10 Cardinal arithmetic

Addition and multiplication of cardinal numbers

Definition of a relation $<^*$ on $On \times On$

$(\alpha_0, \beta_0) <^* (\alpha_1, \beta_1) :\Leftrightarrow (\alpha_0 \cup \beta_0 < \alpha_1 \cup \beta_1) \vee (\alpha_0 \cup \beta_0 = a_1 \cup \beta_1 \wedge [\alpha_0 < \alpha_1 \vee (\alpha_0 = \alpha_1 \wedge \beta_0 < \beta_1)])$

Lemma 10.1. $<^*$ is a wellordering of $On \times On$.

Proof:

1. linearity of $<^*$: left to the reader.

2. $(\alpha, \beta)_{<^*} = \{(x, y) : (x, y) <^* (\alpha, \beta)\} \subseteq (\gamma{+}1) \times (\gamma{+}1)$ with $\gamma := \alpha \cup \beta$. Hence $(\alpha, \beta)_{<^*}$ is a set.

3. Assume $\emptyset \neq u \subseteq On \times On$.

Let $\gamma := \min\{\xi \cup \eta : (\xi, \eta) \in u\}$, $\alpha := \min\{\xi : \exists\eta(\xi \cup \eta = \gamma \wedge (\xi, \eta) \in u)\}$, $\beta := \min\{\eta : \alpha \cup \eta = \gamma \wedge (\alpha, \eta) \in u\}$.

Then $(\alpha, \beta) \in u$ and $\forall(\xi, \eta) \in u((\alpha, \beta) \leq^* (\xi, \eta))$.

Definition.

Let $\Gamma : On \times On \to On$ be the uniquely determined isomorphism from $(On \times On, <^*)$ onto $(On, <)$.

In other words, Γ is the inverse of the ordering function of $(On \times On, <^*)$.

Theorem 10.2. $\Gamma[\aleph_\alpha \times \aleph_\alpha] = \aleph_\alpha$ for all $\alpha \in On$.

Proof by induction on α:

One easily sees that for all β the following holds:

(1) $\Gamma[\beta \times \beta] \in On$,

(2) $\Gamma[\beta \times \beta] = \bigcup_{\xi<\beta} \Gamma[\xi \times \xi]$, if $\beta \in Lim$,

(3) $\xi < \beta \;\Rightarrow\; \Gamma[\xi \times \xi] < \Gamma[\beta \times \beta]$,

(4) $\beta \leq \Gamma[\beta \times \beta]$.

So we have $\aleph_\alpha \leq \Gamma[\aleph_\alpha \times \aleph_\alpha] = \bigcup_{\beta<\aleph_\alpha} \Gamma[\beta \times \beta]$, and it remains to prove $\forall\beta{<}\aleph_\alpha(\Gamma[\beta \times \beta] < \aleph_\alpha)$.

Case 1: $\beta < \aleph_0$. Then $\beta \times \beta$ and thus also $\Gamma[\beta \times \beta]$ is finite. So we get $\Gamma[\beta \times \beta] < \aleph_0 \leq \aleph_\alpha$.

Case 2: $\aleph_0 \leq \beta < \aleph_\alpha$.

Then $|\beta| = \aleph_\xi$ with $\xi < \alpha$. By I.H. we get $\aleph_\xi = \Gamma[\aleph_\xi \times \aleph_\xi] \sim \Gamma[\beta \times \beta]$, hence $\Gamma[\beta \times \beta] < \aleph_\alpha$.

Corollary. $0 < |b| \leq |a| = \aleph_\alpha \;\Rightarrow\; |a \cup b| = |a \times b| = \aleph_\alpha$.

Proof: $\aleph_\alpha \preceq a \cup b \preceq a \times \{0, 1\} \preceq \aleph_\alpha \times \aleph_\alpha \sim \aleph_\alpha$ und $\aleph_\alpha \preceq a \times b \preceq \aleph_\alpha \times \aleph_\alpha$.

Definition. For $\kappa, \mu \in Card$ let $\kappa \hat{+} \mu := |(\{0\} \times \kappa) \cup (\{1\} \times \mu)|$ and $\kappa \hat{\cdot} \mu := |\kappa \times \mu|$.

Remark. If $|a|, |b| \in Card$ then $(a \cap b = \emptyset \Rightarrow |a \cup b| = |a| \hat{+} |b|)$ and $|a \times b| = |a| \hat{\cdot} |b|$.

Theorem 10.3.

(a) $\kappa, \mu \in Kard \setminus \{0\}$ & $\omega \leq \kappa \cup \mu \;\Rightarrow\; \kappa \hat{+} \mu = \kappa \hat{\cdot} \mu = \kappa \cup \mu$,

(b) $\kappa \hat{+} 0 = \kappa$ & $\kappa \hat{\cdot} 0 = 0$,

(c) $m, n \in \omega \;\Rightarrow\; m \hat{+} n \in \omega$ & $m \hat{+} (n{+}1) = (m \hat{+} n){+}1$,

(d) $m, n \in \omega \;\Rightarrow\; m \hat{\cdot} n \in \omega$ & $m \hat{\cdot} (n{+}1) = (m \hat{\cdot} n) \hat{+} m$.

Proof:

(a) follows from the above Corollary. (b) is trivial.

(c), (d) Since $(\{0\} \times m) \cup (\{1\} \times n)$ and $m \times n$ are finite, we have $m \hat{+} n,\ m \hat{\cdot} n \in \omega$.

$(\{0\} \times m) \cup (\{1\} \times (n{+}1)) = (\{0\} \times m) \cup (\{1\} \times n) \cup \{(1, n)\} \sim (m \hat{+} n) \cup \{m \hat{+} n\} = (m \hat{+} n) + 1$.

$m \times (n{+}1) = (m \times n) \cup (m \times \{n\}) \sim (\{0\} \times (m \hat{\cdot} n)) \cup (\{1\} \times m) \sim (m \hat{\cdot} n) \hat{+} m$.

Lemma 10.4.

$\mathrm{Fun}(F)$ & $\mathrm{Fun}(H)$ & $c \subseteq \mathrm{dom}(F) \cap \mathrm{dom}(H)$ & $|c| \in Card$ & $\delta \in On$ & $\forall x \in c (H(x) : F(x) \xrightarrow{1\text{-}1} \delta) \implies$

$\implies |\bigcup_{x \in c} F(x)| \leq |c| \hat{\cdot} |\delta|$.

Proof:

W.l.o.g. $c \in On$. Definition: $h : \bigcup_{x \in c} F(x) \to c \times \delta,\ h(y) := (\xi, H(\xi)(y))$ with $\xi := \min\{x \in c : y \in F(x)\}$.

Obviously h is injective, which yields the assertion.

Theorem 10.5 (AC)

$\mathrm{Fun}(F)$ & $c \subseteq \mathrm{dom}(F) \ \Rightarrow\ |\bigcup_{x \in c} F(x)| \leq |c| \hat{\cdot} \sup_{x \in c} |F(x)|$.

Corollary (AC)

$\mathrm{Fun}(F)$ & $c \subseteq \mathrm{dom}(F)$ & $|c| \leq \aleph_\alpha$ & $\forall x \in c (|F(x)| \leq \aleph_\alpha) \ \Rightarrow\ |\bigcup_{x \in c} F(x)| \leq \aleph_\alpha$.

Proof:

Let $\delta := \sup_{x \in c} |F(x)|$. Due to (AC) we have $|c| \in Card$ and a function $H : c \to V$ such that $H(x) : F(x) \xrightarrow{1\text{-}1} \delta$ for each $x \in c$. Now the assertion follows from Lemma 10.4.

Theorem 10.6

$|a| \leq \aleph_\alpha \ \Rightarrow\ |a^{<\omega}| \leq \aleph_\alpha$, where $a^{<\omega} := \{s :\ \mathrm{Fkt}(s) \wedge \mathrm{dom}(s) \in \omega \wedge \mathrm{ran}(s) \subseteq a\}$.

Proof:

W.o.l.g.: $0 \in a \subseteq \aleph_\alpha$. Let $f : \omega \to V,\ f(n) := \{s \in a^{<\omega} :\ \mathrm{dom}(s) = n\}$, and

$h : \omega \to V,\ h(0) := \{(0, 0)\},\ h(n{+}1) : f(n{+}1) \to \aleph_\alpha,\ s \mapsto \Gamma(h(n)(s \restriction n), s(n))$.

By 10.4 we now obtain $|a^{<\omega}| = |\bigcup_{x \in \omega} f(x)| \leq \omega \hat{\cdot} \aleph_\alpha = \aleph_\alpha$.

Regular Cardinals

Definition

For $\alpha \in Lim$ let $\mathsf{cf}(\alpha) := \min\{|x| : x \subseteq \alpha \wedge \sup(x) = \alpha\}$ *(cofinality of α)*.

A limit number α is *regular* iff $\mathsf{cf}(\alpha) = \alpha$.

Remark. ω is regular.

Lemma 10.7. For every limit number α the following holds:

(a) $\mathsf{cf}(\alpha) = \min\{\gamma : \exists f{:}\gamma \to \alpha (\alpha = \sup f[\gamma])\}$

(b) $\omega \leq \mathsf{cf}(\alpha) \leq \alpha$ & $\mathsf{cf}(\alpha) \in Card$

(c) α regular $\iff\ \forall \gamma < \alpha \forall f{:}\gamma \to \alpha (\sup f[\gamma] < \alpha)$.

Proof:

(a) "$\leq$": $f : \gamma \to \alpha$ & $\alpha = \sup f[\gamma] \ \Rightarrow\ \mathsf{cf}(\alpha) \leq |f[\gamma]| \leq |\gamma| \leq \gamma$.

"$\geq$": $\gamma := \mathsf{cf}(\alpha) = |x|$ & $x \subseteq \alpha$ & $\sup(x) = \alpha \Rightarrow \exists f : \gamma \to \alpha(\alpha = \sup(x) = \sup f[\gamma])$.

(b) $x \subseteq \alpha \in Lim$ & $|x| < \omega \Rightarrow \sup(x) < \alpha$; hence $\omega \leq \mathsf{cf}(\alpha)$. $|\alpha| \leq \alpha$ & $\alpha \subseteq \alpha$ & $\sup(\alpha) = \alpha \Rightarrow \mathsf{cf}(\alpha) \leq \alpha$. $\mathsf{cf}(\alpha) \in Card$ follows immediately from the definition.

(c) $\mathsf{cf}(\alpha) = \alpha \Leftrightarrow \mathsf{cf}(\alpha) \geq \alpha \Leftrightarrow \alpha \leq \min\{\gamma : \exists f : \gamma \to \alpha(\alpha = \sup f[\gamma])\}$.

Lemma 10.8. For every limit number α the following holds:

(a) There is an order preserving function $f : \mathsf{cf}(\alpha) \to \alpha$ such that $\alpha = \sup f[\mathsf{cf}(\alpha)]$.

(b) $f : \gamma \to \alpha$ & $\alpha = \sup f[\gamma]$ & $\forall \xi, \eta(\xi < \eta < \gamma \to f(\xi) \leq f(\eta)) \implies \gamma \in Lim$ & $\mathsf{cf}(\gamma) = \mathsf{cf}(\alpha)$.

(c) $\mathsf{cf}(\aleph_\alpha) = \mathsf{cf}(\alpha)$.

(d) $\mathsf{cf}(\alpha)$ is regular.

Proof:

(a) Let $g : \mathsf{cf}(\alpha) \to \alpha$ such that $\alpha = \sup g[\mathsf{cf}(\alpha)]$.

Def.: $f : \mathsf{cf}(\alpha) \to On$, $f(\xi) := g(\xi) \cup \sup_{\eta<\xi}(f(\eta)+1)$. Then $\forall \xi < \mathsf{cf}(\alpha)(f(\xi) < \alpha)$, f order preserving, $\alpha = \sup g[\mathsf{cf}(\alpha)] \leq \sup f[\mathsf{cf}(\alpha)] \leq \alpha$.

(b) $\gamma \in Lim$. $[\gamma = \gamma_0{+}1 \Rightarrow \sup f[\gamma] = f(\gamma_0) < \alpha]$

I. $\mathsf{cf}(\alpha) \leq \mathsf{cf}(\gamma)$: Let $x \subseteq \gamma$ with $|x| = \mathsf{cf}(\gamma)$ and $\sup(x) = \gamma$. Then $|f[x]| \leq |x|$ and $\alpha = \sup f[x]$. $[\delta < \alpha \Rightarrow \delta < f(\xi)$ for some $\xi < \gamma \Rightarrow \delta < f(\xi)$ & $\xi < \eta$ for some $\eta \in x \Rightarrow \delta < f(\xi) \leq f(\eta) \in f[x]\,]$

II. $\mathsf{cf}(\gamma) \leq \mathsf{cf}(\alpha)$. Def.: $g : \alpha \to \gamma$, $g(\delta) := \min\{\xi \in \gamma : \delta < f(\xi)\}$.

Then we have (1) $\delta_0 < \delta_1 \to g(\delta_0) \leq g(\delta_1)$, and (2) $\sup_{x<\alpha} g(x) = \gamma$ $[\gamma_0 < \gamma \Rightarrow \delta := f(\gamma_0) < \alpha \Rightarrow f(\gamma_0) = \delta < f(g(\delta)) \Rightarrow \gamma_0 < g(\delta)]$ From (1),(2) and I. it follows that $\mathsf{cf}(\gamma) \leq \mathsf{cf}(\alpha)$.

(c) follows from (b), since $\aleph_\alpha = \sup_{\xi<\alpha} \aleph_\xi$.

(d) Let $\gamma := \mathsf{cf}(\alpha)$. (a)$\Rightarrow$ there is an order preserving $f : \gamma \to \alpha$ with $\alpha = \sup f[\gamma] \overset{\text{(b)}}{\Rightarrow} \mathsf{cf}(\gamma) = \mathsf{cf}(\alpha) = \gamma$.

Theorem 10.9 (AC)

$\aleph_{\alpha+1}$ is regular.

Proof:

Let $\gamma < \aleph_{\alpha+1}$ and $f : \gamma \to \aleph_{\alpha+1}$. Then $|\gamma| \leq \aleph_\alpha$ & $\forall x \in \gamma(|f(x)| \leq \aleph_\alpha)$, which by 10.5 implies $|\sup f[\gamma]| = |\bigcup_{x\in\gamma} f(x)| \leq \aleph_\alpha$, hence $\sup(f[\gamma]) < \aleph_{\alpha+1}$.

Theorem 10.10.

$|\bigcup_{x\in c} f(x)| = \aleph_\alpha$ & $|c| < \mathsf{cf}(\aleph_\alpha) \Rightarrow \exists x \in c(|f(x)| = \aleph_\alpha)$.

Proof:

W.l.o.g. $\bigcup_{x\in c} f(x) = \aleph_\alpha$. For $x \in c$ let $h(x) : f(x) \to \tau(x)$ be the inverse of the ordering function of $(f(x), <)$; then $\tau(x) \leq \aleph_\alpha$ for all $x \in c$. *Assumption:* $\forall x \in c(\tau(x) < \aleph_\alpha)$. Since $|c| < \mathsf{cf}(\aleph_\alpha)$, we then have $\delta := \sup_{x\in c} \tau(x) < \aleph_\alpha$ and thus (by 10.4) $\aleph_\alpha = \bigcup_{x\in c} f(x) \leq |c| \dot{\cdot} |\delta| < \aleph_\alpha$. *Contradiction.* Hence $\tau(x) = \aleph_\alpha$ for some $x \in c$. Since $|\tau(x)| = |f(x)|$, this yields $|f(x)| = \aleph_\alpha$.

Cardinal Exponantiation

For the rest of this section we assume (AC).

κ, λ, ν denote cardinals.

Definition. $\kappa^\lambda := |\{f : f{:}\lambda \to \kappa\}| = |{}^\lambda\kappa|$.

Proposition.

(1) $|{}^b a| = |a|^{|b|}$

(2) $\kappa_0 \le \kappa_1 \;\&\; \lambda_0 \le \lambda_1 \implies \kappa_0^{\lambda_0} \le \kappa_1^{\lambda_1}$

(3) $\kappa^0 = 1 \;\&\; \kappa^1 = \kappa$

Lemma 10.11.

(a) $\kappa^{\lambda \hat{+} \mu} = \kappa^\lambda \hat{\cdot} \kappa^\mu$

(b) $\kappa^{\lambda \hat{\cdot} \mu} = (\kappa^\lambda)^\mu$

(c) $0 < \lambda < \omega \le \kappa \implies \kappa^\lambda = \kappa$

Proof:

(a) If $a \cap b = \emptyset$ then ${}^{a \cup b}c \sim {}^a c \times {}^b c$ [$f \mapsto (f{\restriction}a, f{\restriction}b)$].

(b) $\Phi : {}^a({}^b c) \to {}^{a \times b}c$, $\Phi(f)((x,y)) := f(x)(y)$ is a bijection.

Theorem 10.11.

(a) $|a| < 2^{|a|} = |\mathcal{P}(a)|$

(b) $\omega \cup \lambda \le |a| \implies |\{x \in \mathcal{P}(a) : |x| \le \lambda\}| = |\{x \in \mathcal{P}(a) : |x| = \lambda\}| = |a|^\lambda$

Proof:

(a) ${}^a 2 \sim \mathcal{P}(a)$, $a \preceq \mathcal{P}(a)$ and $\mathcal{P}(a) \not\preceq a$.

(b) Let $\lambda > 0$. If $f \in {}^\lambda a$ then $f \subseteq \lambda \times a$ and $|f| = \lambda$. Further we have $\lambda \times a \sim a$.
Hence ${}^\lambda a \preceq \{x \subseteq \lambda \times a : |x| = \lambda\} \sim \{x \in \mathcal{P}(a) : |x| = \lambda\} \subseteq \{x \in \mathcal{P}(a) : |x| \le \lambda\} = \{f[\lambda] : f \in {}^\lambda a\} \cup \{\emptyset\} =: u$.
Finally $|u| \le |{}^\lambda a \cup \{\emptyset\}| = |a|^\lambda$.

