

# Mathematical Logic

## Assignment 4

Ari Feiglin

### Exercise 4.1:

Suppose that a theory with equality  $T$  has arbitrarily large finite models, show that  $T$  has an infinite model.

Let us define the language  $\mathcal{L}^*$  which we obtain by extending  $\mathcal{L}$  with an infinite amount of constant symbols  $c_1, c_2, \dots$ . We then define the theory  $T^* = T \cup \{c_i \neq c_j \mid i \neq j\}$ , the theory obtained by adding axioms  $c_i \neq c_j$  when  $i \neq j$ . Let  $\Delta \subseteq T^*$  be finite, then we have that for some  $m$ ,

$$\Delta \subseteq T \cup \{c_i \neq c_j \mid i \neq j \leq m\}$$

as we can take  $m$  to be the maximum index of  $c_i$  in  $\Delta$ , as it is finite.

Since  $T$  has arbitrarily large finite models, let  $\mathcal{M}$  be a model of  $T$  size  $\geq m$ . We extend  $\mathcal{M}$  to be an  $\mathcal{L}^*$ -interpretation by interpreting  $c_i$  as arbitrary *distinct* values in  $\mathcal{M}$  for  $i \leq m$  (such values exist since the size of  $\mathcal{M}$  is larger than  $m$ . For  $i > m$  we can interpret  $c_i$  as whatever). Thus  $\mathcal{M}$  satisfies  $\Delta$ , as it satisfies  $T$  and satisfies  $\{c_i \neq c_j \mid i \neq j \leq m\}$  as we defined the interpretations of  $c_i$  to be distinct.

So every finite subtheory of  $T^*$  is satisfiable, and so by the compactness theorem,  $T^*$  is satisfiable. But any model of  $T^*$  must be infinite, as its interpretations of  $c_i$  must all be distinct, and there is an infinite number of  $c_i$ s.

### Exercise 4.2:

Show that every torsion-free abelian group  $(A, +)$  can be linearly group ordered.

We begin by showing this for finitely generated torsion-free abelian groups,  $A$ . It is known that  $A$  is isomorphic to  $\mathbb{Z}^n$  for some  $n$ , and thus we can give it a lexicographic ordering:  $(a_1, \dots, a_n) < (b_1, \dots, b_n)$  if  $a_1 < b_1$  or  $a_1 = b_1$  and  $a_2 < b_2$  or  $\dots$ . This obviously preserves group structure since  $(\mathbb{Z}, <)$  is a linearly ordered abelian group (this is obvious, but tedious).

Now let  $A$  be an arbitrary torsion-free abelian group  $(A, +)$ , we define the language  $\mathcal{L} = \{+, <\} \cup \{c_a\}_{a \in A}$  where  $c_a$  is a constant symbol for every  $a \in A$ . We further define the theory  $T$  by taking the axioms of linear group orders and adding the axioms  $\{c_a \neq c_b \mid a \neq b \in A\} \cup \{c_a + c_b = c_c \mid a, b, c \in A, a + b = c\}$ . Let  $\Delta \subseteq T$  be a finite subset, and let us take  $\mathcal{L}_\Delta$ , the set of all constant symbols which show in the axioms of  $\Delta$ . And then we define  $S = \{a \mid c_a \in \mathcal{L}_\Delta\} \subseteq A$ . Since  $\Delta$  is finite, so is  $\mathcal{L}_\Delta$ , and therefore so is  $S$ . So we define  $A' = \langle S \rangle \leq A$  the subgroup of  $A$  generated by  $S$ , and we turn this structure into an interpretation by interpreting  $c_a \in \mathcal{L}_\Delta$  as  $a$ .

Since  $A'$  is a finitely ( $S$  is finite) generated torsion-free ( $A$  is torsion-free) group, it can be linearly ordered with a group ordering. And thus  $A'$  along with its ordering models  $\Delta$  since it is a linear group order, and it is a subgroup of  $A$  (so it models  $c_a + c_b = c_c$  when  $a + b = c$ , since its own group operation is a restriction of  $A$ 's). So  $\Delta$  is satisfiable.

Thus by the compactness theorem,  $T$  is satisfiable. Suppose  $G$  is a model of  $T$ , then it is essentially  $A$ . Formally, there exists an injection

$$f: A \hookrightarrow G, \quad a \mapsto c_a^G$$

So we define  $a < b$  in  $A$  if and only if  $f(a) < f(b)$  in  $G$ . Since  $G$ 's is a linear order, so is  $A$ 's: if  $a < b$  and  $b < c$  then  $f(a) < f(b) < f(c)$  so  $f(a) < f(c)$  and so  $a < c$ , if  $a < a$  then  $f(a) < f(a)$  in contradiction, if  $a < b < a$  then  $f(a) < f(b) < f(a)$  in contradiction, so  $A$  has a partial order. If  $a \neq b \in A$ , then since  $f(a) < f(b)$  or  $f(b) < f(a)$  since  $G$  is a linear order, either  $a < b$  or  $b < a$ , so  $A$  is also a linear order.

And if  $a < b$  and  $c \leq d$ , then  $f(a) < f(b)$  and  $f(c) \leq f(d)$ , and so  $f(a) + f(c) < f(b) + f(d)$ , and since  $f(a) + f(c) = c_a^G + c_c^G$ , and by the axioms of  $T$ , this is equal to  $(c_{a+c})^G = f(a+c)$ , and so

$$f(a+c) = f(a) + f(c) < f(b) + f(d) = f(b+d) \implies a+c < b+d$$

as required. So we have given  $A$  a linear group order.

For the following two exercises, the signature of the theory is just a 3-ary predicate  $C(x, y, z)$  meaning the distance of  $x$  and  $y$  from  $z$  is the same ( $|xz| = |yz|$ ).

#### Exercise 4.3:

Define the property  $|OA| \leq |OB|$  for three points  $O, A, B$ .

First notice that using the predicate  $C$  it is very easy to define two shapes: lines equidistant from two points, and circles whose center is one point and the radius is the distance of that point from another. For points  $x, y$ , we define the predicates

$$\text{Normal}_{x,y}(u): C(x, y, u) \quad \text{Circle}_{x,y}(u): C(u, y, x)$$

so  $\text{Normal}_{x,y}(u)$  if and only if  $u$  is equidistant from  $x$  and  $y$ , this defines the line normal to the line  $\overline{xy}$  which intersects it precisely between  $x$  and  $y$ . And  $\text{Circle}_{x,y}(u)$  if and only if  $u$  has the same distance from  $x$  as  $x$  does to  $y$ , defining the circle about  $x$  of radius  $|xy|$ .

