MM7022, Logic II, HT 2021

Exam 2021-12-15

Solutions

1. <u>Summary</u>: $|S_1| = 2^{\aleph_0}$, $|S_2| = \aleph_0$, $|S_3| = 2^{(2^{\aleph_0})}$, $|S_4| = 2^{\aleph_0}$,

so $|S_2| < |S_1| = |S_4| < |S_3|$.

<u>Proofs</u>:

(a) $|S_1| = 2^{\aleph_0}$: ($S_1 = \{\text{increasing funs } f: \mathbb{N} \to \mathbb{N}\}$)

We know $|\mathbb{N}^{\mathbb{N}}| = 2^{\aleph_0}$,

since $2^{\mathbb{N}} \subseteq \mathbb{N}^{\mathbb{N}} \subseteq \mathcal{P}(\mathbb{N} \times \mathbb{N}) \cong \mathcal{P}(\mathbb{N}) \cong 2^{\mathbb{N}}$.

But we can give a bijection $\mathbb{N}^{\mathbb{N}} \underset{\beta}{\overset{\alpha}{\rightleftarrows}} S_1$ as follows:

for arbitrary $f: \mathbb{N} \to \mathbb{N}$,
define an increasing function $\alpha(f): \mathbb{N} \to \mathbb{N}$
by its sequence of sums, $\alpha(f)(n) := \sum_{0 \leq i \leq n} f(n)$

for increasing $g: \mathbb{N} \to \mathbb{N}$,
define $\beta(g): \mathbb{N} \to \mathbb{N}$ as its sequence of differences,
$\beta(g)(0) = g(0)$,
$\beta(g)(n) = g(n) - g(n-1)$ for $n > 0$.

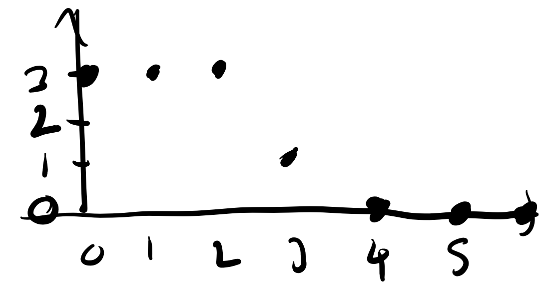
So $|S_1| = |\mathbb{N}^{\mathbb{N}}| = 2^{\aleph_0}$.

(b) $|S_2| = \aleph_0$: ($S_2 = \{\text{decreasing functions } f: \mathbb{N} \to \mathbb{N}\}$)

$\aleph_0 \leq |S_2|$ is clear, since we can give an injection $\mathbb{N} \rightarrowtail S_2$ by e.g. sending $n \in \mathbb{N}$ to the constant function with value n.

To show $|S_2| \le \aleph_0$, note that we can encode any decreasing function f as a <u>finite seq.</u> of <u>pairs</u> of naturals, whose i^{th} element is the i^{th} distinct value f takes, together with the minimal input on which f takes that value;

e.g. if f is the function



it would be coded as $((0,3),(3,1),(4,0))$.

The fact f is decreasing ensures this sequence is finite, & f can clearly be recovered from it;

<u>so</u> this coding gives an injection $S_2 \rightarrowtail (\mathbb{N}\times\mathbb{N})^{<\omega} \cong \mathbb{N}^{<\omega}$

and we know $|\mathbb{N}^{<\omega}| = \aleph_0$

(c) $|S_3| = 2^{(2^{\aleph_0})}$: $\quad (S_3 = \mathbb{N}^{\mathbb{R}})$

$$2^{\mathbb{R}} \subseteq \mathbb{N}^{\mathbb{R}} \subseteq \mathcal{P}(\mathbb{N}\times\mathbb{R}) \cong \mathcal{P}(\mathbb{R}) \cong 2^{\mathbb{R}}$$

