mathbb{N} \times \mathbb{N}$ as embedded in the Euclidean (x, y) plane $\mathbb{R}^2$. Enumerate the pairs by diagonals parallel to the line $y = -x$.) Conclude from this result and the result of Problem 3 that also the set $\mathbb{Q}$ of rational numbers is countably infinite.

6. Let S be an arbitrary nonempty set.
   (a) Give some injective (i.e. one-to-one) function $f : S \to \mathcal{P}(S)$.
   (b) Prove that there cannot exist an injective function $g : \mathcal{P}(S) \to S$. (*Hint:* Assume that such a function g existed. Consider the set $R = \{s \in S \mid s \notin g^{-1}(s)\}$, and denote $r = g(R)$. Is it then the case that $r \in R$?)

   Observe, as a consequence of item (b), that the power set $\mathcal{P}(S)$ of any countably infinite set S is uncountable.