Staff Solutions to In-Class Problems Week 4, Mon.

Problem 1.
Let $\mathbb{N}^\omega$ the set of infinite sequences of nonnegative integers. For example, some sequences of this kind are:

$$
(0, 1, 2, 3, 4, \ldots), \\
(2, 3, 5, 7, 11, \ldots), \\
(3, 1, 4, 5, 9, \ldots).
$$

Prove that this set of sequences is uncountable.

Solution. Proof. One approach is to show that if $\mathbb{N}^\omega$ were countable, then $\mathcal{P}(\mathbb{N})$ would be too, contradicting Cantor’s Theorem 5.2.6.

STAFF NOTE: If needed, offer hint: verify that $\mathbb{N}^\omega$ is as big as $\mathcal{P}(\mathbb{N})$. 

Namely, we can define a surjective function from $f : \mathbb{N}^\omega \rightarrow \mathcal{P}(\mathbb{N})$ as follows:

$$
f(s) ::= \{n \in \mathbb{N} \mid s[n] = 0\}
$$

where $s[n]$ is the $n$th element of sequence $s$.

Now if there was a surjective function from $g : \mathbb{N} \rightarrow \mathbb{N}^\omega$, then the composition of $f$ and $g$ would be a surjective function from $\mathbb{N}$ to $\mathcal{P}(\mathbb{N})$ contradicting Cantor’s Theorem 5.2.6.

Alternatively, to show that $\mathbb{N}^\omega$ is uncountable, we can use a basic diagonal argument directly to show that no function from $\mathbb{N}$ to the set of sequences $\mathbb{N}^\omega$ is a surjection.

Proof. Let $\sigma$ be a function from $\mathbb{N}$ to the infinite sequences of nonnegative integers. To show that $\sigma$ is not a surjection, we will describe a sequence, diag, of nonnegative integers that is not in the range of $\sigma$.

Namely, define a sequence $\text{diag} \in \mathbb{N}^\omega$ as follows:

STAFF NOTE: If needed, offer this def of diag as a hint.

$$
\text{diag}[n] ::= \sigma(n)[n] + 1.
$$

Now by definition,

$$
\text{diag}[n] \neq \sigma(n)[n],
$$

for all $n \in \mathbb{N}$, proving that diag is not equal to $\sigma(n)$ for any $n \in \mathbb{N}$. This means that diag is not in the range of $\sigma$, as claimed.

Problem 2.
The method used to prove Cantor’s Theorem that the power set is “bigger” than the set, leads to many important results in logic and computer science. In this problem we’ll apply that idea to describe a set of binary strings that can’t be described by ordinary logical formulas. To be provocative, we could say that we will describe an undescribable set of strings!
The following logical formula illustrates how a formula can describe a set of strings. The formula

\[ \text{NOT}[\exists y. \exists z. s = yz], \]  

\[ \text{(no-1s)} \]

where the variables range over the set, \( \{0, 1\}^* \), of finite binary strings, says that the binary string, \( s \), does not contain a 1.

We’ll call such a predicate formula, \( G(s) \), about strings a string formula, and we’ll use the notation \( \text{strings}(G) \) for the set of binary strings with the property described by \( G \). That is,

\[ \text{strings}(G) ::= \{ s \in \{0, 1\}^* \mid G(s) \}. \]

A set of binary strings is describable if it equals \( \text{strings}(G) \) for some string formula, \( G \). So the set, \( 0^* \), of finite strings of 0’s is describable because it equals \( \text{strings} \text{(no-1s)}. \)

The idea of representing data in binary is a no-brainer for a computer scientist, so it won’t be a stretch to agree that any string formula can be represented by a binary string. We’ll use the notation \( G_x \) for the string formula with binary representation \( x \in \{0, 1\}^* \). The details of the representation don’t matter, except that there ought to be a display procedure that can actually display \( G_x \) given \( x \).

Standard binary representations of formulas are often based on character-by-character translation into binary, which means that only a sparse set of binary strings actually represent string formulas. It will be technically convenient to have every binary string represent some string formula. This is easy to do: tweak the display procedure so it displays some default formula, say no-1s, when it gets a binary string that isn’t a standard representation of a string formula. With this tweak, every binary string, \( x \), will now represent a string formula, \( G_x \).

Now we have just the kind of situation where a Cantor-style diagonal argument can be applied, namely, we’ll ask whether a string describes a property of itself! That may sound like a mind-bender, but all we’re asking is whether \( x \in \text{strings}(G_x) \).

For example, using character-by-character translations of formulas into binary, neither the string 0000 nor the string 10 would be the binary representation of a formula, so the display procedure applied to either of them would display no-1s. That is, \( G_{0000} = G_{10} = \text{no-1s} \) and so \( \text{strings}(G_{0000}) = \text{strings}(G_{10}) = 0^* \). This means that

\[ 0000 \in \text{strings}(G_{0000}) \quad \text{and} \quad 10 \notin \text{strings}(G_{10}). \]

Now we are in a position to give a precise mathematical description of an “undescribable” set of binary strings, namely, let

**Theorem.** Define

\[ U ::= \{ x \in \{0, 1\}^* \mid x \notin \text{strings}(G_x) \}. \]  

(1)

The set \( U \) is not describable.

Use reasoning similar to Cantor’s Theorem 5.2.6 (repeated below) to prove this Theorem.