so $|\mathbb{N}^{\mathbb{R}}| = |2^{\mathbb{R}}| = 2^{(2^{\aleph_0})}$

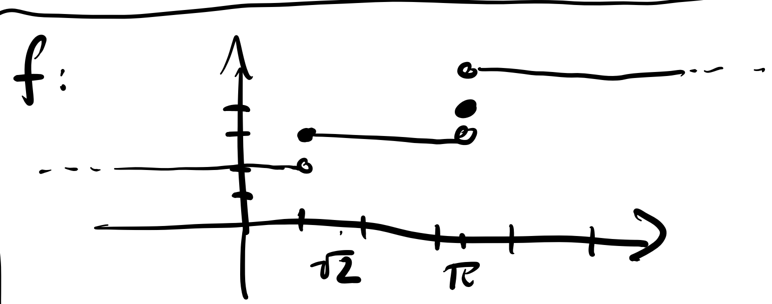
(d) $|S_4| = 2^{\aleph_0}$: $\quad (S_4 = \{\text{increasing } f:\mathbb{R}\to\mathbb{N}\})$

for $2^{\aleph_0} \le |S_4|$ note we can give an injection $\mathbb{R} \rightarrowtail S_4$ by e.g. sending $x\in\mathbb{R}$ to $f_x(y) := \begin{cases} 0 & y\le x \\ 1 & y>x \end{cases}$.

Conversely for $|S_4| \leq 2^{\aleph_0}$,

first note that for any $f : \mathbb{R} \to \mathbb{N}$ increasing, the inverse image $f^{-1}(n)$ of any $n \in \mathbb{N}$ must be an <u>interval</u>, since if $x, y \in f^{-1}(n)$ and $x \leq z \leq y$, then $n = f(x) \leq f(z) \leq f(y) = n$, so $z \in f^{-1}(n)$.

<u>So</u> any such f can be encoded by giving the sequence of endpoints ~~of~~ of those intervals, together with the values at those endpoints, allowing for the possibility that those intervals may be infinite.



n	0	1	2	3	4	5	6
$\mu_f(n)$	$(-\infty,0)$	$(-\infty,0)$	$(-\infty,0)$	$(\sqrt{2},1)$	$(\pi,1)$	$(\pi,0)$	$(\infty,0)$

This may be made precise as e.g. a sequence $\mu_f : \mathbb{N} \to (\mathbb{R} \cup \{\pm\infty\}) \times \{0,1\}$ as illustrated,

$$\mu_f(n)_1 = \inf\{x \mid f(x) \geq n\},$$

$$\mu_f(n)_2 = \begin{cases} 1 & \text{if } f(\mu_f(n)_1) = n, \\ 0 & \text{otherwise} \end{cases}$$

(where we take $\inf(\mathbb{R}) = -\infty$, $\inf(\emptyset) = \infty$).

This gives an <u>injection</u>

$$S_4 \rightarrowtail ((\mathbb{R} \cup \{\pm\infty\}) \times \{0,1\})^{\mathbb{N}} \cong \mathbb{R}^{\mathbb{N}} \cong (2^{\mathbb{N}})^{\mathbb{N}} \cong 2^{\mathbb{N}\times\mathbb{N}} \cong 2^{\mathbb{N}}$$

and so shows $|S_4| \leq 2^{\aleph_0}$.

2 (a) We will show that Zorn's lemma (which is equivalent to AC, over ZF) implies the order extension principle.

Let $(X, \leq)$ be a partial order. Take P to be the poset of partial orderings on X extending $\leq$, ordered by inclusion.

We claim:

(i) P is chain-complete;

(ii) any maximal element of P is a total order.

Together, these will give a total ordering extending $\leq$, as desired: by (i) and Zorn's lemma, P has some maximal element; by (ii), it must be total.

Proof of claim (i): If $C \subseteq P$ is a chain, then $\leq_C := \bigcup C$ is a partial order extending $\leq$

(certainly contains $\leq$, hence is reflexive;

is transitive, since if $x \leq_C y \leq_C z$,

that means $x \leq_1 y \leq_2 z$ for some

$\leq_1, \leq_2$ in C; WLOG $(\leq_1) \subseteq (\leq_2)$ since C is a chain; so $x \leq_2 y \leq_2 z$, so $x \leq_2 z$ and so $x \leq_C z$;

and antisymmetry is similar to transitivity);

so $\leq_C$ gives a (least!) upper bound for C in P.

Proof of claim (ii): Suppose $\leq' \in P$ is <u>not</u> total; we will show it is not maximal in P.