Lemma 10.12.

(a) $2 \le \kappa \;\Rightarrow\; \lambda < 2^\lambda \le \kappa^\lambda \le 2^{\kappa \hat{\cdot} \lambda}$

(b) $2 \le \kappa \;\&\; \omega \cup \kappa \le \lambda \;\Rightarrow\; \kappa^\lambda = 2^\lambda$.

Proof: (a) ${}^\lambda\kappa \subseteq \mathcal{P}(\lambda \times \kappa) \sim {}^{\kappa \times \lambda}2$. (b) follows from (a).

Theorem 10.13. $|c| \le \lambda \;\&\; f : c \to V \;\&\; \forall x \in c(|f(x)| < \kappa) \implies |\bigcup_{x \in c} f(x)| < \kappa^\lambda$.

Proof:

Assumption: $\kappa^\lambda \le |\bigcup f[c]|$. Then ${}^c\kappa \preceq \bigcup f[c]$ and consequently there exists a surjective $F : \bigcup f[c] \to {}^c\kappa$.
For $x \in c$ let $s(x) := \{g(x) : g \in F[f(x)]\}$. Then $s(x) \subseteq \kappa \;\&\; |s(x)| \le |F[f(x)]| \le |f(x)| < \kappa$, hence $s(x) \subsetneq \kappa$.
Therefore there exists a $g \in {}^c\kappa$ with $\forall x \in c(g(x) \notin s(x))$, i.e. $g \in {}^c\kappa \setminus \bigcup_{x \in c} F[f(x)]$. Contradiction.

Corollary

(a) $2 \le \kappa \;\&\; \omega \le \lambda \implies \lambda < \mathsf{cf}(\kappa^\lambda)$.

(b) $\omega \le \kappa \implies \kappa < \kappa^{\mathsf{cf}(\kappa)}$.

Proof:

(a) Let $c \subseteq \kappa^\lambda$ and $|c| \leq \lambda$. From $\forall x \in c(|x| < \kappa^\lambda)$ we get $|\sup(c)| = |\bigcup_{x\in c} x| < (\kappa^\lambda)^\lambda = \kappa^{\lambda\hat{\cdot}\lambda} = \kappa^\lambda$.

(b) Let $c \subseteq \kappa$ with $\sup(c) = \kappa$ and $|c| = \mathsf{cf}(\kappa)$. Then $\kappa = |\bigcup_{x\in c} x| < \kappa^{\mathsf{cf}(\kappa)}$.

Theorem 10.14.

For $\omega \leq \lambda$ the following holds:

(a) $\aleph_{\alpha+1}^\lambda = \aleph_{\alpha+1}\hat{\cdot}\aleph_\alpha^\lambda$.

(b) $\aleph_\alpha^\lambda = \sup_{\xi<\alpha} \aleph_\xi^\lambda$, if $\alpha \in Lim$ and $\lambda < \mathsf{cf}(\alpha)$.

Proof:

Abb.: $\kappa := \aleph_\alpha$. Then $\kappa^+ = \aleph_{\alpha+1}$ is regular.

(a) We have $\kappa^+\hat{\cdot}\kappa^\lambda \leq (\kappa^+)^\lambda$.

Case 1: $\lambda \leq \kappa$. Since κ^+ is regular, we have ${}^\lambda(\kappa^+) = \bigcup_{\beta<\kappa^+} {}^\lambda\beta$ and so $(\kappa^+)^\lambda \leq \kappa^+\hat{\cdot}\sup_{\beta<\kappa^+} |\beta|^\lambda = \kappa^+\hat{\cdot}\kappa^\lambda$.

Case 2: $\kappa < \lambda$. Then $(\kappa^+)^\lambda = 2^\lambda = \kappa^\lambda \leq \kappa^+\hat{\cdot}\kappa^\lambda$.

(b) $\alpha \in Lim$ & $\lambda < \mathsf{cf}(\alpha) \Rightarrow {}^\lambda\aleph_\alpha = \bigcup_{\xi<\alpha} {}^\lambda\aleph_\xi \Rightarrow \aleph_\alpha^\lambda \leq |\alpha|\hat{\cdot}\sup_{\xi<\alpha} \aleph_\xi^\lambda \Rightarrow \aleph_\alpha^\lambda \leq \sup_{\xi<\alpha} \aleph_\xi^\lambda$.

The Generalized Continuum Hypothesis

(GCH) $\forall\alpha(2^{\aleph_\alpha} = \aleph_{\alpha+1})$

Theorem 10.15.

Under (GCH) for all $\kappa, \lambda \geq \omega$ the following holds:

$$\kappa^\lambda = \begin{cases} \kappa & \text{if } \lambda < \mathsf{cf}(\kappa) \\ \kappa^+ & \text{if } \mathsf{cf}(\kappa) \leq \lambda \leq \kappa \\ \lambda^+ & \text{if } \kappa \leq \lambda \end{cases}$$

Proof:

1. If $\mathsf{cf}(\kappa) \leq \lambda \leq \kappa$ then $\kappa < \kappa^{\mathsf{cf}(\kappa)} \leq \kappa^\lambda \leq 2^{\kappa\hat{\cdot}\lambda} = 2^\kappa = \kappa^+$, and thus $\kappa^\lambda = \kappa^+$.

2. If $\kappa \leq \lambda$ then $\kappa^\lambda = 2^\lambda = \lambda^+$.

3. $\lambda < \mathsf{cf}(\kappa)$: Then ${}^\lambda\kappa = \bigcup_{\alpha\in\kappa} {}^\lambda\alpha$ and therefore $\kappa^\lambda \leq \kappa\hat{\cdot}\sup_{\alpha\in\kappa} |\alpha|^\lambda$. It remains to prove $\forall\alpha \in \kappa(|\alpha|^\lambda \leq \kappa)$: $\alpha \in \kappa \Rightarrow \lambda\hat{\cdot}|\alpha| < \kappa \Rightarrow |\alpha|^\lambda \leq 2^{\lambda\hat{\cdot}|\alpha|} = (\lambda\hat{\cdot}|\alpha|)^+ \leq \kappa$.

11 Arithmetic of ordinal numbers

In the following, λ always denotes a limit number.

Lemma 11.1.

(a) $\emptyset \neq u \subseteq On \;\&\; \sup(u) \notin u \implies \sup(u) \in Lim$.

(b) $\alpha \in Lim \iff \alpha \neq 0 \;\&\; \sup(\alpha) = \alpha$.

(c) α successor number $\implies \alpha = \sup(\alpha)+1 \;\&\; \sup(\alpha) = \max(\alpha)$.

(d) $F : On \to On$ order preserving (i.e., $\forall\alpha\forall\beta < \alpha(F(\beta) < F(\alpha))) \implies \forall\alpha(\alpha \leq F(\alpha))$.

Proof:

(a) Let $\emptyset \neq u \subseteq On$ and $\alpha := \sup(u) \notin u$. Then $\alpha \neq 0$, and it remains to prove $\forall\beta < \alpha(\beta{+}1 < \alpha)$.

$\beta < \alpha \;\Rightarrow\; \beta < \xi$ for some $\xi \in u \;\Rightarrow\; \beta{+}1 \leq \xi$ and $\xi \leq \alpha \overset{\alpha\notin u}{\Rightarrow} \beta + 1 \leq \xi < \alpha$, since $\alpha \notin u$.

(b) "$\Rightarrow$": Trivially $\sup(\alpha) \leq \alpha$. From $\sup(\alpha) < \alpha$ we would obtain $\sup(\alpha){+}1 \in \alpha$ and so $\sup(\alpha) < \sup(\alpha)$. Contradiction. "$\Leftarrow$": $\sup(\alpha) = \alpha \neq 0 \;\Rightarrow\; \sup(\alpha) \notin \alpha \neq \emptyset \overset{(a)}{\Rightarrow} \sup(\alpha) \in Lim$.

(c) $\alpha = \beta{+}1 = \beta \cup \{\beta\} \;\Rightarrow\; \beta = \max(\alpha) \;\Rightarrow\; \beta = \sup(\alpha)$.

(d) Induction on α: $\forall\xi < \alpha(\xi \leq F(\xi)) \;\Rightarrow\; \forall\xi < \alpha(\xi < F(\alpha)) \;\Rightarrow\; \alpha \leq F(\alpha)$.

Definition

1. A class $A \subseteq On$ is *closed* iff $\forall u(\emptyset \neq u \subseteq A \;\Rightarrow\; \sup(u) \in A)$.
2. A class $A \subseteq On$ is *club* iff it is closed and unbounded.
3. A function $F : On \to On$ is *continuous* iff $\forall u(\emptyset \neq u \subseteq On \;\Rightarrow\; F(\sup(u)) = \sup(F[u])\,)$.
4. $F : On \to On$ is called a *normal function* iff F is order preserving and continuous.

Lemma 11.2.

For each function $F : On \to On$ holds:

F normal function $\;\Leftrightarrow\; \forall\alpha(F(\alpha) < F(\alpha+1)) \;\&\; \forall\lambda{\in}Lim(F(\lambda) = \sup(F[\lambda])\,)$.

Proof:

"$\Rightarrow$" $\;F(\lambda) = F(\sup(\lambda)) = \sup(F[\lambda])$.

"$\Leftarrow$" 1. By induction on α we obtain $\forall\beta < \alpha(F(\beta) < F(\alpha))$.

2. Let $\emptyset \neq u \subseteq On$ and $\alpha := \sup(u)$. If $\alpha \in u$, then $F(\alpha) = \sup(F[u])$, since F is order preserving.

If $\alpha \notin u$, then $\alpha \in Lim$ and therefore $F(\alpha) = \sup(F[\alpha])$.

Further we have $u \subseteq \alpha \;\&\; \forall\xi < \alpha\exists\eta{\in}u(\xi < \eta)$, which yields $\sup(F[\alpha]) = \sup(F[u])$.

Lemma 11.3.

For each normal function $F : On \to On$ holds:

(a) $F(\alpha) = \sup\{F(\xi+1) : \xi \in \alpha\}$, for all $\alpha > 0$.

(b) $\lambda \in Lim \;\Rightarrow\; F(\lambda) \in Lim$.

(c) $\forall\gamma \geq F(0)\exists!\alpha(\,F(\alpha) \leq \gamma < F(\alpha+1))$.

(d) G normal function $\Rightarrow\; F \circ G$ normal function.

Proof:

(a) From $\forall\xi < \alpha(\xi + 1 \leq \alpha)$ we get $\gamma := \sup\{F(\xi+1) : \xi < \alpha\} \leq F(\alpha)$.

If $\alpha = \beta + 1$, then $F(\alpha) \in \{F(\xi+1) : \xi < \alpha\}$ and therefore $F(\alpha) \leq \gamma$.
If $\alpha \in Lim$, then $F(\alpha) = \sup F[\alpha] \leq \sup\{F(\xi+1) : \xi < \alpha\} = \gamma$.

(b) Obviously $0 \leq F(0) < F(\lambda)$.
From $\gamma < F(\lambda) = \sup F[\lambda]$ we get $\exists \xi < \lambda(\gamma < F(\xi))$ and then $\exists \xi(\gamma + 1 \leq F(\xi) < F(\lambda))$.

(c) Let $\gamma \geq F(0)$. Since $\gamma \leq F(\gamma) < F(\gamma+1)$, there exists $\alpha := \min\{\xi : \gamma < F(\xi+1)\}$. Then $\gamma < F(\alpha+1)$. If $\alpha = 0$, then $F(\alpha) = F(0) \leq \gamma$. If $\alpha > 0$, then $F(\alpha) = \sup\{F(\xi+1) : \xi < \alpha\}$ and $\forall \xi < \alpha(F(\xi+1) \leq \gamma)$, hence $F(\alpha) \leq \gamma$.

(d) $(F \circ G)(\sup(u)) = F(\sup(G[u])) = \sup(F[G[u]]) = \sup((F \circ G)[u])$.

Lemma 11.4.
If F is the ordering function of $A \subseteq On$, then:
F is a normal function $\Leftrightarrow$ A is club.

Proof:
1. $\mathrm{dom}(F) = On \Leftrightarrow A \notin V \Leftrightarrow A$ unbounded.
2. Assume now that $\mathrm{dom}(F) = On$.
"$\Rightarrow$" Let $\emptyset \neq u \subseteq A$ and $v := F^{-1}[u]$. Then $\sup(u) = \sup(F[v]) = F(\sup(v)) \in A$.
"$\Leftarrow$" $\lambda \in Lim \Rightarrow F[\lambda] \subseteq A \Rightarrow \gamma := \sup(F[\lambda]) \in A \Rightarrow \gamma = \min\{x \in A : \forall \xi < \lambda(F(\xi) < x)\} \overset{8.8}{=} F(\lambda)$.

Remark
The function $\alpha \mapsto \aleph_\alpha$ is a normal function. (cf. 9.7 and 9.8a)

Lemma 11.5.
If $F : On \to On$ is a normal function, then the class $\{\beta : F(\beta) = \beta\}$ of all fixpoints of F is club.
The ordering function of this class is denoted by F'.

F' satisfies: $F'(0) = \sup_{n\in\omega} F^{(n)}(0)$, $F'(\beta+1) = \sup_{n\in\omega} F^{(n)}(F'(\beta)+1)$.

Proof:
1. *closed:* Let $\emptyset \neq u \subseteq On$ with $\forall \eta \in u(F(\eta) = \eta)$, and let $\beta := \sup(u)$.
Then $F(\beta) = \sup\{F(\eta) : \eta \in u\} = \sup\{\eta : \eta \in u\} = \beta$.

2. *unbounded:* For $\gamma \in On$ let $\gamma^* := \sup_{n\in\omega} F^{(n)}(\gamma)$. We show $\gamma^* = \min\{\beta : \gamma \leq \beta = F(\beta)\}$. This also yields the remaining two claims. – From $\gamma \leq \beta = F(\beta)$ by induction on n we get $\forall n(F^{(n)}(\gamma) \leq \beta)$, hence $\gamma^* \leq \beta$. On the other side we have $\gamma \leq F(\gamma) \leq \gamma^*$ and $F(\gamma^*) = \sup_{n\in\omega} F^{(n+1)}(\gamma) = \gamma^*$.

Lemma.
If $A, B \subseteq On$ are club then also $A \cap B$ is club.

Proof:
1. $A \cap B$ closed: obvious.
2. Let $\gamma \in On$. Definition: $\alpha_0 := \beta_0 := \gamma$, $\alpha_{n+1} := \min\{\alpha \in A : \alpha_n, \beta_n < \alpha\}$, $\beta_{n+1} := \min\{\beta \in B : \alpha_n, \beta_n < \beta\}$. Then $\alpha^* := \sup\{\alpha_n : 0 < n \in \omega\} \in A$, $\beta^* := \sup\{\beta_n : 0 < n \in \omega\} \in B$ and $\gamma < \alpha^*$. Further we have $\alpha^* \leq \sup\{\beta_{n+1} : 0 < n \in \omega\} = \beta^*$ and as well $\beta^* \leq \alpha^*$; hence $\alpha^* = \beta^* \in A \cap B$.

Definition (of $\alpha+\beta$ by transfinite recursion on β)

$\alpha+0:=\alpha,\quad \alpha+\beta':=(\alpha+\beta)',\quad \alpha+\lambda:=\sup\{\alpha+\eta:\ \eta<\lambda\}$.

[Detailed formulation of the definition: Let $R:=\{((x,y),(x,z)):\ x,y,z\in On\ \&\ y<z\}$ and
$G:(On\times On)\times V\to V,\ G((\alpha,0),f):=\alpha,\ G((\alpha,\beta+1),f):=f((\alpha,\beta))+1,\ G((\alpha,\lambda),f):=\sup(\mathrm{ran}(f))$.
Then R is wellfounded and $\alpha+\beta=F((\alpha,\beta))$ with $F(x):=G(x,F|x_R)$.]

Remark: Note that $\alpha'=\alpha+0'$. Therefore the notation $\alpha+1$ for α' is compatible with the definition of $+$.

Lemma 11.6.

(a) For every α, the mapping $\beta\mapsto\alpha+\beta$ is a normal function,
and $\{\alpha+\beta:\beta\in On\}=\{\gamma:\ \gamma\geq\alpha\}$.

(b) $\beta_0<\beta_1\ \Rightarrow\ \alpha+\beta_0<\alpha+\beta_1$.

(c) $\beta\leq\alpha+\beta$.

(d) $\forall\gamma\geq\alpha\exists!\beta(\alpha+\beta=\gamma)$.

(e) $\alpha_0\leq\alpha_1\ \Rightarrow\ \alpha_0+\beta\leq\alpha_1+\beta$.

(f) $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$.

(g) $\alpha,\beta<\omega\ \Rightarrow\ \alpha+\beta=\beta+\alpha<\omega$.

(h) $0<k<\omega\ \Rightarrow\ k+\omega=\omega<\omega+k$.

Proof:

(a)–(d) By 11.2, $\beta\mapsto\alpha+\beta$ is a normal function. This yields (b) and (c).

Further $\alpha=\alpha+0\leq\alpha+\beta$. By 11.3c we also get $\forall\gamma\geq\alpha\exists!\beta(\alpha+\beta\leq\gamma<\alpha+(\beta+1)=(\alpha+\beta)+1)$, i.e. $\forall\gamma\geq\alpha\exists!\beta(\alpha+\beta=\gamma)$.

(e) Induction on β. (f) Induction on γ.

(g) Using 10.3c,d by induction on β we obtain: $\alpha,\beta<\omega\ \Rightarrow\ \alpha+\beta=\alpha\hat{+}\beta\in\omega$.

(h) $\omega\leq k+\omega=\sup\{k+n:\ n<\omega\}\leq\omega<\omega+k$.

Remark.

