Problem Set 7 Solutions

Problem 1. Show that for all odd natural numbers m there exists an $n \geq 1$ such that $m \mid 2^n - 1$.

Consider the $m+1$ numbers $2^1 - 1, 2^2 - 1, \ldots, 2^{m+1} - 1$ and divide them according to their equivalence class modulo m. By the pigeonhole principle, there are two numbers $2^i - 1$ and $2^j - 1$ belonging to the same class, i.e., $2^i - 1 \approx 2^j - 1 \pmod{m}$. Assume without loss of generality that $i > j$. We have $m|((2^i - 1) - (2^j - 1)) = 2^i - 2^j = 2^j(2^{i-j} - 1)$ and since m is odd m must divide $2^{i-j} - 1$ and $i - j \geq 1$.

Problem 2. Jelly beans of 8 different colors are in 6 jars. There are 20 jelly beans of each color. Use the pigeonhole principle to prove that there is some jar that contains at least two beans each from two different colors of jelly beans.

There are 20 beans of each color. Since there are 6 jars, by the strong pigeonhole principle for each color there is a jar containing at least $20/6 \geq 2$ beans of that color. Since the number of colors is greater then the number of jars, using the pigeonhole principle again, there must be a jar containing two pairs of jelly beans from two different colors of jelly beans.

Problem 3. Let F be the set of all functions $f : \mathbb{R} \to \{0, 1\}$. Show that there is a bijection from $2^{\mathbb{R}}$ to F.

Let ϕ: $2^{\mathbb{R}} \to F$ be the function mapping any set $A \subseteq \mathbb{R}$ to the function ϕ_A defined as follows:

$$\phi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{otherwise} \end{cases}$$

We prove that ϕ is a bijection, i.e., it is injective and surjective.

- Injectivity: Let A and B be two subsets of $\mathbb{R}$ such that $A \neq B$, and assume without loss of generality that there exists some x such that $x \in A$ but $x \notin B$. We have $\phi_A(x) = 1 \neq 0 = \phi_B(x)$. Therefore $\phi_A \neq \phi_B$ and ϕ is injective.
- Surjectivity: Let f be a function from $\mathbb{R}$ to $\{0, 1\}$. We want to show that $f = \phi_A$ for some A. Define the set $A = \{x \in \mathbb{R} \mid f(x) = 1\}$. We have $\phi_A(x) = f(x)$ for all $x \in \mathbb{R}$. Therefore $\phi_A = f$ and ϕ is surjective.

Problem 4. Let P be a relation on a finite set S that makes S into a poset. Define a function f on S by $f(x) = |\{y \in S \colon (x, y) \in P\}|$. Define R to be the relation $\{(x, y) \in S^2 \colon f(x) > f(y) \vee x = y\}$.

(a) Prove that R also makes S into a poset.

We have to prove that R is reflexive, antisymmetric and transitive:

- Reflexive: For all $x \in S$ we have $x = x$ and therefore $(x, x) \in R$.
- Antisymmetric: Assume $(x, y) \in R$ and $(y, x) \in R$. We must prove that $x = y$. Assume for contradiction that $x \neq y$. From the definition of $(x, y) \in R$ and $(y, x) \in R$ we have $f(x) < f(y)$ and $f(y) < f(x)$. But this is a contradiciton because $<$ is asymmetric. So, it must be $x = y$.
- Transitive: Let $x, y, z \in S$ such that $(x, y) \in R$ and $(y, z) \in R$. If $x = y$ or $y = z$ we immediately get $(x, z) \in R$. Therefore, assume $x \neq y \neq z$. From the definition of R we have $f(x) \geq f(y) \geq f(z)$. By transitivity of $\geq$ we get $f(x) \geq f(z)$ and therefore $(x, z) \in R$.

(b) Prove that $P \subseteq R$. Let $x, y \in S$ such that $(x, y) \in P$. We must prove that $(x, y) \in R$. If $x = y$ this is certainly true, so assume $x \neq y$. Let $A = \{z : (x, z) \in S\}$ and $B = \{z : (y, z) \in S\}$. We will prove that $A \supset B$ and therefore $f(x) = |A| > |B| = f(y)$ and $(x, y) \in R$.

