

Chapter udf

Second-order Logic and Set Theory

This section deals with coding powersets and the continuum in second-order logic. The results are stated but proofs have yet to be filled in. There are no problems yet—and the definitions and results themselves may have problems. Use with caution and report anything that’s false or unclear.

set.1 Introduction

sol:set:int:
sec Since second-order logic can quantify over subsets of the domain as well as functions, it is to be expected that some amount, at least, of set theory can be carried out in second-order logic. By “carry out,” we mean that it is possible to express set theoretic properties and statements in second-order logic, and is possible without any special, non-logical vocabulary for sets (e.g., the membership **predicate symbol** of set theory). For instance, we can define unions and intersections of sets and the subset relationship, but also compare the sizes of sets, and state results such as Cantor’s Theorem.

set.2 Comparing Sets

sol:set:cmp:
sec **Proposition set.1.** *The formula $\forall x (X(x) \rightarrow Y(x))$ defines the subset relation, i.e., $\mathfrak{M}, s \models \forall x (X(x) \rightarrow Y(x))$ iff $s(X) \subseteq s(Y)$.*

Proposition set.2. *The formula $\forall x (X(x) \leftrightarrow Y(x))$ defines the identity relation on sets, i.e., $\mathfrak{M}, s \models \forall x (X(x) \leftrightarrow Y(x))$ iff $s(X) = s(Y)$.*

Proposition set.3. *The formula $\exists x X(x)$ defines the property of being non-empty, i.e., $\mathfrak{M}, s \models \exists x X(x)$ iff $s(X) \neq \emptyset$.*

A set X is no larger than a set Y , $X \preceq Y$, iff there is an **injective** function $f: X \rightarrow Y$. Since we can express that a function is injective, and also that its values for arguments in X are in Y , we can also define the relation of being no larger than on subsets of the domain.

Proposition set.4. *The formula*

$$\exists u (\forall x (X(x) \rightarrow Y(u(x))) \wedge \forall x \forall y (u(x) = u(y) \rightarrow x = y))$$

defines the relation of being no larger than.

Two sets are the same size, or “equinumerous,” $X \approx Y$, iff there is a **bijective** function $f: X \rightarrow Y$.

Proposition set.5. *The formula*

$$\begin{aligned} \exists u (\forall x (X(x) \rightarrow Y(u(x))) \wedge \\ \forall x \forall y (u(x) = u(y) \rightarrow x = y) \wedge \\ \forall y (Y(y) \rightarrow \exists x (X(x) \wedge y = u(x)))) \end{aligned}$$

defines the relation of being equinumerous with.

We will abbreviate these **formulas**, respectively, as $X \subseteq Y$, $X = Y$, $X \neq \emptyset$, $X \preceq Y$, and $X \approx Y$. (This may be slightly confusing, since we use the same notation when we speak informally about sets X and Y —but here the notation is an abbreviation for **formulas** in second-order logic involving one-place relation variables X and Y .)

Proposition set.6. *The **sentence** $\forall X \forall Y ((X \preceq Y \wedge Y \preceq X) \rightarrow X \approx Y)$ is valid.*

Proof. The **sentence** is satisfied in a **structure** \mathfrak{M} if, for any subsets $X \subseteq |\mathfrak{M}|$ and $Y \subseteq |\mathfrak{M}|$, if $X \preceq Y$ and $Y \preceq X$ then $X \approx Y$. But this holds for *any* sets X and Y —it is the Schröder-Bernstein Theorem. \square

set.3 Cardinalities of Sets

explanation Just as we can express that the domain is finite or infinite, **enumerable** or **non-enumerable**, we can define the property of a subset of $|\mathfrak{M}|$ being finite or infinite, **enumerable** or **non-enumerable**. **sol:set:crd:sec**

Proposition set.7. *The formula $\text{Inf}(X) \equiv$*

$$\begin{aligned} \exists u (\forall x \forall y (u(x) = u(y) \rightarrow x = y) \wedge \\ \exists y (X(y) \wedge \forall x (X(x) \rightarrow y \neq u(x)))) \end{aligned}$$

is satisfied with respect to a variable assignment s iff $s(X)$ is infinite.