We begin by defining a new predicate  $L(x, y, z)$  to mean that  $x, y$ , and  $z$  are all on the same line. We assume that  $x, y, z$  are all distinct for now. Note that if  $x, y, z$  are on the same line, and suppose that the order of the points is  $xyz$ , then no element on the line normal to  $yz$  ( $\text{Normal}_{y,z}$ ) has the same distance from  $x$  as  $y$  does. This is because the line  $xu$  creates a right triangle with  $xyz$  and  $\text{Normal}_{y,z}$ , and since  $xy$  is a part of the basis of the right triangle. That is for every  $u$ , if  $\text{Normal}_{x,y}(u)$  then  $\neg C(u, y, x)$ . So we get  $\forall u(\text{Normal}_{y,z}(u) \rightarrow \neg C(u, y, x))$  is true if and only if  $xyz$  is a line. We will denote this

$$L_{\text{strict}}(x, y, z): \quad \forall u(\text{Normal}_{y,z}(u) \rightarrow \neg C(u, y, x))$$

Since the order need not be  $xyz$  (eg. it could be  $xzy$ ), we permute the order and get

$$L(x_1, x_2, x_3): \quad \bigvee_{\sigma \in S_3} L_{\text{strict}}(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$$

Now the idea here is to draw a circle about  $O$  whose radius is  $|OA|$ , ie.  $\text{Circle}_{O,A}$ . We can take a point on this circle  $A'$  so that  $OA'B$  is one line, there are two points on exactly opposite sides of the circle where this is true (the ends of the diameter which is incident with  $OB$ ). We will assume that  $A'$  is chosen as the point closer to  $B$ . Then  $|OA| = |OA'|$ , and  $|OA'| < |OB|$  if and only if  $\text{Normal}_{A',B}$  does not intersect  $\text{Circle}_{O,A'}$ . For the point  $A'$  on the other side, we can ignore, since the normal line between it and  $B$  does not intersect the circle only if the distance between  $O$  and  $B$  is much larger than  $O$  and  $A$ . In first order terms

$$|OA| \leq |OB|: \quad C(A, B, O) \vee \exists A'(\text{Circle}_{O,A}(A') \wedge L(O, A', B) \rightarrow \forall X(\text{Normal}_{A',B}(X) \rightarrow \neg \text{Circle}_{O,A}(X)))$$

The first  $C(A, B, O)$  is if  $|AO| = |BO|$ .

#### Exercise 4.4:

Define

- (1) Equality of triangles
- (2) Equality of angles
- (3) An angle being right

- (1) We begin by defining the equality of two lines,  $|AB| = |CD|$ . We do this by rotating  $B$  about  $A$  and  $C$  about  $D$  so that  $ABCD$  is one line (defined by  $L(A, B, C) \wedge L(B, C, D)$ , I will write this as  $L(A, B, C, D)$ ). We take the normal between  $B$  and  $C$ , let point of intersection between the normal and  $ABCD$  be  $O$ . Then the normal between  $A$  and  $D$  coincides with the normal between  $B$  and  $C$  if and only if  $|AO| = |OD|$ , where  $|AO| = |AB| + |BO|$  and  $|OD| = |OC| + |CD|$ . Since  $|BO| = |OC|$  as  $O$  is on their normal, we have that the normals coincide if and only if  $|AB| = |CD|$ .

Since we can rotate  $B$  and  $C$  to get  $BACD$  or  $BADC$  or  $ABDC$ , we worry only about existence, as the above

is true for when  $ABCD$  is a line. Thus

$$|AB| = |CD|: \quad \exists B', C' (\text{Circle}_{A,B}(B') \wedge \text{Circle}_{D,C}(C') \wedge \forall X (\text{Normal}_{B,C}(X) \leftrightarrow \text{Normal}_{A,D}(X)))$$

Then two triangles  $X_1X_2X_3$  and  $Y_1Y_2Y_3$  are equal if through some rotation, all the sides are equal:

$$\triangle X_1X_2X_3 \cong \triangle Y_1Y_2Y_3: \quad \bigvee_{j=1}^3 \bigwedge_{i=1}^3 |X_iX_{i+1}| = |Y_{i+j}Y_{i+j+1}|$$

where addition is done modulo 3. The addition by  $j$  corresponds to rotating the triangle  $Y_1Y_2Y_3$ .

- (2) Two angles are equal,  $\angle ABC = \angle DEF$ , if we can extend the edges  $ED$  and  $EF$  to get a triangle  $D'EF'$  so that  $\triangle ABC \cong \triangle D'EF'$ . We must also ensure that  $D'$  and  $F'$  are on the same side as  $D$  and  $F$  respectively, with respect to the point  $E$  (otherwise we may get that  $\alpha = 180^\circ - \alpha$ ). Thus we must have that  $DD'E$  or  $D'DE$  is a line, and similarly for  $F$ . So we can define this by

$$\angle ABC = \angle DEF:$$

$$\exists D', F' ((L_{\text{strict}}(D, D', E) \vee L_{\text{strict}}(D', D, E)) \wedge (L_{\text{strict}}(F, F', E) \vee L_{\text{strict}}(F', F, E)) \wedge \triangle ABC \cong \triangle D'EF')$$

- (3) This much is simple,  $\angle ABC$  is right if we by flipping  $C$  over  $B$  to get a point  $C'$ , we have that the triangle  $\triangle C'AC$  is isosceles. This is because  $|BC| = |BC'|$  and so  $AB$  is a bisector of the basis, and so the triangle is isosceles if and only if the bisector is also perpendicular. Thus

$$\angle ABC = 90^\circ: \quad \exists C' (L_{\text{strict}}(C', B, C) \wedge C(C', C, B) \wedge C(C', C, A))$$

#### Exercise 4.5:

Prove that there exists a set of natural numbers which is not definable in arithmetic.

Since the language of arithmetic is countable, there is a countable number of arithmetic formulas, and thus a countable number of definable sets. But since there are  $2^{\aleph_0}$  subsets of  $\mathbb{N}$ , and by Cantor's Theorem  $\aleph_0 < 2^{\aleph_0}$ , there is strictly more natural subsets than definable sets. Thus there must exist undefinable subsets of  $\mathbb{N}$ .

#### Exercise 4.6:

Prove that the binary predicate “ $x$  is the  $n$ th prime” is definable in arithmetic.

Let us define the recurrence:

$$F_p(x) = \begin{cases} 0 & x = 0 \\ F_p(x-1) & x \text{ is not prime} \\ F_p(x-1) + 1 & x \text{ is prime} \end{cases}$$

This recurrence gives the index of the largest prime less than or equal to  $x$  (ie.  $F_p(9) = 4$ , since 7 is the closest prime  $\leq 9$  and it is the fourth prime). We can rewrite this as

$$F_p(x) = \begin{cases} 0 & x = 0 \\ g(x-1, F_p(x-1)) & x \neq 0 \end{cases}$$

where

$$g(x, N) = \begin{cases} N & x \text{ is not prime} \\ N + 1 & x \text{ is prime} \end{cases}$$

This is useful since  $g$  is definable, since the property of being prime is definable (as we showed, but it is simply  $\forall y (y \mid x \rightarrow (y = 1 \vee y = x))$ ).

Our predicate is simply equivalent to “ $x$  is prime and  $F(x) = n$ ”. Since “ $x$  is prime”, all we must do is show that “ $F_p(x) = n$ ” is definable.