Assume that (a_0,r_0) and (a_1,r_1) are wellordered sets of order types α_0,α_1, respectively. Assume further that $a_0\cap a_1=\emptyset$. Then $\alpha_0+\alpha_1$ is the order type of the well ordering $(a_0\cup a_1,r)$ with $r:=r_0\cup r_1\cup a_0\times a_1$.

Proof: Let f_i be the ordering function of (a_i,r_i), and define $f:\alpha_0+\alpha_1\to a_0\cup a_1$ by
$f(\xi):=\begin{cases}f_0(\xi) & \text{if } \xi<\alpha_0\\ f_1(\eta) & \text{if } \xi=\alpha_0+\eta\end{cases}$. Then f is the ordering function of $(a_0\cup a_1,r)$.

Definition (of $\alpha\cdot\beta$ by transfinite recursion on β).

$\alpha\cdot 0:=0,\ \alpha\cdot(\beta+1):=(\alpha\cdot\beta)+\alpha,\ \alpha\cdot\lambda:=\sup\{\alpha\cdot\eta:\ \eta<\lambda\}$.

Lemma 11.7.

(a) For each $\alpha\geq 1$, the mapping $\beta\mapsto\alpha\cdot\beta$ is a normal function.

(b) $\alpha_0\leq\alpha_1\ \Rightarrow\ \alpha_0\cdot\beta\leq\alpha_1\cdot\beta$.

(c) $(\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma)$.

(d) $\alpha\cdot(\beta+\gamma)=\alpha\cdot\beta+\alpha\cdot\gamma$.

(e) Let $\alpha\geq 1$. Then for each γ there is a unique pair (β,δ) such that $\gamma=\alpha\cdot\beta+\delta$ and $\delta<\alpha$.

(f) $0 \cdot \alpha = \alpha \cdot 0 = 0$ & $1 \cdot \alpha = \alpha \cdot 1 = \alpha$.

(g) $\alpha, \beta < \omega \ \Rightarrow \ \alpha \cdot \beta = \beta \cdot \alpha < \omega$.

(h) $2 \cdot \omega = \omega < \omega + \omega = \omega \cdot 2$.

Remark.

Let α, β be given, and let $r \subseteq (\alpha \times \beta) \times (\alpha \times \beta)$ be defined by

$(x_0, y_0) r (x_1, y_1) \ :\Leftrightarrow \ x_0 < x_1$ or $x_0 = x_1$ & $y_0 < y_1$.

Then $\beta \cdot \alpha$ is the order type of the wellordering $(\alpha \times \beta, r)$.

Proof: The function $f : \alpha \times \beta \to \beta \cdot \alpha$, $f(\xi, \eta) := \beta \cdot \xi + \eta$ is an isomorphism between $(\alpha \times \beta, r)$ and $\beta \cdot \alpha$.

Definition (of α^β by transfinite recursion on β)

$\alpha^0 := 1$, $\alpha^{\beta+1} := \alpha^\beta \cdot \alpha$, $\alpha^\lambda := \sup\{\alpha^\eta : \eta < \lambda\}$.

Lemma 11.8

For $\alpha \geq 2$ the following holds:

(a) $\beta \mapsto \alpha^\beta$ is a normal function.

(b) $\alpha \leq \gamma \ \Rightarrow \ \alpha^\beta \leq \gamma^\beta$

(c) $\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}$

(d) $(\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma}$

(e) $\beta > \beta_0 > ... > \beta_n$ & $\delta_0, ..., \delta_n < \alpha \ \Rightarrow \ \alpha^\beta > \alpha^{\beta_0} \cdot \delta_0 + ... + \alpha^{\beta_n} \cdot \delta_n$.

Proof of (e) by induction on n:

I.H. $\Rightarrow \ \alpha^{\beta_0} > \alpha^{\beta_1} \cdot \delta_1 + ... + \alpha^{\beta_n} \cdot \delta_n \ \Rightarrow \ \alpha^\beta \geq \alpha^{\beta_0} \cdot \alpha \geq \alpha^{\beta_0} \cdot \delta_0 + \alpha^{\beta_0} > \alpha^{\beta_0} \cdot \delta_0 + ... + \alpha^{\beta_n} \cdot \delta_n$.

Remark. α^n is the ordertype of ${}^n\alpha$ ordered lexicographically.

Theorem 11.9.

(a) For $\alpha \geq 2$ and $\gamma \geq 1$ there are unique β, δ, γ_0 with $0 < \delta < \alpha$ & $\gamma_0 < \alpha^\beta$ & $\gamma = \alpha^\beta \cdot \delta + \gamma_0$.

(b) For $\alpha \geq 2$ and $\gamma \geq 1$ there are unique $\beta_0 > ... > \beta_n$ and $0 < \delta_0, ..., \delta_n < \alpha$ such that
$\gamma = \alpha^{\beta_0} \cdot \delta_0 + ... + \alpha^{\beta_n} \cdot \delta_n$ *(Cantor Normal Form of γ at base α).*

Proof:

(a) *Uniqueness:* Let $\gamma = \alpha^{\beta_0} \cdot \delta_0 + \gamma_0 = \alpha^{\beta_1} \cdot \delta_1 + \gamma_1$ with $0 < \delta_i < \alpha$ & $\gamma_i < \alpha^{\beta_i}$. Then $\alpha^{\beta_i} \leq \gamma < \alpha^{\beta_i + 1}$ for $i = 0, 1$. This yields $\beta_0 = \beta_1$. With $\beta := \beta_0 = \beta_1$ we also have $\alpha^\beta \cdot \delta_i \leq \gamma < \alpha^\beta \cdot (\delta_i + 1)$ for $i = 0, 1$, hence $\delta_0 = \delta_1 =: \delta$. Finally, from $\gamma = \alpha^\beta \cdot \delta + \gamma_i$ for $i = 0, 1$ it follows that $\gamma_0 = \gamma_1$.
Existence: By 11.3c there exists a β with $\alpha^\beta \leq \gamma < \alpha^{\beta+1}$, i.e. $\alpha^\beta \cdot 1 \leq \gamma < \alpha^\beta \cdot \alpha$. Again by 11.3 (essentially) this yields $\alpha^\beta \cdot \delta \leq \gamma < \alpha^\beta \cdot (\delta + 1) = \alpha^\beta \cdot \delta + \alpha^\beta$ with $0 < \delta < \alpha$. Therefore, by 11.6 there exists a $\gamma_0 < \alpha^\beta$ such that $\gamma = \alpha^\beta \cdot \delta + \gamma_0$.

(b) follows from (a) and 11.8e by induction on γ.

Definition (Additive principal numbers)

$\gamma \in On$ is an *additive principal number* iff $\gamma > 0$ & $\forall \xi, \eta < \gamma (\xi + \eta < \gamma)$.

$P :=$ class of all additive principal numbers.

Lemma 11.10.

(a) $\alpha \mapsto \omega^\alpha$ is the ordering function of P.

(b) $\gamma \in P \;\Leftrightarrow\; \gamma > 0 \;\&\; \forall \xi < \gamma(\xi + \gamma = \gamma)$.

Proof:

(a) 1. By induction on α we prove $\omega^\alpha \in P$:

1.1. $\omega^0 \in P$ is trivial.

1.2. $\xi, \eta < \omega^{\alpha+1} \;\Rightarrow\; \xi, \eta < \omega^\alpha \cdot n$ for some $n < \omega \;\Rightarrow\; \xi + \eta < \omega^\alpha \cdot n + \omega^\alpha \cdot n = \omega^\alpha \cdot (n+n) < \omega^{\alpha+1}$.

1.3. $\xi, \eta < \omega^\lambda \;\Rightarrow\; \xi, \eta < \omega^\alpha$ for some $\alpha < \lambda \overset{\text{I.H.}}{\Rightarrow} \xi + \eta < \omega^\alpha < \omega^\lambda$.

2. $\gamma \notin \{\omega^\alpha : \alpha \in On\} \;\Rightarrow\; \gamma \notin P$.

Proof: Let $1 \leq \gamma \notin \{\omega^\alpha : \alpha \in On\}$. Then $\gamma = \omega^\beta \cdot n + \gamma_0$ with $0 < n < \omega \;\&\; \gamma_0 < \omega^\beta$ and $1 < n$ oder $0 < \gamma_0$.
For $\eta := \omega^\beta \cdot (n-1) + \gamma_0$ we now have $0 < \eta < \omega^\beta \cdot n \leq \gamma$ and $\omega^\beta < \omega^\beta + \eta = \gamma$, i.e. $\gamma \notin P$.

(b) 1. Let $\gamma \in P$ and $\xi < \gamma$. Then $\xi + \gamma = \sup\{\xi + \eta + 1 : \eta < \gamma\} \leq \gamma$,
since $(\xi, \eta < \gamma \;\Rightarrow\; \xi + \eta < \gamma \;\Rightarrow\; \xi + \eta + 1 \leq \gamma)$.

2. $\gamma > 0 \;\&\; \forall \xi < \gamma(\xi + \gamma = \gamma) \;\&\; \xi, \eta < \gamma \;\Longrightarrow\; \xi + \eta < \xi + \gamma = \gamma$.

Definition

$\alpha =_{NF} \alpha_0 + ... + \alpha_n \;:\Leftrightarrow\; \alpha = \alpha_0 + ... + \alpha_n \;\&\; \alpha_0 \geq ... \geq \alpha_n \;\&\; \alpha_0, ..., \alpha_n \in P$.

Lemma 11.11.

(a) For each $\alpha > 0$ there exists a unique tupel $\alpha_0, ..., \alpha_n$ such that $\alpha =_{NF} \alpha_0 + ... + \alpha_n$.

(b) $\alpha =_{NF} \alpha_0 + ... + \alpha_n \;\&\; k < n \;\Rightarrow\; \alpha_0 + ... + \alpha_k < \alpha \;\&\; \alpha_{k+1} + ... + \alpha_n < \alpha$.

Proof:

(a) follows from 11.9 (for base $\alpha = \omega$) and the equation $\omega^\beta \cdot n = \omega^\beta + ... + \omega^\beta$.

(b) The first part is trivial. For the second part we observe:
$\alpha_{k+1} + ... + \alpha_n \overset{11.6e}{\leq} \alpha_k + ... + \alpha_{n-1} < \alpha_k + ... + \alpha_n \overset{11.6c}{\leq} \alpha$.

Definition. For $\alpha_0, ..., \alpha_n \in P$ let $\Sigma(\alpha_0, ..., \alpha_n) := \alpha_{p(0)} + \ldots + \alpha_{p(n)}$ where p is a permutation of $n+1$ such that $\alpha_{p(0)} \geq \ldots \geq \alpha_{p(n)}$.

It is intuitively clear that $\Sigma(\alpha_0, ..., \alpha_n)$ is well defined, i.e., if p, q are permutations with $\alpha_{p(0)} \geq \ldots \geq \alpha_{p(n)}$ and $\alpha_{q(0)} \geq \ldots \geq \alpha_{q(n)}$ then $\alpha_{p(0)} + \ldots + \alpha_{p(n)} = \alpha_{q(0)} + \ldots + \alpha_{q(n)}$.

Formally this can be derived from the following Proposition.

Proposition.

If $\alpha_0 \geq ... \geq \alpha_n$, and p is a permutation of $n+1$ such that $\alpha_{p(0)} \geq ... \geq \alpha_{p(n)}$ then $\alpha_i = \alpha_{p(i)}$ for $i = 0, ..., n$.

Proof by induction on n:

Let $k < n$ such that $\alpha_k > \alpha_{k+1} = ... = \alpha_n$. Then $\alpha_{p(k)} > \alpha_{p(k+1)} = ... = \alpha_{p(n)}$, and thus $\forall i \leq k(p(i) \leq k)$.
By IH we get $\alpha_i = \alpha_{p(i)}$ for $i \leq k$. Further we have $\alpha_{k+1} = ... = \alpha_n = \alpha_{p(k+1)} = ... = \alpha_{p(n)}$.

Remark.

Since $\Sigma(\alpha_0, ..., \alpha_n)$ is well defined, we have $\Sigma(\alpha_0, ..., \alpha_n) = \Sigma(\alpha_{q(0)}, ..., \alpha_{q(n)})$ for any permutation q.

Definition (Natural sum or Hessenberg sum)

$\alpha\#0 := 0\#\alpha := \alpha$.

For $\alpha =_{NF} \alpha_0 + ... + \alpha_n$ and $\beta =_{NF} \beta_0 + ... + \beta_m$ let $\alpha\#\beta := \Sigma(\alpha_0, ..., \alpha_n, \beta_0, ..., \beta_m)$.

Lemma 11.12.

(a) $\alpha\#\beta = \beta\#\alpha$,

(b) $(\alpha\#\beta)\#\gamma = \alpha\#(\beta\#\gamma)$,

(c) If $\alpha_0 \geq ... \geq \alpha_n$ are additive principal numbers then $\alpha_0 + ... + \alpha_n = \alpha_0\#...\#\alpha_n$,

(d) $\beta < \gamma \;\Rightarrow\; \alpha\#\beta < \alpha\#\gamma$,

(e) $\alpha, \beta < \omega^\gamma \;\Rightarrow\; \alpha\#\beta < \omega^\gamma$,

(f) $\alpha + \beta \leq \alpha\#\beta$.

Proof:

(a),(b) are intuitively clear. Formally they can be derived from the above Remark:

Let $\alpha =_{NF} \alpha_0 + ... + \alpha_n$, $\beta =_{NF} \beta_0 + ... + \beta_m$, $\gamma =_{NF} \gamma_0 + ... + \gamma_k$.

$\alpha\#\beta = \Sigma(\alpha_0, ..., \alpha_n, \beta_0, ..., \beta_m) = \Sigma(\beta_0, ..., \beta_m, \alpha_0, ..., \alpha_n) = \beta\#\alpha$.

$(\alpha\#\beta)\#\gamma = \Sigma(\alpha_0, ..., \alpha_n, \beta_0, ..., \beta_m)\,\#\,\gamma = \Sigma(\alpha_0, ..., \alpha_n, \beta_0, ..., \beta_m, \gamma_0, ..., \gamma_k) =$

$\alpha\,\#\,\Sigma(\beta_0, ..., \beta_m, \gamma_0, ..., \gamma_k) = \alpha\#(\beta\#\gamma)$.

(c) Induction on n: Let $\alpha := \alpha_0 + ... + \alpha_{n-1}$. Then $\alpha + \alpha_n = \alpha\#\alpha_n \overset{\text{IH}}{=} (\alpha_0\#...\#\alpha_{n-1})\#\alpha_n$.

(d) Due to (b),(c) it suffices to prove the claim for $\alpha \in P$. This is done by induction on γ.

Let $\beta =_{NF} \beta_0 + ... + \beta_n$ and $\gamma =_{NF} \gamma_0 + ... + \gamma_m$. Since $\beta < \gamma$, we have $\beta_0 \leq \gamma_0$.

Case 1: $\alpha \geq \gamma_0$. Then $\alpha\#\beta = \alpha + \beta < \alpha + \gamma = \alpha\#\gamma$.

Case 2: $\beta_0, \alpha < \gamma_0$. Then $\alpha\#\beta < \gamma_0 < \alpha\#\gamma$.

Fall 3: $\alpha < \beta_0 = \gamma_0$. Then $\alpha\#\beta = \beta_0 + (\alpha\#\hat{\beta})$ & $\alpha\#\gamma = \beta_0 + (\alpha\#\hat{\gamma})$ where $\beta_1 + ... + \beta_n = \hat{\beta} < \hat{\gamma} = \gamma_1 + ... + \gamma_m$.

By I.H. we obtain $\alpha\#\hat{\beta} < \alpha\#\hat{\gamma}$ and then $\alpha\#\beta < \alpha\#\gamma$.

(e) obvious.

(f) 1. If $\alpha \in P$, then either $\alpha + \beta = \beta \leq \alpha\#\beta$ or $\alpha + \beta = \alpha\#\beta$.

2. For arbitrary α the claim follows from 1. and (b).

Remark. If $\alpha = \omega^{\gamma_0} \cdot k_0 + \ldots + \omega^{\gamma_n} \cdot k_n$ and $\beta = \omega^{\gamma_0} \cdot l_0 + \ldots + \omega^{\gamma_n} \cdot l_n$ with $\gamma_0 > \ldots > \gamma_n$ and $k_i, l_i \geq 0$ then $\alpha\#\beta = \omega^{\gamma_0} \cdot (k_0 + l_0) + \ldots + \omega^{\gamma_n} \cdot (k_n + l_n)$.

Multisets

Definition.

A *multiset* is a function $M \in V$ with $\mathrm{ran}(M) \subseteq \omega \setminus \{0\}$. x is an *element of the multiset* M (written $x \in' M$), if $x \in \mathrm{dom}(M)$. For M a multiset and $x \notin \mathrm{dom}(M)$ we define $M(x) := 0$.

Union $\sqcup$, *intersection* $\sqcap$ and *difference* $-$ of multisets are defined as follows:

$\mathrm{dom}(M \sqcup N) := \mathrm{dom}(M) \cup \mathrm{dom}(N)$ and $(M \sqcup N)(x) := M(x) + N(x)$,

$\mathrm{dom}(M \sqcap N) := \mathrm{dom}(M) \cap \mathrm{dom}(N)$ and $(M \sqcap N)(x) := \min\{M(x), N(x)\}$,

$\mathrm{dom}(M - N) := \{x \in \mathrm{dom}(M) : N(x) < M(x)\}$ and $(M - N)(x) := M(x) \dot{-} N(x)$.

A multiset M is called *finite*, if $\mathrm{dom}(M)$ is finite. Every finite multiset is of the form $\{(x_0, k_0), ..., (x_{n-1}, k_{n-1})\}$ with $card\{x_0, ..., x_{n-1}\} = n \in \omega$ and $k_0, ..., k_{n-1} \in \omega \setminus \{0\}$.

