Logik MN2
November-December 2004

Contents

Chapter 0

Prerequisites

- Intuitive set theory
- Propositional logic
- Predicate logic
  - Mathematical structure

$$\mathfrak{A} = (\underbrace{A}_{\text{universe}}; \underbrace{R_1, \ldots, R_m}_{\text{relations on } A}; \underbrace{F_1, \ldots, F_n}_{\text{operations on } A}; \underbrace{c_1, \ldots, c_k}_{\text{elements in } A})$$

    Example: $\mathfrak{N} = (\mathbb{N}; <; +, \cdot; 0, 1)$ where $\mathbb{N} = \{0, 1, 2, \ldots\}$.
  - Formal language (syntax)
    - Variables
    - Names for all relations, functions and constants of the structure (signature)
    - Well-formed formulas (using $\vee, \wedge, \neg, \Rightarrow, \forall x, \exists x$)
    - $\mathfrak{A} \models \varphi$ ($\mathfrak{A}$ structure, φ well-formed formula), φ is true in $\mathfrak{A}$ (Tarsky)
  - Proof: $T \vdash \varphi$ (T theory (set of formulas), φ formula), φ is provable in T.
  - Gödel's completeness theorem: $T \vdash \varphi \iff (\forall \mathfrak{A})(\mathfrak{A} \models T \Rightarrow \mathfrak{A} \models \varphi)$. In particular, $\vdash \varphi \iff \underbrace{(\forall \mathfrak{A})(\mathfrak{A} \models \varphi)}_{\models \varphi}$.
- Induction
  - Inductive definition
  - Proof by induction
  - Define functions recursively on inductive definitions

Example: Inductive definition of $\mathbb{N} = \{0, 1, 2, \ldots\}$.

(i) $0 \in \mathbb{N}$ (base)

(ii) If $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$ (induction step)

(iii) (No other objects is in $\mathbb{N}$ if it is not obtained from above)

Example: Inductive definition of $\mathbb{Q}[x]$, polynomials over $\mathbb{Q}$.

$$\text{(i)} \begin{cases} a \in \mathbb{Q}[x] \text{ if } a \in \mathbb{Q} \\ x \in \mathbb{Q}[x] \end{cases} \quad \text{(base)}$$

$$\text{(ii)} \begin{cases} \text{If } p(x), q(x) \in \mathbb{Q}[x], \text{ then } p(x) + q(x) \in \mathbb{Q}[x] \\ \text{If } p(x), q(x) \in \mathbb{Q}[x], \text{ then } p(x) \cdot q(x) \in \mathbb{Q}[x] \end{cases} \quad \text{(induction step)}$$

Example: We want to prove $A(x)$, where x varies over $\mathbb{N}$.

- Prove $A(0)$
- Prove $A(n) \Rightarrow A(n+1)$ for each n
- Conclusion: $\forall n A(n)$

Induction: $(A(0) \wedge \forall n(A(n) \Rightarrow A(n+1))) \Rightarrow \forall n A(n)$

Proof. Suppose $\neg \forall n A(n)$. Then $\exists n. \neg A(n)$. Let n_0 be least such that $\neg A(n_0)$. But $A(0)$ is true so n_0. Then $n_0 = n_1 + 1$. But $A(n_1)$ is true since n_0 was least. But we have proved $A(n_1) \Rightarrow A(n_1 + 1)$. Thus $A(n_0)$ is true. Contradiction. □

Let $S : \mathbb{N} \to \mathbb{N}$ be defined by $S(n) = n + 1$. S is called the successor function.

Example: Recursive definition of $x + y$ over the inductive definition of $\mathbb{N}$.

$$\begin{cases} x + 0 = x \\ x + (y + 1) = (x + y) + 1 = S(x + y) \end{cases}$$

Example: Recursive definition of $x \cdot y$ over the inductive definition of $\mathbb{N}$.

$$\begin{cases} x \cdot 0 = 0 \\ x \cdot (y + 1) = x \cdot y + x \end{cases}$$

Chapter 1

Recursion theory

Recursion theory (computability theory) is the theory of algorithmically computable functions. 1936 a simple inductive definition of the algorithmically computable functions were found.

A concrete object is an object which has a concrete representation.

Thesis 1.0.1. *Any set of concrete objects can be represented by the set of natural numbers.*

Thus we do computability on $\mathbb{N}$.

Notation 1.0.2.

$$\begin{array}{l}\mathbb{N} = \{0, 1, 2, \ldots\} \\ \mathbb{N}^k = \{(n_1, \ldots, n_k) : n_i \in \mathbb{N}\}, \qquad k = 0, 1, 2, \ldots \\ \mathbb{N}^0 = \{()\}, \text{ contains one element}\end{array}$$

1.1 Primitive recursion

Definition 1.1.1. The class PRIM is defined inductively by

(i) Each constant function $f : \mathbb{N}^k \to \mathbb{N}$ is in PRIM.

(ii) The function $P_k^i : \mathbb{N}^k \to \mathbb{N}$ defined by $P_k^i(x_1, \ldots, x_k) = x_i, \ k \geq 1, \ 1 \leq i \leq k$ (projection function) are in PRIM.

(iii) $S : \mathbb{N} \to \mathbb{N}$ defined by $S(n) = n + 1$ (successor function) is in PRIM.

(iv) If $g : \mathbb{N}^n \to \mathbb{N}$ and $h_i : \mathbb{N}^k \to \mathbb{N}$ for $i = 1, \ldots, n$ are in PRIM, then $f : \mathbb{N}^k \to \mathbb{N}$ defined by $f(x_1, \ldots, x_k) = g(h_1(x_1, \ldots, x_k), \ldots, h_n(x_1, \ldots, x_k))$ is in PRIM.

(v) If $g : \mathbb{N}^n \to \mathbb{N}$ and $h : \mathbb{N}^{n+2} \to \mathbb{N}$ are in PRIM, then $f : \mathbb{N}^{n+1} \to \mathbb{N}$ defined by $f(\vec{x}, 0) = g(\vec{x})$ if $y = 0$ and $f(\vec{x}, y) = h(\vec{x}, y - 1, f(\vec{x}, y - 1))$ if $y > 0$ is in PRIM.

Remark 1.1.2. Clause (v) in the above definition is often written as follows:

$$\begin{cases} f(\vec{x}, 0) = g(\vec{x}) \\ f(\vec{x}, y + 1) = h(\vec{x}, y, f(\vec{x}, y)) \end{cases}$$

Examples 1.1.3. (i) Addition $x + y$:
Define the function $\mathrm{ad}(x, y)$ by

$$\begin{cases} \mathrm{ad}(x,0) = P_1^1(x) \\ \mathrm{ad}(x, y+1) = S(\mathrm{ad}(x,y)) = S(P_3^3(x,y,\mathrm{ad}(x,y))) = h(x,y,\mathrm{ad}(x,y)), \end{cases}$$

where $h(x, y, z) = S(P_3^3(x, y, z))$.

Projection functions are very useful, here is another example: Suppose

$$f(x_1, x_2, x_3) = g(h_1(x_1, x_2), h_2(x_3)),$$

where g, h_1 and h_2 are primitive recursive. Show that f is primitive recursive. To see this we define the following two functions:

$$\begin{array}{l} \bar{h}_1(x_1, x_2, x_3) = h_1(P_3^1(x_1, x_2, x_3), P_3^2(x_1, x_2, x_3)) \\ \bar{h}_2(x_1, x_2, x_3) = h_2(P_3^3(x_1, x_2, x_3)) \end{array}.$$

Then $f(x_1, x_2, x_3) = g(\bar{h}_1(x_1, x_2, x_3), \bar{h}_2(x_1, x_2, x_3))$ is primitive recursive.

Thus: Thanks to the P_k^i we can rearrange variables rather freely.

(ii) Multiplication $x \cdot y$:

$$\begin{cases} x \cdot 0 = 0 \\ x \cdot (y+1) = x \cdot y + x \end{cases}$$

(iii) Exponentiation x^y:

$$\begin{cases} x^0 = 1 \\ x^{(y+1)} = x^y \cdot x \end{cases}$$

(iv) Predecessor $P(x)$:
Define the predecessor by

$$P(x) = \begin{cases} 0 & \text{if } x = 0 \\ x - 1 & \text{if } x > 0 \end{cases}$$

Then $P(x)$ is primitive recursive since

$$\begin{cases} x \cdot 0 = 0 \\ P(x+1) = x = P_2^1(x, P(x)) \end{cases}$$

(v) Subtraction $x \dot{-} y$:
Define the minus function by

$$x \dot{-} y = \begin{cases} x - y & \text{if } x \geq y \\ 0 & \text{if } x < y \end{cases}$$

Then $x \dot{-} y$ is primitive recursive since

$$\begin{cases} x \dot{-} 0 = x \\ x \dot{-} (y+1) = (x \dot{-} y) \dot{-} 1 = P(x \dot{-} y) \end{cases}$$

(vi) The sg-function:
Define sg-function by

$$\mathrm{sg}(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x > 0 \end{cases}$$

So $\mathrm{sg}(x) = 1 \dot{-} (1 \dot{-} x)$ and hence primitive recursive by clause (iv) of definition 1.1.1.

Definition 1.1.4. Let $A \subseteq \mathbb{N}^k$. A is primitive recursive if its characteristic function

$$\chi_A(\vec{x}) = \begin{cases} 1 & \text{if } \vec{x} \in A \\ 0 & \text{if } \vec{x} \notin A \end{cases}$$

is primitive recursive.

Notation 1.1.5. We often write $A(\vec{x})$ for $\vec{x} \in A$.

Examples 1.1.6. (i) The relation $<$ on $\mathbb{N}^2$ is primitive recursive since

$$x < y \iff \mathrm{sg}(y \dot{-} x) = 1,$$

so $\chi_< = \mathrm{sg}(y \dot{-} x)$.

(ii) $\leq$ is primitive recursive.

(iii) The primitive recursive relations are closed under propositional connectives $\wedge, \vee, \neg$

Proof. We have

$$A(\vec{x}) \wedge B(\vec{x}) \iff \chi_A(\vec{x}) \cdot \chi_B(\vec{x}) = 1,$$

so $\chi_{A \wedge B} = \chi_A(\vec{x}) \cdot \chi_B(\vec{x})$.
For $\vee$ we have

$$A(\vec{x}) \vee B(\vec{x}) \iff \mathrm{sg}(\chi_A(\vec{x}) + \chi_B(\vec{x})) = 1,$$

so $\chi_{A \vee B} = \mathrm{sg}(\chi_A(\vec{x}) + \chi_B(\vec{x}))$.
$\chi_{\neg A} = 1 - \chi_A$. □

(iv) Definition by cases:
Suppose $f_1(\vec{x}), \ldots, f_n(\vec{x})$ are primitive recursive and $A_1(\vec{x}), \ldots, A_n(\vec{x})$ are primitive recursive relations such that for each $\vec{x}$ precisely one of the $A_i(\vec{x})$ holds. Then f defined by

$$f(\vec{x}) = \begin{cases} f_1(\vec{x}) & \text{if } A_1(\vec{x}) \\ \vdots & \vdots \\ f_n(\vec{x}) & \text{if } A_n(\vec{x}) \end{cases}$$

is primitive recursive.

Proof. We have that

$$f(\vec{x}) = f_1(\vec{x}) \cdot \chi_{A_1}(\vec{x}) + f_2(\vec{x}) \cdot \chi_{A_2}(\vec{x}) + \ldots + f_n(\vec{x}) \cdot \chi_{A_n}(\vec{x}).$$

Hence, since addition and multiplication is primitive recursive and since f_i and A_i was primitive recursive, f is primitive recursive. □

(v) Bounded μ-operator:
Let $A \subset \mathbb{N}^{k+1}$ be primitive recursive. Then

$$\mu t_{t<z} A(\vec{x}, t) = \begin{cases} \text{Least } t < z \text{ such that } A(\vec{x}, t) \text{if such exists} \\ z \text{ otherwise} \end{cases}$$

is primitive recursive.

Proof. Define a function f by

$$f(\vec{x}, 0) = 0$$
$$f(\vec{x}, z+1) = \begin{cases} f(\vec{x}, z) & \text{if } f(\vec{x}, z) < z \\ z & \text{if } f(\vec{x}, z) = z \text{ and } A(\vec{x}, z) \\ z+1 & \text{otherwise.} \end{cases}$$

Then f is primitive recursive and $f(\vec{x}, z) = \mu t_{t<z} A(\vec{x}, t)$. □

(vi) Bounded quantifiers:
Let $A(\vec{x}, t)$ be primitive recursive. Define $B(\vec{x}, z) \iff (\exists t < z) A(\vec{x}, t)$. Then $B(\vec{x}, z)$ is primitive recursive.

Proof. We have $B(\vec{x}, t) \iff \mu t_{t<z} A(\vec{x}, t) < z$, so B is primitive recursive. □

1.2 Codings

Recall that for all $x \geq 2$ there exists a unique prime factorization

$$x = p_0^{n_0} p_1^{n_1} \cdot \ldots \cdot p_k^{n_k} \qquad (n_k > 0),$$

where $p_o, p_1, p_2, \ldots$ is the list of all primes.

Definition 1.2.1.

(i) Define $\langle \cdot, \cdot, \ldots, \cdot \rangle : \mathbb{N}^k \to \mathbb{N}$ to be the function

$$\langle x_1, x_2, \ldots, x_k \rangle = p_0^k p_1^{x_1} p_2^{x_2} \cdot \ldots \cdot p_k^{x_k}$$

(ii) $(x)_i$ = exponent of p_i in the unique factorization.

(iii) $\mathrm{lh}(x) = (x)_0$ (length of tuple coded by x)

(iv) $\mathrm{Seq}(x) \iff x \neq 0 \wedge (\forall n \leq x)(n > 0 \wedge (x)_n \neq 0 \Rightarrow n \leq \mathrm{lh}(x))$

Note 1.2.2.

- Everything above is primitive recursive.
- $\langle \cdot, \cdot, \ldots, \cdot \rangle$ are injective.
- $(x)_i = i^{th}$ element of tuple coded by x.
- $x_i < \langle x_1, \ldots, x_k \rangle$

Fact: There is a "computable" function $f : \mathbb{N} \to \mathbb{N}$ such that for each primitive recursive $g : \mathbb{N} \to \mathbb{N}$ there is n_0 such that $n \geq n_0 \Rightarrow f(n) > g(n)$ (i.e. f dominates g). The Ackerman function is such a function. Hence f is not primitive recursive.

1.3 Partial (computable) functions

A function $f : \mathbb{N}^k \to \mathbb{N}$ is a partial function if we do not require $f(\vec{x})$ to be defined for each $\vec{x}$. f is total if $f(\vec{x})$ is defined for each $\vec{x}$.

Notation 1.3.1.

(i) $f(\vec{x})\downarrow$ means that $f(\vec{x})$ is defined. $f(\vec{x})\uparrow$ means that $f(\vec{x})$ is undefined.

(ii) If $Expr_1, Expr_2$ are expressions, then we write $Expr_1 \simeq Expr_2$ if either $Expr_1$ and $Expr_2$ are both undefined or both are defined and equal. ($Expr_1$ and $Expr_2$ are said to be strongly equal or satisfy Kleene equality).

Example 1.3.2. (Composition) Suppose $g, h_1, \ldots, h_k$ are partial functions and we define $f(\vec{x}) \simeq g(h_1(\vec{x}), \ldots, h_k(\vec{x}))$. Then $f(\vec{x})\downarrow$ if and only if $h_i(\vec{x})$ for $1 \leq i \leq k$ and if $h_i(\vec{x}) = a_i$ for $1 \leq i \leq k$ then $g(a_1, \ldots, a_k)\downarrow$.

Note 1.3.3. If the h_i and g are "computable" then f is "computable".

Example 1.3.4. (Primitive recursion) Let f be a function defined by

$$\begin{cases} f(\vec{x}, 0) = g(\vec{x}) \\ f(\vec{x}, y+1) = h(\vec{x}, y, f(\vec{x}, y)). \end{cases}$$

To compute $f(\vec{x}, y)$ we have to compute $f(\vec{x}, 0)$, then $f(\vec{x}, 1), \ldots$, then $f(\vec{x}, y-1)$ and then $h(\vec{x}, y, f(\vec{x}, y))$. So

$$\begin{aligned} f(\vec{x}, 0)\downarrow &\iff g(\vec{x})\downarrow \\ f(\vec{x}, y+1)\downarrow &\iff (\forall z \leq y)(f(\vec{x}, z)\downarrow) \wedge h(\vec{x}, y, f(\vec{x}, y))\downarrow \end{aligned}$$

Example 1.3.5. (The μ-operator) Let $g : \mathbb{N}^{n+1} \to \mathbb{N}$ be a partial recursive function. Define $f(\vec{x}) \simeq \mu y[g(\vec{x}, y) \simeq 0]$. $f(\vec{x})$ "equals the least y" such that $g(\vec{x}, y) \simeq 0$.