Since $\leq'$ is not total, there are some , $\in X$ s.t.

$a \not\leq' b$, $b \not\leq' a$. Define $\leq''$ to be

$$\leq' \cup \{(x,y) \mid x \leq a,\ b \leq y\}$$

Clearly $\leq''$ contains $\leq$, & is reflexive.

Transitivity: if $x \leq'' y \leq'' z$, there are four possibilities:

$$x \leq' y \leq' z$$

$$x \leq' a \quad b \leq' y \leq' z$$

$$x \leq' y \leq' a \quad b \leq' z$$

$$x \leq' a \quad b \leq' y \leq' a \quad b \leq' z$$

The first three each imply $x \leq'' z$. The fourth cannot occur, since it would imply $b \leq a$; but we chose a, b such that $b \not\leq a$.

Finally, antisymmetry. If $x \leq'' y$ and $y \leq'' x$, then again, we have four possibilities as above:

$$x \preceq' y \preceq' x$$

$$x \preceq' a \quad b \preceq' y \preceq' x$$

$$x \preceq' y \preceq' a \quad b \preceq' x$$

$$x \preceq' a \quad b \preceq' y \preceq' a \quad b \preceq' x$$

Now, all of the last 3 imply $b \preceq' a$, so cannot occur. So only the first case is possible, which implies $x = y$.

<u>So</u> $\preceq''$ is a partial order extending $\preceq$, and indeed <u>strictly</u> extending $\preceq'$, (since $a \preceq'' b$ but $a \not\preceq' b$)

so $\preceq''$ shows that $\preceq'$ is not maximal in P, so we're done.

(b) The order extension principle implies that every set admits <u>some</u> total ordering (since it carries the "discrete" partial order $=$, which can then be extended to some total order.

So given a family of non-empty finite sets $\langle X_i \rangle_{i \in I}$,

we may take some total order $\leq$ on the union $\bigcup_{i \in I} X_i$.

Now since any finite n.-e. subset of a total order has a unique minimal element, we get the function

$$i \longmapsto \min(X_i)$$

giving a choice function for the original family.

3 (a) Given consistent T over L as in the question, we know by completeness T has some model M. If M is finite, then $\|M\| < \aleph_0 \leq \|L\|$ so we're done. Otherwise, M is infinite, so by downward L-S, has some elementary substructure $N \prec M$ with $\|N\| \leq \|L\|$. So N is a model of T of size $\leq \max(\|T\|, \|L\|)$ as required.

(b) Take T to be the theory of a total order with no maximal element. Then T is finite & $\|L\| = \aleph_0$; & T has no finite model, so every model is of size $\geq \aleph_0 = \max(\|T\|, \|L\|)$.

(c) Take L to be the empty language, T the theory $\{\forall x, y,\ x = y\}$. Then $\max(\|T\|, \|L\|) = \|L\| = \aleph_0$, but every model of T is of size ≤ 1.

(d) Yes: any consistent, infinite T has some model of size $\leq T$. Proof: Given such T, let $L' \subseteq L$ be the sub language specified by just the symbols appearing in T.

The set of such symbols is of size $\leq T$ (since each formula in T contain only fin. many symbols, & T is infinite), so $\|L'\| \leq \|T\|$. Now let T' be T viewed as a theory over L'. By (a), T' has some model M of size $\leq \max(\|T'\|, \|L'\|) = \|T\|$. But now we can expand M to an L-structure N by picking some arbitrary interpretation for the symbols of L that are not in L'; then N is a model of T of size $\leq \|T\|$, as desired.

4. (a) Predecessor satisfies

$$p(0) = 0$$
$$p(S(n)) = n$$

So it is the function specified by the single recursive def'n

$$p(0) = g()$$
$$p(S(n)) = h(n, p(n))$$

where $g: \mathbb{N}^0 \to \mathbb{N}$ is the constant 0

& $h: \mathbb{N}^2 \to \mathbb{N}$ is the projection $h(x,y) = x$.

So it is a (primitive) recursive function.