Finite multisets can also be represented as equivalence classes of finite sequences. Loosely said, a multiset is a finite sequence where the order does not matter. To make this precise we introduce the following equivalence relation $\sim$ between finite sequences, and a mapping ms from finite sequences to multisets.

Definition.

$$(a_0, ..., a_{m-1}) \sim (b_0, ..., b_{n-1}) :\Leftrightarrow \begin{cases} m = n \text{ and there is a permutation } p \text{ of } n \\ \text{such that } (a_{p(0)}, ..., a_{p(n-1)}) = (b_0, ..., b_{n-1}) \end{cases}.$$

For each finite sequence $(a_0, ..., a_{n-1})$ we define a finite multiset $ms(a_0, ..., a_{n-1}) := M$ by $\mathrm{dom}(M) := \{a_0, ..., a_{n-1}\}$ and $M(x) := |\{i < n : a_i = x\}|$.

Lemma 11.13. $a \sim b \Leftrightarrow ms(a) = ms(b)$.

Proof: "$\Rightarrow$": obvious.

"$\Leftarrow$": Let $a = (a_0, ..., a_{n-1})$, $b = (b_0, ..., b_{m-1})$ and $ms(a) = M = ms(b)$. Then $\{a_0, ..., a_{n-1}\} = \mathrm{dom}(M) = \{b_0, ..., b_{m-1}\}$. For $k < m$ let $p(k) := \min\{i < n : a_i = b_k \;\&\; i \notin \{p(0), ..., p(k-1)\}\}$. By induction on $k < m$ one proves that $p(k)$ is defined: Assume that $p(0), ..., p(k-1)$ are defined. Then $a_{p(j)} = b_j$ for $j < k$. Assumption: $\forall i < n(a_i = b_k \Rightarrow i \in \{p(0), ..., p(k-1)\})$. Then $M(b_k) = |\{i < n : a_i = b_k\}| = |\{j < k : a_{p(j)} = b_k\}| = |\{j < k : b_j = b_k\}| < |\{j < m : b_j = b_k\}| = M(b_k)$. Contradiction. Hence p is an injective mapping from m into n with $a_{p(j)} = b_j$. From this the claim follows, since $n = \sum_{x \in \mathrm{dom}(M)} M(x) = m$.

Remark.

For multisets M, N we have (a) $M = (M \sqcap N) \sqcup (M - N)$. (b) $N = (M - (M - N)) \sqcup (N - M)$.

Proof: (a) $\min\{M(x), N(x)\} + (M(x) \dot{-} N(x)) = M(x)$. (b) $M(x) \dot{-} (M(x) \dot{-} N(x)) = \min\{M(x), N(x)\}$.

Definition.

Let $\prec$ be a relation. The *multiset ordering* $\prec_{mul}$ is defined by:

$N \prec_{mul} M :\Leftrightarrow N \neq M \;\&\; \forall x \in' N - M \exists y \in' M - N(x \prec y)$.

Lemma 11.14

Let $\prec$ be a relation, and $o : V \to On$ such that $\forall x, y(x \prec y \to o(x) < o(y))$.

For each finite multiset $M = \{(x_1, k_1), \ldots, (x_n, k_n)\}$ let $\hat{o}(M) := \omega^{o(x_1)} \cdot k_1 \# \ldots \# \omega^{o(x_n)} \cdot k_n$.

(*Remark.* If $M = ms((a_1, ..., a_m))$ then $\hat{o}(M) = \omega^{o(a_1)} \# \ldots \# \omega^{o(a_m)}$.)

Then for all finite multisets M, N we have:

(a) $\hat{o}(M \sqcup N) = \hat{o}(M) \# \hat{o}(N)$, (b) $N \prec_{mul} M \Rightarrow \hat{o}(N) < \hat{o}(M)$.

Proof:

(a) obvious.

(b) By (a) $\hat{o}(N) = \hat{o}(M \sqcap N) \# \hat{o}(N - M)$ and $\hat{o}(M) = \hat{o}(M \sqcap N) \# \hat{o}(M - N)$.

It remains to prove $\hat{o}(N - M) < \hat{o}(M - N)$.

Case 1: $N - M = \emptyset$. Then $\hat{o}(N - M) = 0$ and $M - N \neq \emptyset$ (since $N \neq M$). Hence $0 < \hat{o}(M - N)$.

Case 2: $N - M \neq \emptyset$. Then also $M - N \neq \emptyset$ (since $N \prec_{mul} M$), and for $\alpha := \max\{o(x) : x \in' N - M\}$ and $\beta := \max\{o(x) : x \in' M - N\}$ we have $\alpha < \beta$. Hence $\hat{o}(N - M) < \omega^{\alpha+1} \leq \omega^{\beta} \leq \hat{o}(M - N)$.

Corollary

If $\prec$ is wellfounded, then $\prec_{mul}$ restricted to the class of finite multisets is also wellfounded.

Proof: 1. $N \prec_{mul} M \Rightarrow \mathrm{dom}(N) \subseteq \mathrm{dom}(M) \cup \bigcup_{x\in\mathrm{dom}(M)}\{y : y \prec x\}$. Hence $\{N : N \prec_{mul} M\}$ is a set.

2. By $\prec$-recursion we define $o(x) := \sup\{o(y)+1 : y \prec x\}$.

From this by 11.14b we obtain the wellfoundedness of $\prec_{mul}$.

Supplement to §8

Axiom of Dependent Choice (DC)

If $A \neq \emptyset$ is a set and $R \subseteq A \times A$ then the following holds:

(*) $\forall x \in A \exists y \in A(yRx) \implies \exists f : \omega \to A$ with $\forall n \in \omega(f(n{+}1)Rf(n))$.

Lemma 8.13. (AC) implies (DC).

Proof: For $x \in A$ let $x_R := \{y \in A : yRx\}$. By (AC) there exists a function $g : A \to A$ such that $\forall x \in A(g(x) \in x_R)$. Take some $a_0 \in A$ and define $f : \omega \to A$ by recursion: $f(0) := a_0$, $f(n{+}1) := g(f(n))$.

Remark. If the set A can be wellordered, then (*) holds without (AC).

Lemma 8.14. Let A be a set and $R \subseteq A \times A$.

(a) R wellfounded $\implies \neg\exists f : \omega \to A \forall n(f(n{+}1)Rf(n))$.

(b) (DC) implies the reverse direction of (a).

Proof:

(a) Assume $f : \omega \to A$ with $\forall n(f(n{+}1)Rf(n))$. Then $f[\omega]$ is a nonempty set without R-minimal element.

(b) Assume that R is not wellfounded. Then there exists a nonempty set $X \subseteq A$ such that $\forall x \in X \exists y \in X(yRx)$. By (DC) $\exists f : \omega \to A \forall n(f(n{+}1)Rf(n))$.

Definition

If R is wellfounded then $|x|_R$ *(the rank of x w.r.t. R)* is defined by R-recursion as follows:

$|x|_R := \sup\{|y|_R{+}1 : yRx\}$.

$\|R\| := \{|x|_R : x \in V\}$.

Convention. For each class $A \subseteq On$ we set $\sup(A) := \bigcup A$. Hence $\sup(A) = On$ if A is a proper class.

Lemma 8.15.

Let R be wellfounded.

(a) $\|R\|$ is transitive and thus $\|R\| = \sup\{|x|_R{+}1 : x \in V\}$.

(b) If $R \subseteq A{\times}A$ and $A \neq \emptyset$ then $\|R\| = \{|x|_R : x \in A\} = \sup\{|x|_R{+}1 : x \in A\}$.

(c) If R is a wellordering on $A \neq \emptyset$ then $A \ni x \mapsto |x|_R$ is the inverse of the ordering function of (A, R), and $\|R\|$ is the ordertype of (A, R).

Proof:

(a) By R-induction one shows $\forall x(|x|_R \subseteq \|R\|)$: $\beta \in |x|_R \Rightarrow \beta \leq |y|_R$ for some $yRx \overset{\mathrm{IH}}{\Rightarrow} \beta \in \|R\|$.

(b) $A \neq \emptyset \Rightarrow$ A has an R-minimal element $x_0 \Rightarrow 0 = |x_0|_R \in \{|x|_R : x \in A\}$.

If $x \notin A$ then $|x|_R = 0 \in \{|x|_R : x \in A\}$.

(c) We have to prove that $x \mapsto |x|_R$ is an isomorphism from (A, R) onto $(\|R\|, <)$. But this is obvious.

§12 Inductive Definitions

Definition

Let M be a set and $\Phi : \mathcal{P}(M) \to \mathcal{P}(M)$.

We assume that Φ *is monotone, i.e.,* $\forall X, Y \in \mathcal{P}(M)(\, X \subseteq Y \;\Rightarrow\; \Phi(X) \subseteq \Phi(Y)\,)$.

$\mathrm{I}_\Phi := \bigcap\{X \in \mathcal{P}(M) : \Phi(X) \subseteq X\}$ *(the intersection of all* Φ*-closed subsets of* M*)*

We say that the set I_Φ is *inductively defined by* Φ.

Definitions of this kind are called *(generalized) inductive definitions*.

Theorem 12.1

(a) $\Phi(X) \subseteq X \implies \mathrm{I}_\Phi \subseteq X$, for each set $X \subseteq M$.

(b) $\Phi(\mathrm{I}_\Phi) = \mathrm{I}_\Phi$.

So, I_Φ is the least Φ-closed set and also the least fixpoint of Φ.

Proof:

(a) trivial.

(b) HS: $\Phi(\mathrm{I}_\Phi) \subseteq \mathrm{I}_\Phi$. Proof: Let $Q := \{X \in \mathcal{P}(M) : \Phi(X) \subseteq X\}$. For each $X \in Q$ we have $\mathrm{I}_\Phi \subseteq X$ and thus $\Phi(\mathrm{I}_\Phi) \subseteq \Phi(X) \subseteq X$, since Φ is monotone. Hence $\Phi(\mathrm{I}_\Phi) \subseteq \bigcap Q = \mathrm{I}_\Phi$.

Now let $Y := \Phi(\mathrm{I}_\Phi)$. By HS $Y \subseteq \mathrm{I}_\Phi$. By monotonicity of Φ this yields $\Phi(Y) \subseteq \Phi(\mathrm{I}_\Phi) = Y$; hence $\mathrm{I}_\Phi \subseteq Y = \Phi(\mathrm{I}_\Phi)$ by (a).

Remark. Theorem 12.1a comprises an important proof principle:

To show that a propotition $A(x)$ holds for all $x \in \mathrm{I}_\Phi$, it suffices to prove that

the set $\{x \in M : A(x)\}$ is Φ-closed, i.e. $\Phi(\{x \in M : A(x)\}) \subseteq \{x \in M : A(x)\}$.

This principle is called *induction on the (inductive) definition of* I_Φ or briefly Φ*-induction*.

Example 1

$M :=$ set of all finite strings (words) over the alphabet $\textsc{Vars} \cup \mathcal{L}$, where $\mathcal{L}$ is a set of function symbols;

$\mathcal{L}^n := \{f \in \mathcal{L} : f \text{ is } n\text{-ary}\}$.

$\Phi : \mathcal{P}(M) \to \mathcal{P}(M)$, $\Phi(X) := \textsc{Vars} \cup \{ft_1...t_n : n \in \mathbb{N} \;\&\; f \in \mathcal{L}^n \;\&\; t_1, ..., t_n \in X\}$

By 12.1 I_Φ is the least set $X \subseteq M$ such that $\Phi(X) \subseteq X$, i.e. the least set X satisfying:

1. $\textsc{Vars} \subseteq X$;

2. If $n \in \mathbb{N}$, $f \in \mathcal{L}^n$ and $t_1, ..., t_n \in X$, then $ft_1...t_n \in X$.

This means that I_Φ is the set of all $\mathcal{L}$-terms.

Induction on the definition of I_Φ in this case runs as follows:

From $\forall x \in \textsc{Vars}.A(x)$ and $\forall n \in \mathbb{N} \forall f \in \mathcal{L}^n \forall t_1, ..., t_n \in M(A(t_1)\;\&\;...\;\&\;A(t_n) \Rightarrow A(ft_1...t_n))$

it follows that $A(t)$ holds for all $t \in \mathrm{I}_\Phi$.

Example 2

Let M be an vector space over $\mathbb{R}$ and $B \subseteq M$ fixed.

$\Phi : \mathcal{P}(M) \to \mathcal{P}(M)$, $\Phi(X) := B \cup \{0\} \cup \{x + y : x, y \in X\} \cup \{\alpha x : x \in X \ \& \ \alpha \in \mathbb{R}\}$.

Then $\mathrm{I}_\Phi = \bigcap\{X \in \mathcal{P}(M) : \Phi(X) \subseteq X\} = \bigcap\{X \in \mathcal{P}(M) : B \subseteq X \ \& \ X \text{ subspace of } M\} = \mathrm{Span}(B)$ is the subspace generated by B.

Lemma 12.2 (Modified Induction). $\Phi(\mathrm{I}_\Phi \cap X) \subseteq X \implies \mathrm{I}_\Phi \subseteq X$.

Proof:

Since Φ is monotone, we have $\Phi(\mathrm{I}_\Phi \cap X) \subseteq \Phi(\mathrm{I}_\Phi) \overset{12.1\mathrm{b}}{=} \mathrm{I}_\Phi$.

Hence: $\Phi(\mathrm{I}_\Phi \cap X) \subseteq X \ \Rightarrow \ \Phi(\mathrm{I}_\Phi \cap X) \subseteq \mathrm{I}_\Phi \cap X \overset{(a)}{\Rightarrow} \mathrm{I}_\Phi \subseteq \mathrm{I}_\Phi \cap X \subseteq X$.

For Example 1, the modified induction principle reads as follows:

From $\forall x \in \mathrm{VARS}\, A(x)$ and $\forall n \in \mathbb{N} \forall f \in \mathcal{L}^n \forall t_1, ..., t_n \in \mathrm{I}_\Phi (A(t_1) \ \& \ ... \ \& \ A(t_n) \Rightarrow A(f t_1 ... t_n))$

it follows that $A(t)$ holds for all $t \in \mathrm{I}_\Phi$.

Definition. $\mathrm{I}_\Phi^\alpha := \Phi(\mathrm{I}_\Phi^{<\alpha})$ with $\mathrm{I}_\Phi^{<\alpha} := \bigcup_{\xi<\alpha} \mathrm{I}_\Phi^\xi$ $(\alpha \in On)$

Theorem 12.3.

(a) $\alpha < \beta \ \Rightarrow \ \mathrm{I}_\Phi^\alpha \subseteq \mathrm{I}_\Phi^\beta$; (b) $\mathrm{I}_\Phi^{\alpha+1} = \Phi(\mathrm{I}_\Phi^\alpha)$;

(c) $\mathrm{I}_\Phi^{<\alpha} = \mathrm{I}_\Phi^\alpha$ for some $\alpha \in On$; (d) If $\mathrm{I}_\Phi^{<\alpha} = \mathrm{I}_\Phi^\alpha$, then $\mathrm{I}_\Phi^{<\alpha} = \bigcup\limits_{\xi \in On} \mathrm{I}_\Phi^\beta = \mathrm{I}_\Phi$.

Proof:

(a) trivial.

(b) $\mathrm{I}_\Phi^{\alpha+1} = \Phi(\mathrm{I}_\Phi^{<\alpha+1}) \overset{(a)}{=} \Phi(\mathrm{I}_\Phi^\alpha)$.

(c) Otherwise $F : On \to \mathcal{P}(M)$, $\alpha \mapsto \mathrm{I}_\Phi^\alpha$ would be injective. But then $\mathcal{P}(M)$ would not be a set.

(d) 1. By induction on β we get $\mathrm{I}_\Phi^\beta \subseteq \mathrm{I}_\Phi$ for all β: I.H. $\Rightarrow \mathrm{I}_\Phi^{<\beta} \subseteq \mathrm{I}_\Phi \Rightarrow \mathrm{I}_\Phi^\beta = \Phi(\mathrm{I}_\Phi^{<\beta}) \subseteq \Phi(\mathrm{I}_\Phi) = \mathrm{I}_\Phi$.

2. $\mathrm{I}_\Phi^{<\alpha} = \mathrm{I}_\Phi^\alpha = \Phi(\mathrm{I}_\Phi^{<\alpha}) \Rightarrow \mathrm{I}_\Phi \subseteq \mathrm{I}_\Phi^{<\alpha}$.

Definition. Φ is *continuous* iff $\Phi(X) \subseteq \bigcup\{\Phi(X_0) : X_0 \subseteq X \ \& \ X_0 \text{ finite}\}$ for all $X \in \mathcal{P}(M)$.

Satz 12.4. If Φ is continuous, then $\mathrm{I}_\Phi = \mathrm{I}_\Phi^{<\omega}$.

Beweis:

Let $J := \mathrm{I}_\Phi^{<\omega}$. By 12.3d $J \subseteq \mathrm{I}_\Phi$. On the other side $\Phi(J) \subseteq \bigcup\{\Phi(X_0) : X_0 \subseteq J \ \& \ X_0 \text{ finite}\} \subseteq \bigcup_{n\in\omega} \Phi(\mathrm{I}_\Phi^n) = \bigcup_{n\in\mathbb{N}} \mathrm{I}_\Phi^{n+1} = J$ and therefore $\mathrm{I}_\Phi \subseteq J$.

Remark. The operator Φ from Example 1 is continuos.

Proof: $t \in \Phi(X) \ \Rightarrow \ t \in \mathrm{VARS}$ or $\exists n \exists f \in \mathcal{L}^n \exists t_1, ..., t_n \in X (\, t = f t_1 ... t_n \,) \ \Rightarrow$

$\exists X_0 \subseteq X (\, X_0 \text{ finite } \& \, [\, t \in \mathrm{VARS}$ or $\exists n \exists f \in \mathcal{L}^n \exists t_1, ..., t_n \in X_0 (\, t = f t_1 ... t_n \,)\,])$.