To compute $f(\vec{x})$ we proceed as follows: Compute $g(\vec{x}, 0)$. If it is defined an greater than 0 then compute $g(\vec{x}, 1)$, and so on until we find y such that $g(\vec{x}, y) \simeq 0$ Suppose for example that $g(\vec{x}, 0)\uparrow$ and $g(\vec{x}, 1) \simeq 0$. In this case the computation will go on forever and we will not find the least y. So

$$f(\vec{x})\downarrow \iff \exists y(g(\vec{x}, y) \simeq 0 \wedge (\forall z < y)(g(\vec{x}, z)\downarrow \wedge g(\vec{x}, z) > 0)).$$

If $f(\vec{x})\downarrow$ then the witness y is unique and we set $f(\vec{x}) = y$.

Definition 1.3.6. (Inductive definition of the class μ-R of partial μ-recursive functions. Simultaneously we give an index (a name as a number) of the functions.)

(i) All constant functions are in μ-R. If $f : \mathbb{N}^n \to \mathbb{N}$ is a constant function with value m, then $\langle 0, m, n \rangle$ is an index for f.

(ii) All projection functions are in μ-R. $\langle 1, n, i \rangle$ is an index for P^i_n.

(iii) The successor function $S(x) = x + 1$ is in μ-R. $\langle 2 \rangle$ is an index for S.

(iv) If $g, h_1, \ldots, h_n \in \mu$-$\mathsf{R}$, then $f(\vec{x}) \simeq g(h_1(\vec{x}), \ldots, h_n(\vec{x})) \in \mu$-$\mathsf{R}$. Let e be an index for g and e_i index for h_i. Then $\langle 3, e, e_1, \ldots, e_k \rangle$ is an index for f.

(v) If $g, h \in \mu\text{-R}$ with indices e, e', then

$$\left\{ \begin{array}{l} f(\vec{x}, 0) = g(\vec{x}) \\ f(\vec{x}, y+1) = h(\vec{x}, y, f(\vec{x}, y)) \end{array} \right. \in \mu\text{-R},$$

and is given index $\langle 4, e, e' \rangle$.

(vi) If $g \in \mu\text{-R}$ with index e, then $f(\vec{x}) \simeq \mu y[g(\vec{x}, y) \simeq 0] \in \mu\text{-R}$ and is given index $\langle 5, e \rangle$.

If $f \in \mu\text{-R}$ we say f is partial μ-recursive or partial recursive.

Definition 1.3.7. A relation $R \subseteq \mathbb{N}$ is recursive if the characteristic function χ_R is recursive.

Note 1.3.8. Each $f \in \mu\text{-R}$ has infinitely many indices.

Proposition 1.3.9. *Each $f \in \mu$-R is "computable".*

Thesis 1.3.10 (Church-Turing thesis). *Each "computable" function is in μ-R.*

Theorem 1.3.11 (Normal form theorem). *There is a primitive recursive function $U : \mathbb{N} \to \mathbb{N}$ and $\forall n \geq 1$ there is a primitive recursive $(n+2)$-ary relation T_n such that for each partial recursive f, n-ary, there is $e \in \mathbb{N}$ such that*

(i) $f(x_1, \ldots, x_n)\downarrow \iff \exists y T_n(e, x_1, \ldots, x_n, y)$, where $f(\vec{x}) \simeq z$ and $y = \langle z, w \rangle$, z is the value of computation and w is a code for the computation.

(ii) $f(x_1, \ldots, x_n) \simeq U(\mu y T_n(e, x_1, \ldots, x_n, y))$. $U(x) = (x)_1$ so it is primitive recursive.

Remark 1.3.12. T_n is Kleenes T-predicate.

Terminology 1.3.13. e is an index for f.

Note 1.3.14. Each $e \in \mathbb{N}$ is an index for a partial recursive function $f(\vec{x}) \simeq U(\mu y T_n(e, \vec{x}, y))$.

Definition 1.3.15. $\phi_e^{(n)}(x_1, \ldots, x_n) = U(\mu y T_n(e, x_1, \ldots, x_n, y))$.

Remark 1.3.16. If $n = 1$, then we write ϕ_e.

Remark 1.3.17. The family $\phi_e^{(n)}$ for $e \in \mathbb{N}$ make up all the partial n-ary recursive functions.

Theorem 1.3.18. *There is an $(n+1)$-ary partial recursive function Φ such that for each $e, \vec{x}$*

$$\Phi(e, \vec{x}) \simeq \phi_e^{(n)}(\vec{x}),$$

the universal function or universal machine.

Proof. $\Phi(e, \vec{x}) \simeq U(\mu y T(e, \vec{x}, y))$. □

Example 1.3.19. Let $f(\vec{x}) \simeq z$, f partial recursive. We want to code computation as a labelled tree. Each label is of the form $\langle e, \langle x \rangle, z \rangle$, where e is an index, $\vec{x}$ is the arguments and z is the value.

(i) Constant n-ary function with value m:

$$\langle \langle 0, m, n \rangle, \langle \vec{x} \rangle, m \rangle$$

(ii) Projection $P_n^i(\vec{x}) = x_i$:

$$\langle\langle 1, n, i\rangle, \langle\vec{x}\rangle, x_i\rangle$$

(iii) Successor function $S(x) = x + 1$:

$$\langle\langle 2\rangle, \langle x\rangle, x + 1\rangle$$

(iv) Composition $f(\vec{x}) \simeq g(h_1(\vec{x}), \ldots, h_n(\vec{x})) \simeq z$. We know that $h_i(\vec{x}) \simeq z_i$ and $g(z_1, \ldots, z_k) \simeq z$. Assume that h_i has index e_i and that g has index e. Inductively we have trees for these:

$$\left.\begin{array}{rr} T_1\} & \langle e_1, \langle\vec{x}\rangle, z_1\rangle \\ \vdots & \\ T_k\} & \langle e_k, \langle\vec{x}\rangle, z_k\rangle \\ T\} & \langle e, \langle\vec{x}\rangle, z\rangle \end{array}\right\} \langle\langle 4, e, e_1, \ldots, e_k\rangle, \langle\vec{x}\rangle, z\rangle$$

(v) Primitive recursion:

$$\begin{cases} f(\vec{x}, 0) = g(\vec{x}) \\ f(\vec{x}, y+1) = h(\vec{x}, y, f(\vec{x}, y)) \end{cases}$$

(vi) μ-operator: $f(\vec{x}) \simeq \mu t[h(\vec{x}, t) \simeq 0] \simeq t$. Suppose g has index e.

$$\left.\begin{array}{rrr} (\text{Tree for } g(\vec{x}, 0) \simeq z_0 > 0) & T_0\} & \langle e, \langle\vec{x}, 0\rangle, z_0\rangle \\ & \vdots & \vdots \\ (\text{Tree for } g(\vec{x}, t-1) \simeq z_{t-1} > 0) & T_{t-1}\} & \langle e, \langle\vec{x}, t-1\rangle, z_{t-1}\rangle \\ (\text{Tree for } g(\vec{x}, t) \simeq 0) & T_t\} & \langle e, \langle\vec{x}, t\rangle, 0\rangle \end{array}\right\} \langle\langle 5, e\rangle, \langle\vec{x}\rangle, t\rangle$$

Suppose that we have a computation tree

$$T : \left.\begin{array}{r} T_1\} \\ \vdots \\ T_k\} \end{array}\right\} v,$$

where v is the label of the top node. Inductively we can code T_i as a number $\hat{T}_i$. Then code T as $\hat{T} = \langle v, \hat{T}_1, \ldots, \hat{T}_k\rangle$.
Fact: The set of codes for computation trees is primitive recursive.
$T_n(e, \vec{x}, y) \iff e$ is an index for μ-recursive function f, $y = \langle z, w\rangle, z \simeq f(\vec{x})$ and w is a code for the computation tree of $f(\vec{x}) \simeq z$.
Fact: T_n is primitive recursive.

1.4 Recursively enumerable sets

Definition 1.4.1. $R \subseteq \mathbb{N}^k$ is recursive if χ_R is recursive.

Proposition 1.4.2. *Recursive relations are closed under propositional connectives, i.e.* $\vee, \wedge, \neg, \ldots$.

Proof. ($\wedge$) Suppose R and S are k-ary recursive relations. Then $\chi_{R\wedge S}(\vec{x}) = \chi_R(\vec{x}) \cdot \chi_S(\vec{x})$ and hence $R \wedge S$ is recursive. □

Proposition 1.4.3. *Recursive relations are closed under bounded quantification.*

Proof. As for primitive recursive relations. □

Note 1.4.4. Recursive relations are not closed under bounded quantification.

Definition 1.4.5. A relation $R \subseteq \mathbb{N}$ is recursively enumerable (r.e.) if there is a partial recursive function f such that $R(\vec{x}) \iff f(\vec{x})\downarrow$.

Definition 1.4.6. Define dom(f) and ran(f) as follows:

$$\begin{aligned} \text{dom}(f) &\simeq \{\vec{x} \in \mathbb{N}^k : f(\vec{x})\downarrow\} \\ \text{ran}(f) &\simeq \{y \in \mathbb{N} : \exists \vec{x} \in \mathbb{N}^k . f(\vec{x}) \simeq y\}. \end{aligned}$$

Proposition 1.4.7. *If R is recursive, then R is recursively enumerable.*

Proof. Define

$$f(\vec{x}) \simeq \mu y[y + 1 = \chi_R(\vec{x})].$$

Then $R = \text{dom}(f)$. □

Definition 1.4.8. $W_e^{(n)} = \left\{(x_1, \ldots, x_n) \in \mathbb{N}^n : \phi_e^{(n)}(x_1, \ldots, x_n)\downarrow\right\}$.

Remark 1.4.9. We have an indexing or enumeration of all the recursively enumerable relations.

Remark 1.4.10. If $n = 1$ we write W_e for $W_e^{(1)}$.

Proposition 1.4.11. *Recursively enumerable relations are closed under $\wedge, \vee$.*

Proof. ($\wedge$) Suppose R and S are recursively enumerable. So $R = \text{dom}(f)$, $S = \text{dom}(g)$, where f, g are partial recursive functions. Define $h(\vec{x}) \simeq f(\vec{x}) + g(\vec{x})$ and $h(\vec{x})\downarrow \iff f(\vec{x})\downarrow \wedge g(\vec{x})\downarrow$

($\vee$)

$$\begin{aligned} R(\vec{x}) &\iff \exists y T(e_1, \vec{x}, y), \qquad R = W_{e_1}^{(k)} \\ S(\vec{x}) &\iff \exists y T(e_2, \vec{x}, y), \qquad S = W_{e_2}^{(k)}. \end{aligned}$$

Define

$$h(\vec{x}) \simeq \mu y(T(e_1, \vec{x}, y) \vee T(e_2, \vec{x}, y)).$$

Then $h(\vec{x})\downarrow \iff R(\vec{x}) \vee S(\vec{x})$. □

Proposition 1.4.12. *A k-ary relation R is recursive if and only if R and the complement of R are recursively enumerable.*

Proof. ($\Rightarrow$) Already done.
($\Leftarrow$) Suppose $R = \text{dom}(f)$ and $\neg R = \text{dom}(g)$. Let $W_{e_1}^{(k)} = R$ and $W_{e_2}^{(k)} = \neg R$. Define

$$f(\vec{x}) \simeq \mu y[T(e_1, \vec{x}, y) \vee T(e_2, \vec{x}, y)].$$

We know that $\forall \vec{x} \exists y f(\vec{x}) \simeq y$ so f is total. Define χ_R by

$$\chi_R(\vec{x}) = \begin{cases} 1 & \text{if } T(e_1, \vec{x}, f(\vec{x})) \\ 0 & \text{if } T(e_2, \vec{x}, f(\vec{x})). \end{cases}$$

□

Proposition 1.4.13. *A set $A \subseteq \mathbb{N}$ is recursively enumerable if and only if $A = \emptyset$ or $A = \mathrm{ran}(f)$ for some total recursive f.*

Proof. ($\Leftarrow$) If $A = \emptyset$, then $A = \mathrm{dom}(g)$, where g is always undefined, for example $g(y) \simeq \mu z[z \neq z]$. Suppose $A = \mathrm{ran}(f)$, f total recursive. Define

$$g(x) \simeq \mu y[f(y) = x]$$

($f(y) = x$ is recursive since f is total). Clearly $\mathrm{dom}(g) = \mathrm{ran}(f)$.
($\Rightarrow$) Recall that $(x)_n$ is the exponent of p_n in the unique prime decomposition of x. Suppose $A = W_e$, so $x \in A \iff \exists y T(e, x, y)$. Suppose $A \neq \emptyset$. Let $a \in A$. Define

$$f(x) = \begin{cases} (x)_1 & \text{if } (\exists y \leq (x)_2) T(e, (x)_1, y) \\ a & \text{otherwise.} \end{cases}$$

Note that f is total and recursive. *Claim:* $A = \mathrm{ran}(f)$. Clearly $\mathrm{ran}(f) \subseteq A$. Suppose $z \in A$. Then $\exists w.T(e, z, w)$. Let $x = \langle z, w \rangle$, so $(x)_1 = z$ and $(x)_2 = w$. Hence $(\exists y \leq (x)_2) T(e, (x)_1, y)$ is true so $f(x) = (x)_1 = z$, so $z \in \mathrm{ran}(f)$ □

Proposition 1.4.14. *If $R(\vec{x}, y)$ is recursively enumerable, then $\exists y R(\vec{x}, y)$ is recursively enumerable. (Recursively enumerable relations are closed under $\exists$.)*

Note 1.4.15. This is not true for recursive relations.

Proof. Since R is r.e. we have $R(\vec{x}, y) \iff \exists z T(e, \vec{x}, y, z)$ for some e. Thus

$$\exists y R(\vec{x}, y) \iff \exists y \exists z T(e, \vec{x}, y, z) \iff \exists w T(e, \vec{x}, (w)_1, (w)_2).$$

Define

$$f(\vec{x}) \simeq \mu y[T(e, \vec{x}, (w)_1, (w)_2)].$$

f is partial recursive and $\mathrm{dom}(f) = R$. Hence $\exists y R(\vec{x}, y)$ is r.e. □

Definition 1.4.16. Let $f : \mathbb{N} \to \mathbb{N}$. Then $\mathcal{G}_f = ((\vec{x}, y) : f(x) \simeq y)$, the graph of f.

Proposition 1.4.17. *A function f is partial recursive if and only if $\mathcal{G}_f$ is recursively enumerable.*

Definition 1.4.18. $K_0 = \{\langle x, y \rangle : \phi_x(y)\downarrow\}$ and $K = \{x \in \mathbb{N} : \phi_x(x)\downarrow\}$

Theorem 1.4.19. *K_0 is a recursively enumerable set which is not recursive.*

Proof. Let Φ be the partial recursive enumeration function. Then define

$$f(x) \simeq \begin{cases} \Phi((x)_1, (x)_2) & \text{if } \mathrm{Seq}(x) \wedge \mathrm{lh}(x) = 2 \\ \downarrow & \text{otherwise.} \end{cases}$$

Then we have

$$f(x)\downarrow \iff x = \langle y, z \rangle \wedge \Phi(y, z)\downarrow \iff \langle y, z \rangle \in K_0 \iff x \in K_0.$$

Hence K_0 is recursively enumerable.

Suppose K_0 is recursive. Then define

$$g(x) = \begin{cases} \phi_x(x) + 1 & \text{if } \phi_x(x)\downarrow \\ 0 & \text{otherwise.} \end{cases}$$

Thus g is total recursive since K_0 is recursive. So $g = \phi_e$ for some e. We know that $\langle e, e \rangle \in K_0$. Hence $\phi_e(e) = g(e) = \phi_e(e)+1$. Contradiction. Hence K_0 is not recursive. □

Proposition 1.4.20. *Let $g_1, \ldots, g_n$ be partial recursive functions. Let $R_1, \ldots, R_n$ be recursively enumerable relations (all k-ary) such that $\forall \vec{x}$ at most one of the $R_i(\vec{x})$ holds. Then*

$$f(\vec{x}) \simeq \begin{cases} g_1(\vec{x}) & \text{if } R_1(\vec{x}) \\ \vdots & \vdots \\ g_n(\vec{x}) & \text{if } R_n(\vec{x}) \\ \uparrow & \text{otherwise} \end{cases}$$

is partial recursive.