Let us generalize, suppose we have a recurrence  $F(0) = c$  and  $F(x+1) = g(x, F(x))$  for some function  $g$ . We would like to define the predicate “ $F(x) = y$ ”. This is equivalent to saying that there exists a sequence  $a_0, \dots, a_x$  such that  $a_0 = c$  and  $a_x = y$  where  $g(i, a_i) = a_{i+1}$  as this literally means that  $a_i = F(i)$ , and thus  $F(x) = a_x = y$ . Since any finite sequence can be written as  $a_i = \beta(a, b, i)$  for some  $a, b$  where  $\beta$  is Gödel’s beta function, meaning any finite sequence can be encoded by just two values  $a$  and  $b$ . Thus we want  $a$  and  $b$  such that  $\beta(a, b, 0) = c$  and  $\beta(a, b, x) = y$  where  $g(i, \beta(a, b, i)) = \beta(a, b, i+1)$  for every  $i < x$ .

Thus the predicate  $F(x) = y$  can be defined be

$$\exists a, b (\beta(a, b, 0) = c \wedge \beta(a, b, x) = y \wedge \forall i (i < x \rightarrow g(i, \beta(a, b, i)) = \beta(a, b, i+1)))$$

Formally, we’d say  $\exists c(\beta(a, b, 0, c))$  and similar since functions are defined as formulas.

Since our  $F_p$  is a specific occurrence of such a recurrence, “ $F(x) = y$ ” is necessarily also definable (using the same formula as above). Thus, as stated above, the first order formula defining the predicate “ $x$  is the  $n$ th prime” is

$$x \text{ is prime} \wedge F_p(x) = n$$

#### Exercise 4.7:

Show that the predicate “ $y = x + 1$ ” is not definable in the interpretation  $(\mathbb{Z}, =, f)$  where  $f$  is a unary function  $x \mapsto x + 2$ .

Let us define the automorphism  $\Phi(x) = -x - 4$ , this is obviously a bijection. It also preserves  $f$  since

$$f(\Phi(x)) = f(-x - 4) = -x - 2, \quad \Phi(f(x)) = \Phi(x + 2) = -x - 2$$

thus  $\Phi$  is indeed an automorphism. But it does not preserve the predicate “ $y = x + 1$ ” since  $\Phi(y) = \Phi(x + 1) = -x - 1 - 4 = -x - 5$ , but  $\Phi(x) + 1 = -x - 3$ , thus  $\Phi(y) \neq \Phi(x) + 1$ , and so the predicate is not definable.

#### Exercise 4.8:

Show that the predicate “ $x = 2$ ” is not definable in the interpretation  $(\mathbb{N}, =, |)$ .

Let us take the automorphism defined by  $\Phi(2) = 3$  and  $\Phi(3) = 2$  and for every other prime  $p$ ,  $\Phi(p) = p$  (also  $\Phi(1) = 1$  and  $\Phi(0) = 0$ ). We further define that

$$\Phi(p_1^{n_1} \dots p_k^{n_k}) = \Phi(p_1)^{n_1} \dots \Phi(p_k)^{n_k}$$

If  $n = p_1^{n_1} \dots p_k^{n_k}$  then let  $m = \Phi^{-1}(p_1)^{n_1} \dots \Phi^{-1}(p_k)^{n_k}$  where  $\Phi^{-1}$  is  $\Phi$ ’s inverse over the primes. Then  $\Phi(m) = n$  by definition, and so  $\Phi$  is surjective. Note that if  $a = p_1^{n_1} \dots p_k^{n_k}$  and if  $b = q_1^{t_1} \dots q_m^{t_m}$  and  $\Phi(a) = \Phi(b)$  then  $\Phi(p_1)^{n_1} \dots \Phi(p_k)^{n_k} = \Phi(q_1)^{t_1} \dots \Phi(q_m)^{t_m}$ . Since these are both products of primes, we have that the factorizations are the same. Without loss of generality, we have  $\Phi(p_i) = \Phi(q_i)$  and  $n_i = t_i$ , and since  $\Phi$  is bijective over the primes,  $p_i = q_i$  and so  $a = b$ . Thus  $\Phi$  is also an injection and therefore a bijection.

Suppose  $n \mid m$  then  $n = p_1^{n_1} \dots p_k^{n_k}$  and  $m = p_1^{t_1} \dots p_k^{t_k}$  where  $0 \leq n_i \leq t_i$  for all relevant  $i$ . Thus  $\Phi(n) = \Phi(p_1)^{n_1} \dots \Phi(p_k)^{n_k}$  and  $\Phi(m) = \Phi(p_1)^{t_1} \dots \Phi(p_k)^{t_k}$ , and so we still have  $\Phi(n) \mid \Phi(m)$ , so  $\Phi$  is an automorphism.

But since  $\Phi(2) = 3$ , the predicate “ $x = 2$ ” is not stable (since if  $x = 2$  then  $\Phi(x) = 3 \neq 2$ ).

#### Exercise 4.9:

Let  $\mathcal{L} = \{\sim\}$  where  $\sim$  is a binary relation symbol. Let  $T$  be the  $\mathcal{L}$ -theory of an equivalence relation with infinitely many infinite classes, and no finite classes.

- (1) Write axioms for  $T$
- (2) How many models are there of each cardinality  $\aleph$ ?
- (3) Is  $T$  complete?

The original question posed this simply as the theory with infinitely many infinite classes, but if we allow finite classes this is not first order axiomizable. To prove this we will find an elementary extension of a model, such that the model does not satisfy the theory but the extension does. Since an  $\mathcal{L}$ -model is elementarily equivalent to an elementary extension of it (when viewed also as an  $\mathcal{L}$ -model), this would be a contradiction, since they both must satisfy the same  $\mathcal{L}$ -theories.

Let  $\mathcal{M}$  be an infinite model with only finite equivalence classes, but these finite equivalence classes are arbitrarily large. We define a new language  $\mathcal{L}^*$  as an extension of the language  $\mathcal{L}_{\mathcal{M}}$  with constant symbols  $\{c_{i,j} \mid i, j \in \mathbb{N}\}$ . We define the  $\mathcal{L}^*$ -theory  $T^*$  as  $\text{Diag}_{\text{el}}(\mathcal{M})$  along with the axioms

$$\begin{aligned} c_{i,j} &\neq c_{i',j'} & i \neq i' \text{ or } j \neq j' \\ c_{i,j} &\sim c_{i',j} \\ c_{i,j} &\not\sim c_{i,j'} & j \neq j' \end{aligned}$$

ie. all the new constants are distinct, constants whose second index is the same are equivalent, and constants whose second index are not equivalent are not equivalent. Thus any model of  $T$  must have infinitely many infinite classes: each  $C_j = \{c_{i,j} \mid i \in \mathbb{N}\}$  is a subset of a class, and no two  $C_j$  are part of the same class. Since  $C_j$  is infinite as  $c_{i,j}$  are distinct, and there are infinitely many  $C_j$ , we have as required.