Lemma 12.5 (Simultaneous inductive definitions)

For $j = 1, 2$ let $\Phi_j : \mathcal{P}(M) \times \mathcal{P}(M) \to \mathcal{P}(M)$ with

$\forall X_1, X_2, Y_1, Y_2 \in \mathcal{P}(M) [\, X_1 \subseteq Y_1 \ \& \ X_2 \subseteq Y_2 \ \Rightarrow \ \Phi_j(X_1, X_2) \subseteq \Phi_j(Y_1, Y_2)\,]$.

Then there are uniquely determined sets $\mathcal{I}_1, \mathcal{I}_2 \subseteq M$ such that

(a) $\Phi_j(\mathcal{I}_1, \mathcal{I}_2) = \mathcal{I}_j$ für $j = 1, 2$.

(b) $\forall X_1, X_2 \in \mathcal{P}(M)[\bigwedge_{j=1,2}(\Phi_j(X_1, X_2) \subseteq X_j) \Longrightarrow \bigwedge_{j=1,2}(\mathcal{I}_j \subseteq X_j)]$.

Proof:

Uniqueness follows immediately from (a) and (b). — Existence:

Definitions: $M' := \{1, 2\} \times M$. $\pi_j(X) := \{x \in M : (j, x) \in X\}$, for $X \subseteq M'$.

$\Phi : \mathcal{P}(M') \to \mathcal{P}(M')$, $\Phi(X) := \bigcup_{j=1,2}(\{j\} \times \Phi_j(\pi_1(X), \pi_2(X)))$

For $X \subseteq M'$ we obviously have $\pi_j(\Phi(X)) = \Phi_j(\pi_1(X), \pi_2(X))$.

Φ monotone: $X \subseteq Y \Rightarrow \pi_1(X) \subseteq \pi_1(Y)$ & $\pi_2(X) \subseteq \pi_2(Y) \implies$

$\Phi_j(\pi_1(X), \pi_2(X)) \subseteq \Phi_j(\pi_1(Y), \pi_2(Y))$ für $j = 1, 2 \implies \Phi(X) \subseteq \Phi(Y)$.

By Theorem 12.1 there exists the least fixpoint I_Φ of Φ. Let $\mathcal{I}_j := \pi_j(\mathrm{I}_\Phi)$ $(j = 1, 2)$.

(a) $\Phi_j(\mathcal{I}_1, \mathcal{I}_2) = \Phi_j(\pi_1(\mathrm{I}_\Phi), \pi_2(\mathrm{I}_\Phi)) = \pi_j(\Phi(\mathrm{I}_\Phi)) = \pi_j(\mathrm{I}_\Phi) = \mathcal{I}_j$

(b) Assume $\Phi_j(X_1, X_2) \subseteq X_j$ for $j = 1, 2$.

Let $X := \bigcup_{j=1,2}(\{j\} \times X_j)$. Then $\pi_j(X) = X_j$ and

$\Phi(X) = \bigcup_{j=1,2}(\{j\} \times \Phi_j(X_1, X_2)) \subseteq \bigcup_{j=1,2}(\{j\} \times X_j) = X$.

Hence $\mathrm{I}_\Phi \subseteq X$ and thus $\mathcal{I}_j = \pi_j(\mathrm{I}_\Phi) \subseteq \pi_j(X) = X_j$.

Example.

Let M be the set of all finite words over the alphabet $\{*\}$.

Let $\Phi_1(X_1, X_2) := \{*\} \cup \{w* : w \in X_2\}$ and $\Phi_2(X_1, X_2) := \{w* : w \in X_1\}$.

Claim: $\mathcal{I}_1 = \{w \in M : \mathrm{lh}(w) \text{ odd}\} =: O$ and $\mathcal{I}_2 = \{w \in M : 0 < \mathrm{lh}(w) \text{ even}\} =: E$.

Proof: Obviously $\Phi_1(O, E) \subseteq O$ and $\Phi_2(O, E) \subseteq E$; hence $\mathcal{I}_1 \subseteq O$ and $\mathcal{I}_2 \subseteq E$.

For the other direction, by induction on $\mathrm{lh}(w)$ one shows: $(w \in O \Rightarrow w \in \mathcal{I}_1)$ & $(w \in E \Rightarrow w \in \mathcal{I}_2)$.

Definition.

For each relation $R \subseteq M \times M$ let $\Phi_R : \mathcal{P}(M) \to \mathcal{P}(M)$, $\Phi_R(X) := \{x \in M : \forall y R x (y \in X)\}$.

$\mathrm{Acc}(M, R) := \mathrm{I}_{\Phi_R}$ *(the accessible part of* (M, R) *)*

$(\mathrm{Acc}(M, R) = \bigcap\{X \subseteq M : \forall x \in M(\forall y R x (y \in X) \Rightarrow x \in X)\})$

Theorem 12.6.

Let R be a binary relation on M, and $\mathrm{Acc} := \mathrm{Acc}(M, R)$.

(a) $\forall x[x \in M$ & $\forall y R x (y \in \mathrm{Acc}) \Leftrightarrow x \in \mathrm{Acc}]$.

(b) $\forall x \in \mathrm{Acc}[\forall y R x (y \in X) \Rightarrow x \in X] \implies \mathrm{Acc} \subseteq X$, for every $X \subseteq M$. ($R{\restriction}\mathrm{Acc}$ is wellfounded)

(c) R wellfounded $\Leftrightarrow M = \mathrm{Acc}$.

Proof:

(a) follows from 12.1b. (b) follows from "$\mathrm{I}_\Phi \cap \Phi(X) \subseteq X \Rightarrow \mathrm{I}_\Phi \subseteq X$", which follows from 12.2.

(c) "⇒": By (a) we have $\forall x \in M(\forall y R x (y \in \mathrm{Acc}) \Rightarrow x \in \mathrm{Acc})$.

By R-induction from this we get $\forall x \in M(x \in \mathrm{Acc})$.

"⇐": follows from (b).

Definition. For $x \in \mathrm{I}_\Phi$ let $|x|_\Phi := \min\{\alpha : x \in \mathrm{I}_\Phi^\alpha\}$

Lemma 12.7. If $\Phi = \Phi_R$ then $|x|_\Phi = \sup\{|y|_\Phi{+}1 : yRx\}$ for every $x \in \mathrm{Acc}(M, R)$.

Proof:

$x \in \mathrm{I}_\Phi^\alpha \Leftrightarrow x \in \Phi(\mathrm{I}_\Phi^{<\alpha}) \Leftrightarrow \forall yRx(y \in \mathrm{I}_\Phi^{<\alpha}) \Leftrightarrow \forall yRx(|y|_\Phi < \alpha)$.

Hence $|x|_\Phi = \min\{\alpha : x \in \mathrm{I}_\Phi^\alpha\} = \min\{\alpha : \forall yRx(|y|_\Phi < \alpha)\} = \sup\{|y|_\Phi{+}1 : yRx\}$

Theorem 12.8 (Recursion over an inductively defined set).

For each function $G : \mathrm{I}_\Phi \times V \to V$ there is a unique function $F : \mathrm{I}_\Phi \to V$ such that $F(x) = G(x, F{\restriction}\mathrm{I}_\Phi^{<|x|_\Phi})$ for all $x \in \mathrm{I}_\Phi$.

Proof:

Let $R \subseteq \mathrm{I}_\Phi \times \mathrm{I}_\Phi$ be defined by $R(y, x) :\Leftrightarrow |y|_\Phi < |x|_\Phi$.

Then R is wellfounded and $x_R = \{y : x, y \in \mathrm{I}_\Phi \,\&\, |y|_\Phi < |x|_\Phi\} = \begin{cases} \mathrm{I}_\Phi^{<|x|_\Phi} & \text{if } x \in \mathrm{I}_\Phi \\ \emptyset & \text{otherwise} \end{cases}$.

Definition (Trees)

Let M be a set.

$M^{<\omega} := \{(x_0, ..., x_{n-1}) : n \in \mathbb{N} \,\&\, x_0, ..., x_{n-1} \in M\}$

An *M-tree* is a subset T of $M^{<\omega}$ such that

(i) $() \in T$,

(ii) if $(x_0, ..., x_n) \in T$ then $(x_0, ..., x_{n-1}) \in T$.

$\mathcal{T}_M :=$ set of all M-trees.

$\sigma \sqsubset \tau :\Leftrightarrow \sigma$ is a proper initial segment of τ (i.e., $\exists\rho(\tau = \sigma * \rho) \,\&\, \sigma \neq \tau$).

T is *wellfounded* $:\Leftrightarrow \sqsupset{\restriction}T$ is wellfounded.

Definition

$T|_\sigma := \{\nu : \sigma * \nu \in T\}$.

$S \ll T :\Leftrightarrow \exists x[(x) \in T \,\&\, S = T|_{(x)}]$ *(S is an immediate subtree of T)*

Inductive Definition of $\mathcal{WT}_M$

$T \in \mathcal{T}_M \,\&\, \forall S \ll T(S \in \mathcal{WT}_M) \implies T \in \mathcal{WT}_M$.

For $T \in \mathcal{WT}_M$ let $\mathsf{hgt}(T) := |T|_\Phi$ where Φ is the operator of the inductive definition of $\mathcal{WT}_M$.

So, $\mathsf{hgt}(T) = \sup\{\mathsf{hgt}(S){+}1 : S \ll T\}$. We call $\mathsf{hgt}(T)$ the *height of T*.

Theorem 12.9

$\forall T \in \mathcal{T}_M(\, T$ wellfounded $\Leftrightarrow T \in \mathcal{WT}_M\,)$.

Proof:

"⇒": Let T be wellfounded. By $\sqsupset{\restriction}T$-induction we get $\forall\sigma \in T(T|_\sigma \in \mathcal{WT}_M)$:

$\sigma \in T \,\&\, \forall\nu \in T(\nu \sqsupset \sigma \Rightarrow T|_\nu \in \mathcal{WT}_M) \Rightarrow T|_\sigma \in \mathcal{T}_M \,\&\, \forall S \ll T|_\sigma(S \in \mathcal{WT}_M) \Rightarrow T|_\sigma \in \mathcal{WT}_M$.

"$\Leftarrow$": Assume $\forall S \ll T (S \text{ wellfounded})$ and let $\emptyset \neq X \subseteq T$.

We have to prove that there is a $\nu_0 \in X$ such that $\neg\exists \sigma \in X(\nu_0 \sqsubset \sigma)$.

Case 1: $X = \{()\}$. Trivial.

Case 2: $(x_0) * \nu \in X$. Let $X' := \{\sigma : (x_0) * \sigma \in X\}$. Then $\emptyset \neq X' \subseteq S := T|_{(x_0)}$. By assumption S is wellfounded. Hence there is a $\nu_0 \in X'$ such that $\neg\exists \sigma \in X'(\nu_0 \sqsubset \sigma)$. From this we get $(x_0) * \nu_0 \in X$ and $\neg\exists \tau \in X((x_0) * \nu_0 \sqsubset \tau)$.

Definition.

If T is a wellfounded tree and $\sigma \in T$ then $|\sigma|_T := |\sigma|_{\sqsupset\restriction T}$.

Lemma 12.10. If T is a wellfounded tree then

(a) $|\sigma|_T = \sup\{|\sigma*(x)|_T{+}1 : \sigma*(x) \in T\}$ for each $\sigma \in T$;

(b) $\mathsf{hgt}(T) = |()|_T$;

(c) $\mathsf{hgt}(T){+}1 = \|\sqsupset\restriction T\|$

Proof:

(a) By definition $|\sigma|_T = \sup\{|\nu|_T{+}1 : \sigma \sqsubset \nu \in T\}$ (for all $\sigma \in T$). Hence $\forall \sigma, \tau \in T(\sigma \sqsubseteq \tau \Rightarrow |\tau|_T \leq |\sigma|_T\}$. Since $\forall \nu(\sigma \sqsubset \nu \in T \Rightarrow \exists x(\sigma*(x) \in T \;\&\; \sigma*(x) \sqsubseteq \nu))$, it follows that $|\sigma|_T = \sup\{|\sigma*(x)|_T{+}1 : \sigma*(x) \in T\}$.

(b) HS: If $S = T|_{(x)} \ll T$ and $\sigma \in S$ then $|\sigma|_S = |(x)*\sigma|_T$.

Proof by induction on $|\sigma|_S$:

$|\sigma|_S = \sup\{|\nu|_S{+}1 : \sigma \sqsubset \nu \in S\} \overset{\text{IH}}{=} \sup\{|(x)*\nu|_T{+}1 : \sigma \sqsubset \nu \in S\} = \sup\{|\tau|_T{+}1 : (x)*\sigma \sqsubset \tau \in T\} = |(x)*\sigma|_T$.

Now we prove the claim by induction over the definition of $\mathcal{WT}_M$:

$\mathsf{hgt}(T) = \sup\{\mathsf{hgt}(S){+}1 : S \ll T\} \overset{\text{IH}}{=} \sup\{|()|_S{+}1 : S \ll T\} \overset{\text{HS}}{=} \sup\{|(x)|_T{+}1 : (x) \in T\} \overset{\text{(a)}}{=} |()|_T$.

(c) $\mathsf{hgt}(T) \overset{\text{(b)}}{=} |()|_T \overset{\text{Def}}{=} \sup\{|\sigma|_T{+}1 : () \sqsubset \sigma \in T\} \;\Rightarrow\; \mathsf{hgt}(T){+}1 = \sup\{|\sigma|_T{+}1 : \sigma \in T\} \overset{8.15\text{c}}{=} \|\sqsupset\restriction T\|$.

Lemma 12.11. Assuming (DC) or "M can be wellordered", the following holds for each $T \in \mathcal{T}_M$:

T wellfounded $\Leftrightarrow\; \neg\exists (a_i)_{i\in\mathbb{N}} \forall n \in \mathbb{N}[\,(a_0, ..., a_{n-1}) \in T\,]$.

Proof:

Note that with M also $M^{<\omega}$ can be wellordered.

T wellfounded $\overset{8.14}{\Leftrightarrow}\; \neg\exists f : \mathbb{N} \to T\, \forall n[\, f(n) \sqsubset f(n{+}1)\,] \;\Leftrightarrow$

$\neg\exists (a_i)_{i\in\mathbb{N}} \forall n[\,(a_0, ..., a_{n-1}) \in T\,]$.

§13 Elementary recursion theory

Definition.

An *n-ary partial function* is a function f with $\mathrm{dom}(f) \subseteq \mathbb{N}^n$ and $\mathrm{ran}(f) \subseteq \mathbb{N}$.

Notation: $f : \mathbb{N}^n \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$.

For partial functions f, g we define:

$f(\vec{a}) \simeq g(\vec{c}) \;:\Leftrightarrow\; [\vec{a} \in \mathrm{dom}(f) \,\&\, \vec{c} \in \mathrm{dom}(g) \,\&\, f(\vec{a}) = g(\vec{c})]$ or $[\vec{a} \notin \mathrm{dom}(f) \,\&\, \vec{c} \notin \mathrm{dom}(g)]$.

Similarly for more complex expressions containing (symbols for) partial functions.

Definition of the operations $\circ$, R, μ *for partial functions:*

1. For $h : \mathbb{N}^m \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$ and $g_1, ..., g_m : \mathbb{N}^n \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$ let $(\circ h g_1 ... g_m) : \mathbb{N}^n \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$ be defined by:
   $(\circ h g_1 ... g_m)(\vec{a}) = b \;\Leftrightarrow\; \exists b_1 \ldots \exists b_m [h(b_1, ..., b_m) = b \,\&\, g_1(\vec{a}) = b_1 \,\&\, \ldots \,\&\, g_m(\vec{a}) = b_m]$.
2. For $g : \mathbb{N}^n \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$ and $h : \mathbb{N}^{n+2} \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$ let $(\mathsf{R}gh) : \mathbb{N}^{n+1} \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$ be defined by:
   $(\mathsf{R}gh)(\vec{a}, 0) \simeq g(\vec{a})$,
   $(\mathsf{R}gh)(\vec{a}, k+1) = b \;\Leftrightarrow\; \exists c [\,(\mathsf{R}gh)(\vec{a}, k) = c \,\&\, h(\vec{a}, k, c) = b\,]$.
3. For $g : \mathbb{N}^{n+1} \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$ let $(\mu g) : \mathbb{N}^n \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$ be defined by:
   $(\mu g)(\vec{a}) = b \;\Leftrightarrow\; g(\vec{a}, b) = 0 \,\&\, \forall i < b \exists c [c \neq 0 \,\&\, g(\vec{a}, i) = c]$.

Abbreviation:

For $R \subseteq \mathbb{N}^{n+1}$ and $\vec{a} \in \mathbb{N}^n$ let: $\mu y.R(\vec{a}, y) :\simeq \begin{cases} \min\{k : \; R(\vec{a}, k)\} & \text{if } \exists k \, R(\vec{a}, k) \\ \text{undefined} & \text{otherwise} \end{cases}$.

In other words, $\vec{a} \mapsto \mu y.R(\vec{a}, y)$ denotes the partial function (μg) with $g(\vec{a}, b) := 1 \dot{-} \mathbf{1}_R(\vec{a}, b)$.

Definition

Let $f : \mathbb{N}^n \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$.

f is *partial-recursive* $:\Leftrightarrow$ $\mathsf{Graph}(f)$ is recursive enumerable.

f is *total* $:\Leftrightarrow$ $\mathrm{dom}(f) = \mathbb{N}^n$.

$\mathbb{P}^n$ denotes the set of all n-ary partial recursive functions. $\mathbb{P} := \bigcup_{n \in \mathbb{N}} \mathbb{P}^n$.

Remark.

A function $f : \mathbb{N}^n \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$ is recursive if and only if it is partial-recursive and total.

Theorem 13.1

$\mathbb{P}$ is the least set of functions containing the basic functions C^n_k, S, I^n_i and being closed under the operations $\circ$ (composition), R (primitive recursion), μ (μ-operator or minimization).

Proof: cf. proof of 4.15.