We first prove $A \supseteq B$. Let $z \in B$. We have $(y, z) \in S$ and $(x, y) \in S$. By transitivity $(x, z) \in S$ and $z \in A$.

We now prove that containment is strict. Since $(x, y) \in S$ and S is antisymmetric, (y, x) cannot be in S and therefore $x \notin B$. Since $x \in A$, $A \supset B$.

Problem 5. Minimal elements of posets.

(a) Let (S, R) be a poset. Show that (S, R^{-1}) is also a poset, where R^{-1} is the inverse of R. We must prove that R^{-1} is reflexive, transitive and antisymmetric.

- Reflexive: for every $x \in S$ we have $(x, x) \in R$ and therefore $(x, x) \in R^{-1}$.
- Transitive: assume $(x, y) \in R^{-1}$ and $(y, z) \in R^{-1}$. By definition of inverse relation $(y, x) \in R$ and $(z, y) \in R$. Since R is transitive, this implies $(z, x) \in R$ and and from the definition of inverse relation $(x, z) \in R^{-1}$.
- Antisymmetric: assume $(x, y) \in R^{-1}$ and $(y, x) \in R^{-1}$. By definition of inverse relation $(y, x) \in R$ and $(x, y) \in R$. Since R is antisymmetric, this implies $x = y$.

(b) Give a pigeonhole-free proof using induction on the size of the poset that any finite poset has a minimal element.

Let (S, R) be a finite poset. We prove by induction on $|S|$ that (S, R) has a minimal element.

- Base case: $|S| = 1$. S has a single element x which is vacuously minimal.
- Inductive step: Let $n > 1$ be the size of $|S|$ and assume that any poset with $n - 1$ elements has a minimal element. We prove that also (S, R) has a minimal element. Pick an element $a \in S$. There are two cases:

- if a is minimal in S then we are done.
- if a is not minimal in S then there exists some $b \neq a$ such that $(b, a) \in R$. Define the poset (S', R') by $S' = S - \{a\}$ and $R' = \{(x, y) : x, y \in S' \wedge (x, y) \in R\}$. Since (S', R') has $n - 1$ elements, it has a minimal element c. We claim that c is a minimal element of (S, R). We already know that no element in S' is smaller then c. It remains to be shown that also a cannot be smaller then c. Assume for contradiction that $(a, c) \in R$. Since $(b, a) \in R$ it follows by transitivity that $(b, c) \in R$. But this contradicts the minimality of c in S', so it cannot be $(b, c) \in R$.

(c) Combining the previous two parts, prove that every poset has a *maximal* element that is not less than or equal to any other.

An element $a \in S$ is minimal in (S, R) if and only if it is maximal in (S, R^{-1}). Let (S, R) be a finite poset. We want to prove that (S, R) has a maximal element. From the previous parts, (S, R^{-1}) is a poset and therefore it has a minimal element a. We will prove that a is maximal in (S, R). Assume this is not true. There exits some $b \neq a$ in S such that $(a, b) \in R$. By definition of inverse relation, $(b, a) \in R^{-1}$ contradicting the minimality of a in (S, R^{-1}).

Problem 6. A real number is *algebraic* if it is the root of a polynomial with rational number coefficients. Algebraic numbers form an important part in the study of (what else) modern algebra. A number that is not algebraic is called *transcendental.*

(a) Let $S_1, S_2, S_3, \ldots$ be a collection of countably many sets. Suppose each S_i is countable. Prove $\cup S_i$ is countable.

Since each S_i is countable there is a surjection f_i from the naturals to S_i. Now define the function $f : \mathbb{N} \times \mathbb{N} \to \bigcup_{i \in \mathbb{N}} S_i$ by $f(i, j) = f_i(j)$. Clearly, f is a surjection and since $\mathbb{N} \times \mathbb{N}$ is countable, also $\cup S_i$ is countable.