Proof. Recall that f is partial recursive if and only if its graph $\mathcal{G}_f$ is recursively enumerable. So

$$f(\vec{x}) \simeq y \iff (R_1(\vec{x}) \wedge g_1(\vec{x}) \simeq y) \vee (R_2(\vec{x}) \wedge g_2(\vec{x}) \simeq y) \vee \ldots \vee (R_n(\vec{x}) \wedge g_n(\vec{x}) \simeq y).$$

Recursively enumerable relations are closed under $\wedge, \vee$ so $\mathcal{G}_f$ is recursively enumerable, and hence f is partial recursive. □

1.5 Smn theorem

Suppose that $f : \mathbb{N}^n \times \mathbb{N}^m \to \mathbb{N}$ is partial recursive. Let $a_1, \ldots, a_n \in \mathbb{N}$. Define

$$g(y_1, \ldots, y_m) \simeq f(a_1, \ldots, a_n, y_1, \ldots, y_m).$$

Thus g is partial recursive. The Smn theorem then tells us that we can calculate an index for g from the index for f and from $a_1, \ldots, a_n$.

Theorem 1.5.1 (Smn theorem). *Let $m, n \geq 1$. Then there is a primitive rcursive function S^n_m such that*

$$\phi_{S^n_m(e,x_1,\ldots,x_m)}(y_1, \ldots, y_n) \simeq \phi_e(x_1, \ldots, x_m, y_1, \ldots, y_n)$$

for each $e, \vec{x}, \vec{y}$.

Remark 1.5.2. The universal function $\Phi(e, \vec{x}) \simeq \phi_e(\vec{x})$ tells us that a program can be viewed as data. Smn theorem tells us that data can be incorporated into programs.

Proof. Recall our indexing of μ-R:

- $t(x) = \langle 0, x, 1 \rangle$ index for the constant function with value x.
- $\langle 1, 1, 1 \rangle$ index for P^1_1 (Projection function)
- If e is an index for g, e_1 index for h_1 and e_2 index for h_2, then $\langle 3, e, e_1, e_2 \rangle$ is an index for $f(x) \simeq g(h_1(x), h_2(x))$

So $\phi_{t(x)}(y) = x$ and $\phi_{\langle 1,1,1 \rangle}(y) = y$. Suppose for simplicity that $m = n = 1$. Then

$$\phi_e(x, y) \simeq \phi_e(\phi_{t(x)}(y), \phi_{\langle 1,1,1 \rangle}(y)) \simeq \phi_{\langle 3,e,t(x),\langle 1,1,1 \rangle \rangle}(y).$$

Let $S^1_1(e, x) = \langle 3, e, t(x), \langle 1, 1, 1 \rangle \rangle$, so S^1_1 is primitive recursive. Hence $\phi_e(x, y) \simeq \phi_{S^1_1(e,x)}(y)$. □

1.6 Uniformities

Suppose $f_1, \dots, f_k$ are partial recursive functions, and that we from these functions construct a new partial recursive function g. Then g is said to be obtained uniformly from $f_1, \dots, f_k$ if there exists a primitive recursive function S such that if $e_1, \dots, e_k$ is an index for $f_1, \dots, f_k$, then $S(e_1 \dots, e_k)$ is an index for g (similar for recursively enumerable relations).

Example 1.6.1. Union of recursively enumerable sets are uniformly recursively enumerable, i.e. there is a primitive recursive function S such that for each e_1, e_2

$$W_{e_1} \cup W_{e_2} = W_{S(e_1,e_2)}.$$

Proof. By definition we have

$$\begin{aligned} x \in W_{e_1} &\iff \exists z T(e_1, x, z) \\ x \in W_{e_2} &\iff \exists z T(e_2, x, z). \end{aligned}$$

Then

$$x \in W_{e_1} \cup W_{e_2} \iff \exists z T(e_1, x, z) \vee \exists z T(e_2, x, z).$$

The righthand side above is a recursively enumerable relation $R(e_1, e_2, x)$. Let e be an index for R. So

$$\phi_e(e_1, e_2, x)\downarrow \iff R(e_1, e_2, x) \iff x \in W_{e_1} \cup W_{e_2}.$$

Now the Smn theorem gives

$$\phi_{S^1_2(e,e_1,e_2)}(x) \simeq \phi_e(e_1, e_2, x).$$

Let $S(e_1, e_2) = S^1_2(e, e_1, e_2)$, so S is primitive recursive. Thus $\phi_{S(e_1,e_2)}(x) \simeq \phi_e(e_1, e_2, x)$, and

$$\phi_{S(e_1,e_2)}(x)\downarrow \iff x \in W_{e_1} \cup W_{e_2}.$$

Hence $W_{S(e_1,e_2)} = W_{e_1} \cup W_{e_2}$. □

1.7 m-reducibility

Definition 1.7.1. Let $A, B \subseteq \mathbb{N}$. A is m-reducible to B, $A \leq_m B$, if there is a total recursive function $f : \mathbb{N} \to \mathbb{N}$ such that

$$x \in A \iff f(x) \in B.$$

Remark 1.7.2. B at least as complicated as A. Suppose that we can decide B. To decide A we do as follows: Calculate $f(x)$. If $f(x) \in B$, then $x \in A$. If $f(x) \notin B$, then $x \notin A$.

Remark 1.7.3.

- $A \leq_m A$ via the identity.
- If $A \leq_m B$ and $B \leq_m C$, then $A \leq_m C$. If f is a witness to $A \leq_m B$ and g is a witness to $B \leq_m C$, then $h = g \circ f$ is a witness to $A \leq_m C$.

Hence $\leq_m$ is reflexive and transitive.

Definition 1.7.4. $A \equiv_m B \iff A \leq_m B$ and $B \leq_m A$

Example 1.7.5. If A and B are recursive (and not equal $\emptyset$ or $\mathbb{N}$), then $A \equiv_m B$.

Example 1.7.6. Suppose A is recursively enumerable. Let $K_0 = \{\langle x, y\rangle : \phi_x(y)\downarrow\}$ Then $A \leq_m B$.

Proof. Let $A = W_e$, so $y \in A \iff y \in W_e \iff \phi_e(y)\downarrow$. Define $f(y) = \langle e, y\rangle$, total primitive recursive function. Now

$$y \in A \iff \phi_e(y)\downarrow \iff \langle e, y\rangle \in K_0 \iff f(y) \in K_0.$$

□

Example 1.7.7. (Method to show that A is not recursive)
Show that there is a non-recursive set B such that $B \leq_m A$.

Proof. Suppose A is recursive. Given x, compute $f(x)$ and decide $f(x) \in A$. But then B is decidable. Contradiction. Hence A is not recursive. □

1.8 Rice's theorem

Given a class $\mathcal{C}$ of partial recursive functions, can we decide $\mathcal{C}$? To make the problem precise, we study indices for partial recursive functions. Given such a class $\mathcal{C}$, let $A = \{e \in \mathbb{N} : \phi_e \in \mathcal{C}\}$. Then A has the following property:

$$e \in A \wedge \phi_e = \phi_{e'} \to e' \in A.$$

Definition 1.8.1. A set $A \subseteq \mathbb{N}$ is called an index set if $e \in A \wedge \phi_e = \phi_{e'} \to e' \in A$.

Remark 1.8.2. If A is an index set, then $\mathbb{N} \setminus A$ is an index set.

Theorem 1.8.3 (Rice's theorem). *If A is a recursive index set, then $A = \emptyset$ or $A = \mathbb{N}$.*

Corollary 1.8.4. *If C is a decidable class of partial recursive functions, then $C = \emptyset$ or C contains all partial recursive functions.*

Example 1.8.5. None of the following sets are recursive.

$$\begin{array}{l} \{e : W_e \neq \emptyset\} \\ \{e : W_e \text{ finite}\} \\ \{e : W_e \text{ infinite}\} \\ \{e : \phi_e \text{ total function}\} \end{array}$$

Proof of Rice's theorem. Let A be an index set, $A \neq \emptyset$ and $A \neq \mathbb{N}$. We show $K \leq_m A$, so then A is not recursive. We need to find $S : \mathbb{N} \to \mathbb{N}$, total recursive such that $x \in K \iff S(x) \in A$. Assume that indices from the totally undefined function are not in A. Let $a \in A$. Now we use the following idea:

$$\begin{array}{l} x \in K \Rightarrow \phi_{S(x)} = \phi_a \Rightarrow S(x) \in A \\ x \notin K \Rightarrow S(x) \text{ index for the totally undefined function } \Rightarrow S(x) \notin A. \end{array}$$

Define

$$f(x,y) \simeq \begin{cases} \phi_a(y) & \text{if } x \in K \\ \uparrow & \text{otherwise.} \end{cases}$$

Thus f is partial recursive, say $f = \phi_e$. Fix such e. By the Smn theorem

$$\phi_{S_1^1(e,x)}(y) \simeq f(x,y) \simeq \begin{cases} \phi_a(y) & \text{if } x \in K \\ \uparrow & \text{otherwise.} \end{cases}$$

Let $S(x) = S_1^1(e,x)$, S is primitive recursive. Now

$$\begin{aligned} &x \in K \Rightarrow \phi_{S(x)}(y) = \phi_a(y) \forall y \\ &x \notin K \Rightarrow \phi_{S(x)}(y) \forall y \end{aligned}$$

□

1.9 Recursion theorem

Theorem 1.9.1. *[Second recursion theorem, Kleene]*
For each $(n+1)$-ary partial recursive function f there is an index e s.th. for all $\vec{x}$

$$\phi_e^{(n)}(\vec{x}) \simeq f(e,\vec{x}).$$

Proof. Given f partial recursive, define

$$h(y,\vec{x}) = f(S_n^1(y,y),\vec{x}).$$

Thus h is partial recursive, so $h = \phi_a^{(n+1)}$ for some fixed a. That is $\phi_a^{(n+1)}(y,\vec{x}) = h(y,\vec{x})$ for all y and $\vec{x}$. By smn-theorem $\phi_a^{(n+1)}(y,\vec{x}) \simeq \phi_{S_n^1(a,y)}^{(n)}(\vec{x})$, so

$$\phi_{S_n^1(a,y}^{(n)}(\vec{x}) \simeq h(y,\vec{x}) \simeq f(S_n^1(y,y),\vec{x}).$$

Now put $a = y$. Then

$$\phi_{S_n^1(a,a)}^{(n)}(\vec{x}) \simeq f(S_n^1(a,a),\vec{x}).$$

Let $e = S_n^1(a,a)$, and the statement follows. □

Remark 1.9.2. e is obtained uniformly (can be computed) from an index for f.

Corollary 1.9.3. *Let $f : \mathbb{N} \to \mathbb{N}$ be a total recursive function. Then there is an $e \in \mathbb{N}$ such that $\forall \vec{x}$*

$$\phi_{f(e)}^{(n)}(\vec{x}) \simeq \phi_2^{(n)}(\vec{x})$$

(i.e. $\phi_{f(e)} = \phi_e$).

Proof. We have that

$$\phi_{f(y)}^{(n)}(\vec{x}) \simeq \Phi^{(n)}(f(y),\vec{x}) \simeq h(y,\vec{x}).$$

By the second recursion theorem there is $e \in \mathbb{N}$ such that $\phi_e(\vec{x}) \simeq h(e,\vec{x}) \forall x$. Then

$$\phi_e(\vec{x}) \simeq h(e,\vec{x}) \simeq \phi_e(\vec{x}) \simeq \phi_{f(e)}(\vec{x})$$

for all $\vec{x}$, and hence $\phi_e = \phi_{f(e)}$ □

Corollary 1.9.4. *Suppose $f : \mathbb{N} \to \mathbb{N}$ is total recursive. Then there is $e \in \mathbb{N}$ such that*

$$W_{f(e)} = W_e.$$

Proof. There is e such that $\phi_{f(e)} = \phi_e$ by Corollary 1.9.3. We have $W_{f(e)} = \mathrm{dom}(\phi_{f(e)})$ and $W_e = \mathrm{dom}(\phi_e)$. Hence $W_{f(e)} = W_e$ □

Example 1.9.5. *Show:* There is $e \in \mathbb{N}$ such that $W_e = \{e\}$.
Strategy: Construct total recursive f such that for each y, $W_{f(y)} = \{y\}$. Suppose done. Then by Corollary 1.9.4 there is $e \in \mathbb{N}$ such that $W_{f(e)} = W_e$..

Construct such f. Define

$$g(x, y) \simeq \begin{cases} 0 & \text{if } x = y \\ \uparrow & \text{otherwise.} \end{cases}$$

g is partial recursive so it has an index, say a. The Smn theorem now gives $\phi_{S^1_1(a,x)}(y) \simeq g(x, y)$ and $g(x, y)\downarrow \iff x = y$. Hence $\phi_{S^1_1(a,x)}(y)\downarrow \iff x = y$, and $W_{S^1_1(a,x)} = \{x\}$. Let $f(x) = S^1_1(a, x)$. Then $W_{f(x)} = \{x\}$.

Example 1.9.6. Let g, h, α be partial recursive functions. Define f by

$$\begin{cases} f(0, y) \simeq g(y) \\ f(x + 1, y) \simeq h(x, y, f(x, \alpha(y))). \end{cases}$$

Is there such an f? Is f partial recursive?

Define

$$\psi(e, x, y) \simeq \begin{cases} g(y) & \text{if } x = 0 \\ h(x - 1, y, \Phi(e, x - 1, \alpha(y)) & \text{if } x > 0. \end{cases}$$

Note that ψ is partial recursive. By Theorem 1.9.1 there is a fixed e such that

$$\phi_e(x, y) \simeq \psi(e, x, y) \simeq \begin{cases} g(y) & \text{if } x = 0 \\ h(x - 1, y, \Phi(e, x - 1, \alpha(y)) & \text{if } x > 0. \end{cases}$$

Let $f = \phi_e$. Then f satisfies the original equation and f is partial recursive.

Chapter 2

Gödel's theorems

Theorem (First incompleteness theorem). If T is a consistent, first-order theory with a decidable set of axioms containing a sufficient amount of arithmetic, then there is a sentence φ such that neither φ nor $\neg\varphi$ is provable from T. So then T is incomplete.

We have the following fact: If T has a bit of arithmetic, then there is a sentence $\mathrm{Con}(T)$ which says "T is consistent".

Theorem (Second incompleteness theorem). With the assumptions on T above, then $Con(T)$ is not provable in T.

So to prove "T is consistent" we have to use a stronger theory T'.

2.1 Structure of the proof

The idea of the proof is the lier paradox "I lie". Gödel's variant of this is "I am unprovable". To prove the theorem we go through the following steps:

- Define a theory P_0, a finitely axiomatized fragment of Peano arithmetic.
- P_0 shall talk about formulas, proofs etc.
- Show that every total recursive function is representable in P_0 (by formulas).
- Code syntax, proofs using primitive recursive functions (Gödelization), so these are representable in P_0.
- Using self-references and diagonalization, we obtain the result.

The assumptions are the following:

- First-order language with equality.
- Formal proof $T \vdash \varphi$.
- Truth and truth in a model $\mathfrak{M} \models \varphi$.
- Completeness: $T \vdash \varphi \iff$ for each model $\mathfrak{M} \models T$ we have $\mathfrak{M} \models \varphi$.

Notation 2.1.1.

- We use $x, y, x_1, \dots$ as formal variables.
- $\varphi(x_1, \dots, x_n)$ stands for a formula where all the free variables are *among* $x_1, \dots, x_n$.
- We use "=" for equality in the formal language.

In the proof we use the standard model of arithmetic, $\mathfrak{N} = (\mathbb{N}; 0; S, +, \cdot; <)$, where $\mathbb{N} = \{0, 1, 2, \dots\}$, S is the successor function and $<$ is the usual less-than relation. The language L we use consists of a constant symbol $\underline{0}$, a unary function symbol $\underline{S}$, two binary function symbols $\underline{+}, \underline{\cdot}$ and a binary relation symbol $\underline{<}$.

We also have $\underline{0}^{\mathfrak{N}} = 0, \underline{S}^{\mathfrak{N}} = S, \dots$, the interpretations of the symbols.

2.2 Peano's axioms

Axioms 2.2.1 (Peanos axioms).

1. *0 is a number.*
2. *If n is a number, then there is a number n', the successor of n.*
3. *For each number n, $n' \neq 0$.*
4. *For numbers m, n, if $m' = n'$ then $m = n$.*
5. *Induction: For each set $A \subseteq \mathbb{N}$, if $0 \in A$ and if $n \in A \to n' \in A$, then A consists of all numbers ($A = \mathbb{N}$).*

Remark 2.2.2. Axiom 5 of Peano's axioms (2.2.1) is a second order statement.

Axioms 2.2.3 (Axioms for P_0, Robinson's arithmetic).