Proposition set.8. *The formula $\text{Count}(X) \equiv$*

$$\exists z \exists u (X(z) \wedge \forall x (X(x) \rightarrow X(u(x))) \wedge \forall Y ((Y(z) \wedge \forall x (Y(x) \rightarrow Y(u(x)))) \rightarrow X = Y))$$

*is satisfied with respect to a variable assignment s iff $s(X)$ is **enumerable**.*

We know from Cantor’s Theorem that there are **non-enumerable** sets, and in fact, that there are infinitely many different levels of infinite sizes. Set theory develops an entire arithmetic of sizes of sets, and assigns infinite cardinal numbers to sets. The natural numbers serve as the cardinal numbers measuring the sizes of finite sets. The cardinality of **denumerable** sets is the first infinite cardinality, called \aleph_0 (“aleph-nought” or “aleph-zero”). The next infinite size is \aleph_1 . It is the smallest size a set can be without being countable (i.e., of size \aleph_0). We can define “ X has size \aleph_0 ” as $\text{Aleph}_0(X) \leftrightarrow \text{Inf}(X) \wedge \text{Count}(X)$. X has size \aleph_1 iff all its subsets are finite or have size \aleph_0 , but is not itself of size \aleph_0 . Hence we can express this by the formula $\text{Aleph}_1(X) \equiv \forall Y (Y \subseteq X \rightarrow (\neg \text{Inf}(Y) \vee \text{Aleph}_0(Y))) \wedge \neg \text{Aleph}_0(X)$. Being of size \aleph_2 is defined similarly, etc.

There is one size of special interest, the so-called cardinality of the continuum. It is the size of $\wp(\mathbb{N})$, or, equivalently, the size of \mathbb{R} . That a set is the size of the continuum can also be expressed in second-order logic, but requires a bit more work.

set.4 The Power of the Continuum

sol:set:pow:
sec

In second-order logic we can quantify over subsets of the **domain**, but not over sets of subsets of the **domain**. To do this directly, we would need *third-order* logic. For instance, if we wanted to state Cantor’s Theorem that there is no **injective** function from the power set of a set to the set itself, we might try to formulate it as “for every set X , and every set P , if P is the power set of X , then not $P \preceq X$ ”. And to say that P is the power set of X would require formalizing that the **elements** of P are all and only the subsets of X , so something like $\forall Y (P(Y) \leftrightarrow Y \subseteq X)$. The problem lies in $P(Y)$: that is not **a formula** of second-order logic, since only terms can be arguments to one-place relation variables like P .

explanation

We can, however, *simulate* quantification over sets of sets, if the domain is large enough. The idea is to make use of the fact that two-place relations R relates **elements** of the **domain** to **elements** of the **domain**. Given such an R , we can collect all the **elements** to which some x is R -related: $\{y \in |\mathfrak{M}| : R(x, y)\}$ is the set “coded by” x . Conversely, if $Z \subseteq \wp(|\mathfrak{M}|)$ is some collection of subsets of $|\mathfrak{M}|$, and there are at least as many **elements** of $|\mathfrak{M}|$ as there are sets in Z , then there is also a relation $R \subseteq |\mathfrak{M}|^2$ such that every $Y \in Z$ is coded by some x using R .

Definition set.9. If $R \subseteq |\mathfrak{M}|^2$, then x *R-codes* $\{y \in |\mathfrak{M}| : R(x, y)\}$.

If an element $x \in |\mathfrak{M}|$ R -codes a set $Z \subseteq |\mathfrak{M}|$, then a set $Y \subseteq |\mathfrak{M}|$ codes a set of sets, namely the sets coded by the elements of Y . So a set Y can R -code $\wp(X)$. It does so iff for every $Z \subseteq X$, some $x \in Y$ R -codes Z , and every $x \in Y$ R -codes a $Z \subseteq X$.