$T^*$  is finitely satisfiable, since we can extend  $\mathcal{M}$  to a model of a finite subset of  $T^*$  since  $\mathcal{M}$  has arbitrarily large finite equivalence classes. More precisely, let  $\Delta \subseteq T^*$  be finite, then it contains finitely many instances of  $c_{i,j}$ . Thus it contains finitely many equivalence classes, and each equivalence class is finite. For each of the equivalence classes of  $\Delta$ , take an equivalence class of  $\mathcal{M}$ 's of at least that size and properly interpret the constants in  $\Delta$ 's equivalence class as elements of the chosen equivalence class of  $\mathcal{M}$ . We can do this since  $\mathcal{M}$  has arbitrarily large finite equivalence classes.

Thus by the compactness theorem,  $T^*$  is satisfiable. Suppose  $\mathcal{N} \models T^*$ , but then since  $\text{Diag}_{\text{el}}(\mathcal{M}) \subseteq T^*$ , we have  $\mathcal{N} \models \text{Diag}_{\text{el}}(\mathcal{M})$ , so  $\mathcal{N}$  is an elementary extension of  $\mathcal{M}$  (or there exists an elementary embedding of  $\mathcal{M}$  into  $\mathcal{N}$ ). But  $\mathcal{N}$  has infinitely many infinite classes, by the axioms of  $T^*$ , and so  $\mathcal{N} \models T$  (the original theory of there being infinitely many infinite classes). But since  $\mathcal{N}$  is an elementary extension of  $\mathcal{M}$ , they are elementarily equivalent, and so  $\mathcal{M} \models T$  which is a contradiction since  $\mathcal{M}$  has no infinite classes. Thus  $T$  cannot exist as a first order theory.

There is the small nuance of  $\mathcal{M}$ 's existence, but this is trivial. We can define a partition of  $\mathbb{N}$  like  $\{\{0\}, \{1, 2\}, \{3, 4, 5\}, \dots\}$ , and  $\mathbb{N}$  along with the equivalence relation induced by this partition is obviously such a model.

This proof is not entirely mine, I was pointed in the correct direction by briefly looking at a Math Stack Exchange post.

- (1) We start with the standard axioms for equivalence relations:

$$\begin{aligned} \forall x \forall y (x = y \rightarrow x \sim y) \\ \forall x \forall y (x \sim y \rightarrow y \sim x) \\ \forall x \forall y \forall z (x \sim y \wedge y \sim z \rightarrow x \sim z) \end{aligned}$$

Now we need the condition that there exist infinite classes. We do this by adding an axiom that there exist at least  $n$  distinct equivalence classes. So for every  $n \in \mathbb{N}$ , add

$$\exists x_1, \dots, x_n \left( \bigwedge_{i \neq j=1}^n x_i \not\sim x_j \right)$$

Now we need the condition that every equivalence class is infinite. We do this by adding axioms that every equivalence class has at least  $n$  distinct elements. So for every  $n \in \mathbb{N}$ , add

$$\forall x \exists x_1, \dots, x_n \left( \bigwedge_{i \neq j=1}^n x_i \neq x_j \wedge \bigwedge_{i=1}^n x_i \sim x \right)$$

- (2) First let us claim that two models of this theory are isomorphic if and only if for every cardinality, both models have the same number of classes of that cardinality. Suppose that  $\mathcal{M}$  and  $\mathcal{N}$  are two isomorphic models of the theory, let  $\iota: \mathcal{M} \rightarrow \mathcal{N}$  be an isomorphism. Let  $C$  be an equivalence class in  $\mathcal{M}$  then  $\iota(C)$  has the same cardinality of  $\mathcal{M}$  since  $\iota: C \rightarrow \iota(C)$  is still a bijection. Furthermore,  $x \sim y$  if and only if  $\iota(x) \sim \iota(y)$  then if  $\iota(x), \iota(y) \in \iota(C)$  then since  $x \sim y$ ,  $\iota(x) \sim \iota(y)$  and thus  $\iota(C)$  is a subset of an equivalence class in  $\mathcal{N}$ . And if  $y \sim \iota(C)$ , then there exists an  $x \in \mathcal{M}$  such that  $\iota(x) = y$ , and so  $\iota(x) \sim \iota(C)$  and so  $x \sim C$  and so  $x \in C$  and thus  $y = \iota(x) \in \iota(C)$ , so  $\iota(C)$  is an equivalence class in  $\mathcal{N}$  as required.

Thus if  $\{C_\lambda\}_{\lambda \in \Lambda}$  is the set of all equivalence classes of cardinality  $\alpha$  in  $\mathcal{M}$  then  $\{\iota(C_\lambda)\}_{\lambda \in \Lambda}$  are all distinct (since  $\iota$  is injective) equivalence classes of cardinality  $\alpha$  in  $\mathcal{N}$  and so there are at least  $|\Lambda|$  equivalence classes of cardinality  $\alpha$  in  $\mathcal{N}$ . By symmetry, this is an equality (since we can reverse the process for an isomorphism  $\mathcal{N} \rightarrow \mathcal{M}$ ). This proves one direction.

Now suppose two models of the theory have the same number of classes of each cardinality. Then for every cardinality  $\alpha$  let  $\{C_\lambda^\alpha(X)\}_{\lambda \in \Lambda(\alpha)}$  be the set of equivalence classes of  $X$  (where  $X = \mathcal{M}$  or  $\mathcal{N}$ ) of cardinality  $\alpha$ . Then for each  $\alpha$  and  $\lambda \in \Lambda(\alpha)$  there exists a bijection  $\iota_\lambda^\alpha: C_\lambda^\alpha(\mathcal{M}) \rightarrow C_\lambda^\alpha(\mathcal{N})$  since they both have cardinality  $\alpha$ . Then we define  $\iota: \mathcal{M} \rightarrow \mathcal{N}$  where if  $x \in C_\lambda^\alpha(\mathcal{M})$  then we set  $\iota(x) = \iota_\lambda^\alpha(x)$ . Since each  $\iota_\lambda^\alpha$  is a bijection, and have disjoint domains and codomains, this  $\iota$  is well-defined and a bijection (it is surjective since every equivalence class of  $\mathcal{N}$  is one of the form  $C_\lambda^\alpha(\mathcal{N})$ ).

We claim that  $\iota$  also preserves  $\sim$ , this is true since  $x \sim^\mathcal{M} y$  then  $x, y \in C_\lambda^\alpha(\mathcal{M})$  for some  $\alpha, \lambda$  and so  $\iota(x), \iota(y) \in C_\lambda^\alpha(\mathcal{N})$ , and thus  $\iota(x) \sim \iota(y)$ . And the converse holds similarly, since  $\iota^{-1}$  maps  $C_\lambda^\alpha(\mathcal{N})$  to  $C_\lambda^\alpha(\mathcal{M})$ . Thus  $\iota$  is an isomorphism, concluding our proof.

We now move onto our second claim: For every infinite cardinality  $\kappa$ , let  $\Gamma(\kappa) = \{\alpha \leq \kappa \text{ infinite cardinal}\}$  then for every function  $(\xi_\alpha)_{\alpha \in \Gamma(\kappa)}: \Gamma(\kappa) \rightarrow \Gamma(\kappa)$ , there exists a partition of a set  $X$  of cardinality  $\kappa$  with  $\xi_\alpha$  equivalence classes of cardinality  $\alpha$ .