A1. $\forall x(\underline{S}(x) \neq \underline{0})$

A2. $\forall x \exists y(x \neq \underline{0} \to x = \underline{S}(y))$

A3. $\forall x \forall y(\underline{S}(x) = \underline{S}(y) \to x = y)$

A4. $\forall x(x \mathbin{\underline{+}} \underline{0} = x)$

A5. $\forall x \forall y(x \mathbin{\underline{+}} \underline{S}(y) = \underline{S}(x \mathbin{\underline{+}} y))$

A6. $\forall x(x \mathbin{\underline{\cdot}} \underline{0}) = \underline{0})$

A7. $\forall x \forall y(x \mathbin{\underline{\cdot}} \underline{S}(y) = x \mathbin{\underline{\cdot}} y \mathbin{\underline{+}} x)$

A8. $\forall x(\neg(x \mathbin{\underline{<}} \underline{0}))$

A9. $\forall x \forall y(x \mathbin{\underline{<}} \underline{S}(y) \leftrightarrow x \mathbin{\underline{<}} y \lor x = y)$

A10. $\forall x \forall y(x \mathbin{\underline{<}} y \lor x = y \lor y \mathbin{\underline{<}} x)$

Now $P_0 = A1, A2, \ldots, A10$. Suppose we want to show $P_0 \vdash \varphi$. We have $P_0 \vdash \varphi \iff P_0 \models \varphi$. $P_0 \models \varphi$ means that $\mathfrak{M} \models P_0 \Rightarrow \mathfrak{M} \models P_0$. We show that φ holds for an arbitrary $\mathfrak{M}$ such that $\mathfrak{M} \models P_0$.

Definition 2.2.4. For each $n \in \mathbb{N}$ let $\underline{n} = \underbrace{SSS \ldots S}_{n \text{ times}}(0)$. $\underline{n}$ is called a numeral and is a term in the formal language (syntactic object).

Definition 2.2.5. Suppose $\mathfrak{M} \models P_0$. Then the standard numbers in $\mathfrak{M}$ is the set $\{\underline{n}^{\mathfrak{M}} : n \in \mathbb{N}\}$ (where $\mathfrak{M} = (M; 0; S, +, \cdot; <)$).

Lemma 2.2.6. *Let $\mathfrak{M} \models P_0$. Let $a \in M$ be standard. Let $b < a$ (in $\mathfrak{M}$). Then b is standard.*

Proof. (Induction on n)
$n = 0$, i.e. $a = \underline{0}^{\mathfrak{M}}$. We know that $\mathfrak{M} \models \forall x(\neg(x \leq \underline{0}))$, so no such b exists and hence we have nothing to prove.

Suppose true for n. Consider $n+1$. Suppose $b < \underline{n+1}^{\mathfrak{M}}$ in $\mathfrak{M}$. By Axiom A9 (of 2.2.3) we have $b < \underline{n}^{\mathfrak{M}} \vee b = \underline{n}^{\mathfrak{M}}$. If $b < \underline{n}^{\mathfrak{M}}$, then b is standard by induction hypothesis. Otherwise $b = \underline{n}^{\mathfrak{M}}$ so it is standard. □

Lemma 2.2.7. $P_0 \vdash \forall x(x < \underline{n} \rightarrow x = \underline{0} \vee x = \underline{1} \vee \ldots \vee x = \underline{n-1})$ *for each* $\underline{n}$.

Lemma 2.2.8. $P_0 \vdash \underline{m} < \underline{n}$ *if and only if* $m < n$.

Lemma 2.2.9.

$$P_0 \vdash \underline{n} + \underline{m} = \underline{n+m}$$
$$P_0 \vdash \underline{n} \cdot \underline{m} = \underline{n \cdot m}$$

2.3 Representability

Definition 2.3.1. Let $f : \mathbb{N} \rightarrow \mathbb{N}$ be a total function. Let $\varphi(y, x_1, \ldots, x_k)$ be a formula in L. Then φ represents f if for each tuple $n_1, \ldots, n_k \in \mathbb{N}$

$$P_0 \vdash \forall y(\varphi(y, \underline{n_1}, \ldots, \underline{n_k}) \leftrightarrow y = \underline{f(n_1, \ldots, n_k)}).$$

Definition 2.3.2. Let $A \subseteq \mathbb{N}$ be a k-ary relation and $\varphi(x_1, \ldots, x_k)$ a formula. Then φ represents A if $\forall n_1, \ldots, n_k \in \mathbb{N}$

$$\begin{array}{l} A(n_1, \ldots, n_k) \Rightarrow P_0 \vdash \varphi(\underline{n_1}, \ldots, \underline{n_k}) \\ \neg A(n_1, \ldots, n_k) \Rightarrow P_0 \vdash \neg\varphi(\underline{n_1}, \ldots, \underline{n_k}) \end{array}.$$

Note 2.3.3. φ represents $A \iff \chi_A$ is representable.

Theorem 2.3.4. *Every total recursive function is representable.*

Lemma 2.3.5.

(i) All constant functions are representable.

(ii) Projection functions are representable.

(iii) The successor function $S : \mathbb{N} \rightarrow \mathbb{N}$ is representable.

Proof.

(i) $c_n(\vec{x}) = n$, constant function with value n, is represented by $y = \underline{n}$.

(ii) $P^i_k(n_1, \ldots, n_k) = n_i$ represented by $y = x_i$.

(iii) $S : \mathbb{N} \to \mathbb{N}$ represented by $y = S(x) \equiv \varphi(y, x)$.

□

Lemma 2.3.6. *Suppose $h : \mathbb{N}^m \to \mathbb{N}$ and $g_i : \mathbb{N}^k \to \mathbb{N}$ for $i = 1, \ldots, m$ and that these are representable. Then $f : \mathbb{N}^k \to \mathbb{N}$ defined by $f(\vec{x}) = h(g_1(\vec{x}), \ldots, g_k(\vec{x}))$ is representable.*

Proof. Let $\varphi(y, z_1, \ldots, z_m)$ represent h and $\psi_i(z_i, x_1, \ldots, x_k)$ represent g_i. Define $\theta(y, x_1, \ldots, x_k)$ by

$$\exists z_1, \ldots, \exists z_m \left(\varphi(y, z_1, \ldots, z_m) \wedge \bigwedge_{i=1}^{m} \psi_i(z_i, x_1, \ldots, x_k) \right).$$

Then $\theta(y, x_1, \ldots, x_k)$ represents f. □

Lemma 2.3.7. *Suppose $g : \mathbb{N}^{k+1} \to \mathbb{N}$ is representable, and suppose furthermore $\forall \vec{x}\, \exists y : g(\vec{x}, y) = 0$. Then $f(\vec{x}) = \mu y[g(\vec{x}, y) = 0]$ is representable.*

Now we want to prove Theorem 2.3.4 for primitive recursion

$$\begin{cases} f(\vec{x}, 0) = g(\vec{x}) \\ f(\vec{x}, y+1) = h(\vec{x}, y, f(\vec{x}, y)). \end{cases}$$

To compute $f(\vec{x}, n+1)$ we need compute the following quantities:

$$\begin{aligned} & f(\vec{x}, 0) = g(\vec{x}) = w_0 \\ & f(\vec{x}, 1) = h(\vec{x}, 0, f(\vec{x}, 0)) = h(\vec{x}, 0, w_0) = w_1 \\ & \vdots \\ & f(\vec{x}, n+1) = h(\vec{x}, n, w_n) = w_{n+1}. \end{aligned}$$

So $\langle w_0, w_1, \ldots, w_n \rangle$ codes computation of $f(\vec{x}, n)$. We want a formula $\varphi(v, \vec{x}, y)$ such that $P_0 \vdash \varphi(v, \underline{m}, \underline{n}) \leftrightarrow v = \underline{f(\vec{x}, n)}$.

Informally we can write

$$\varphi(v, \vec{x}, y) \equiv \exists a((a)_0 = g(m) \wedge (\forall i < n)(h(m, i, (a)_i) = (a)_{i+1}) \wedge v = (a)_n).$$

Suppose g, h are representable, then replace g and h by their representing formulas to get a representation for f. The problem that now arises is that we have used projection functions before we have shown that these are representable. To prove the statement we need the following lemma by Gödel.

Lemma 2.3.8 (Gödel). *There is a total representable (recursive) function $\beta(i, a, b)$ ($\beta : \mathbb{N}^3 \to \mathbb{N}$) such that if $n_0, \ldots, n_k \in \mathbb{N}$ are given, then there is a, b such that $\beta(i, a, b) = n_i$, $i = 0, \ldots, k$.*

2.4 Coding of syntax

We have to code the following:

- Language (Terms, formulas, sentences,...)
- Substitution of terms into terms/formulas
- Proofs (Formal proofs)
- Theorems

For this we fix a coding $\langle \cdot, \cdot, \cdot \rangle : \mathbb{N}^3 \to \mathbb{N}$ such that $\langle (x)_1, (x)_2, (x)_3 \rangle = x$, $(\cdot)_i$ primitive recursive.

2.4.1 Language and substitution

We have the language $L = \{0, S, +, \cdot, <\}$, "=" logical symbol. Let $v_0, v_1, v_2, \ldots$ be variables in the language.

Definition 2.4.1 (Coding of terms). We code terms in the language as follows:

$$\begin{array}{ll} \text{Base} & \begin{cases} 0 & \#0 = \langle 0,0,0 \rangle \\ v_i & \#v_i = \langle i+1, 0, 0 \rangle \end{cases} \\ \text{Ind.} & \begin{cases} t \equiv S(t_1) & \#t = \langle \#t_1, 0, 1 \rangle \\ t = t_1 + t_2 & \#t = \langle \#t_1, \#t_2, 2 \rangle \\ t = t_1 \cdot t_2 & \#t = \langle \#t_1, \#t_2, 3 \rangle \end{cases} \end{array}$$

Assume $\langle \cdot, \cdot, \cdot \rangle$ is bijective and $(x)_i < x$.

Lemma 2.4.2. *$\mathsf{Term} = \{\#t : t$ is a term$\}$ is primitive recursive.*

Proof.

$$\begin{aligned} x \in \mathsf{Term} \iff \big(((x)_1 = (x)_2 = 0) \;&\vee ((x)_2 = 1 \wedge (x)_1 = 0 \wedge (x)_0 \in \mathsf{Term}) \\ &\vee ((x)_2 = 2 \wedge (x)_1 \in \mathsf{Term} \wedge (x)_0 \in \mathsf{Term}) \\ &\vee ((x)_2 = 3 \wedge (x)_1 \in \mathsf{Term} \wedge (x)_0 \in \mathsf{Term})\big) \end{aligned}$$

□

Definition 2.4.3 (Coding of formulas). We code formulas as follows:

$$\begin{array}{ll} \text{Base} & \begin{cases} \#(t_1 = t_2) & = \langle \#t_1, \#t_2, 4 \rangle \\ \#(t_1 < t_2) & = \langle \#t_1, \#t_2, 5 \rangle \end{cases} \\ \text{Ind.} & \begin{cases} \#(\neg\varphi) & = \langle \#\varphi, 0, 6 \rangle \\ \#(\varphi \wedge \psi) & = \langle \#\varphi, \#\psi, 7 \rangle \\ \#(\varphi \to \psi) & = \langle \#\varphi, \#\psi, 8 \rangle \\ \#(\forall v_n \varphi) & = \langle \#\varphi, n, 9 \rangle \\ \#(\exists v_n \varphi) & = \langle \#\varphi, n, 10 \rangle \end{cases} \end{array}$$

Lemma 2.4.4. *$\mathsf{Form} = \{\#\varphi : \varphi$ is a formula$\}$ is primitive recursive.*

Suppose s, t are terms. Then $s[t/v_n]$ is the term where each occurrence of v_n is replaced by t. Suppose φ is a formula. Then $s\varphi[t/v_n]$ is the formula where each occurrence of v_n is replaced by t.

Lemma 2.4.5. *$sub_t(n, \#t, \#s) = \#s[t/v_n]$ and $sub_f(n, \#t, \#\varphi) = \#\varphi[t/v_n]$ are primitive recursive.*

2.4.2 Proofs and theorems

- A proof is a list of formulas (finite) such that each formula is either an axiom (logical or non-logical) or the formula is the conclusion of the rule whose premisses appears earlier in the list.
- A theorem is the last formula of a proof.
- Examples of logical axioms
  - $\varphi \to (\psi \to \varphi)$
  - $(\varphi \to (\psi \to \theta)) \to ((\varphi \to \psi) \to (\varphi \to \theta))$
  - $\neg\neg\varphi \to \varphi$
  - $\forall v_n.\varphi \to \varphi[t/v_n]$ (t is substitutable for v_n in φ)
  - Axioms for equality "="
- Logical rules:
  - $\dfrac{\varphi \qquad \varphi \to \psi}{\psi}$ (Modus ponens)
  - $\dfrac{\varphi \to \psi}{\varphi \to \forall v_n \psi}$

Suppose we have a proof $\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_n$.
Then we code the proof by $\langle \#\varphi_1, \#\varphi_2, \ldots, \#\varphi_n \rangle$.

2.5 First incompleteness theorem

2.5.1 Preliminaries

We have coded syntax primitive recursively, i.e. terms, formulas etc., so we can talk primitive recursively about free variables, sentences etc. We also know that there is a primitive recursive function $sub_f : \mathbb{N}^3 \to \mathbb{N}$ such that if $\#t$ is a code for a term and $\#\varphi$ is a code for a formula, then $sub_f(n, \#t, \#\varphi) = \#(\varphi[t/v_n])$.

Definition 2.5.1. A theory T is axiomatizable if there is a set of axioms Ax_T such that $\{\#\varphi : \varphi \in \mathsf{Ax}_T\}$ is recursive.

Definition 2.5.2. $\mathrm{Th}(T) = \{\#\varphi : T \vdash, \varphi \text{ is a sentence}\}$.

Proposition 2.5.3. *If T is axiomatizable, then the set of (codes for) proofs in T is a recursive set.*

Definition 2.5.4. $\mathsf{Drv}(T)$ is the set of pairs (n, m) with $n = \#\varphi$ and m is a code for a proof with φ as the last formula.

Lemma 2.5.5. *$\mathsf{Drv}(T)$ is recursive if T is axiomatizable.*

Corollary 2.5.6. *If T is axiomatizable, then $\mathrm{Th}(T)$ is recursively enumerable.*

Proof. $\#\varphi \in \mathrm{Th}(T) \iff$ "φ is a sentence" $\wedge\, \exists m.(\#\varphi, m) \in \mathsf{Drv}(T)$. □

Definition 2.5.7. T is complete if for each sentence φ $T \vdash \varphi$ or $T \vdash \neg\varphi$.

Theorem 2.5.8. *If T is axiomatizable and complete, then T is decidable, i.e.* $\mathrm{Th}(T)$ *is recursive.*

Proof. $\mathrm{Th}(T)$ is recursively enumerable so it suffices to show that the complement is recursively enumerable.

$$m \notin \mathrm{Th}(T) \iff \text{“}m \text{ is not a code for a sentence”} \vee (m = \#\varphi \wedge \#(\neg\varphi) \in \mathrm{Th}(T))$$

Hence the complement is recursively enumerable, and by Proposition 1.4.12 $Th(T)$ is recursive. □

Lemma 2.5.9 (Cantor's diagonal lemma). *Let $P(n, m)$ be a binary relation on bbN. For each n let $P_{(n)} \iff P(n, m)$, so $P_{(n)}$ is a unary relation for each n. Define a unary relation Q by $Q(n) \iff \neg P(n, m)$. Then Q differs from each $P_{(n)}$.*

Proof. If $Q = P_{(n)}$ for some n, then

$$P_{(n)}(n) \iff Q(n) \overset{\text{def.}}{\iff} \neg P(n, n) \overset{\text{def.}}{\iff} \neg P_{(n)}$$

so we have a contradiction. Hence $Q = P_{(n)}$ for all n. □

2.5.2 Assumptions

Suppose T is consistent, axiomatizable and extends P_0. Assume the variables are $v_0, v_1, \ldots$. Define

$$A = \{\#\varphi \in \mathsf{Form} : \mathrm{FV}(\varphi) \subseteq \{v_0\}\}$$

(i.e. A is the set of codes for formulas with v_0 as the only possible free variable). Then A is primitive recursive since $\mathrm{FV}(\varphi)$ is primitive recursive.