(b) Prove that for any particular d, the set of degree d polynomials with rational coefficients is countable.

Let P_d be the set of degree d polynomials with rationals coefficients. The function

$$f : (q_0, q_1, \ldots, q_d) \mapsto q_0 x^d + q_1 x^{d-1} + \cdots + q_d$$

is a surjection from $(\mathbb{Q} - \{0\}) \times \mathbb{Q}^d$ to P_d. Since the set $(\mathbb{Q} - \{0\}) \times \mathbb{Q}^d$ is countable (the cartesian product of finitely many countable sets is countable), then also the set P_d is countable.

(c) Prove that the set of all roots of degree d polynomials with rational coefficients is countable (you may use the fact that a degree d polynomial has at most d roots).

Since each degree d polynomial has at most d roots we can give a surjection from $P_d \times \{1, \ldots, d\}$ to the set of all roots of degree d polynomials with rational coefficients. For example we can define $f(p(x), i) = x_i$, where $x_1, \ldots, x_d$ are the roots of $p(x)$ (if $p(x)$ has less then d roots, just repeat the last one many times).

(d) Prove that the set of algebraic numbers (which is just the union of the sets in the previous part) is countable.

The set of algebraic numbers is the union of the sets of the roots of polynomials with rationals coefficients of degree d, for all d. This is a countable union of countable sets, and from the result in part (a) it is countable.

(e) Prove that there is a trancendental number.

If there were no trascendental numbers, all numbers would be algebraic, i.e., the set of algebraic numbers equals $\mathbb{R}$. But this is not possible because the reals are not countable.

Optional Problem 7. I stated in class that to prove countability it suffices to show that there is a surjection from $\mathbb{N}$ to a set. Prove this statement. That is, Suppose that S is not finite and we have a surjection $f : \mathbb{N} \to S$. Prove that there is a bijection from $\mathbb{N}$ to S.

This proves that there is no countably infinite set "smaller" than $\mathbb{N}$. Since we know that (by definition) there is no set that is "bigger", we have shown that all countably infinite sets are the same size.

Let $f : \mathbb{N} \to S$ be a surjection. We define a bijection $g : \mathbb{N} \to S$. First define an auxiliary function $h : \mathbb{N} \to \mathbb{N}$ as follows:

$$h(i) = min\{j : |f(\{1, \dots, j\})| = i\}.$$

Notice that h is strictly monotone, i.e., if $i < j$ then $h(i) < h(j)$. To see this, assume for contradiction that $i < j$ and $h(j) \leq h(i)$. We have $\{1, \dots, h(j)\} \subseteq \{1, \dots, h(i)\}$ and therefore $j = |f(\{1, \dots, h(j)\})| \leq |f(\{1, \dots, h(i)\})| = i$, contradicting $i < j$.

We claim that the function $g(i) = f(h(i))$ is a bijection, i.e., it is injective and surjective:

- Injective: Assume for contradiction that $g(i) = g(j)$ for some $i \neq j$. Since $\leq$ is a total order over $\mathbb{N}$ we can assume wlog that $i < j$. This implies $h(i) < h(j)$ and since $f(h(i)) = f(h(j))$, then $f(\{1, \dots, h(j)\}) = f(\{1, \dots, h(j) - 1\})$. From this we get $|f(\{1, \dots, h(j) - 1\})| = |f(\{1, \dots, h(j) - 1\})| = j$ which contradicts the minimality of $h(j)$.
- Surjective: Let $s \in S$. Since f is a surjection, there exists some i such that $f(i) = s$. Let j be the smallest i such that $f(i) = s$. Let also $k = |f(\{1, \dots, j\})|$. We have $h(k) \leq j$ by definition of h. Since $f(j) = s \notin f(\{1, \dots, j-1\})$, we also have $|f(\{1, \dots, j-1\})| = k - 1$ and therefore $h(k) > j - 1$. So, $h(k) = j$ and $g(k) = f(h(k)) = f(j) = s$.