Note that in order to create such a partition, it is necessary and sufficient to have

$$\sum_{\alpha \in \Gamma(\kappa)} \alpha \cdot \xi_\alpha \leq \kappa$$

room, as the partition will need that much room, as  $\alpha$  classes of cardinality  $\xi_\alpha$  has cardinality  $\alpha \cdot \xi_\alpha$ . Since  $\xi_\alpha \leq \kappa$  we have that

$$\sum_{\alpha \in \Gamma(\kappa)} \alpha \cdot \xi_\alpha \leq \sum_{\alpha \in \Gamma(\kappa)} \alpha \cdot \kappa = \sum_{\alpha \in \Gamma(\kappa)} \kappa = |\Gamma(\kappa)| \cdot \kappa$$

But  $\Gamma(\kappa) \subseteq \kappa + 1$  (the successor ordinal), we have that  $|\Gamma(\kappa)| \leq \kappa$ , and so

$$\leq \kappa \cdot \kappa = \kappa$$

as required.

For an equivalence relation (I will also refer to this as a partition), let such a function  $(\xi_\alpha): \Gamma(\kappa) \rightarrow \Gamma(\kappa)$  be defined where  $\xi_\alpha$  is equal to the number of equivalence classes of cardinality  $\alpha$ . Since every model has only infinite classes, this is well-defined (otherwise the codomain would have to include finite cardinals as well). Thus two partitions are isomorphic if and only if their induced  $(\xi_\alpha)$ s are equal (by the first claim). And for every such function  $(\xi_\alpha)$ , there exists a partition which induces that function. Thus the set of all functions  $\Gamma(\kappa) \rightarrow \Gamma(\kappa)$  describes exactly all the isomorphism classes of the partitions. Meaning that there are, up to isomorphism,

$$|\Gamma(\kappa)|^{|\Gamma(\kappa)|}$$

unique models of the theory.

For  $\kappa = \aleph_n$ , we know that by definition  $\Gamma(\aleph_n) = \{\aleph_1, \dots, \aleph_n\}$  and thus there are

$$\aleph_n^{\aleph_n}$$

unique models of the theory of cardinality  $\aleph_n$ , up to isomorphism.

- (3) For  $n = 1$ , the number above becomes  $1^1 = 1$ , and thus there is only one model of the theory whose cardinality is  $\aleph_0$ . In other words, the theory is  $\aleph_0$ -categorical, and has no finite models (since you need infinite elements in order to have infinite equivalence classes). Thus by Vaught's test, the theory is complete.

#### Exercise 4.10:

Let  $T$  be the theory of abelian groups where every element has order 2. Show that  $T$  is  $\kappa$ -categorical for every infinite cardinal  $\kappa$ , but not complete. Find  $T \subseteq T'$  a complete theory with the same infinite models as  $T$ .

Let  $A \models T$ , ie let  $A$  be an abelian group of order  $\kappa$  where every element has order 2. Then  $A$  is a  $\mathbb{Z}/2\mathbb{Z}$ -module, where scalar multiplication is defined normally. This is a module precisely since  $A$ 's elements all have order 2:  $(1+1)a = 0a = 0$  and  $a+a=0$  for every  $a \in A$ , and similarly  $(1+0)a = a$ , etc. it is trivial to see that all the other axioms of being a module are satisfied.

Since  $\mathbb{Z}/2\mathbb{Z}$  is a field,  $A$  is a vector space, and thus has a basis  $B$ . We know then that

$$A \cong \bigoplus_{b \in B} \mathbb{Z}/2\mathbb{Z}$$

(In general for a vector space  $V$  over  $\mathbb{F}$  with basis  $B$ ,  $V \cong \bigoplus_{b \in B} \mathbb{F}$ . This isomorphism can be generated by mapping  $v$  to its coordinate vector under  $B$ .)

Further note that assuming  $B$  is finite, the cardinality of the direct sum is  $|\mathbb{F}| \cdot |B|$ , as for every  $n \in \mathbb{N}$  we choose a set of  $n$  elements in  $B$  whose coordinates are non-zero and so we have  $\mathbb{F} \setminus \{0\}$  elements to choose from. There are  $|B|$  choices of coordinates for any  $n \in \mathbb{N}$  and  $(|\mathbb{F}| - 1)^n$  choices of coordinate values, and so for each  $n$  there are  $|B| \cdot (|\mathbb{F}| - 1)^n$  choices. If  $\mathbb{F}$  is finite, this is simply  $|B|$  and since we have  $\aleph_0$  choices for  $n$ , this becomes  $\aleph_0 \cdot |B| = |B|$ , and  $|\mathbb{F}| \cdot |B| = |B|$ . Ans if  $\mathbb{F}$  is infinite, this is  $|B||\mathbb{F}|$ , and so in total  $\aleph_0 |B||\mathbb{F}| = |B||\mathbb{F}|$  as required.

In our case, the field has cardinality 2 and the basis *is* infinite (otherwise the direct sum would have finite cardinality, contradicting the infiniteness of  $A$ ). So the cardinality of the direct sum is  $|B|$  and since the direct sum is isomorphic to  $A$ , we have  $|B| = \kappa$ .

Set an arbitrary set  $X$  of cardinality  $\kappa$ , then every  $A \models T$  of cardinality  $\kappa$  is isomorphic to

$$A \cong \bigoplus_{b \in B} \mathbb{Z}/2\mathbb{Z} \cong \bigoplus_{x \in X} \mathbb{Z}/2\mathbb{Z}$$

and in particular, every two models of  $T$  of cardinality  $\kappa$  are isomorphic (since they're both isomorphic to the direct product over  $X$ ). Thus  $T$  is  $\kappa$ -categorical.

Since  $T$  has finite models, we can simply take

$$\varphi = \exists x \forall y (x = y)$$

the formula that the structure has only one element. Since the trivial group satisfies  $T$ , and also satisfies  $\varphi$ , and so  $\neg\varphi$  cannot be proven by  $T$  (as then this would contradict the trivial group modelling  $T$ ). But take any other model of  $T$  (eg.  $\mathbb{Z}/2\mathbb{Z}$ ), and this model does not satisfy  $\varphi$ . Thus  $\varphi$  cannot be proven by  $T$  either. So  $T \not\models \varphi$ ,  $\neg\varphi$  and so  $T$  is incomplete.

Let us define  $T'$  by taking the axioms of  $T$  and adding the axioms for every  $n \in \mathbb{N}$ :

$$\varphi_n: \quad \exists x_1, \dots, x_n \left( \bigwedge_{i \neq j=1}^n x_i \neq x_j \right)$$

the axiom that there exists at least  $n$  distinct elements. So  $T'$  is the theory of infinite abelian groups where every element has order 2.

Any infinite model of  $T$  is a model of  $T'$  since it obviously satisfies the new axioms, and any (infinite) model of  $T'$  models  $T$  since  $T \subset T'$ . Thus  $T'$  and  $T$  have the same infinite models.