**Solution.** By definition (1),

\[ x \in U \quad \text{iff} \quad x \notin \text{strings}(G_x). \]  

(2)

for \( x \in \{0, 1\}^* \).

Also, \( U = \text{strings}(G_{x_U}) \) by assumption. This means:

\[ x \in U \quad \text{iff} \quad x \in \text{strings}(G_{x_U}). \]  

(3)

Combining (3) and (2), we have

\[ x \notin \text{strings}(G_x) \iff x \in \text{strings}(G_{x_U}). \]  

(4)

for all \( x \in \{0, 1\}^* \). Now plugging in \( x_U \) for \( x \) in (4) gives an immediate contradiction.

So there cannot be any formula that describes \( U \).
Cantor’s Theorem

There is no bijection between any set $A$ and its powerset $\mathcal{P}(A)$.

Proof. We show that if $g$ is a total function from $A$ to $\mathcal{P}(A)$, then $g$ does not have the $[\geq 1\text{ in}]$, surjection property, and so is certainly not a bijection.

Define

$$A_g := \{a \in A \mid a \notin g(a)\}.$$ 

Since $g$ is total, $A_g$ is a well-defined subset of $A$, which means it is a member of $\mathcal{P}(A)$. We claim $A_g$ is not in the range of $g$, and so $g$ is not a surjection.

To prove that $A_g \notin \text{range}(g)$, assume to the contrary that it was in range($g$). That is,

$$A_g = g(a_0)$$

for some $a_0 \in A$. Then by definition of $A_g$,

$$a \in g(a_0) \iff a \in A_g \iff a \notin g(a)$$

for all $a \in A$. Now letting $a = a_0$ yields the contradiction

$$a_0 \in g(a_0) \iff a_0 \notin g(a_0).$$

Problem 3.

Let $R : A \rightarrow A$ be a binary relation on a set, $A$. If $a_1 R a_0$, we’ll say that $a_1$ is “$R$-smaller” than $a_0$. $R$ is called well founded when there is no infinite “$R$-decreasing” sequence:

$$\cdots R a_n R \cdots R a_1 R a_0,$$  \hspace{1cm} (5)

of elements $a_i \in A$.

For example, if $A = \mathbb{N}$ and $R$ is the $<$-relation, then $R$ is well founded because if you keep counting down with nonnegative integers, you eventually get stuck at zero:

$$0 < \cdots < n - 1 < n.$$ 

But you can keep counting up forever, so the $>$-relation is not well founded:

$$\cdots > n > \cdots > 1 > 0.$$ 

Also, the $\leq$-relation on $\mathbb{N}$ is not well founded because a constant sequence of, say, 2’s, gets $\leq$-smaller forever:

$$\cdots \leq 2 \leq \cdots \leq 2 \leq 2.$$ 

(a) If $B$ is a subset of $A$, an element $b \in B$ is defined to be $R$-minimal in $B$ iff there is no $R$-smaller element in $B$. Prove that $R : A \rightarrow A$ is well founded iff every nonempty subset of $A$ has an $R$-minimal element.

Solution. If there was an infinite $R$-decreasing sequence (5), then $\{a_0, a_1, \ldots\}$ would itself be a nonempty subset of $A$ with no minimal element. This proves the right-to-left direction of the “iff” (by contrapositive).

We’ll also prove the left-to-right direction by contrapositive. So suppose $B$ is a nonempty subset of $A$ with no $R$-minimal element. We will show how to find an infinite $R$-decreasing sequence of elements of $B$: 

Since $B$ is nonempty, there is an element $b_0 \in B$. Since $b_0$ cannot be minimal in $B$, there must be an element $b_1 \in B$ that is $R$-smaller than $b_0$. Again, since $b_1$ cannot be minimal in $B$, there must be an $R$-smaller $b_2 \in B$. Continuing in this way, we obtain an infinite $R$-decreasing sequence

$$\ldots R b_n R \ldots R b_1 R b_0.$$ 

A logic formula of set theory has only predicates of the form “$x \in y$” for variables $x, y$ ranging over sets, along with quantifiers and propositional operations. For example,

$$\text{isempty}(x) ::= \forall w. \text{NOT}(w \in x)$$

is a formula of set theory that means that “$x$ is empty.”

(b) Write a formula, $\text{member-minimal}(u, v)$, of set theory that means that $u$ is $\epsilon$-minimal in $v$.

Solution.

$$\text{member-minimal}(u, v) ::= u \in v \AND \forall x \in v. x \notin u.$$ 

(c) The Foundation axiom of set theory says that $\in$ is a well founded relation on sets. Express the Foundation axiom as a formula of set theory. You may use “member-minimal” and “isempty” in your formula as abbreviations for the formulas defined above.

Solution.

$$\forall x. \text{NOT}(\text{isempty}(x)) \IMPLIES \exists m. \text{member-minimal}(m, x).$$ 

(d) Explain why the Foundation axiom implies that no set is a member of itself.

Solution. If $x \in x$, then

$$\ldots \in x \in \ldots \in x \in x$$

is a $\epsilon$-decreasing sequence, violating well foundedness of the $\epsilon$-relation. Alternatively, $\{x\}$ would be a nonempty set with no $\epsilon$-minimal element.

STAFF NOTE: Question: How about a set being a member of a member of itself? In other words, sets $S, T$ such that $S \in T \in S$?

Answer: the would have infinite $\epsilon$-decreasing sequence

$$\hat{S} \in T \in S \in T \in S \in T,$$

violating Foundation.