Next define f by $f(n) = \#\underline{n}$ (code for the numeral $\underline{n}$). Then f is primitive recursive since

$$f(0) = \langle 0, 0, 0\rangle$$
$$f(n+1) = \langle f(n), 0, 1\rangle.$$

Now define $g\colon \mathbb{N}^2 \to \mathbb{N}$ by $g(n, m) = \mathrm{sub}_f(0, f(n), m)$. Thus g is primitive recursive. Now note that if $\#\varphi \in A$ then

$$g(n, \#\varphi) = \#(\varphi[\underline{n}/v_0]) = \#\varphi(\underline{n}).$$

Let B be defined by $B = \{(n, m) : m \in A \wedge g(n, m) \in \mathrm{Th}(T)\}$, so B is recursively enumerable. Then

$$(n, m) \in B \iff m = \#\varphi(v_0) \text{ and } T \vdash \varphi(\underline{n}).$$

2.5.3 Main argument

Assume that $\mathrm{Th}(T)$ is recursive (to obtain a contradiction). Then B is recursive. Note that if $\#\varphi \in A$ then

$$B(\#\varphi, \#\varphi) \iff T \vdash \varphi(\underline{\#\varphi}).$$

Let $Q(n) \overset{\text{def.}}{\iff} \neg B(n,n)$ (diagonalize). Then Q is recursive. By Theorem 2.3.4 there is a formula $\psi(v_0)$ representing Q. Thus

$$Q(n) \Rightarrow P_0 \vdash \psi(\underline{n}) \Rightarrow T \vdash \psi(\underline{n}) \tag{2.1a}$$

$$\neg Q(n) \Rightarrow P_0 \vdash \neg\psi(\underline{n}) \Rightarrow T \vdash \neg\psi(\underline{n}) \tag{2.1b}$$

So it follows that $T \vdash \psi(\underline{n})$ or $\mathrm{T} \vdash \neg\psi(\underline{n})$. Now

$$Q(\#\psi) \overset{\text{def.}}{\iff} \neg B(\#\psi, \#\psi) \overset{\text{def.}}{\iff} \mathrm{not}(T \vdash \psi(\underline{\#\psi})). \tag{2.2}$$

But $Q(\#\psi) \Rightarrow T \vdash \psi(\underline{\#\psi})$ by (2.1a), so if $Q(\#\psi)$ we obtain a contradiction. Hence $\neg Q(\#\psi)$. By (2.1b) $T \vdash \neg\psi(\underline{\#\psi})$. But by (2.2) not not$(T \vdash \psi(\underline{\#\psi}))$, i.e. $T \vdash \psi(\underline{\#\psi})$. Now since T is consistent and cannot prove both $\psi(\underline{\#\psi})$ and $\neg\psi(\underline{\#\psi})$, so we get a contradiction. We conclude that $\mathrm{Th}(T)$ is not recursive. So the theorem below is proved.

Theorem 2.5.10 (First incompleteness theorem). *If T is a consistent, first-order theory with a decidable set of axioms containing a sufficient amount of arithmetic, then there is a sentence φ such that neither φ nor $\neg\varphi$ is provable from T. So then T is incomplete.*

2.6 Church's theorem and the second incompleteness theorem

Theorem 2.6.1 (Church's theorem). *Predicate calculus is undecidable (at least with the language L). Predicate calculus consists of logical axioms only. That is* $\mathrm{Th}(\emptyset)$ *is not recursive.*

Proof. P_0 has only finitely many axioms $A_1, \ldots, A10$. Let $\varphi \equiv A1 \vee A2 \vee \ldots \vee A10$. Then $P_0 \vdash \psi \iff \varphi \vdash \psi$ for each ψ.

We use the deduction theorem $\varphi \vdash \psi \iff \vdash \varphi \to \psi$:
$P_0 \vdash \varphi$ is undecidable, so $\varphi \vdash \psi$ is undecidable, so $\vdash \varphi \to \psi$ is undecidable. □

Remark 2.6.2. Church's theorem holds if L contains at least one binary relation.

Recall the definition of $\mathsf{Drv}(T)$:

$$\mathsf{Drv}(T) = \{(n,m) : n = \#\varphi \text{ and } m \text{ codes proof } T \vdash \varphi\}.$$

$\mathsf{Drv}(T)$ is recursive, so $\mathsf{Drv}(T)$ is representable by a formula, say $\mathrm{Proof}_t(v,w)$. Now define

$$\mathrm{Con}(T) \equiv \neg\exists w \, \mathrm{Proof}_t(\underline{\#(0=1)}, w),$$

a formula in L saying that T is consistent. Let P be the full Peano arithmetic, i.e. P_0 and all induction axioms.

Theorem 2.6.3 (Second incompleteness theorem). *With the assumptions on T above, then* $\mathrm{Con}(T)$ *is not provable in T.*

Chapter 3

Set theory

Set theory is a universal theory. Functions, relations, etc. are sets. Set theory is axiomatizable, so Gödel's theorems apply:

- Not everything can be proved, nor disproved
- Set theory cannot prove its own consistency

But what is a set?

> *Proposal:* A set is a collection of objects.

But what are objects? Concrete objects, numbers, sets are objects. If x is a set, then $\{x\}$ and $\{\{x\}, \{\{x\}\}\}$ are sets.

Georg Cantor created set theory. He developed arithmetic for infinite objects (ordinals, cardinals).

> *Proposal:* A set is a collection of objects satisfying a given property (extension of a property).

Russell: Consider a set

$$A = \{X \text{ a set } : X \notin X\}.$$

Suppose $A \in A$. Then $A \notin A$. Contradiction. So $A \notin A$. But then $A \in A$, so we have a new contradiction. Conclusion: A must not be a set!

We axiomatize set theory. Zermelo gave axioms for set theory (1908). Fraenkel added one axiom (1922). This is the Zermelo-Fraenkel (ZF) set theory.

3.1 ZF set theory

The language of ZF is $L_{ZF} = \{\in\}$, ZF is a first-order theory with equality. Let V be the universe of sets.

Axiom 0 (Existence of a set). *There is a set.*

Axiom 1 (Extensionality). *Given sets a and b, then $a = b$ if and only if a and b has the same members.*

Axiom 2 (Pairing). *If a and b are sets, then there is a set c such that the members of c are precisely a and b.*

Note 3.1.1. Extensionality tells us that the set c is unique. Define $\{a, b\}$ as the unique c.

Definition 3.1.2. Let a, b be sets. Then define $(a, b) = \{\{a\}, \{a, b\}\}$. (a, b) is a set by pairing.

Proposition 3.1.3. $(a, b) = (a', b') \iff a = a'$ *and* $b = b'$.

Proof. Suppose $a = b$. Then $(a, b) = \{\{a\}, \{a, b\}\} = \{\{a\}\}$. By assumption $\{\{a\}\} = \{\{a'\}, \{a', b'\}\}$. So by extensionality $\{a'\} = \{a', b'\}$. Extensionality again gives $a' = b'$. So we have $\{\{a\}\} = \{\{a'\}\}$. Extensionality gives first $\{a\} = \{a'\}$ and then $a = a'$. The case $a \neq b$ is similar. □

Definition 3.1.4. We define ordered n-tuples inductively by

$$(a) = a$$
$$(a_1, \ldots, a_{n+1}) = ((a_1, \ldots, a_n), a_{n+1}).$$

We cannot yet prove that $\{a, b, c\}$ is a set. For this we need the following axiom.

Axiom 3 (Union). *Let a be a set. Then there is a set b such that*

$$x \in b \iff \exists c \in a. x \in c.$$

Note 3.1.5. Extensionality tells us that b is unique (given a). We define $\bigcup A$ as the unique b.

Definition 3.1.6. $a \cup b = \bigcup\{a, b\}$

Notation 3.1.7. $\bigcup a = \bigcup_{x \in a} x = \bigcup\{x : x \in a\}$

Now $\{a, b, c\}$ is a set, since $\bigcup\{\{a, b\}, \{c\}\} = \{a, b, c\}$.

Definition 3.1.8. Define $z \subseteq x \iff \forall t(t \in z \to t \in x)$.

Axiom 4 (Power set). *Let a be a set. Then there is a set b s.th. b has as members precisely the subsets of a. Formally:*

$$\forall x \forall y \forall z(z \in y \leftrightarrow z \subseteq x).$$

Note 3.1.9. Extensionality tells us that b is unique.

Definition 3.1.10. Given a set a, then $\wp(a)$ is the set of all subsets of a, the power set of a.

Axiom 5. *Given a property P and a set a, then the collection of all $y \in a$ such that $P(y)$ is a set.*

What is a property? A property is a set that can be expressed in the language of ZF.

Axiom 5 (Separation, Comprehension). *Let a be a set. Let $\varphi(x, y_1, \ldots, y_k)$ be a formula of ZF. Let $p_1, \ldots, p_k$ be sets. Then there is a set b such that*

$$x \in b \iff x \in a \text{ and } \varphi(x, p_1, \ldots, p_k) \text{ holds.}$$

Formally:

$$\forall y_1 \ldots \forall y_k \forall x \exists w \forall z[z \in w \leftrightarrow x \in x \wedge \varphi(z, y_1, \ldots, y_k)].$$

Remark 3.1.11. We have infinitely many axioms, one for each formula φ.

Remark 3.1.12. Extensionality tells us that b is unique.

Notation 3.1.13. Denote b by $b = \{x \in a : \varphi(x, p_1, \ldots, p_k)\}$.

Example 3.1.14. Let a, b be sets. Then $a \cap b = \{x \in a : x \in b\}$ is a set.

Example 3.1.15. let a be a set (Axiom 0). Define $\emptyset = \{x \in a : x \neq x\}$. Then $\emptyset$ is a set by separation, the empty set.

Is the universe V a set? Assume yes. Then $A = \{x \in V : x \notin x\}$ is a set. Is $A \in A$? A is a set so $A \in V$. If $A \in A$ then $A \notin A$, so $A \notin A$. But then $A \in A$ (Russell). Thus V is not a set. V is a class.

3.2 Classes

Definition 3.2.1. A class is an extension of a definable property,

$$\mathbf{A} = \{x : \varphi(x, p_1, \ldots, p_k)\},$$

where p_i are sets and φ is a formula in the language. Classes are denoted by boldface letters $\mathbf{A}, \mathbf{B}, \ldots$.

Terminology 3.2.2. A class that is not a set is called a proper class.

Example 3.2.3. V is a class since $V = \{x : x = x\}$.

Example 3.2.4. A set is a class. Suppose a is a set. Then $a = \{x : x \in a\}$, so a is a class.

Definition 3.2.5 (Cartesian product). Let a, b be sets. Then $a \times b = \{(x, y) : x \in a \wedge y \in b\}$, the cartesian product.

Proposition 3.2.6. *Let a, b be sets. Then the cartesian product $a \times b$ is a set.*

Proof. Note that $a \times b$ is a class. Recall that $(x, y) = \{\{x\}, \{x, y\}\}$. So $x \in a, y \in b \Rightarrow x, y \in a \cup b$, a set. Hence $\{x\}, \{x, y\} \in \wp(a \cup b)$, a set. Hence $\{\{x\}, \{x, y\}\} \in \wp\wp(a \cup b)$, a set. Now

$$a \times b = \{(x, y) \in \wp\wp(a \cup b) : x \in a \wedge y \in b\},$$

so it is a set by separation. □

Note 3.2.7. Inductively we can define $a_1 \times a_2 \times \ldots \times a_n$.

Definition 3.2.8. Suppose $\mathbf{A} = \{x : \varphi(x)\}$ and $\mathbf{B} = \{x : \psi(x)\}$. Then

(i) $\mathbf{A} = \mathbf{B} \iff \forall x(\varphi(x) \leftrightarrow \psi(x))$

(ii) $\mathbf{A} \cup \mathbf{B} = \{x : \varphi(x) \vee \psi(x)\}$

(iii) $\mathbf{A} \cap \mathbf{B} = \{x : \varphi(x) \wedge \psi(x)\}$

(iv) $\mathbf{A} \setminus \mathbf{B} = \{x : \varphi(x) \wedge \neg\psi(x)\}$

(v) $\bigcap \mathbf{A} = \{x : \forall y(\varphi(y) \rightarrow x \in y)\}$.

Note 3.2.9. If **A** has at least one set, then $\cap\mathbf{A}$ is a set (by separation).

Definition 3.2.10. **R** is an n-ary class if

$$\mathbf{R} = \{(x_1, \ldots, x_m) : \varphi(x_1, \ldots, x_n, p_1, \ldots, p_k)\}.$$

Definition 3.2.11. A class function **F** is a binary class such that if $(a, b) \in \mathbf{F}$ and $(a, c) \in \mathbf{F}$ then $b = c$.

Notation 3.2.12. If **F** is a class function and a is a set, then $\mathbf{F}(a) = b$ means $(a, b) \in \mathbf{F}$. If **A** is a class, then

$$\mathbf{F}[\mathbf{A}] = \{b : \exists a \in \mathbf{A} : \mathbf{F}(a) = b\},$$

the image of **A** under **F**. Hence $\mathbf{F}[\mathbf{A}]$ is a class.

Axiom 6 (Replacement, by Fraenkel). *If* $\boldsymbol{F}$ *is a class function and* a *is a set, then* $\boldsymbol{F}[a]$ *is a set.*

Axiom 7. *There is an infinite set.*

How to express Axiom 7 in the formal language?

Definition 3.2.13. A set a is inductive if $\emptyset \in a \wedge \forall x(x \in a \to x \cup \{x\} \in a)$.

Definition 3.2.14. Define $0, 1, 2, \ldots$ by

$$\begin{array}{ll} 0 & = \emptyset \\ 1 & = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\} \\ 2 & = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\} \\ \vdots & \vdots \\ n+1 & = n \cup \{n\} = \{0, 1, \ldots, n\}. \end{array}$$

Note 3.2.15. If a is inductive, then $0 \in a, 1 \in a, 2 \in a, \ldots$.

Now, using our definition of an inductive set, we can reformulate Axiom 7.

Axiom 7. *There is an inductive set.*

This is an axiom in the language. Now let $\mathbf{C} = \{a : a \text{ inductive}\}$. Then $\bigcap \mathbf{C}$ is a set (by Note 3.2.9 since $\mathbf{C} \neq \emptyset$).

Note 3.2.16. $\bigcap \mathbf{C}$ is inductive. So $\bigcap \mathbf{C}$ is the smallest inductive set (w.r.t. $\subset$).

Definition 3.2.17. $\omega = \bigcap \mathbf{C}$. In fact $\omega = \{0, 1, 2, \ldots\}$, so in set theory ω plays the role of the natural numbers.

Note 3.2.18. We have de successor function $S \colon \omega \to \omega$, $S(n) = n \cap \{n\} = n + 1$.

Definition 3.2.19. Define (in ω) $n < m \iff n \in m$.

Note 3.2.20. $<$ is the usual order in $\mathbb{N}$.

We can prove all of Peano's axioms in our theory, including induction.

3.3 Well-ordered sets

Definition 3.3.1. Let P be a set and $\leq$ a binary relation on P. $\leq$ is a partial order if for all $x, y, z \in P$

- $x \leq x$ (reflexivity)
- $x \leq y \wedge y \leq x \Rightarrow x = y$ (antisymmetry)
- $x \leq y \wedge y \leq z \Rightarrow z \leq z$ (transitivity).

If this holds, we say $(P, \leq)$ is a poset. $\leq$ is total (linear) if $\forall x, y \in P(x \leq y \vee y \leq x)$.

Examples 3.3.2. $\leq$ on $\mathbb{N}$ and $\leq$ on $\mathbb{Q}$ are total orders. If X is a set, then $\subseteq$ on $\wp(X)$ is a partial order, not a total order.

Notation 3.3.3. $x < y \iff x \leq y \wedge x \neq y$.

Definition 3.3.4. Let $W = (W, \leq)$ be a total order. Then W is a well-order if whenever $X \subseteq W$ such that $X \neq \emptyset$, then X has a least element (a least element in X if for $a \in X$ $(\forall y \in X)(a \leq y)$).

Examples 3.3.5. $(\mathbb{N}, \leq)$ is a well-order. $(\mathbb{Z}, \leq)$ is not a well-order. $([0, 1], \leq)$ is not a well-order since $X = \{\frac{1}{n} : n \in \mathbb{N}\}$ has no least element. If W is finite and $\leq$ is a total order, then $(W, \leq)$ is a well-order.

Theorem 3.3.6. *Let $(W, \leq)$ be a well-order. Suppose $X \subset W$ such that the least element in W is in X and*

$$\forall x(\forall y(y < x \rightarrow y \in X) \rightarrow x \in X).$$

Then $X = W$

Proof. Suppose not. Then $W \neq X$, so $W \setminus X \neq \emptyset$. Let a be least in $W \setminus X$ (since well-order). Note that a is not least the least element in W. Furthermore if $y < a$ then $y \in X$ (since a is least). But then $a \in X$ by second condition. Contradiction. □

Definition 3.3.7. Suppose $(P, \leq)$ and $(Q, \leq')$ are posets. Then

- $f : P \rightarrow Q$ is order preserving if for each $x, y \in P$, $x \leq y \iff f(x) \leq' f(y)$.
- $f : P \rightarrow Q$ is increasing if for each $x, y \in P$, $x < y \iff f(x) <' f(y)$.

Definition 3.3.8. Two well-orders $(P, \leq)$ and $(Q, \leq')$ are isomorphic, $(P, \leq) \simeq (Q, \leq')$, if there is $f \colon P \rightarrow Q$ such that f is 1-1, onto and order preserving.