Corollary

If $R \subseteq \mathbb{N}^{n+1}$ is recursive, the function f defined by $f(\vec{a}) :\simeq \mu y.R(\vec{a}, y)$ is partial recursive.

Churchsch's Thesis

A function $f : \mathbb{N}^n \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$ is computable in the intuitive sense iff it is partial recursive.

Lemma 13.2

A $Q \subseteq \mathbb{N}^n$ is recursively enumerable iff $Q = \mathrm{dom}(f)$ for some n-ary partial recursive function f.

Proof:

1. Let Q be recursively enumerable. Then $Q = \{\vec{a} : \exists b\, g(\vec{a}, b) = 0\}$ for some $g \in \mathrm{PR}^{n+1}$. Hence $Q = \mathrm{dom}((\mu g))$ and $(\mu g) \in \mathbb{P}$.

2. If $f \in \mathbb{P}$, then $\mathsf{Graph}(f)$ is recursively enumerable, and hence $\mathrm{dom}(f) = \{\vec{a} : \exists b\, (\vec{a}, b) \in f\}$ is recursively enumerable too.

Lemma. For every recursively enumerable relation $R \subseteq \mathbb{N}^n$ there exists an n-ary arithmetic formula A such that $R = \{\vec{a} \in \mathbb{N}^n : \mathsf{Q} \vdash A(\underline{\vec{a}})\}$.

Proof: Let $R(\vec{a}) \Leftrightarrow \exists b R_0(\vec{a}, b)$ with primitive recursive R_0. By Theorem 6.5 there exists an $n{+}1$-ary arithmetic formula B such that (1) $R_0(\vec{a}, b) \Rightarrow \mathsf{Q} \vdash B(\underline{\vec{a}}, \underline{b})$; (2) $\neg R_0(\vec{a}, b) \Rightarrow \mathsf{Q} \vdash \neg B(\underline{\vec{a}}, \underline{b})$. Since the standard model $\mathcal{N}$ is a model of Q, it follows that Q is ω-consistent (cf. §5, pg.34). Now we have:

$R(\vec{a}) \Rightarrow R_0(\vec{a}, b)$ for some $b \overset{(1)}{\Rightarrow} \mathsf{Q} \vdash B(\underline{\vec{a}}, \underline{b}) \Rightarrow \mathsf{Q} \vdash \exists y B(\underline{\vec{a}}, y)$;

$\neg R(\vec{a}) \Rightarrow \neg R_0(\vec{a}, b)$ for all $b \overset{(2)}{\Rightarrow} \mathsf{Q} \vdash \neg B(\underline{\vec{a}}, \underline{b})$ for all $b \overset{\omega\text{-consistency}}{\Rightarrow} \mathsf{Q} \nvdash \exists y B(\underline{\vec{a}}, y)$.

Theorem 13.3 (Kleene's Normalform Theorem)

There is a primitive recursive function U and for each $n \geq 1$ a primitive recursive relation T^n, such that

$\mathbb{P}^n = \{\{e\}^n : e \in \mathbb{N}\}$, where $\{e\}^n : \mathbb{N}^n \overset{\text{part}}{\longrightarrow} \mathbb{N}$, $\{e\}^n(\vec{a}) :\simeq U(\mu y.\mathrm{T}^n(e, \vec{a}, y))$.

The relations T^n $(n \geq 1)$ are called *Kleene's T-predicates*.

Proof:

Definition: $\mathsf{Sb}^n_{n+1}(e) := e$, $\mathsf{Sb}^n_k(e, a_k, ..., a_n) := \mathsf{Sub}(\mathsf{Sb}^n_{k+1}(e, a_{k+1}, ..., a_n), \ulcorner v_k \urcorner, \ulcorner \underline{a_k} \urcorner)$.

Then $\mathsf{Sb}^n_k(\ulcorner A \urcorner, a_k, ..., a_n) = \ulcorner A_{v_k,...,v_n}(\underline{a_k}, ..., \underline{a_n}) \urcorner$.

Definition:

$\mathrm{T}^n(e, a_1, ..., a_n, c) :\Leftrightarrow \mathsf{Prf}_{\mathsf{Q}}(\mathsf{Sb}^n_0(e, (c)_0, a_1, ..., a_n), (c)_1)$

$U(c) := (c)_0$,

$\{e\}^n(\vec{a}) :\simeq U(\mu y.\mathrm{T}^n(e, \vec{a}, y))$.

Obviously U, T^n are primitive recursive. From this it follows immediately, that for each $n \geq 1$ the function $(e, \vec{a}) \mapsto \{e\}^n(\vec{a})$ is partial recursive. Hence for each $e \in \mathbb{N}$ and $n \geq 1$ the function $\{e\}^n$ is partial recursive.

Assume now that $f : \mathbb{N}^n \overset{\text{part}}{\longrightarrow} \mathbb{N}$ is partial recursive. By the above Lemma we then have an $n{+}1$-ary arithmetic formula A such that $\forall \vec{a}, b(f(\vec{a}) = b \Leftrightarrow \mathsf{Q} \vdash A(\underline{b}, \underline{\vec{a}}))$.

Let $e := \ulcorner A \urcorner$. Then the following holds: $f(\vec{a}) = b \Leftrightarrow \exists d.\mathsf{Prf}_{\mathsf{Q}}(\ulcorner A(\underline{b}, \underline{\vec{a}}) \urcorner, d) \Leftrightarrow \exists d.\mathsf{Prf}_{\mathsf{Q}}(\mathsf{Sb}^n_0(e, b, \vec{a}), d) \Leftrightarrow \exists c[\, b = (c)_0 \;\&\; \mathsf{Prf}_{\mathsf{Q}}(\mathsf{Sb}^n_0(e, (c)_0, \vec{a}), (c)_1)] \Leftrightarrow \exists c[\, b = U(c) \;\&\; \mathrm{T}^n(e, \vec{a}, c)\,]$.

From this we get $\mathrm{dom}(f) \subseteq \mathrm{dom}(\{e\}^n)$ and $(\,\{e\}^n(\vec{a}) = b \Rightarrow f(\vec{a}) = b\,)$, hence $f = \{e\}^n$.

Remark. *The $(n{+}1)$-ary function $(e, \vec{a}) \mapsto \{e\}^n(\vec{a})$ is partial recursive.*

Abbreviation. $W^n_e := \mathrm{dom}(\{e\}^n)$ $(= \{\vec{a} \in \mathbb{N}^n : \exists c\, \mathrm{T}^n(e, \vec{a}, c)\})$.

Remark. By 13.2 and 13.3, $\{W^n_e : e \in \mathbb{N}\}$ is the set of all n-ary recursively enumerable relations.

Theorem 13.4 (Unsolvability of the halting problem)

$K := \{e \in \mathbb{N} : e \in W^1_e\}$ is recursively enumerabel but not recursive.

Proof:

1. K is r.e., since $(e \in W_e^1 \Leftrightarrow \exists c\, \mathrm{T}^1(e,e,c))$ and T^1 prim. recursive.

2. *Assumption*: K recursive. Then also $\mathbb{N} \setminus K$ is recursive (thence r.e.) and by 13.3 there exists e_0 with $\mathbb{N} \setminus K = W_{e_0}^1$. Hence: $e_0 \in K \Leftrightarrow e_0 \in W_{e_0}^1 \Leftrightarrow e_0 \notin K$. *Contradiction.*

Remark.

Intuitively T^n has the following meaning:

$$\mathrm{T}^n(e,\vec{a},\langle b,k\rangle) \iff \left\{ \begin{array}{l} e \text{ is the number of a program which on the} \\ \text{input } \vec{a} \text{ after } k \text{ steps delivers the output } b. \end{array} \right.$$

Then K is the set of all program numbers e such that *the program with number e terminates on input e.*

Theorem 13.5 (s-m-n Theorem)

For each $m, n \geq 1$ there is an $(m+1)$-ary primitive recursive function $\mathbf{s}_n^m$ such that the following holds for all $e, c \in \mathbb{N}$, $\vec{a} \in \mathbb{N}^n$, $\vec{b} \in \mathbb{N}^m$:

(a) $\mathrm{T}^{n+m}(e,\vec{a},\vec{b},c) \iff \mathrm{T}^n(\mathbf{s}_n^m(e,\vec{b}),\vec{a},c)$,

(b) $\{e\}^{n+m}(\vec{a},\vec{b}) \simeq \{\mathbf{s}_n^m(e,\vec{b})\}^n(\vec{a})$.

Corollary. For each $g \in \mathbb{P}^{n+m}$ there is an $s \in \mathrm{PR}^m$, so daß $g(\vec{a},\vec{b}) \simeq \{s(\vec{b})\}^n(\vec{a})$ for all $\vec{a} \in \mathbb{N}^n$, $\vec{b} \in \mathbb{N}^m$.

Proof: (a) We have:

$\mathrm{T}^{n+m}(e,\vec{a},\vec{b},c) \Leftrightarrow \mathsf{Prf}_{\mathsf{Q}}(\mathsf{Sb}_0^{n+m}(e,(c)_0,\vec{a},\vec{b}),(c)_1)$ and

$\mathrm{T}^n(\mathbf{s}_n^m(e,\vec{b}),\vec{a},c) \Leftrightarrow \mathsf{Prf}_{\mathsf{Q}}(\mathsf{Sb}_0^n(\mathbf{s}_n^m(e,\vec{b}),(c)_0,\vec{a}),(c)_1)$.

Therefore we have to define $\mathbf{s}_n^m$ so that $\mathsf{Sb}_0^{n+m}(e,c,\vec{a},\vec{b}) = \mathsf{Sb}_0^n(\mathbf{s}_n^m(e,\vec{b}),c,\vec{a})$.

But for $e = \ulcorner A \urcorner$ we have

$\mathsf{Sb}_0^{n+m}(e,c,\vec{a},\vec{b}) = \ulcorner A_{v_0,\ldots,v_{n+m}}(\underline{c},\underline{\vec{a}},\underline{\vec{b}}) \urcorner = \ulcorner A_{v_{n+1},\ldots,v_{n+m}}(\underline{b}_1,\ldots,\underline{b}_m)_{v_0,\ldots,v_n}(\underline{c},\underline{\vec{a}}) \urcorner = \mathsf{Sb}_0^n(\mathsf{Sb}_{n+1}^{n+m}(e,\vec{b}),c,\vec{a})$.

Therefore we define: $\mathbf{s}_n^m = \mathsf{Sb}_{n+1}^{n+m}$.

Claim: $e \in \mathbb{N}$ & $\vec{b} \in \mathbb{N}^m$ & $k \leq n+1 \Rightarrow \mathsf{Sb}_k^{n+m}(e,a_k,\ldots,a_n,\vec{b}) = \mathsf{Sb}_k^n(\mathsf{Sb}_{n+1}^{n+m}(e,\vec{b}),a_k,\ldots,a_n)$.

Proof by induction on $n+1-k$: Abb.: $e^* := \mathsf{Sb}_{n+1}^{n+m}(e,\vec{b})$.

1. $\mathsf{Sb}_{n+1}^{n+m}(e,\vec{b}) = e^* = \mathsf{Sb}_{n+1}^n(e^*)$.

2. $\mathsf{Sb}_k^{n+m}(e,a_k,\ldots,a_n,\vec{b}) \overset{\text{Def}}{=} \mathsf{Sub}(\mathsf{Sb}_{k+1}^{n+m}(e,a_{k+1},\ldots,a_n,\vec{b}),\ulcorner v_k \urcorner,\ulcorner \underline{a}_k \urcorner) \overset{\text{IH}}{=}$

$= \mathsf{Sub}(\mathsf{Sb}_{k+1}^n(e^*,a_{k+1},\ldots,a_n),\ulcorner v_k \urcorner,\ulcorner \underline{a}_k \urcorner) \overset{\text{Def}}{=} \mathsf{Sb}_k^n(e^*,a_k,\ldots,a_n)$.

Proof of the corollary: Take e such that $g = \{e\}^{n+m}$. Then $g(\vec{a},\vec{b}) = \{\mathbf{s}_n^m(e,\vec{b})\}^n(\vec{a})$.

Theorem 13.6 (Recursion Theorem)

For each $g \in \mathbb{P}^{n+1}$ there exists an $e \in \mathbb{N}$ such that $\{e\}^n(\vec{a}) \simeq g(e,\vec{a})$ for all $\vec{a} \in \mathbb{N}^n$.

Proof:

By 13.3 there exists a k with $\{k\}^{n+1}(\vec{a},e) \simeq g(\mathbf{s}_n^1(e,e),\vec{a})$, for all $\vec{a},e$. — Let $e := \mathbf{s}_n^1(k,k)$.

Then $\{e\}^n(\vec{a}) \simeq \{\mathbf{s}_n^1(k,k)\}^n(\vec{a}) \overset{13.5}{\simeq} \{k\}^{n+1}(\vec{a},k) \simeq g(\mathbf{s}_n^1(k,k),\vec{a}) \simeq g(e,\vec{a})$.

Corollary

For each $n \geq 1$ und every 1-ary recursive function f there exists an $e \in \mathbb{N}$ such that $\{f(e)\}^n = \{e\}^n$.

Proof: Let $g(e,\vec{a}) :\simeq \{f(e)\}^n(\vec{a})$ and apply 13.6.

Example to the Recursion Theorem

The Ackermann function $\mathcal{A} : \mathbb{N}^2 \to \mathbb{N}$ is define by

$$\mathcal{A}(m,k) := \begin{cases} k+1 & \text{if } m = 0 \\ \mathcal{A}(m \dot{-} 1, 1) & \text{if } m > 0 \,\&\, k = 0 \\ \mathcal{A}(m \dot{-} 1, \mathcal{A}(m, k \dot{-} 1)) & \text{otherwise} \end{cases} .$$

In order to prove that $\mathcal{A}$ is recursive we define a partial recursive function g by:

$$g(e,m,k) :\simeq \begin{cases} k+1 & \text{if } m = 0 \\ \{e\}^2(m \dot{-} 1, 1) & \text{if } m > 0 \,\&\, k = 0 \\ \{e\}^2(m \dot{-} 1, \{e\}^2(m, k \dot{-} 1)) & \text{otherwise} \end{cases} .$$

By the Recursion Theorem there is an e such that $\{e\}^2(m,k) \simeq g(e,m,k)$ for all m, k.

By main induction on m and side induction on k one proves $\{e\}^2(m,k) \simeq \mathcal{A}(m,k)$ for all k, m. Hence $\mathcal{A}$ is recursive.

Theorem (Recursion Lemma).

Let $\prec \subseteq \mathbb{N} \times \mathbb{N}$ be wellfounded, and $R \subseteq \mathbb{N}^{n+2}$.

Assume that $h \in \mathbb{P}^{n+2}$ with $\forall e \forall x \forall \vec{a} [\forall y \prec x \, R(y, \vec{a}, \{e\}(y, \vec{a})) \to R(x, \vec{a}, h(e, x, \vec{a}))]$.

Then there exists an $f \in \mathbb{P}$ such that $\forall \vec{a} \forall x \, R(x, \vec{a}, f(x, \vec{a}))$.

Proof:

By the Recursion Theorem there is an $e \in \mathbb{N}$ such that $\{e\}(x, \vec{a}) \simeq h(e, x, \vec{a})$ for all $x, \vec{a}$.

By $\prec$-indcution on x we prove $R(x, \vec{a}, \{e\}(x, \vec{a}))$:

$\forall y \prec x \, R(y, \vec{a}, \{e\}(y, \vec{a})) \;\Rightarrow\; R(x, \vec{a}, h(e, x, \vec{a})) \;\Rightarrow\; R(x, \vec{a}, \{e\}(x, \vec{a}))$.

Theorem 13.7 (Rice)

If $\emptyset \neq \mathcal{F} \subsetneqq \mathbb{P}^n$, then the set $\{e \in \mathbb{N} : \{e\}^n \in \mathcal{F}\}$ is not recursive.

Proof:

By assumption there are $e_0, e_1 \in \mathbb{N}$ with $\{e_0\} \notin \mathcal{F}$ and $\{e_1\} \in \mathcal{F}$.

Let $R \subseteq \mathbb{N}$ be recursive. We prove $R \neq \{e : \{e\}^n \in \mathcal{F}\}$.

We define $g \in \mathbb{P}^{n+1}$ by $g(e,a) :\simeq \begin{cases} \{e_0\}^n(a) & \text{if } e \in R \\ \{e_1\}^n(a) & \text{if } e \notin R \end{cases}$.

By the Recursion Theorem there exists an e with $\forall a \in \mathbb{N}^n (\{e\}^n(a) \simeq g(e,a))$.

Hence:

$e \in R \;\Rightarrow\; \forall a (\{e\}^n(a) \simeq g(e,a) \simeq \{e_0\}^n(a)) \;\Rightarrow\; \{e\}^n = \{e_0\}^n \;\Rightarrow\; \{e\} \notin \mathcal{F}$.

$e \notin R \;\Rightarrow\; \forall a (\{e\}^n(a) \simeq g(e,a) \simeq \{e_1\}^n(a)) \;\Rightarrow\; \{e\}^n = \{e_1\}^n \;\Rightarrow\; \{e\} \in \mathcal{F}$.

Recursive ordinals, Kleene's $\mathcal{O}$

Definition

A wellordering (A, R) is called *recursive* if $A \subseteq \mathbb{N}$ and R are recursive.

$\omega_1^{CK} := \sup\{\|(A,R)\| : (A,R) \text{ is a recursive wellordering}\}$,
where $\|(A,R)\|$ is the ordertype of a (A,R) (cf. 8.15).

Obviously ω_1^{CK} is the least ordinal which is not the ordertype of a recursive wellordering.

Definition For $s, t, e \in \mathbb{N}$:
$s \sqsubset t \iff \mathrm{lh}(s) < \mathrm{lh}(t)\ \&\ \forall i < \mathrm{lh}(s)[(s)_i = (t)_i]$;
$s \sqsubseteq t \iff s \sqsubset t$ or $s = t$.