Furthermore, any two models of infinite cardinality  $\kappa$  of  $T'$  are still models of  $T$  and are thus isomorphic, and so  $T'$  is also  $\kappa$ -categorical for every infinite cardinality  $\kappa$ . And  $T'$  does not have any finite models, since for any interpretation  $\mathcal{M}$ , take  $n > |\mathcal{M}|$ , and then  $\mathcal{M} \not\models \varphi_n$  and so  $\mathcal{M}$  does not satisfy  $T'$ . Thus by Vaught's test,  $T'$  is complete as required.

#### Exercise 4.11:

Let  $\mathcal{L}_3 = \{<, c_0, c_1, c_2, \dots\}$  where  $c_i$  are constant symbols. Let  $T_3$  be the theory of dense linear orders without endpoints along with sentences asserting  $c_0 < c_1 < c_2 < \dots$ . Show that  $T_3$  has exactly three countable models up to isomorphism.

Since  $DLO$  is  $\aleph_0$ -categorical, all countable models of  $DLO$  are isomorphic to  $(\mathbb{Q}, <)$ . Since  $T_3$  is an extension of  $DLO$

it is sufficient to prove this fact while only focusing on models which extend  $(\mathbb{Q}, <)$ .

Note that  $\{c_i\}$  as an increasing sequence of rational numbers has a limit in the extended reals. Meaning that there are precisely three options for a model of  $T_3$ : that  $\lim c_n = \infty$ ,  $\lim c_n \in \mathbb{Q}$ ,  $\lim c_n \in \mathbb{R} \setminus \mathbb{Q}$ .

We will show that for every one of these options, for any two models of  $T_3$  in this category are isomorphic. Then we will show that two models which satisfy different options are not isomorphic.

(1) Let  $\mathcal{M}$  and  $\mathcal{N}$  be two models such that

$$\lim_{n \rightarrow \infty} c_n^{\mathcal{M}} = \lim_{n \rightarrow \infty} c_n^{\mathcal{N}} = \infty$$

then let us define for  $X = \mathcal{M}, \mathcal{N}$  subsets of  $\mathbb{Q}$

$$I_n^X = (c_n^X, c_{n+1}^X]$$

for  $n \geq 0$  and

$$I_{-1}^X = (-\infty, c_0^X]$$

For every  $n \geq 0$  let us define  $f_n: I_n^{\mathcal{M}} \rightarrow I_n^{\mathcal{N}}$  as the unique linear function mapping  $c_n^{\mathcal{M}}$  to  $c_n^{\mathcal{N}}$  and  $c_{n+1}^{\mathcal{M}}$  to  $c_{n+1}^{\mathcal{N}}$ . Such a function is obviously a bijection, since any linear function between two points (which do not share coefficients) is a bijection. This function is also strictly increasing since  $c_n^{\mathcal{M}} < c_{n+1}^{\mathcal{M}}$  and their images also preserve this order  $f_n(c_n^{\mathcal{M}}) = c_n^{\mathcal{N}} < c_{n+1}^{\mathcal{N}} = f_n(c_{n+1}^{\mathcal{M}})$ , and so this is an increasing linear map (all linear functions between two points is either constant, increasing, or decreasing. This is not decreasing or constant, and is thus increasing).

We also define  $f_{-1}: I_{-1}^{\mathcal{M}} \rightarrow I_{-1}^{\mathcal{N}}$  as an increasing linear function which maps  $c_0^{\mathcal{M}}$  to  $c_0^{\mathcal{N}}$ , this could even be the same linear function used to define  $f_0$ .

Since the  $I_n^X$ s partition  $\mathbb{Q}$ , we can define Then we will define an isomorphism  $f: \mathcal{M} \rightarrow \mathcal{N}$  by  $f(x) = f_n(x)$  if  $x \in I_n^{\mathcal{M}}$ . Since the  $I_n^{\mathcal{M}}$ s partition  $\mathbb{Q}$  each  $x$  can only be in one  $I_n^{\mathcal{M}}$  so this is well-defined. Since each  $f_n$  is injective and their codomains are disjoint,  $f$  is also injective. Since for every  $y \in \mathbb{Q}$  there exists an  $n$  such that  $y \in I_n^{\mathcal{N}}$ , and  $f_n$  is surjective, there exists an  $x$  such that  $f_n(x) = y$  and so  $f(x) = y$ , meaning  $f$  is also surjective and thus a bijection.

Since each  $f_n$  is increasing, and  $I_n^X < I_{n+1}^X$ ,  $f$  is increasing. And by definition  $f(c_n^{\mathcal{M}}) = f_{n+1}(c_n^{\mathcal{M}}) = c_n^{\mathcal{N}}$ , so  $f$  preserves constants and relations, and is thus an isomorphism as required.

(2) We prove this much the same as before. But if

$$\lim_{n \rightarrow \infty} c_n^X = p^X \in \mathbb{Q}$$

Then the  $I_n^X$ s defined above do not partition all of  $\mathbb{Q}$ , as they are disjoint from  $[p^X, \infty)$  since every  $c_n^X < p^X$ . So we also define

$$I_{\infty}^X = [p^X, \infty)$$

And so in addition to the  $f_n$ s as above, we define  $f_{\infty}: I_{\infty}^{\mathcal{M}} \rightarrow I_{\infty}^{\mathcal{N}}$  as a linear function which maps  $p^{\mathcal{M}}$  to  $p^{\mathcal{N}}$ .

Now we define  $f$  much the same as before, but for every  $x \in \mathbb{Q}$  we must also consider  $f_n$  for  $n = \infty$  (ie. for every  $x \in \mathbb{Q}$  there exists a unique  $n \in \mathbb{N} \cup \{-1, \infty\}$  where  $x \in I_n^{\mathcal{M}}$ , take  $f(x) = f_n(x)$ ). The rest of the proof holds, and  $f$  is still an isomorphism.

(3) Here,  $p^X \notin \mathbb{Q}$  so we define

$$I_{\infty}^X = (p^X, \infty)$$

And define  $f$  the same as before, and we still have an isomorphism.

Thus we have shown that there are at most three unique models up to isomorphism. We will show that any two models which satisfy different conditions on the limit of  $c_n$  are not isomorphic. We take three models, all extensions of the model  $(\mathbb{Q}, <)$  but where  $c_n$  is defined differently.

Suppose  $\mathcal{M}_1$  is a model where  $\lim c_n^1 = \infty$  and  $\mathcal{M}_2$  is defined where  $\lim c_n^2 = y \in \mathbb{R}$ , recall that this means  $c_n^2 < y$  for every  $n$ . Suppose that the two models are isomorphic, then suppose  $f$  is an isomorphism from  $\mathcal{M}_1$  to  $\mathcal{M}_2$ . Since  $f$  is a bijection, suppose  $f(x) = y$ . Then since  $f$  preserves order (it is an isomorphism between models with  $<$ ), and  $\lim c_n^1 = \infty$ , take a  $c_n^1 > x$  then  $f(c_n^1) > f(x)$ , meaning  $c_n^2 > y$  which is a contradiction. Thus a model where  $c_n \rightarrow \infty$  cannot be isomorphic to any model where  $c_n$  converges finitely.