Proposition 3.3.9. *Let $(W, \leq)$ be a well-order. Let $f : W \rightarrow W$ be increasing. Then $f(x) \geq x$ for each $x \in W$.*

Proof. Suppose not. Then there is x such that $f(x) < x$. W is a well-order, so there is a least a such that $f(a) < a$. Now apply f. Then $f(f(a)) < f(a)$. But $f(a) < a$, so a was not least. Contradiction. □

Corollary 3.3.10. *Let $(W, \leq)$ be a well-order. Then the only isomorphism from W to W is the identity (so $(W, \leq)$ is rigid).*

Proof. Suppose $f\colon W \to W$ is an isomorphism. Thus f^{-1} is also an isomorphism. So $f^{-1}(x) \geq x \quad \forall x \in W$. Then $x = f(f^{-1}(x)) \geq f(x) \Rightarrow f(x) = x$. But $f(x) \geq x$, and hence $f(x) = x$. □

Proposition 3.3.11. *Let $(W_1, \leq_1)$ and $(W_2, \leq_2)$ be well-orders. If $W_1 \simeq W_2$, then the isomorphism is unique.*

Proof. Suppose $f\colon W_1 \to W_2$ and $g\colon W_1 \to W_2$ are isomorphisms. We will show that $f = g$. We know that $g^{-1}\colon W_2 \to W_1$ is an isomorphism, so $g^{-1} \circ f\colon W_1 \to W_1$ is an isomorphism. But by Corollary 3.3.10 $g^{-1} \circ f = \mathrm{id}_{w_1}$, so $g \circ g^{-1} \circ f = g \circ \mathrm{id}_w$ and hence $f = g$. □

Definition 3.3.12. Let $a \in W$. Then $W(a) = \{x \in W : x < a\}$, the initial segment of W.

Proposition 3.3.13. *If $(W, \leq)$ be a well-order, then W is not isomorphic to an initial segment of W.*

Proof. Let $a \in W$ and suppose $f\colon W \to W(a)$ is an isomorphism. Consider $f(a) \in W(a)$. Then $f(a) < a$. But by Proposition 3.3.9 $f(a) \geq a$. Contradiction. □

Corollary 3.3.14. *Let $(W, \leq)$ be a well-order. Then*

$$W(a) \simeq W(b) \Rightarrow a = b.$$

Theorem 3.3.15. *Let $(W_1, \leq_1)$ and $(W_2, \leq_2)$ be well-orders. Then exactly one of the following holds:*

- $W_1 \simeq W_2$
- $W_1 \simeq$ *initial segment of* W_2
- $W_2 \simeq$ *initial segment of* W_1.

Proof sketch. Define

$$f = \{(x, y) \in W_1 \times W_2 : W_1(x) \simeq W_2(y)\}.$$

By Corollary 3.3.14 we get that f is a function. For if $W_1(x) \simeq W_2(y)$ and $W_1(x) \simeq W_2(y')$, then $W_2(y) \simeq W_2(y')$ so $y = y'$. Now f does the job. □

3.4 Ordinals

Let the order type have the following properties: $\mathrm{o.t.}(W_1) = \mathrm{o.t.}(W_2)$ if $W_1 \simeq W_2$ (that is $\mathrm{o.t.}(W) = \{W' : W \simeq W'\}$) and $\mathrm{o.t.}(W_1) < \mathrm{o.t.}(W_2)$ if $W_1 \simeq$ init segment of W_2. We know that $\simeq$ is an equivalence relation. We want to pick precisely one set in each equivalence class. That set will be an ordinal.

Definition 3.4.1. A set a is transitive if $x \in y \in a \Rightarrow x \in a$. Equivalently $y \in a \Rightarrow y \subseteq a$. Equivalently $\bigcup a \subseteq a$.

Note 3.4.2. If x is transitive, then $x \cup \{x\}$ is transitive.

Definition 3.4.3. A set a is an ordinal if it is transitive and $\in$ is a strict well-order on a.

Notation 3.4.4. Let $\alpha, \beta, \gamma, \ldots$ vary over ordinals. Let $\mathbf{On}$ be the class of all ordinals. Say $\alpha < \beta$ means $\alpha \in \beta$.

Examples 3.4.5.

(i) $\emptyset$ is an ordinal.

(ii) $\alpha \in \mathbf{On} \Rightarrow \alpha \cup \{\alpha\} \in \mathbf{On}$

Proof. $\alpha \in y \in \alpha \cup \{\alpha\}$. Then either $y \in \alpha$ or $y = \alpha$. If $y \in \alpha$, then $x \in \alpha$ since α is transitive. If $y = \alpha$, then since $x \in y$ we have $x \in \alpha$. Hence $x \in \alpha \cup \{\alpha\}$. □

Hence $0, 1, 2, \ldots \in \mathbf{On}$, so $\omega \subseteq \mathbf{On}$.

(iii) $\omega \in \mathbf{On}$.

Lemma 3.4.6.

(i) If $\alpha \in \mathbf{On}$ and $\beta \in \alpha$, then $\beta \in \mathbf{On}$

(ii) If $\alpha, \beta \in \mathbf{On}$ and $\alpha \subset \beta$, then $\alpha \in \beta$

(iii) If $\alpha \in \mathbf{On}$ then $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$.

Proof of (i). Suppose $\beta \in \alpha$, $\alpha \in \mathbf{On}$. α is transitive so $\beta \subseteq \alpha$. But α is strictly well-ordered by $\in$, so β is strictly well-ordered by $\in$. We must show that β is transitive. Suppose $x \in y \in \beta$. But $\beta \subseteq \alpha$, so $y \in \alpha$. Hence $x \in y \in \alpha$. α is transitive so $x \in \alpha$.

$y \in \beta \in \alpha$ so $y \in \alpha$. Thus $\{x, y, \beta\} \in \alpha$. $\in$ strictly well-orders α so $\in$ is transitive onα. We have $x \in y \in \beta$. Hence $x \in \beta$ (since $\in$ is transitive on α). □

Proposition 3.4.7. *Some facts about ordinals:*

(i) $\subseteq$ linearly orders $\mathbf{On}$. So $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$.

(ii) $\alpha = \{\beta \in \mathbf{On} : \beta < \alpha\}$

(iii) Let $\boldsymbol{C}$ be a class of ordinals. Then $\bigcap \boldsymbol{C}$ is an ordinal, inf $\boldsymbol{C}$ *(least ordinal in $\boldsymbol{C}$).*

(iv) Let X be a set of ordinals. Then $\bigcup X \in \mathbf{On}$ and $\bigcup X = \sup X$.

Definition 3.4.8. Let $\alpha \in \mathbf{On}$. Then $\alpha + 1 = \alpha \cup \{\alpha\}$ (successor). $\alpha + 1$ is the least ordinal greater than α.

Ordinals comes in three shapes:

- 0, least ordinal,
- $\alpha = \beta + 1$, alpha a successor, or
- α not successor, we say that α is a limit ordinal. In this case $\alpha = \sup\{\beta : \beta < \alpha\}$.

Examples 3.4.9. ω is a limit ordinal, the least limit. Define

$$X = \{\omega + 1, \omega + 1 + 1, \omega + 1 + 1 + 1, \ldots\}.$$

Then $\sup X$ is the least ordinal greater than $\omega + n$ for all $n \in \omega$, so $\sup X = \omega + \omega$.

Proposition 3.4.10. $<$ *well-orders* **On** *and* **On** *is transitive.*

Proposition 3.4.11. **On** *is not a set.*

Proof. Suppose yes. Then **On** is an ordinal. So $\mathbf{On} + 1 \in \mathbf{On}$. But $\mathbf{On} + 1 > \mathbf{On}$. On the other hand $\mathbf{On}+1 \in \mathbf{On}$ so $\mathbf{On}+1 < \mathbf{On}$. Contradiction (Burali-Forti paradox). □

Theorem 3.4.12. *Each well-order* $(W, \leq)$ *is isomorphic to a unique ordinal.*

Theorem 3.4.13 (Transfinite induction). *Let* $\boldsymbol{A}$ *be a class of ordinals (*$\boldsymbol{A} \in \mathbf{On}$*). Suppose*

(i) $0 \in \boldsymbol{A}$,

(ii) $\alpha \in \boldsymbol{A} \Rightarrow \alpha + 1 \in \boldsymbol{A}$,

(iii) If $\alpha > 0$, α *is a limit ordinal, and* $\beta \in \boldsymbol{A}$ *for each* $\beta < \alpha$*. Then* $\alpha \in \boldsymbol{A}$.

Then $\boldsymbol{A} = \mathbf{On}$.

Proof. Suppose not. Then $\mathbf{On} \setminus \mathbf{A} \neq \emptyset$. Let α be the least ordinal in $\mathbf{On} \setminus \mathbf{A}$. By condition (i) $\alpha \neq 0$. Suppose $\alpha = \beta + 1$. So $\beta \in \mathbf{A}$. But by condition (ii) $\beta + 1 \in \mathbf{A}$. Contradiction. Suppose α is a limit. Then $\beta < \alpha \Rightarrow \beta \in \mathbf{A}$. But then by condition (iii) $\alpha \in \mathbf{A}$. Contradiction. □

Recall that a function $f \colon \mathbb{N} \to X$ can be viewed as a sequence in X.

Definition 3.4.14. Let $\alpha \in \mathbf{On}$. Then $f \colon \alpha \to X$ is called an α-sequence. A function $\mathbf{F} \colon \mathbf{On} \to V$ is an **On**-sequence (where V is the universe of sets).

Notation 3.4.15. An α-sequence is denoted by $(a_\beta)_{\beta<\alpha}$ or $\{a_\beta : \beta < \alpha\}$.

Example 3.4.16 (Cumulative hiearchy). Since **On** is inductive we can do recursive definitions on **On**. Define V_α by

$$\begin{aligned} V_0 &= \emptyset \\ V_{\alpha+1} &= \wp(V_\alpha) \\ V_\alpha &= \bigcup \{V_\beta : \beta < \alpha\} \text{ a limit.} \end{aligned}$$

This can be done in set theory. That is, $(V_\alpha)_{\alpha \in \mathbf{On}}$ is an **On**-sequence.

Axiom 8 (Regularity). *Let* $W = \bigcup_{\alpha \in \mathbf{On}} V_\alpha$*. Then* $V = W$ *(*V *is the universe).*

Variant: $\forall x \exists \alpha . x \in V_\alpha$.

Axiom 8 proves that $\in$ is well-founded, i.e. there is no sequence of sets $(x_n)_{n<\omega}$ such that $x_0 \ni x_1 \ni x_2 \ni \ldots$.

3.5 Ordinal arithmetic

Definition 3.5.1. Let α and β be ordinals. Consider the disjoint union of α and β

$$A = (\alpha \times \{0\}) \cup (\beta \times \{1\}).$$

Let

$$(\gamma, i) < (\delta, j) \iff i < j \vee (i = j \wedge \gamma < \delta)$$

be an order on A. Then $<$ is a well-order. Define $\alpha+\beta$ to be the unique ordinal isomorphic to $(A, <)$.

Example 3.5.2. $\alpha + 1$ is the least ordinal greater than α. $1 + \omega = \omega$. $\omega + 1 > \omega$. Hence addition is not commutative.

Definition 3.5.3. Define $<$ on $a \times b$ by

$$(\gamma, \delta) < (\xi, \eta) \iff \gamma < \xi \vee (\gamma = \xi \wedge \delta < \eta.$$

Then $a \cdot b$ is the unique ordinal isomorphic to $(A, <)$.

Example 3.5.4. $\alpha \cdot 2 = \alpha + \alpha$ but $2 \cdot \omega = \omega$, so multiplication is not commutative.

Definition 3.5.5.

$$\begin{cases} \alpha^0 = 1 \\ \alpha^{\beta+1} = \alpha^\beta \cdot \alpha \\ \alpha^\beta = \lim\limits_{\xi<\beta} \alpha^\xi = \sup\limits_{\xi<\beta} \alpha^\xi, \beta \text{ limit.} \end{cases}$$

Example 3.5.6. Let $\omega_0 = \omega$ and $\omega_{n+1} = \omega_n^\omega$. Then let

$$\epsilon_0 = \lim_{n<\omega} \omega_n = \omega^{\omega^{\omega^{\omega^{\cdots}}}}.$$

Theorem 3.5.7. *Peano arithmetic P is consistent iff we can do transfinite induction on ϵ_0 from the above example.*

Definition 3.5.8. A class function $\mathbf{F}\colon \mathbf{On} \to \mathbf{On}$ is normal if

(i) $\alpha < \beta \Rightarrow \mathbf{F}(\alpha) < \mathbf{F}(\beta)$ ($\mathbf{F}$ increasing)

(ii) If α is a limit ordinal, then $F(\alpha) = \sup\{\mathbf{F}(\beta) : \beta < \alpha\} = \sup\limits_{\beta<\alpha} \mathbf{F}(\beta)$ ($\mathbf{F}$ continuous).

Proposition 3.5.9. *Let $\boldsymbol{F}$ be normal. Then there are arbitrarily large fixpoints (i.e. α such that $\boldsymbol{F}(\alpha) = \alpha$).*

Proof. $\mathbf{F}$ is increasing, so $\mathbf{F}(\alpha) \geq \alpha$ by Proposition 3.3.9. Now suppose we are given an arbitrary β. We want to find $\alpha \geq \beta$ such that $\mathbf{F}(\alpha) = \alpha$. Consider $\mathbf{F}(\beta)$. We know that $\mathbf{F}(\beta) \geq \beta$. If $\mathbf{F}(\beta) = \beta$ we are done. Otherwise define

$$\begin{aligned} &\alpha_0 = \beta \\ &\alpha_1 = \mathbf{F}(\alpha_0) \\ &\vdots \\ &\alpha_{n+1} = \mathbf{F}(\alpha_n) \\ &\vdots \end{aligned}$$

So we get a chain $\alpha_0 < \alpha_1 < \ldots$. Set $\alpha = \sup_n \alpha_n$, α is a limit ordinal. Now by continuity

$$\mathbf{F}(\alpha) = \sup_{n<\omega} \mathbf{F}(\alpha_n) = \sup_{n<\omega} \alpha_{n+1} = \sup_{n<\omega} \alpha_n = \alpha,$$

so α is a fixpoint and $\alpha > \beta$. $\square$

3.6 Axiom of choice

Axiom 9 (Axiom of choice, AC). *Let $\mathcal{F}$ be a family of non-empty sets. Then there is a function $f\colon \mathcal{F} \to \bigcup \mathcal{F}$ such that for each $X \in \mathcal{F}$, $f(X) \in X$.*

Remark 3.6.1.

- The f is called a choice function.
- $ZFC = ZF + AC$.

Axiom 3.6.2 (Well-ordering axiom, WO). *Every set can be well-ordered.*

$$\forall a \exists < (< \textit{ binary relation}, (a,<) \textit{ well-order}).$$

Theorem [ZF] 3.6.3. $AC \leftrightarrow WO$.

Proof. Assume (WO). Let $\mathcal{F}$ be a family of non-empty sets. Consider $\bigcup \mathcal{F}$, a set. Let $<$ be a well-order of $\bigcup \mathcal{F}$ (here we used (WO)). Define $f\colon \mathcal{F} \to \bigcup \mathcal{F}$ by letting $f(x)$ be the least $y \in x$ with respect to $<$. f is a set by separation.

Assume (AC). Given a set a we well-order it. Let f be a choice function for $\wp(a) \setminus \{\emptyset\}$ (exists by (AC)). Now define a class function $\mathbf{G}\colon \mathbf{On} \to a \cup \{a\}$ by

$$\mathbf{G}(\alpha) = \begin{cases} f(a \setminus \{\mathbf{G}(\beta) : \beta < \alpha\}) & \text{if } \mathbf{G}(\beta) : \beta < \alpha\} \neq \emptyset \\ a & \text{if } \mathbf{G}(\beta) : \beta < \alpha\} = \emptyset \end{cases}$$

This is a valid recursive definition.

Suppose that we know that there is an α such that $\mathbf{G}(\alpha) = a$. For $x, y \in a$ let $x < y \iff \exists \gamma, \delta < \alpha (\mathbf{G}(\gamma) = x \wedge \mathbf{G}(\delta) = y \wedge \gamma < \delta)$. Then $<$ is a well-order on a, since $\gamma, \delta < \alpha$ and $\mathbf{G}$ is 1-1 and onto a.