$B \subseteq \mathbb{N}$ is called a *tree* iff $\forall s,t(s \in B\ \&\ t \sqsubset s \Rightarrow t \in B)$

A tree B is called *wellfounded* iff $\sqsupset\restriction B$ is wellfounded.

Lemma 13.8. A tree $B \subseteq \mathbb{N}$ is wellfounded if and only if $\forall f : \mathbb{N} \to \mathbb{N} \exists n(\overline{f}(n) \notin B)$.

Proof: cf. 12.11.

Definition (Kleene-Brouwer ordering).
$s <_{\mathrm{KB}} t \iff t \sqsubset s$ or $\exists c,a,b(c * \langle a\rangle \sqsubseteq s\ \&\ c * \langle b\rangle \sqsubseteq t\ \&\ a < b)$.

Lemma 13.9.
(a) $(\mathbb{N}, <_{\mathrm{KB}})$ is a primitive recursive linear ordering.
(b) For every tree $B \subseteq \mathbb{N}$: B is wellfounded $\iff$ $(B, <_{\mathrm{KB}}\restriction B)$ is a wellordering.
(c) If $B \subseteq \mathbb{N}$ is a wellfounded tree then $\|\sqsupset\restriction B\| \le \|<_{\mathrm{KB}}\restriction B\|$.

Proof:
(a) Obviously $<_{\mathrm{KB}}$ is primitive recursive.
Transitivity:
1. $c * \langle a\rangle \sqsubseteq r\ \&\ c * \langle b\rangle \sqsubseteq s\ \&\ a < b\ \&\ t \sqsubset s$: If $t \sqsubseteq c$, then also $t \sqsubset r$. Otherwise $c * \langle b\rangle \sqsubseteq t$.
2. $c * \langle a\rangle \sqsubseteq r\ \&\ c * \langle b\rangle \sqsubseteq s\ \&\ a < b\ \&\ d * \langle a'\rangle \sqsubseteq s\ \&\ d * \langle b'\rangle \sqsubseteq t\ \&\ a' < b'$:
2.1. $c * \langle b\rangle \sqsubseteq d$: Then also $c * \langle b\rangle \sqsubseteq t$. 2.2. $d = c$: $a < b = a' < b'$. 2.3. $d \sqsubset c$: $d * \langle a'\rangle \sqsubseteq c \sqsubseteq r$.
(b) "$\Leftarrow$": $\forall n(\overline{f}(n) \in B) \Rightarrow (\overline{f}(n))_{n\in\mathbb{N}}$ is an infinite descending sequence in $<_{\mathrm{KB}}\restriction B$.
"$\Rightarrow$": Assume $g : \mathbb{N} \to B$ with $\forall n(g(n{+}1) <_{\mathrm{KB}} g(n))$.
By recursion on n define $f(n) := \min\{a \in \mathbb{N} : \exists k(\overline{f}(n) * \langle a\rangle \sqsubseteq g(k))\}$.
Claim: $f(n)$ is defined for all n.
Proof by induction on n:
1. $n = 0$: Since $g(1) <_{\mathrm{KB}} g(0)$ we have $g(1) \neq 0$ and there exists a such that $\langle a\rangle \sqsubseteq g(0)$.
2. $n \to n{+}1$: By I.H. and definition we have $r := \overline{f}(n{+}1) \sqsubseteq g(k)$ for some k.
If $r \sqsubset g(k)$ or $r \sqsubset g(k{+}1)$, we are done. Assume now $r = g(k) \not\sqsubset g(k{+}1)$. Since $g(k{+}1) <_{\mathrm{KB}} g(k)$, there exist t, a, b with $a < b\ \&\ t * \langle a\rangle \sqsubseteq g(k{+}1)\ \&\ t * \langle b\rangle \sqsubseteq g(k) = r = \overline{f}(n{+}1)$.

Hence there exists an $m \leq n$ such that $t * \langle b \rangle = \overline{f}(m{+}1)$ and thus $\overline{f}(m) * \langle a \rangle \sqsubseteq g(k{+}1)$ & $a < b = f(m)$, which is in contradiction with the definition of $f(m)$. This proves the claim.

Now $\forall n \exists k(\overline{f}(n{+}1) \sqsubseteq g(k))$ and thus $\forall n(\overline{f}(n) \in B)$.

(c) Let $R_0 := \sqsupset \restriction B$ and $R_1 := <_{\mathrm{KB}} \restriction B$. Then $\|R_i)\| = \sup\{|s|_{R_i}{+}1 : s \in B\}$.
Since $R_0 \subseteq R_1$, by R_0-induction one obtains $|s|_{R_0} \leq |s|_{R_1}$:
$|s|_{R_0} = \sup\{|t|_{R_0}{+}1 : tR_0s\} \overset{\mathrm{IH}}{\leq} \sup\{|t|_{R_1}{+}1 : tR_0s\} \leq \sup\{|t|_{R_1}{+}1 : tR_1s\} = |s|_{R_1}$.

Inductive Definition of $\mathcal{O}$ and of $|a|_{\mathcal{O}} \in On$ für $a \in \mathcal{O}$
1. $0 \in \mathcal{O}$ und $|0|_{\mathcal{O}} := 0$.
2. $a \in \mathcal{O} \implies \langle 1, a \rangle \in \mathcal{O}$ and $|\langle 1, a \rangle|_{\mathcal{O}} := |a|_{\mathcal{O}} + 1$.
3. $\forall n(\{e\}(n) \in \mathcal{O}) \implies \langle 2, e \rangle \in \mathcal{O}$ and $|\langle 2, e \rangle|_{\mathcal{O}} := \sup_{n \in \mathbb{N}}(|\{e\}(n)|_{\mathcal{O}} + 1)$.

Remark. $|a|_{\mathcal{O}} = |a|_{\Phi}$ where Φ is the operator of the inductive definition of $\mathcal{O}$.

Proof: Exercise.

Theorem 13.10. $\omega_1^{CK} = \sup\{|a|_{\mathcal{O}} : a \in \mathcal{O}\}$.

Proof:
"$\geq$": *Definition* of a wellfounded tree $B_a \subseteq \mathbb{N}$ for each $a \in \mathcal{O}$:
$B_0 := \{0\}$, $B_{\langle 1,a \rangle} := \{0\} \cup \{\langle 0 \rangle * s : s \in B_a\}$, $B_{\langle 2,e \rangle} := \{0\} \cup \bigcup_n \{\langle n \rangle * s : s \in B_{\{e\}(n)}\}$.

Claim: $a \in \mathcal{O} \Longrightarrow B_a$ is wellfounded and $|a|_{\mathcal{O}} = \|B_a\|$.

Proof: this follows essentially from 12..., since B_a is the only immediate subtree of $B_{\langle 1,a \rangle}$, and $B_{\{e\}(n)}$ $(n \in \mathbb{N})$ are the immediate subtrees of $B_{\langle 2,e \rangle}$.

Now we are going to show that there is a recursive function f such that, for each $a \in \mathcal{O}$, $\{f(a)\}^1 = \mathbf{1}_{B_a}$.
Then $(B_a, <_{\mathrm{KB}} \restriction B_a)$ is a recursive wellordering with ordertype $> |a|_{\mathcal{O}}$.
$[\ |a|_{\mathcal{O}} + 1 = \|B_a\| + 1 = \|\sqsupset \restriction B_a\| \leq \|<_{\mathrm{KB}} \restriction B_a\|\ ]$.

We have to find $f = \{\mathtt{f}\}$ such that

$$\{f(a)\}(s) \simeq h(\mathtt{f}, a, s), \text{ where } h(\mathtt{f}, a, s) :\simeq \begin{cases} 1 & \text{if } s = 0 \\ \{\{\mathtt{f}\}(b)\}(s') & \text{if } a = \langle 1, b \rangle \ \&\ s = \langle 0 \rangle * s' \\ \{\{\mathtt{f}\}(\{e\}(n))\}(s') & \text{if } a = \langle 2, e \rangle \ \&\ s = \langle n \rangle * s' \\ 0 & \text{otherwise} \end{cases}$$

By the s-m-n Theorem there exists an $\hat{h} \in \mathrm{PR}$ with $\{\hat{h}(z, a)\}(s) \simeq h(z, a, s)$.

By the recursion theorem there exists $f = \{\mathtt{f}\}$ with $f(x) = \hat{h}(\mathtt{f}, x)$. Then $\{f(a)\}(s) \simeq h(\mathtt{f}, a, s)$.

"$\leq$": Let $R \subseteq \mathbb{N} \times \mathbb{N}$ be a recursive and wellfounded. Below we will show that there exists a recursive function f such that for each $n \in \mathbb{N}$: $f(n) = \langle 2, e \rangle$ with $\{e\}(m) = \begin{cases} f(m) & \text{if } mRn \\ 0 & \text{otherwise} \end{cases}$.
Then (*) $\forall n \in \mathbb{N}(f(n) \in \mathcal{O}\ \&\ |n|_R \leq |f(n)|_{\mathcal{O}})$ and thus
$b := \langle 2, \mathtt{f} \rangle \in \mathcal{O}$ and $\|R\| = \sup_{n \in \mathbb{N}}(|n|_R{+}1) \leq \sup_{n \in \mathbb{N}}(|f(n)|_{\mathcal{O}}{+}1) = |b|_{\mathcal{O}}$.
Proof of (*) by R-induction: I.H. $\Rightarrow$ $\forall mRn(\, f(m) \in \mathcal{O}\ \&\ |m|_R \leq |f(m)|_{\mathcal{O}}) \Rightarrow$
$\forall m(\{e\}(m) \in \mathcal{O})\ \&\ |n|_R = \sup_{mRn}(|m|_R{+}1) \leq \sup_{m \in \mathbb{N}}(|\{e\}(m)|_{\mathcal{O}}{+}1) = |f(n)|_{\mathcal{O}}$.
Existence of f: Let $h(\mathtt{f}, m, n) :\simeq \begin{cases} \{\mathtt{f}\}(m) & \text{if } mRn \\ 0 & \text{otherwise} \end{cases}$ and $\hat{h} \in \mathrm{PR}$ such that $\{\hat{h}(\mathtt{f}, n)\}(m) \simeq h(\mathtt{f}, m, n)$.
By the Recursion Theorem there exists an $\mathtt{f}$ with $\{\mathtt{f}\}(n) = \langle 2, \hat{h}(\mathtt{f}, n) \rangle$. Let $f := \{\mathtt{f}\}$.

THE TURING MACHINE

The historical first abstract computing model is the *Turing machine* called so after the english logician A.M. Turing. The Turing machine consists of a *finite control*, a *tape* that is divided into *cells*, and a tape *head* that scans one cell of the tape at each time. The tape is infinite in both directions. Each cell of the tape holds exactly one of a finite number of tape symbols. There is special symbol "blank" which is hold by almost all cells. In one move the Turing machine, depending upon the symbol scanned by the tape head and the *state* of the finite control will perform one of the following actions:

(1) print a symbol on the scanned tape cell, replacing what was written there,
(2) move the head one cell left or right.

Definitions

Let Σ be a fixed alphabet with $\Sigma \cap \{0, \mathsf{L}, \mathsf{R}\} = \emptyset$.

$\Sigma_0 := \Sigma \cup \{0\}, \quad \Sigma_1 := \Sigma_0 \cup \{\mathsf{L}, \mathsf{R}\}$.

$\Sigma^{\#} := \{\varphi : \varphi : \mathbb{Z} \to \Sigma_0 \ \& \ \{i \in \mathbb{Z} : \varphi(i) \neq 0\} \text{ finite } \}$.

A *Turing program* is a finite function $P : n \times \Sigma_0 \to (n{+}1) \times \Sigma_1$.

$0, ..., n$ are called the *states* of P.

$l(P) := n$ is called the *length* of P.

0 is the *initial state* of P.

$stop(P) := n$ is the *final state* of P.

For P we define a *state transition function* $\delta_P : \mathbb{N} \times \Sigma^{\#} \to \mathbb{N} \times \Sigma^{\#}$ as follows:

1. If $i \geq n$, then $\delta_P(i, \varphi) := (i, \varphi)$.
2. If $i < n$ and $P(i, \varphi(0)) = (j, x) \in (n{+}1) \times \Sigma_1$,
   then $\delta_P(i, \varphi) := (j, \psi)$, where $\psi \in \Sigma^{\#}$ is defined as follows:

2.1. $x \in \Sigma_0$: $\psi(0) := x$ und $\psi(i) := \varphi(i)$ für $i \neq 0$.

2.2. $x = \mathsf{R}$: $\psi(i) := \varphi(i{+}1)$.

2.3. $x = \mathsf{L}$: $\psi(i) := \varphi(i{-}1)$.

Definition of a funktion $[P] : \Sigma^{\#} \xrightarrow{\text{part}} \Sigma^{\#}$ *for each Turing program* P

$[P](\varphi) \simeq \psi \ :\Leftrightarrow$ There is a $k \in \mathbb{N}$ such that $\delta_P^{(k)}(0, \varphi) = (stop(P), \psi)$.

Definition

We assume that Σ contains the symbol 1.

For $a_1, ..., a_n \in \mathbb{N}$ let $\varphi_{a_1,...,a_n}$ denote the following $\varphi \in \Sigma^{\#}$:

$\varphi(i) := \begin{cases} 1 & \text{if } i = a_1 + ... + a_k + k + j \text{ with } 0 \leq k < n \text{ and } 1 \leq j \leq a_{k+1} \\ 0 & \text{otherwise} \end{cases}$

For each Turing program P and $n \geq 1$ let

$f_P^n : \mathbb{N}^n \xrightarrow{\text{part}} \mathbb{N}$, $f_P^n(a_1, ..., a_n) :\simeq out([P](\varphi_{a_1,...,a_n}))$, where $out(\psi) := \min\{i \geq 0 : \ \psi(i+1) = 0\}$.

Definition

$f : \mathbb{N}^n \xrightarrow{\text{part}} \mathbb{N}$ is called *Turing computable*, if there exists a Turing program P with $f = f_P^n$ gibt.

Theorem

A partial function $f : \mathbb{N}^n \xrightarrow{\text{part}} \mathbb{N}$ is Turing computable iff it is partial recursive.

§14 Proof theoretic analysis of the axiom system Z of arithmetic

Ter_0 := set of all closed PR-terms.

If $t \in Ter_0$ then $t^{\mathcal{N}}$ denotes the value of t in the standard model $\mathcal{N}$.

Abbreviation: $u_x(n) := u_x(\underline{n})$ for each PR-expression u and $n \in \mathbb{N}$.

Let $\mathcal{L}_0$:= PR. The **language of** Z is $\mathcal{L}_0(\mathcal{X}) := \mathcal{L}_0 \cup \{X_0, X_1, ...\}$, where $X_0, X_1, ...$ are unary predicate symbols; we call them *set variables*. But note that they are not considered as variables in the proper sense (e.g. $\mathrm{FV}(X_i\mathbf{0}) = \emptyset$). We use X as syntactic variable for $X_0, X_1, ...$. TRUE (FALSE, resp.) denotes the set of all $\mathcal{L}_0$-sentences which are true (false, resp.) in the standard model $\mathcal{N}$. $\mathrm{TRUE}_0 := \{A \in \mathrm{TRUE} : A \text{ atomic}\}$, $\mathrm{FALSE}_0 := \{A \in \mathrm{FALSE} : A \text{ atomic}\}$,

The **axioms of** Z are the universal closures of the following $\mathcal{L}_0(\mathcal{X})$-formulas:

$\neg(\mathsf{S}x \approx \mathbf{0})$,

$\mathsf{S}x \approx \mathsf{S}y \to x \approx y$,

$\mathsf{C}^n_k x_1...x_n \approx \underline{k}$,

$\mathrm{I}^n_i x_1...x_n \approx x_i$,

$(\circ h g_1...g_m)x_1...x_n \approx h g_1 x_1...x_n \dots g_m x_1...x_n$,

$(\mathsf{R}gh)x_1...x_n\mathbf{0} \approx g x_1...x_n$,

$(\mathsf{R}gh)x_1...x_n\mathsf{S}y \approx h x_1...x_n y(\mathsf{R}gh)x_1...x_n y$,

$F_x(0) \to \forall x(F \to F_x(\mathsf{S}x)) \to F_x(z)$, for each $\mathcal{L}_0(\mathcal{X})$-formula F

Definition

Let R be a 2-ary $\mathcal{L}_0$-formula such that the relation

$\prec\ := \{(m,n) \in \mathbb{N}^2 : \mathcal{N} \models R(m,n)\}$ is wellfounded.

Abbreviations:

$s \prec t\ :=\ R(s,t)\ ,\quad \forall y{\prec}t\, F(y)\ :=\ \forall y(y{\prec}t \to F(y))$,

$|t|_\prec := |t^{\mathcal{N}}|_\prec$ for $t \in Ter_0$,

$\mathrm{Prog}_\prec(F) := \forall x(\forall y{\prec}x F(y)\ \to F(x))$,

$\mathrm{TI}_\prec(F,t) := \mathrm{Prog}_\prec(F) \to \forall x{\prec}t F(x), \quad \mathrm{TI}_\prec(F) := \mathrm{Prog}_\prec(F) \to \forall x F(x)$

In this section we will show that *transfinite induction up to* ε_0 is not provable in Z, more precisely we will establish the following

Theorem $\mathrm{Z} \vdash \mathrm{TI}_\prec(X) \implies \| \prec \| < \varepsilon_0$.

Definition ($\mathrm{rk}(A)$)

1. $\mathrm{rk}(A) := 0$, for atomic A,
2. $\mathrm{rk}(A \to B) := \max\{\mathrm{rk}(A), \mathrm{rk}(B)\} + 1$,
3. $\mathrm{rk}(\forall x A) := \mathrm{rk}(A) + 1$.

Corollary. $\mathrm{rk}(A_x(t)) = \mathrm{rk}(A)$.