Now suppose  $\mathcal{M}_1$  is a model where  $\lim c_n^1 = x \notin \mathbb{Q}$  and  $\mathcal{M}_2$  a model where  $\lim c_n^2 = p \in \mathbb{Q}$ . Then suppose that the two models are isomorphic, then let  $f$  be an isomorphism from  $\mathcal{M}_1$  to  $\mathcal{M}_2$ . Suppose  $f(a) = p$ . If  $a \leq c_n^1$  for some  $n$  then  $f(a) \leq f(c_n^1) = c_n^2 < p$  in contradiction, so  $a > c_n^1$  for every  $n$ . This means that  $a > x$  and so there exists a rational  $q$  such that  $x < q < a$  and so  $c_n^1 < q$  for every  $n$  and thus  $c_n^2 = f(c_n^1) < f(q)$  and so taking the supremum  $p \leq f(q)$ , meaning  $f(a) \leq f(q)$ . But  $q < a$  so  $f(q) < f(a)$  in contradiction. Thus a model where  $c_n$  converges rationally cannot be isomorphic to a model where  $c_n$  converges irrationally.

So these are the three isomorphism classes of countable models of  $T_3$ , and for each class there exists such a model (for  $\lim = \infty$  take  $c_n = n$ , for  $\lim \in \mathbb{Q}$  take  $c_n = 1 - \frac{1}{n}$ , and for  $\lim \notin \mathbb{Q}$  take a sequence  $c_n \nearrow \sqrt{2}$  which exists since  $\mathbb{Q}$  is dense in  $\mathbb{R}$ ).

#### Exercise 4.12:

Let  $\mathcal{L} = \{\sim\}$  where  $\sim$  is a binary relation symbol. For each of the following theories, prove or disprove that they have quantifier elimination. The following theories are extensions of the theory of an equivalence relation.

- (1)  $\sim$  has infinitely many classes of size 2.
- (2)  $\sim$  has infinitely many classes, all of which are infinite.
- (3)  $\sim$  has infinitely many classes of size 2, infinitely many classes of size 3, and every class has size either 2 or 3.
- (4)  $\sim$  has one class of size  $n$  for every  $n < \omega$ .

- (1) We will show that this theory does have quantifier elimination through formula induction. For prime formulas, this is trivial as they have no quantifiers by definition. For formulas which are boolean combinations of other formulas, we can simply induct on their subformulas. Thus all we care about are formulas of the form  $\varphi = \exists x \psi$ . Inductively, we can assume that  $\psi$  has no quantifiers, as our inductive hypothesis assures that it is equivalent to a quantifier-free formula. Since  $\psi$  has a normal form of the form

$$\psi \leftrightarrow \bigvee_{i=1}^n \bigwedge_{j=1}^m \psi_{i,j}$$

Where  $\psi_{i,j}$  are literals (atomic formulas or their negations)

$$\exists x \psi \leftrightarrow \bigvee_{i=1}^n \exists x \bigwedge_{j=1}^m \psi_{i,j}$$

it is sufficient to show that formulas of the form

$$\exists x \psi, \quad \psi = \bigwedge_{i=1}^n \psi_i$$

has quantifier elimination. This is true in general.

We know  $\psi$  has the form

$$\psi = \bigwedge_{i \in I} x = x_i \wedge \bigwedge_{j \in J} x \neq x_j \wedge \bigwedge_{h \in H} x \sim x_h \wedge \bigwedge_{k \in K} x \not\sim x_k \wedge \bar{\psi}$$

where  $\bar{\psi}$ 's variables do not include  $x$ . Thus  $\exists x \psi$  is equivalent to  $(\exists x \hat{\psi}) \wedge \bar{\psi}$  where  $\hat{\psi}$  is the first part of the formula above. Thus we can ignore  $\bar{\psi}$ . We can ignore  $I$  since if  $x = x_i$  then we can replace every instance of  $x$  in  $\psi$  with  $x_i$  and thus remove the quantifier in  $\varphi$  since  $\psi$  would no longer have  $x$  as a variable. If  $H \cap K$  is non-empty then this formula is logically invalid, and thus equivalent to a formula of the form  $x_1 \neq x_1$ . Thus we assume  $\psi$  has the form

$$\psi = \bigwedge_{i \in I} x \sim x_i \wedge \bigwedge_{j \in J} x \not\sim x_j \wedge \bigwedge_{h \in H} x \neq x_h$$

So we know for every  $i, i' \in I$ ,  $x_i \sim x_{i'}$ , and for  $i \in I$  and  $j \in J$   $x_i \not\sim x_j$ . Since every equivalence class has size 2, for every  $h, h' \in H \cap I$ ,  $x_h = x_{h'}$ . Thus we can look at the formula

$$\bigwedge_{i, i' \in I} x_i \sim x_{i'} \wedge \bigwedge_{i \in I, j \in J} x_i \not\sim x_j \wedge \bigwedge_{h, h' \in H \cap I} x_h = x_{h'}$$

Now the issue is is that while  $\varphi$  implies this, it does not imply  $\varphi$ . The issue is we can take an  $x$  where  $x \sim x_i$  and  $x \not\sim x_h$  for  $h \in H \cap I$  but we cannot assure that this holds for all  $h \in H$ . Essentially the issue is is that there may be some  $x_h$  where  $h \in H \setminus I$ ,  $x_h \sim x_i$ , and is distinct from other  $x_h$ s, as this formula does not restrict  $h$  for  $h \notin I$ . Thus we'd like to say "for every two  $h, h' \in H$  where  $x_h \sim x_i$  then  $x_h = x_{h'}$ ", this is a stronger statement than what is in the formula right now. We write this as

$$\bigwedge_{h, h' \in H, i \in I} (x_h \sim x_i \wedge x_{h'} \sim x_i) \rightarrow x_h = x_{h'}$$

So we claim that  $\varphi$  is equivalent to the quantifier-free formula

$$\varphi' = \bigwedge_{i, i' \in I} x_i \sim x_{i'} \wedge \bigwedge_{i \in I, j \in J} x_i \not\sim x_j \wedge \bigwedge_{h, h' \in H, i \in I} (x_h \sim x_i \wedge x_{h'} \sim x_i) \rightarrow x_h = x_{h'}$$

Obviously still  $\varphi \rightarrow \varphi'$ . And if  $\varphi'$  is true, then we can take an  $x$  such that  $x \sim x_i$  and for every  $h \in H$ ,  $x \not\sim x_h$  since there is only one value of  $x_h$  where  $x_h \sim x \sim x_i$ , and so we can simply take the other value in the equivalence class. And still  $x \not\sim x_j$ . Thus  $\varphi \leftrightarrow \varphi'$  as required.