(b) Similarly, "monus" satisfies $m \dot{-} 0 = m$

$$m \dot{-} Sn = p(m \dot{-} n)$$

so is the function $f: \mathbb{N}^2 \to \mathbb{N}$ specified by the (parametrised) recursive def $f(m, 0) = g'(m)$

$$f(m, Sn) = h'(m, n, f(m,n))$$

where $g'(x) = x$ $h'(x,y,z) = p(z)$. Now g' is a projection function, & h' is the composite of p with the 3rd projection $\mathbb{N}^3 \to \mathbb{N}$. So g' & h' are recursive; so monus is recursive.

5. As described in the question, if ZFC is consistent, then it has some countable model; call this (M, ε^M).
(Note that the relation ε^M need not be actual set membership — it is just some binary relation on M.)
Since $M \models ZFC$, we know that $M \models$ "there exists some uncountable set":

that is, there is some $a \in M$ such that

$$M \models \text{"}a \text{ is uncountable"}.$$

However, this does not mean that $\{x \in M \mid x \,\varepsilon^M a\}$ is uncountable! It means that $M \models$ "there is no surjection $\omega \twoheadrightarrow a$",
i.e. there is no $f \in M$ such that

$$M \models \text{"}f \text{ is a surjection } \omega \twoheadrightarrow a\text{"}.$$

Even if ε^M is $\in$, $[\![\omega]\!]^M = \omega$, and all el'ts of a are in M, just means that M does not contain any surjection $\omega \twoheadrightarrow a$.

So a may be countable — such surjections may exist — they just cannot lie in M.

6. (a) To show T is consistent, it suffices (by the compactness thm) to show that every finite subset $T' \subseteq T$ is consistent.

But given such T', take

$$N := \max\{ n \in \mathbb{N} \mid \text{"} c \geq \bar{n} \text{"} \in T' \}$$

and observe that taking the standard model $\mathbb{N}$ of PA, with c interpreted as N, gives a model of T'.

So every such T' is consistent; so T is consistent, & has some model M. But now M (or to be pedantic, its reduct to L_A) is a non-standard model of PA, since for each $n \in \mathbb{N}$,

$$T \vdash c \neq \bar{n} \quad \left(\text{since } T \vdash c \geq \overline{n+1}, \ \& \ PA \vdash \forall x, y,\ x \geq S(y) \to x \neq y\right)$$

so $[\![c]\!]^M \neq [\![\bar{n}]\!]^M$.

(b) Again, we use compactness.

Given $X \subseteq \mathbb{P}$, let T_X be the theory (again in L_A plus one new constant symbol c)

$$PA \cup \{\bar{p} \mid c \mid p \in X\} \cup \{\bar{p} \nmid c \mid p \in \mathbb{P} \setminus X\}.$$

Any finite $T' \subseteq T_X$ is contained in

$$PA \cup \{\bar{p} \mid c \mid p \in X'\} \cup \{\bar{p} \nmid c \mid p \in X''\}$$

for some finite, disjoint sets of primes X', X'', and so is modelled by $\mathbb{N}$, with c interpreted as $\prod_{p \in X'} p$. So by compactness, T has some model; the defn of T ensures that in any such model, the standard prime divisors of $[\![c]\!]$ are precisely X.

Finally, by downward Löwenheim-Skolem, since $|\mathcal{L}_A| = \aleph_0$, there must exist some <u>countable</u> such model.

(c) For any model M of PA, write $A_M := \{ X \subseteq \mathbb{P} \mid$ there is some $a \in M$ whose standard prime divisors are precisely $X \}$.

If $M \cong M'$, then $A_M = A_{M'}$, so we can speak of $A_{\underline{M}}$ for any iso class of models $\underline{M}$. Moreover, if M is a <u>countable</u> model, A_M is certainly countable.

Part (b) tells us that

$$\mathcal{P}(\mathbb{P}) = \bigcup_{\substack{\underline{M} \text{ an iso class} \\ \text{of ctble models of PA}}} A_{\underline{M}}$$

so if there were only countably many iso classes of ctble models of PA, $\mathcal{P}(\mathbb{N})$ would be a ctble union of ctble sets and hence would be countable. But $|\mathbb{N}| = \aleph_0$, so $\mathcal{P}(\mathbb{N})$ is uncountable.
So there must be uncountably many iso classes of countable models of PA.