Now we have to prove that there is an α such that $\mathbf{G}(\alpha) = a$. Suppose not. Then $\mathbf{G}\colon \mathbf{On} \to a$. Now $\mathbf{G}$ is 1-1 so

$$b = \{x \in a : \exists \alpha (\mathbf{G}(\alpha) = x)\}$$

is a set by separation. $\mathbf{G}^{-1} : b \to \mathbf{On}$ is an onto class function. But now by replacement, $\mathbf{G}^{-1}[b]$ is a set, that is $\mathbf{On}$ is a set. Contradiction. □

Lemma 3.6.4 (Zorn's lemma, ZL). *Let $(P, \leq)$ be a partial order. Suppose every chain in P has an upper bound. Then P has a minimal element.*

Remark 3.6.5. A chain is a linearly (total) ordered subset. An upper bound of $A \subseteq P$ is an a such that $\forall x \in A (x \leq a)$. A element a is maximal in$P$ if $a \leq x \Rightarrow a = x$ (or $\neg \exists x (a < x)$).

Theorem [ZF] 3.6.6. *(AC)$\leftrightarrow$(ZL).*

Definition 3.6.7.

(i) A set a is countable if a is finite or there is a bijection $f\colon \omega \to a$.

(ii) A set a is finite if for some $n \in \omega$ there is a bijection $f\colon n \to a$.

Axiom 3.6.8 (Countable axiom of choice, CAC). *Each countable family of non-empty sets has a choice function.*

Remark 3.6.9. (CAC) is not provable in ZF. (AC) is much stronger than (CAC).

3.7 Cardinal numbers

Cardinals measure the size of a set.

Definition 3.7.1. We define a relation between sets. Let X, Y be sets.

(i) $|X| = |Y| \iff \exists f\colon X \to Y$ such that f is a bijection.

(ii) $|X| \leq |Y| \iff \exists f\colon X \to Y$ such that f is one-to-one.

Theorem [ZF] 3.7.2 (Schröder-Bernstein theorem). *If $|X| \leq |Y|$ and $|Y| \leq |X|$ then $|X| = |Y|$.*

But what should $|X|$ itself mean? The relation is reflexive, symmetric and transitive. We could say that $|X| = \{Y : |Y| = |X|\}$. The problem is that $|X|$ then is a proper class.

We work in ZFC (i.e. ZF+AC). We know that for each set X there is $\alpha \in \mathbf{On}$ such that $f\colon \alpha \to X$ is a bijection. That is because X can be well-ordered by say $\leq$. Then $(X, \leq) \simeq \alpha$ for some $\alpha \in \mathbf{On}$, the isomorphism is witnessed by an order preserving bijection.

Definition 3.7.3.

(i) $|X|$ is the least $\alpha \in \mathbf{On}$ such that $|X| = |\alpha|$.

(ii) $\alpha \in \mathbf{On}$ is a cardinal if $|\alpha| = \alpha$.

Notation 3.7.4. $\kappa, \lambda, \mu, \ldots$ vary over cardinals.

Examples 3.7.5.

(i) Each $n \in \omega$ is a cardinal.

(ii) ω is a cardinal.

(iii) Let $\beta \in \mathbf{On}, \beta \geq \omega$. Is $\beta + 1$ a cardinal? Let f be a map that sends $\beta + 1$ to 0, $0 \mapsto 1, 1 \mapsto 2, \ldots, n \mapsto n + 1$. Then f is a bijection, so $|\beta| = |\beta + 1|$. But $\beta + 1$ is not least so it is not a cardinal.

Lemma 3.7.6. *κ is a cardinal if and only if $(\forall\alpha < \kappa)(|\alpha| \neq |\kappa|)$ if and only if $(\forall\alpha < \kappa)$(there is no one-to-one $f\colon \kappa \to \alpha$) if and only if $(\forall\alpha < \kappa)$(there is no onto $f\colon \alpha \to \kappa$).*

Theorem 3.7.7 (Cantor's theorem). *For each set X,*

$$|X| < |\wp(X)|.$$

It follows that $|\wp(\omega)| > \omega$, so we have at least infinitely many cardinals.

Proof. First show $|X| \leq |\wp(X)|$. Define $f\colon X \to \wp(X)$ by $f(a) = \{a\}$. Clearly f is one-to-one.

Now suppose $|X| = |\wp(X)|$. Let $f\colon X \to \wp(X)$ be onto. Let $Y = \{a \in X : a \notin f(a)\}$. Note that Y is a set. Note further that $Y \subseteq X$ so $Y \in \wp(X)$. Thus there is $a \in X$ such that $f(a) = Y$. Is $a \in f(a)$? If $a \in f(a)$ then $a \notin f(a)$ by definition. Contradiction, so $a \notin f(a)$. But then $a \in f(a)$ by definition, so we get a new contradiction. Hence f is not onto and hence $|X| \neq |\wp(X)|$. □

Lemma 3.7.8. *Suppose X is a set of cardinals. Then* $\sup X$ *is a cardinal.*

Proof. Let $\alpha = \sup(X)$. Suppose $f\colon \alpha \to \beta$ is a bijection for some $\beta < \alpha$. We want a contradiction. We know there is $\kappa \in X$ such that $\beta < \kappa \leq \alpha$. But then

$$\kappa = |\kappa| = |f[\kappa]| \leq |f[\alpha]| = |\beta| < \kappa,$$

so we get a contradiction. □

Definition 3.7.9. Let κ be a cardinal. Then κ^+ denotes the least cardinal greater than κ. κ^+ is the successor cardinal of κ. κ is a limit cardinal if κ is not a successor cardinal.

Definition 3.7.10. Define $\aleph\colon \mathbf{On} \to \mathbf{On}$ by recursion:

$$\begin{cases} \aleph(0) = \aleph_0 = \omega_0 = \omega \\ \aleph(\alpha+1) = \aleph_{\alpha+1} = \omega_{\alpha+1} = \aleph_\alpha^+ \\ \aleph(\alpha) = \sup\{\aleph_\beta : \beta < \alpha\}, \alpha \text{ limit.} \end{cases}$$

$\aleph$ enumerates all infinite cardinals.

Note 3.7.11. $\aleph$ is a normal class function. Hence there are arbitrarily large α such that $\aleph_\alpha = \alpha$.

3.8 Cardinal arithmetic

Definition 3.8.1. Let κ, λ be cardinals. Then

(i) $\kappa + \lambda = |\kappa \mathbin{\dot\cup} \lambda| = |\kappa \times \{0\} \cup \lambda \times \{1\}|$

(ii) $\kappa \cdot \lambda = |\kappa \times \lambda| = |\{(\alpha, \beta) : \alpha \in \kappa, \beta \in \lambda\}|$

(iii) $\kappa^\lambda = |\{f : (f\colon \lambda \to \kappa)\}|$

Note 3.8.2. The above definition generalizes the notions for finite cardinals.

Note that the operations are increasing. We shall prove that if $\kappa \geq \aleph_0$, then $\kappa \cdot \kappa = \kappa$. Define a well-ordering on $\mathbf{On} \times \mathbf{On}$ by

$$\begin{aligned} (\alpha, \beta) < (\gamma, \delta) \iff \quad & \max(\alpha, \beta) < \max(\delta, \gamma) \\ & \vee(\max(\alpha, \beta) < \max(\delta, \gamma) \wedge \alpha < \gamma) \\ & \vee(\max(\alpha, \beta) < \max(\delta, \gamma) \wedge \alpha = \gamma \wedge \beta < \delta) \end{aligned}$$

Definition 3.8.3. Define the function $\Gamma\colon \mathbf{On} \to \mathbf{On}$ by letting $\Gamma(\alpha, \beta)$ be the unique ordinal isomorphic to $\{(\gamma, \delta) : (\gamma, \delta) < (\alpha, \beta)\}$.

For example, $\Gamma(0, \omega) = \omega$. Let $\Gamma[a \times b]$ be the image of $a \times b$ under Γ. Note that $\Gamma[\alpha \times \beta]$ is an ordinal, and that $\alpha \mapsto \Gamma[\alpha \times \alpha]$ is increasing. Note also that Γ is one-to-one.

Theorem 3.8.4. *If $\kappa \geq \aleph_0$, then $\kappa \cdot \kappa = \kappa$.*

Proof. It suffices to show that $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$ for all $\alpha \in \mathbf{On}$. We do this by induction on the ordinals. Clearly true for $\alpha = 0$ since $\Gamma[\omega \times \omega] = \omega$.

We know that $\Gamma[\omega_\alpha \times \omega_\alpha] \supseteq \omega_\alpha$. The induction hypothesis is that for each $\xi < \alpha, \aleph_\xi \cdot \aleph_\xi = \aleph_\xi$. If $\omega_\alpha = \Gamma[\omega_\alpha \times \omega_\alpha]$ we are done since Γ is one-to-one. Suppose $\omega_\alpha \subsetneq \Gamma[\omega_\alpha \times \omega_\alpha]$. Thus there is $(\gamma, \delta) \in \omega_\alpha \times \omega_\alpha$ such that $\Gamma(\gamma, \delta) = \omega_\alpha$. ω_α is a limit ordinal since it is a cardinal. Choose ξ such that $\gamma, \delta < \xi < \omega_\alpha$. Thus $\Gamma[\xi \times \xi] \supset \omega_\alpha$. But then $|\xi \times \xi| \geq \omega_\alpha = \aleph_\alpha$. But $|\xi \times \xi| = |\xi| \cdot |\xi|$. $\xi < \omega_\alpha$ so $|\xi| < \omega_\alpha$. Then by induction hypothesis $\omega_\alpha = \Gamma[\omega_\alpha, \omega_\alpha]$. Hence $\omega_\alpha = \omega_\alpha \cdot \omega_\alpha$. □

Corollary 3.8.5. *Let* $\kappa, \lambda \geq \aleph_0$. *Then* $\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda)$.

Proof. $\max(\kappa, \lambda) \geq \kappa + \lambda \geq \kappa \cdot \lambda \geq \max(\kappa, \lambda) \cdot \max(\kappa, \lambda) = \max(\kappa, \lambda)$. □

Note 3.8.6. $|\{f : \kappa \to 2 = \{0, 1\}\}| = |\wp(\kappa)|$. So by Cantor's theorem $\kappa < 2^\kappa$.

Hypothesis 3.8.7 (Continuum Hypothesis, CH). $2^{\aleph_0} = \aleph_1$.

Gödel proved that $\text{Con}(ZFC) \Rightarrow \text{Con}(ZFC{+}CH)$. Cohen proved that $\text{Con}(ZFC) \Rightarrow \text{Con}(ZFC + \neg CH)$.

Hypothesis 3.8.8 (Generalized Continuum Hypothesis, GCH). $2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

Theorem 3.8.9. *Suppose* κ, λ *are cardinals,* $2 \geq \kappa \geq \lambda$ *and* λ *infinite. Then* $\kappa^\lambda = 2^\lambda$.

Proof. Clearly $\kappa^\lambda \geq 2^\lambda$ since $2 \leq \kappa$. By definition

$$\kappa^\lambda = |\{f : (f\colon \lambda \to \kappa)\}| = |F|.$$

Note that $F \subseteq \wp(\lambda \times \kappa)$. Hence

$$\kappa^\lambda = |F| \leq |\wp(\kappa \times \lambda)| = 2^{|\kappa \times \lambda|} = 2^{\kappa \cdot \lambda} = 2^\lambda.$$

□

Theorem 3.8.10. *Suppose* $\{A_i : i \in I\}$ *is a family of sets indexed by* I *such that* $|A_i| < \kappa$ *for each* i *and* $|I| < \kappa$. *Then*

$$\left| \bigcup_{i \in I} A_i \right| \leq \kappa.$$

In particular, a countable union of countable sets is countable.

Proof. $\left|\bigcup_{i \in I} A_i\right| \leq \left|\dot{\bigcup}_{i \in I} A_i\right| = \left|\bigcup_{i \in I} A_i \times \{i\}\right| \leq \left|\bigcup_{i \in I} \kappa \times \{i\}\right| = |\kappa \times I| \leq |\kappa \times \kappa| = \kappa \cdot \kappa = \kappa$. □

Examples 3.8.11.

(i) $|\mathbb{Z}| = \aleph_0$

(ii) $|\mathbb{Q}| = \aleph_0$

(iii) $|\{\text{algebraic numbers}\}| = \aleph_0$

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

(v) $|\mathbb{C}| = 2^{\aleph_0}$

(vi) $|\{f : (f\colon \mathbb{R} \to \mathbb{R} \text{ continuous}\}| = 2^{\aleph_0}$

(vii) $|\{f : (f\colon \mathbb{R} \to \mathbb{R}\}| = (2^{\aleph_0})^{2^{\aleph_0}} = 2^{\aleph_0 \cdot 2^{\aleph_0}} = 2^{2^{\aleph_0}}$

Chapter 4

Model theory

4.1 Basic definitions and theorems

Definition 4.1.1. A mathematical structure is a tuple

$$A = (A; \mathcal{R}_A; \mathcal{F}_A; \mathcal{C}_A),$$

where $\mathcal{R}_A$ is a set of relations, $\mathcal{F}_A$ is a set of functions $A^n \to A$ and $\mathcal{C}_A$ is a set of constants.

Examples 4.1.2.

(i) $\mathfrak{N} = (\mathbb{N}; \{<\}; \{+, \cdot, S\}; \{0\})$. We usually write $(\mathbb{N}; <; +, \cdot, S; 0)$.

(ii) $(\mathbb{N}, <)$.

(iii) $G = (\mathbb{N}, \cdot)$, a group.

Definition 4.1.3. A signature or language is a triple

$$L = (\mathcal{R}, \mathcal{F}, \mathcal{C}),$$

where $\mathcal{R}$ is a set of relation symbols with an arity, $\mathcal{F}$ is a set of function symbols with an arity and $\mathcal{C}$ is a set of constant symbols.

A structure A is an L-structure if there is a one-to-one correspondence $R^A \leftrightarrow R$ for $R \in \mathcal{R}$, where R^A is a relation in A, and similar for $\mathcal{F}$ and $\mathcal{C}$ (respects arities).

Given a language L we can define terms, atomic formulas and formulas. If $|L| \leq \aleph_0$, then $|\text{formulas over } L| \leq \aleph_0$.

Definition 4.1.4 (Interpretation of terms in A). Let L be a language and A be an L-structure. Let $t(\vec{x})$ be a term (i.e. variables of t are among $x_1, \dots, x_n$), and let $\vec{a} = (a_1, \dots, a_n) \in A^n$.

(i) If $t \equiv x_i$, then $t(\vec{a})^A = a_i$.

(ii) If $t = c \in \mathcal{C}$, then $t(\vec{a})^A = c^A$.

(iii) If $t = F(t_1, \dots, t_k)$, then $F(t_1, \dots, t_k)(\vec{a}) = F^A(t_1(\vec{a})^A, \dots, t_k(\vec{a})^A)$.

Definition 4.1.5 (Truth of $\varphi(\vec{a})$ in A, Tarski). Let L be a language and A be an L-structure. Let φ be a formula in L.

(i) If $\varphi \equiv t_1 = t_2$, then $A \models \varphi(\vec{a}) \iff t_1^A(\vec{a}) = t_2^A(\vec{a})$.

(ii) If R is a relation symbol in $\mathcal{R}$, then $A \models R(\vec{a}) \iff R^A(\vec{a})$.

(iii) $A \models \varphi(\vec{a}) \wedge \psi(\vec{a}) \iff A \models \varphi(\vec{a})$ and $\psi(\vec{a})$.

$\vdots$

(iv) $A \models \exists x \varphi(x, \vec{a}) \iff$ there is $b \in A$such that $A \models \varphi(b, \vec{a})$.

Recall that a sentence is a formula with no free variables.

Theorem 4.1.6 (Completeness theorem). *A set of sentences T is consistent if and only if T has a model, i.e. there is an L-structure A such that $A \models T$ (i.e. $A \models \varphi$ for all $\varphi \in T$).*

Definition 4.1.7. A theory is a set of sentences.

Theorem 4.1.8 (Compactness theorem). *A theory T has a model if and only if every finite $T' \subseteq T$ has a model.*

Proof. ($\Rightarrow$) is trivial.
($\Leftarrow$) Prove the contrapositive. Suppose T does not have a model. By completeness theorem, T is inconsistent. Thus $T \vdash \bot$. Note that a proof is a finite object. So only finitely many φ from T goes into the proof. Let T' be the set of formulas φ that is a part of the proof. Hence $T' \vdash \bot$ (same proof). Then T has no model by completeness. □

Theorem 4.1.9 (Löwenheim-Skolem theorem). *Let L be a countable language and let T be a theory. If T has an infinite model, then T has a countable model.*

Theorem 4.1.10 (Lindström's theorem). *If $\mathcal{L}$ is a logic for which the compactness theorem and Löwenheim-Skolem theorem holds, then $\mathcal{L}$ is contained in first order logic.*

Example 4.1.11. Let $\mathbb{N} = (\mathbb{N}, <, +, \cdot, S, 0)$, an L-structure. Let

$$\mathrm{Th}(\mathbb{N}) = \{\varphi : \varphi \text{ is an } L\text{-sentence and } \mathbb{N} \models \varphi\},$$

a consistent set of formulas. Note that $\mathrm{Th}(\mathbb{N})$ is complete, i.e. for each sentence φ $\mathrm{Th}(\mathbb{N}) \vdash \varphi$ or $\mathrm{Th}(\mathbb{N}) \vdash \neg\varphi$. $\mathrm{Th}(\mathbb{N}) \vdash \varphi \iff \mathbb{N} \models \varphi$. Expand the language L with a new constant symbol c to get L'. Add sentences $\{0 < c, 1 < c, 2 < c, \ldots\}$ (where $1 = S(0)$ etc.).