- (2) Here again we assume

$$\psi = \bigwedge_{i \in I} x \sim x_i \wedge \bigwedge_{j \in J} x \not\sim x_j \wedge \bigwedge_{h \in H} x \neq x_h$$

And now we define

$$\varphi' = \bigwedge_{i, i' \in I} x_i \sim x_{i'} \wedge \bigwedge_{i \in I, j \in J} x_i \not\sim x_j$$

Again, obviously  $\varphi \rightarrow \varphi'$ . And if  $\varphi'$  is true, then since the equivalence classes are infinite, there exists an  $x \sim x_i$  for every  $i \in I$  which is not equal to any  $x_h$ , since there is a finite number of  $x_h$ s. And since  $x \sim x_i \not\sim x_j$ , we have  $x \not\sim x_j$  for every  $j \in J$  as required. And thus  $\varphi \leftrightarrow \varphi'$  and we have finished.

- (3) Notice that in this theory, for any model  $\mathcal{M}$  let  $a, b \in \mathcal{M}$  then  $\{a\}$  and  $\{b\}$  are isomorphic substructures of  $\mathcal{M}$  (they are substructures since there is no function or constant symbols). Thus if  $\varphi$  is quantifier-free with at most one free variable, then  $\mathcal{M} \models \varphi(a)$  if and only if  $\mathcal{M} \models \varphi(b)$ . This is because  $\varphi$  has no quantifiers, so we are only substituting the single value with  $a$ , meaning  $\mathcal{M} \models \varphi(a)$  if and only if  $\{a\} \models \varphi(a)$  if and only if  $\{b\} \models \varphi(b)$  (as isomorphic structures), if and only if  $\mathcal{M} \models \varphi(b)$ .

Let us define

$$\psi(x) = \exists x_1, x_2 (x_1 \neq x_2 \wedge x \neq x_1 \wedge x \neq x_2 \wedge x \sim x_1 \wedge x \sim x_2)$$

the predicate that  $x$  is in an equivalence class of size 3. Then we take the equivalence relation on  $\mathbb{N}$  defined by the partition  $\{0, 1\}, \{2, 3, 4\}, \{5, 6\}, \dots$ . Thus  $\psi(3)$  is true, but  $\psi(1)$  is not.

So if  $\psi$  had a quantifier-free equivalent  $\varphi$ , then since  $\varphi$  is quantifier-free  $\varphi(3) \leftrightarrow \varphi(1)$ , meaning  $\psi(3) \leftrightarrow \psi(1)$ , in contradiction. Thus  $\psi$  has no quantifier-free equivalent, and thus the theory is not allow quantifier elimination.

- (4) We will use the same result that we used as above. Thus let us look at the equivalence relation which defines the partition over  $\mathbb{N}$  of  $\{0\}, \{1, 2\}, \{3, 4, 5\}, \dots$ . Let us also use the formula  $\psi$  used above, in this case it means that  $x$  is in an equivalence class of at least size 3. Thus  $\psi(3)$  is true but  $\psi(1)$  is not again, which results in the same contradiction.

#### Exercise 4.13:

- (1) Show that the theory of  $(\mathbb{Z}, s)$  where  $s$  is the successor function has quantifier elimination.
- (2) Show that the theory of  $(\mathbb{N}, s)$  does not have quantifier elimination.

- (1) As above, it is sufficient to show that formulas of the form

$$\varphi = \exists x (L_1 \wedge \dots \wedge L_n)$$

where  $L_i$  are literals (atomic formulas or their negation) containing  $x$ . We will show that every conjunction of literals can be written equivalently without using  $x$ . Without loss of generality, we assume that every  $L_i$  is of one

of the following forms

$$S^m(x) = S^n(x), \quad S^m(x) \neq S^n(x), \quad S^m(x) = S^n(x_i), \quad S^m(x) \neq S^n(x_i)$$

Note that formulas of the form  $S^m(x) = S^n(x)$  are either logically valid or false, depending on whether  $m = n$ , thus  $L_i$ s of this form can be replaced with  $\top$  or  $\perp$ .

Suppose there exists a formula of the form  $S^m(x) = S^n(x_i)$  where  $x_i$  is some variable. If  $m \leq n$  then this is equivalent to  $x = S^{n-m}(x_i)$  and thus we can replace  $x$  in every  $L_i$  with  $S^{n-m}(x_i)$  and we have an equivalent conjunction without the use of  $x$ , and we have finished.

If every formula of the form  $S^m(x) = S^n(x_i)$  has  $m > n$  then suppose  $L_i$  is of the form  $S^m(x) = S^n(x_i)$ . Notice that for every formula  $L_j$  of the form  $S^k(x) = S^t(x_j)$ , where  $L_j$  is not  $L_i$ ,  $L_j$  is equivalent to  $S^{k+m}(x) = S^k(S^m(x)) = S^{t+m}(x_j)$  since  $S$  is a bijection over  $\mathbb{Z}$  (since it is not a bijection over  $\mathbb{N}$ , this proof will not work for  $(\mathbb{N}, s)$ ), and so we replace  $L_j$  with  $S^k(S^n(x_i)) = S^{k+n}(x_i) = S^{t+m}(x_j)$ . And if  $L_j$  is of the form  $S^k(x) \neq S^t(x_j)$ , then we replace it with  $S^{k+n}(x_i) \neq S^{t+m}(x_j)$ . Thus we can replace every literal with another literal which doesn't have  $x$  as a variable, and thus we can remove the quantifier.

Otherwise every formula is of the form  $S^m(x) \neq S^n(x_i)$ , but then  $\varphi$  is logically valid or false. If there exists an  $L_i = \perp$  then since  $\varphi$  is a conjunction of  $L_i$ s,  $\varphi$  is false. If there is no such  $L_i$ , then notice that every  $L_i$  is of the form  $S^m(x) \neq S^n(x_i)$  or  $\top$ . Let  $A = \{x_i + n - m \mid \text{There exists a literal of the form } S^m(x) \neq S^n(x_i)\}$ , then  $A$  is finite and thus there exists an  $x \notin A$ . Such an  $x$  satisfies  $x \neq x_i + n - m$  meaning  $S^m(x) \neq S^n(x_i)$  for every  $i$  and so  $\varphi$  is logically valid.

Thus we have that either  $\varphi$  is logically valid or false, or for every  $i$  there exists a literal  $L'_i$  without  $x$  such that  $L_i \leftrightarrow L'_i$  and so

$$\varphi \leftrightarrow \exists x(L'_1 \wedge \dots \wedge L'_n) \leftrightarrow L'_1 \wedge \dots \wedge L'_n$$

as required.

- (2) Notice that every literal with one variable is either true or false, since it is of the form  $S^m(x) = S^n(x)$  or its negation, which is true or false depending on whether  $n = m$ . Thus since a quantifier-free formula is the boolean combination of literals, every quantifier-free formula is either logically valid or false. But let us define

$$\varphi(x) = \exists y(S(y) = x)$$

the predicate that  $x \neq 0$ . This is not logically valid or false since it is true for  $\varphi(0)$  but false for any other  $x \neq 0$ , and thus cannot have a quantifier-free equivalent.