Proposition set.10. *The formula*

$$\text{Codes}(x, R, Z) \equiv \forall y (Z(y) \leftrightarrow R(x, y))$$

expresses that $s(x)$ $s(R)$ -codes $s(Z)$. *The formula*

$$\begin{aligned} \text{Pow}(Y, R, X) \equiv \\ \forall Z (Z \subseteq X \rightarrow \exists x (Y(x) \wedge \text{Codes}(x, R, Z))) \wedge \\ \forall x (Y(x) \rightarrow \forall Z (\text{Codes}(x, R, Z) \rightarrow Z \subseteq X)) \end{aligned}$$

expresses that $s(Y)$ $s(R)$ -codes the power set of $s(X)$, i.e., the elements of $s(Y)$ $s(R)$ -code exactly the subsets of $s(X)$.

explanation

With this trick, we can express statements about the power set by quantifying over the codes of subsets rather than the subsets themselves. For instance, Cantor's Theorem can now be expressed by saying that there is no injective function from the domain of any relation that codes the power set of X to X itself.

Proposition set.11. *The sentence*

$$\begin{aligned} \forall X \forall Y \forall R (\text{Pow}(Y, R, X) \rightarrow \\ \neg \exists u (\forall x \forall y (u(x) = u(y) \rightarrow x = y) \wedge \\ \forall x (Y(x) \rightarrow X(u(x)))))) \end{aligned}$$

is valid.

explanation

The power set of a denumerable set is non-enumerable, and so its cardinality is larger than that of any denumerable set (which is \aleph_0). The size of $\wp(\mathbb{N})$ is called the "power of the continuum," since it is the same size as the points on the real number line, \mathbb{R} . If the domain is large enough to code the power set of a denumerable set, we can express that a set is the size of the continuum by saying that it is equinumerous with any set Y that codes the power set of set X of size \aleph_0 . (If the domain is not large enough, i.e., it contains no subset equinumerous with \mathbb{R} , then there can also be no relation that codes $\wp(X)$.)

Proposition set.12. *If $\mathbb{R} \preceq |\mathfrak{M}|$, then the formula*

$$\begin{aligned} \text{Cont}(Y) \equiv \exists X \exists R ((\text{Aleph}_0(X) \wedge \text{Pow}(Y, R, X)) \wedge \\ \forall x \forall y ((Y(x) \wedge Y(y) \wedge \forall z R(x, z) \leftrightarrow R(y, z)) \rightarrow x = y)) \end{aligned}$$

expresses that $s(Y) \approx \mathbb{R}$.

Proof. $\text{Pow}(Y, R, X)$ expresses that $s(Y)$ $s(R)$ -codes the power set of $s(X)$, which $\text{Aleph}_0(X)$ says is countable. So $s(Y)$ is at least as large as the power of the continuum, although it may be larger (if multiple elements of $s(Y)$ code the same subset of X). This is ruled out by the last conjunct, which requires the association between elements of $s(Y)$ and subsets of $s(Z)$ via $s(R)$ to be **injective**. \square

Proposition set.13. $|\mathfrak{M}| \approx \mathbb{R}$ iff

$$\mathfrak{M} \models \exists X \exists Y \exists R (\text{Aleph}_0(X) \wedge \text{Pow}(Y, R, X) \wedge \\ \exists u (\forall x \forall y (u(x) = u(y) \rightarrow x = y) \wedge \\ \forall y (Y(y) \rightarrow \exists x y = u(x)))).$$

The Continuum Hypothesis is the statement that the size of the continuum [explanation](#) is the first **non-enumerable** cardinality, i.e., that $\wp(\mathbb{N})$ has size \aleph_1 .

Proposition set.14. *The Continuum Hypothesis is true iff*

$$\text{CH} \equiv \forall X (\text{Aleph}_1(X) \leftrightarrow \text{Cont}(X))$$

is valid.

Note that it isn't true that $\neg\text{CH}$ is valid iff the Continuum Hypothesis is false. In **an enumerable** domain, there are no subsets of size \aleph_1 and also no subsets of the size of the continuum, so CH is always true in **an enumerable** domain. However, we can give a different sentence that is valid iff the Continuum Hypothesis is false:

Proposition set.15. *The Continuum Hypothesis is false iff*

$$\text{NCH} \equiv \forall X (\text{Cont}(X) \rightarrow \exists Y (Y \subseteq X \wedge \neg\text{Count}(Y) \wedge \neg X \approx Y))$$

is valid.

Photo Credits

Bibliography