Let $T = P \cup \{0 < c, 1 < c, 2 < c, \ldots\}$. Suppose $T' \subseteq T$ be finite. Then T' has a model. In T' there are only finitely many terms and hence there is a number $n \in \mathbb{N}$ such that if t is a term appearing in T', then $t^{\mathbb{N}} < n$.

Now interpret c as n. Let $\mathbb{N}' = (\mathbb{N}, <, +, \cdot, S, 0, n)$. Compactness gives a model for P. let $\mathfrak{M}$ be the new model. Note that $n \in \mathbb{N} \Rightarrow n < c^{\mathfrak{M}}$.

Suppose A is an L-structure. Suppose that $X \subseteq A$. We want to require X to be an L-structure with relations, operations, constants inherited from A. For this we require that each c^A is in X. Furthermore, suppose $F \in \mathcal{F}$, F is n-ary. Then if $\vec{a} = (a_1, \ldots, a_n) \in X^n$ we require $F^A(\vec{a}) \in X$ (i.e. X is closed under each F^A). Note that we need not worry about relations.

Definition 4.1.12. $X \subseteq A$ is a substructure if the following holds:

(i) Each c^A is in X.

(ii) Suppose $F \in \mathcal{F}$, F is n-ary. Then if $\vec{a} = (a_1, \ldots, a_n) \in X^n$ we require $F^A(\vec{a}) \in X$.

Definition 4.1.13. Suppose $X \subseteq A$. Then $\langle X \rangle_A$ is defined to be the substructure generated by X, i.e. the least (with respect to $\subseteq$) Y such that $Y \supseteq X$.

Example 4.1.14. Let $X \subseteq A$, where A is an L-structure. We want to construct $\langle X \rangle_A$.

First method: Let

$$\langle X \rangle_A = \bigcap \{Y : X \subseteq Y \text{ and } Y \text{ is a substructure of } A\}.$$

Note that this is an impredicative definition.

Second method: Define $\langle X \rangle_A$ in stages. Let $X_0 = X \cup \{c^A : c \in \mathcal{C}\}$. Suppose X_n is defined. Then define

$$X_{n+1} = X_n \cup \{F^A(\vec{a}) : F \in \mathcal{F}, \vec{a} \in X_n\}.$$

Now let

$$\langle X \rangle_A = \bigcup_{n=1}^{\infty} X_n.$$

Suppose $a_1, \ldots, a_n \in \langle X \rangle_A$. Then $a_1, \ldots, a_n \in X_k$ for some k. Hence $F^A(\vec{a}) \in X_{k+1} \subseteq \langle X \rangle_A$, so $\langle X \rangle_A$ is a substructure.

Suppose A is a substructure of B, $R \in \mathcal{F}$ and $\vec{a} \in A$. Then

$$A \models R(\vec{a}) \iff B \models R(\vec{a}).$$

But suppose $B \models \exists x \varphi(x)$. Thus there is $b \in B$ such that $B \models \varphi(b)$. This does not imply that $A \models \exists x \varphi(x)$, since there may not be a witness in A.

Definition 4.1.15. Let A, B be L-structures. A is elementary equivalent to B, $A \equiv B$, if for each L-sentence φ

$$A \models \varphi \iff b \models \varphi$$

(so we cannot distinguish A, B via language).

Proposition 4.1.16. *$A \simeq B \Rightarrow A \equiv B$, but not conversely.*

Definition 4.1.17. Let A, B be L-structures. Then A is an elementary substructure of B, $A \preccurlyeq B$, if A is a substructure of B and for each L-formula $\varphi(\vec{x})$ and each tuple $\vec{a} \in A$

$$A \models \varphi(\vec{a}) \iff B \models \varphi(\vec{a}).$$

Example 4.1.18. Let $L = \{<\}, A = (\mathbb{N} \setminus \{0\}, <)$ and $B = (\mathbb{N}, <)$. Clearly A is a substructure of B. Note also that $A \simeq B$ by $n \mapsto n - 1$. Consider the formula $\varphi(x) = \forall y(x < y \vee x = y)$. Then $A \models \varphi(1)$ but $B \not\models \varphi(1)$.

4.2 Non-standard analysis

Let $\mathbb{R}$ be the real numbers. $\mathbb{R}$ is characterized by the following properties:

- $\mathbb{R}$ is an archimedian ordered field without least or greatest element.
- $\mathbb{R}$ is separable, i.e. there is a countable dense subset (in each interval (a, b), $a < b$ there is an element of the set, $\mathbb{Q}$ is such a set).
- If $A \subseteq \mathbb{R}$ and A is bounded from above, then $\sup A$ exists.

Note that the last "axiom" is a second order axiom, since it varies over all sets of reals.

We want to construct $\mathbb{R}^*$ such that $\mathbb{R} \preccurlyeq \mathbb{R}^*$ such that whatever is true in $\mathbb{R}$ (expressible in a first-order language) is also true of $\mathbb{R}^*$.

Let $L_{\mathbb{R}}$ be the following language:

- For each real $r \in \mathbb{R}$, a constant symbol $\bar{r}$.
- For each partial n-ary function f on $\mathbb{R}$, an n-ary function symbol $\bar{f}$.
- For each n-ary relation R on $\mathbb{R}$, an n-ary relation symbol $\bar{R}$.

Clearly $\mathbb{R}$ is an $L_{\mathbb{R}}$-structure where $\bar{r}^{\mathbb{R}} = r, \bar{f}^{\mathbb{R}} = f, \bar{R}^{\mathbb{R}} = R$. So

$$\mathrm{Th}(\mathbb{R}) = \{\varphi : \varphi \text{ is an } L_{\mathbb{R}}\text{-sentence}, \mathbb{R} \models \varphi\}$$

is a complete theory.

Let c be a new constant symbol, i.e. $c \notin L_{\mathbb{R}}$. Let

$$T = \mathrm{Th}(\mathbb{R}) \cup \{\bar{0} < c, \bar{1} < c, \bar{2} < c, \ldots\}.$$

Compactness tells us that T has a model if and only if every finite subset of T has a model. Given a finite subset $T_0 \subseteq T$ let n be largest such that $\bar{n} < c$. $\mathbb{R}$ is a model of T_0 by interpreting c as some $r \in \mathbb{R}$ such that $n < r$. Hence $\mathbb{R}$ is a $(L_{\mathbb{R}} \cup \{c\})$-structure and $\mathbb{R} \models T_0$. Compactness tells us that T has a model. let the model be $\mathbb{R}^*$. Note that $\mathbb{R}^*$ is not unique, but $\mathbb{R}$ is unique up to isomorphism.

What does $\mathbb{R}^*$ look like? Suppose $f \colon \mathbb{R} \to \mathbb{R}$. Then $\bar{f} \in L_{\mathbb{R}}$, so $\bar{f}$ has an interpretation $\bar{f}^{\mathbb{R}^*} : \mathbb{R}^* \to \mathbb{R}^*$, which is denoted f^*. Hence every n-ary function f on $\mathbb{R}$ gives rise to an n-ary function f^* on $\mathbb{R}^*$. Whatever (as long as expressed in the first-order language $L_{\mathbb{R}}$) holds true for f on $\mathbb{R}$ is also true for f^* on $\mathbb{R}^*$. Note that c is not a part of the language.

The same is true for each relation R on $\mathbb{R}$, which gives rise to R^* on $\mathbb{R}^*$.

Example 4.2.1. $\mathbb{N} \subseteq \mathbb{R}$ and $\mathbb{N}^* \subseteq \mathbb{R}^*$. $\mathbb{N}^*$ is a non-standard model of arithmetic.

Suppose $r_1, r_2 \in \mathbb{R}$ and $f(r_1) = r_2$. Then $\mathbb{R} \models \bar{f}(\bar{r}_1) = \bar{r}_2$ so $\mathbb{R}^* \models \bar{f}(\bar{r}_1) = \bar{r}_2$, so $f^*(\bar{r}_1^{\mathbb{R}^*}) = \bar{r}_2^{\mathbb{R}^*} = r_2$. But $\bar{r}_1^{\mathbb{R}^*} = r_1$, so $f^*(r_1) = r_2$. Hence f^* restricted to $\mathbb{R}$ is f, f^* is an extension of f. Usually we write f for both f and f^*. Similar for relations.

Example 4.2.2. $<$ is a relation on $\mathbb{R}$. We have a corresponding relation $<^*$ on $\mathbb{R}^*$. If $r_1, r_2 \in \mathbb{R}$, then $r_1 < r_2$ (in $\mathbb{R}$) $\iff$ $r_1 <^* r_2$ (in $\mathbb{R}^*$). Again we do not write the star.

Now we have $\mathbb{R}^* \preccurlyeq \mathbb{R}$ and $\mathbb{R}$ has an infinite element (i.e. $a \in \mathbb{R}^*$ and $a > r$ for each $r \in \mathbb{R}$). Let $a \in \mathbb{R}^*$ be infinite and positive. Then $\frac{1}{a} \in \mathbb{R}^*$. But $0 < r < a \Rightarrow 0 < \frac{1}{a} < \frac{1}{r}$. Since a infinite, $a > r \; \forall r \in \mathbb{R}$. Hence $0 < \frac{1}{a} < \frac{1}{r}$.

Definition 4.2.3.

(i) $\mathbb{R}^*_f = \{a \in \mathbb{R}^* \big| \exists r \in \mathbb{R} : |a| < r\}$

(ii) $\mathbb{R}^*_i = \{a \in \mathbb{R}^* \big| |a| < \frac{1}{n} \text{ for each } n \in \mathbb{N}\}$

Definition 4.2.4. Let $a, b \in \mathbb{R}^*$. Then $a \simeq b$ if $|a - b| \in \mathbb{R}^*_i$.

Note 4.2.5. If $a \simeq b$ and $b \simeq c$, then $a \simeq c$, since $|a-c| = |a-b+b-c| \leq |a-b|+|b-c|$. Infinitesimals (elements in $\mathbb{R}^*_i$) are closed under addition and multiplication.

Proposition 4.2.6. *For each $a \in \mathbb{R}^*_f$ there is a unique $r \in \mathbb{R}$ such that $a \simeq r$ (r is denoted by* $\operatorname{std}(a)$*).*

Proof. Suppose $r_1, r_2 \in \mathbb{R}$ such that $r_1 \simeq a \simeq r_2$. Then $r_1 \simeq r_2$, and hence $|r_1 - r_2| < \frac{1}{n}\ \forall n \in \mathbb{N}$. Given $a \in \mathbb{R}^*_f$. Let $r_0 = \inf\{r \in \mathbb{R} : a \leq r\}$. Note that the set is a bounded subset of $\mathbb{R}$, so r_0 exists by completeness $(\sup, \inf)$ of $\mathbb{R}$. Now $a < r_0 \vee a = r_0 \vee r_0 < a$.

Suppose $a = r_0$, then we are done. Suppose $r_0 < a$. Then$r_0 + \frac{1}{n} > a$, so $\frac{1}{n} > a - r_0 > 0$ is true for each $n \in \mathbb{N}$. Hence $a - r_0 \in \mathbb{R}^*_i$ so $a \simeq r_0$. Similar for the case $a < r_0$. □

Consider a sequence $(S_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$. This is a function $S : \mathbb{N} \to \mathbb{R}$. It gives rise ro a function $S^* : \mathbb{N}^* \to \mathbb{R}^*$ such that for $n \in \mathbb{N}$, $S^*(n) = S(n)$. Note that $\mathbb{N}^*$ contains an infinite natural number.

Theorem 4.2.7. *A sequence $(S_n)_{n\in\mathbb{N}}$ is bounded (in $\mathbb{R}$) if and only if $S_\omega \in \mathbb{R}^*_f$ for each $\omega \in \mathbb{N}^* \setminus \mathbb{N}$, where $S_\omega = S(\omega)$.*

Proof. Suppose (S_n) is bounded. Thus $\exists r \in R$ such that $\forall n \in \mathbb{N} : |S_n| < r$. Let $\bar{r}$ be a name for such r. Then

$$\mathbb{R} \models \forall x(\bar{\mathbb{N}}(x) \to |\bar{S}(x)| < \bar{r}).$$

Thus $\mathbb{R}^*$ is a model of the same formula. That is, $\omega \in \mathbb{N}^* \Rightarrow |S_\omega| < r$.

Suppose $S_\omega \in \mathbb{R}^*_f$ for each $\omega \in \mathbb{N}^* \setminus \mathbb{N}$. let $a \in \mathbb{R}^*$ such that $a > 0$ and a infinite. Each $S_\omega \in \mathbb{R}_f$ so each $S_\omega < a$. We have no name for a, but we can say that such an a exists. So

$$\mathbb{R}^* \models \exists y \forall x(\bar{\mathbb{N}}(x) \to |S(x)| < y),$$

i.e. a is a witness for $\exists y$. Thus $\mathbb{R}$ is a model of the same formula. That is, there is $r \in \mathbb{R}$ such that $\forall n \in \mathbb{N} : |S_n| < r$. Hence $(S_n)_n$ is bounded. □

Remark 4.2.8. Existential quantifier for a is all that is needed.

Theorem 4.2.9. *Let S_n be a standard sequence. Then $\lim_{n\to\infty} s_n = r$ (in standard world) if and only if $r \simeq S_\omega$ for each $\omega \in \mathbb{N}^* \setminus \mathbb{N}$.*

Proof. Assume $\lim_{n\to\infty} S_n = r$. So $\forall \epsilon > 0\ \exists n_0 \in \mathbb{N}.(\forall n \geq n_0)(|S_n - r| < \epsilon)$. Then

$$\forall x(\bar{\mathbb{N}}(x) \wedge x > \bar{n}_0 \to |S(x) - \bar{r}| < \bar{\epsilon}).$$

Thus $\mathbb{R}^*$ is a model of the same formula. Let $\omega \in \mathbb{N}^* \setminus \mathbb{N}$. Hence $\omega > n_0$, and hence $|S_\omega - r| < \epsilon$. $\epsilon > 0$ was arbitrary, so $S_\omega \simeq r$.

Suppose $S_\omega \simeq r$ for all $\omega \in \mathbb{N}^* \setminus \mathbb{N}$. Let $\epsilon > 0, \epsilon \in \mathbb{R}$, and let $\omega_0 \in \mathbb{N}^* \setminus \mathbb{N}$. If $\omega > \omega_0 \Rightarrow |S_\omega - r| < \epsilon$ since $s_\omega \simeq r$. Thus

$$\mathbb{R}^* \models \exists y(\bar{\mathbb{N}}(y) \wedge \forall x(\bar{\mathbb{N}}(x) \wedge x > y \to |S(x) - \bar{r}| < \bar{\epsilon})),$$

namely ω_0 is a witness to $\exists y$. Thus $\mathbb{R}$ is a model of the same formula. That is, $\exists n_0 \in \mathbb{N}\ \forall n > n_0\ |S_n - r| < \epsilon$, and hence $\lim_{n\to\infty} S_n = r$. □

Theorem 4.2.10. *Let (S_n) be a standard sequence. Then (S_n) is convergent if and only if $S_\omega \simeq S_\lambda$ for all $\omega, \lambda \in \mathbb{N}^* \setminus \mathbb{N}$.*

Theorem 4.2.11. *Let f be a function $f\colon \mathbb{R} \to \mathbb{R}$. Then f is continuous at $x \in \mathbb{R}$ if and only if $f(x+\eta) \simeq f(x)$ for each $\eta \in \mathbb{R}_i^*$.*

Theorem 4.2.12. *Suppose f is continuous at x and g continuous at $f(x)$. Then $g \circ f$ is continuous at x.*

Proof. Given x we must show that $g(f(x+\eta)) \simeq g(f(x))$ for all $\eta \in \mathbb{R}_i^*$. But

$$g(f(x+\eta)) = g(f(x)+\xi) = g(f(x)) + \gamma,$$

so the statement is proved. □

Theorem 4.2.13. *$f\colon \mathbb{R} \to \mathbb{R}$ is uniformly continuous if and only if for each $x, y \in \mathbb{R}^*$, $x \simeq y \Rightarrow f(x) \simeq f(y)$.*

Index