In the following, $\alpha, \beta, \gamma, \delta, \xi, \eta$ always denote ordinals $< \varepsilon_0 := \min\{\alpha : \omega^\alpha = \alpha\}$.

The infinitary proof system Z^∞

We use Γ as syntactic variable for finite sets of closed formulas.

An expression of the form $\Gamma \supset C$ is called a *sequent* (with *antecedent* Γ and *succedent* C).

Notation. We write A, Γ for $\{A\} \cup \Gamma$, and Γ, Γ' for $\Gamma \cup \Gamma'$, etc.

Axioms and inference rules of Z^∞

(Ax1) $\Gamma \supset C$, if $C \in \mathrm{TRUE}_0$ or $\Gamma \cap \mathrm{FALSE}_0 \neq \emptyset$

(Ax2) $Xs, \Gamma \supset Xt$, if $s^{\mathcal{N}} = t^{\mathcal{N}}$

$(\to r)$ $\dfrac{A, \Gamma \supset B}{\Gamma \supset A \to B}$, $(\forall r)$ $\dfrac{\dots \Gamma \supset A_x(n) \dots (n \in \mathbb{N})}{\Gamma \supset \forall x A}$,

$(\to l)$ $\dfrac{\Gamma \supset A \quad B, \Gamma \supset C}{A \to B, \Gamma \supset C}$, $(\forall l)$ $\dfrac{A_x(k), \Gamma \supset C}{\forall x A, \Gamma \supset C}$,

(Cut) $\dfrac{\Gamma \supset D \quad D, \Gamma \supset C}{\Gamma \supset C}$,

$(\bot)$ $\dfrac{\neg C, \Gamma \supset \bot}{\Gamma \supset C}$ (C atomic).

A Z^∞-derivation is a tree of sequents generated from the above axioms and rules.

In other words: A Z^∞-derivation d is a wellfounded tree of sequents being locally correct w.r.t. the above axioms and rules, which means:

(i) the sequents at the top nodes of d are axioms,

(ii) every other sequent is obtained from the sequent(s) immediately above it by one of the rules.

The sequent at the root of a derivation d is called its endsequent.

d is called a *derivation of* $\Gamma \supset C$ if $\Gamma \supset C$ is its endsequent.

The cut-rank of a Z^∞-derivation d is the least number m such that $\mathrm{rk}(D) < m$ for every cut-formula D of d.

Abb.: $\vdash_m^\alpha \Gamma \supset C \ :\Longleftrightarrow$ there exists a Z^∞-derivation d of $\Gamma \supset C$ with height $\leq \alpha$ and cut-rank $\leq m$.

Note that $\vdash_m^\alpha \Gamma \supset C$ implies $\vdash_m^\alpha \Delta, \Gamma \supset C$ (just add Δ to each sequent in the derivation of $\Gamma \supset C$).

Therefore the relation $\vdash_m^\alpha \Gamma \supset C$ can be characterized recursively as follows

$\vdash_m^\alpha \Gamma \supset C$ iff one of the following cases holds

(Ax1) $C \in \mathrm{TRUE}_0$ oder $\Gamma \cap \mathrm{FALSE}_0 \neq \emptyset$,

(Ax2) $C = Xt$ and $Xs \in \Gamma$ with $s^{\mathcal{N}} = t^{\mathcal{N}}$,

$(\to r)$ $C = A \to B$ & $\vdash_m^{\alpha_0} A, \Gamma \supset B$ & $\alpha_0 < \alpha$,

$(\forall r)$ $C = \forall x A$ & $\vdash_m^{\alpha_n} \Gamma \supset A_x(n)$ & $\alpha_n < \alpha$ $(\forall n \in \mathbb{N})$,

$(\to l)$ $(A \to B) \in \Gamma$ & $\vdash_m^{\alpha_0} \Gamma \supset A$ & $\vdash_m^{\alpha_0} B, \Gamma \supset C$ & $\alpha_0 < \alpha$,

$(\forall l)$ $\forall x A \in \Gamma$ & $\vdash_m^{\alpha_0} A_x(k), \Gamma \supset C$ & $\alpha_0 < \alpha$,

(Cut) $\mathrm{rk}(D) < m$ & $\vdash_m^{\alpha_0} \Gamma \supset D$ & $\vdash_m^{\alpha_0} D, \Gamma \supset C$ & $\alpha_0 < \alpha$,

$(\bot)$ C atomic & $\vdash_m^{\alpha_0} \neg C, \Gamma \supset \bot$ & $\alpha_0 < \alpha$.

In the following we will take this as the official definition of $\vdash_m^\alpha \Gamma \supset C$.

Lemma 14.1

(a) $\vdash_m^\alpha \Gamma \supset C \,\&\, \Gamma \subseteq \Gamma_1 \,\&\, \alpha \leq \alpha_1 \,\&\, m \leq m_1 \;\Rightarrow \vdash_{m_1}^{\alpha_1} \Gamma_1 \supset C$.

(b) $\vdash_m^\alpha A, \Gamma \supset C \,\&\, A \in \textsc{True} \;\Rightarrow \vdash_m^\alpha \Gamma \supset C$.

(c) $\vdash_m^\alpha \Gamma \supset A \,\&\, A \in \textsc{False} \;\Rightarrow \vdash_m^\alpha \Gamma \supset C$.

(d) $\vdash_m^\alpha \Gamma \supset Xs \,\&\, s^{\mathcal{N}} = t^{\mathcal{N}} \;\Rightarrow \vdash_m^\alpha \Gamma \supset Xt$.

(e) $\vdash_m^\alpha \neg Xs, \Gamma \supset C \,\&\, s^{\mathcal{N}} = t^{\mathcal{N}} \;\Rightarrow \vdash_m^\alpha \neg Xt, \Gamma \supset C$.

Proof by induction on α:

(a) trivial.

(b) and (c) are proved simultaneously by induction on α. The proof is left to the reader.

(d) and (e) are proved simultaneously by induction on α:

(d) Assume $\vdash_m^{\alpha_0} \neg Xs, \Gamma \supset \bot \,\&\, \alpha_0 < \alpha$. Then IHe yields $\vdash_m^{\alpha_0} \neg Xt, \Gamma \supset \bot$, and by $(\bot)$ we obtain $\vdash_m^\alpha \Gamma \supset Xt$.
The other cases are trivial or follow immediately from the I.H.

(e) The only nontrivial case is $(\to l)$ with principal part $\neg Xs = Xs \to \bot$.

In this case we have $\vdash_m^{\alpha_0} \neg Xs, \Gamma \supset Xs \,\&\, \vdash_m^{\alpha_0} \bot, \neg Xs, \Gamma \supset C \,\&\, \alpha_0 < \alpha$. Then I.H.d,e yields
$\vdash_m^{\alpha_0} \neg Xt, \Gamma \supset Xt \,\&\, \vdash_m^{\alpha_0} \bot, \neg Xt, \Gamma \supset C \,\&\, \alpha_0 < \alpha$, and by $(\to l)$ we obtain the claim.

In the following, applications of Lemma 14.1a will not be mentioned!

Lemma 14.2 (Inversion)

(a) $\vdash_m^\alpha \Gamma \supset A \to B \implies \vdash_m^\alpha A, \Gamma \supset B$,

(b) $\vdash_m^\alpha \Gamma \supset \forall x A \implies \vdash_m^\alpha \Gamma \supset A_x(n)$ for all $n \in \mathbb{N}$.

Proof by induction on α: We only treat (b).

(Ax1) In this case $\Gamma \cap \textsc{False}_0 \neq \emptyset$, and $\Gamma \supset A_x(n)$ is an axiom (Ax1) too.

The remaining cases are $(\forall r)$, $(\to l)$, $(\forall l)$, (Cut).

$(\to l)$ $B \to C \in \Gamma \,\&\, \vdash_m^{\alpha_0} \Gamma \supset B \,\&\, \vdash_m^{\alpha_0} C, \Gamma \supset \forall x A \,\&\, \alpha_0 < \alpha$:

By I.H. $\vdash_m^{\alpha_0} C, \Gamma \supset A_x(n)$. From this together with $\vdash_m^{\alpha_0} \Gamma \supset B$ we obtain $\vdash_m^\alpha \Gamma \supset A_x(n)$ by $(\to l)$.

(Cut) and $(\forall l)$: analogous to $(\to l)$.

$(\forall r)$ $\vdash_m^{\alpha_n} \Gamma \supset A_x(n) \,\&\, \alpha_n < \alpha$ for all $n \in \mathbb{N}$:

Then also $\vdash_m^\alpha \Gamma \supset A_x(n)$.

Lemma 14.3 (Reduction)

$\mathrm{rk}(D) \le m \;\&\; \vdash_m^\alpha \Gamma \supset D \;\&\; \vdash_m^\beta D, \Gamma \supset C \;\Rightarrow \vdash_m^{\alpha+2\beta} \Gamma \supset C.$

Proof by induction on β:

(Ax1) If $D \in \mathrm{FALSE}_0$ then the claim follows from $\vdash_m^\alpha \Gamma \supset D$ by 14.2c.

If $D \notin \mathrm{FALSE}_0$ then $\Gamma \supset C$ is also an axiom (Ax1).

(Ax2) If $D = Xs \;\&\; C = Xt$ with $s^{\mathcal{N}} = t^{\mathcal{N}}$ then the claim follows from $\vdash_m^\alpha \Gamma \supset D$ by 14.2d.

Otherwise, $\Gamma \supset C$ is also an axiom (Ax2).

$(\to l)$ $A \to B \in D, \Gamma \;\&\; \vdash_m^{\beta_0} D, \Gamma \supset A \;\&\; \vdash_m^{\beta_0} B, D, \Gamma \supset C \;\&\; \beta_0 < \beta$:

By I.H. we obtain (1) $\vdash_m^{\alpha+2\beta_0} \Gamma \supset A$, (2) $\vdash_m^{\alpha+2\beta_0} B, \Gamma \supset C$.

If $A \to B \in \Gamma$, then the assertion follows from (1),(2) by $(\to l)$.

Assume now $A \to B = D$. Then the Inversion Lemma (14.3b) yields (3) $\vdash_m^\alpha A, \Gamma \supset B$.

From (2) and (3) we obtain $\vdash_m^{\alpha+2\beta_0+1} \Gamma \supset B$ by (Cut).

Together with (2) and another (Cut) this yields the assertion.

$(\forall l)$ $\forall x A \in D, \Gamma \;\&\; \vdash_m^{\beta_0} A_x(k), D, \Gamma \supset C \;\&\; \beta_0 < \beta$:

Mit I.H. and inversion we obtain (1) $\vdash_m^{\alpha+2\beta_0} A_x(k), \Gamma \supset C$, (2) $\vdash_m^\alpha \Gamma \supset A_x(k)$.

If $\forall x A \in \Gamma$, then the assertion follows from (1) by $(\forall l)$.

If $\forall x A = D$, then the assertion follows from (1), (2) by (Cut) with $A_x(k)$ (note that $\mathrm{rk}(A_x(k)) < \mathrm{rk}(D) \le m$).

The remaining cases $(\to r)$, $(\forall r)$, (Cut), $(\bot)$ are easy.

Lemma 14.4 (Cut Elimination)

$\vdash_{m+1}^\alpha \Gamma \supset C \;\Rightarrow \vdash_m^{3^\alpha} \Gamma \supset C.$

Proof by induction on α:

We only consider the case (Cut). All other cases are easy.

So we have $\vdash_{m+1}^{\alpha_0} \Gamma \supset D \;\&\; \vdash_{m+1}^{\alpha_0} D, \Gamma \supset C \;\&\; \mathrm{rk}(D) \le m \;\&\; \alpha_0 < \alpha$.

By I.H. then $\vdash_m^{3^{\alpha_0}} \Gamma \supset D$ and $\vdash_m^{3^{\alpha_0}} D, \Gamma \supset C$. From this together with $\mathrm{rk}(D) \le m$ we get $\vdash_m^{3^{\alpha_0}+2\cdot 3^{\alpha_0}} \Gamma \supset C$.

But $3^{\alpha_0} + 2 \cdot 3^{\alpha_0} \le 3^{\alpha_0} + 3^{\alpha_0} \cdot 2 = 3^{\alpha_0+1} \le 3^\alpha$.

EMBEDDING

Lemma 14.5.

(a) $\vdash_0^{2\mathrm{rk}(A)} A_x(s) \supset A_x(t)$, if $s^{\mathcal{N}} = t^{\mathcal{N}}$

(b) $\vdash_0^{k+3} (C \to (A \to B)), C \to A, C \supset B$, wobei $k := 2\max\{\mathrm{rk}(A), \mathrm{rk}(B), \mathrm{rk}(C)\}$.

(c) $\vdash_0^4 \neg\neg A \supset A$, if A is atomic.

(d) $\vdash_0^{k+4} \forall x(A \to B), \forall x A \supset \forall x B$, where $k := 2\max\{\mathrm{rk}(A), \mathrm{rk}(B)\}$.

(e) $\vdash_0^{2\mathrm{rk}(A)+1} \forall x A \supset A_x(t)$.

(f) $\vdash_0^2 \supset (x \approx y \to A \to A_x(y))_{x,y}(m,n)$, for atomic A and $x \neq y$.

Proof:

(a) Induction on A: 1. For atomic A this is an axiom.

2. From $\vdash_0^k A_x(t) \supset A_x(s)$ and $\vdash_0^k B_x(s) \supset B_x(t)$ we obtain

$\vdash_0^{k+2} A_x(s) \to B_x(s) \supset A_x(t) \to B_x(t)$ by $(\to l)$ and $(\to r)$.

3. Let $A = \forall y B$ and w.l.o.g. $y \neq x$. By I.H. $\vdash_0^k B_y(n)_x(s) \supset B_y(n)_x(t)$ for all n.

$\vdash_0^k B_x(s)_y(n) \supset B_x(t)_y(n)$ for all n.

$\vdash_0^{k+2} \forall y B_x(s) \supset \forall y B_x(t)$ for all n.

(b)

$\vdash_0^k A \supset A \;\mid\; \vdash_0^k B \supset B$

$\vdash_0^k C \supset C \;\mid\; \vdash_0^{k+1} A \to B, A \supset B$

$\vdash_0^k C \supset C \;\mid\; \vdash_0^{k+2} A, C \to (A \to B), C \supset B$

$\vdash_0^{k+3} C \to A, C \to (A \to B), C \supset B$

(c) 1. $A \in \mathrm{TRUE}_0$: trivial.

2. $A \in \mathrm{FALSE}_0$: $\vdash_0^0 A \supset \bot$ & $\vdash_0^0 \bot \supset A \;\Rightarrow \vdash_0^1 \supset \neg A$ & $\vdash_0^0 \bot \supset A \;\Rightarrow \vdash_0^2 \neg A \to \bot \supset A$.

3. $A = Xt$: $\vdash_0^2 \neg A \supset \neg A$ & $\vdash_0^0 \bot \supset \bot \;\Rightarrow \vdash_0^3 \neg\neg A, \neg A \supset \bot \;\Rightarrow \vdash_0^4 \neg\neg A \supset A$.

(d) $\vdash_0^k A(n) \supset A(n) \;\mid\; \vdash_0^k B(n) \supset B(n)$

$\vdash_0^{k+1} A(n) \to B(n), A(n) \supset B(n)$

$\vdash_0^{k+2} \forall x(A \to B), A(n) \supset B(n)$

$\vdash_0^{k+3} \forall x(A \to B), \forall x A \supset B(n)$, für alle n

$\vdash_0^{k+4} \forall x(A \to B), \forall x A \supset \forall x B$.

(e) Let $n := t^{\mathcal{N}}$. $\vdash_0^{2\mathrm{rk}(A)} A_x(n) \supset A_x(t)$ implies $\vdash_0^{2\mathrm{rk}(A)+1} \forall x A \supset A_x(t)$.

(f) Note that $(x \approx y \to A \to A_x(y))_{x,y}(m,n) = m \approx n \to A_{x,y}(m,n) \to A_{x,y}(n,n)$, and

$\vdash_0^0 m \approx n, A_{x,y}(m,n) \supset A_{x,y}(n,n)$ holds for all m, n.

Lemma 14.6 (Induction Lemma)

$\vdash_0^\omega A(0), \forall x(A(x) \to A(\mathsf{S}x)) \supset \forall x A(x)$.

Proof:

Let $k := 2\mathrm{rk}(A)$. By induction on n we prove: $\vdash_0^{k+2n} A(0), \forall x(A(x) \to A(\mathsf{S}x)) \supset A(n)$.

1. For $n = 0$ this follows from 14.5a.

2. $\vdash_0^{k+2n} A(0), \forall x(A(x) \to A(\mathsf{S}x)) \supset A(n) \;\mid\; \vdash_0^k A(\mathsf{S}n) \supset A(\mathsf{S}n)$,

$\vdash_0^{k+2n+1} A(0), \forall x(A(x) \to A(\mathsf{S}x)), (A(n) \to A(\mathsf{S}n)) \supset A(\mathsf{S}n)$,

$\vdash_0^{k+2n+2} A(0), \forall x(A \to A(\mathsf{S}x)) \supset A(\mathsf{S}n)$.

Theorem 14.7. (Embedding)

$\mathrm{Z} \vdash C$ & $\mathrm{FV}(C) = \emptyset \implies \vdash_m^{\omega+k} \supset C$ for some $k, m \in \mathbb{N}$.

Proof by induction on the derivation of C:

W.l.o.g. we may assume that all formulas in the derivation of C are closed (otherwise we replace all free variables in the derivation by 0).

1. C has been derived from A and $A \to C$. Then by I.H. there are k, m such that $\vdash_m^{\omega+k} \supset A$, $\vdash_m^{\omega+k} \supset A \to C$, and $\mathrm{rk}(A) < m$. From $\vdash_m^{\omega+k} \supset A \to C$ we obtain $\vdash_m^{\omega+k} A \supset C$ by Lemma 14.2a.
Now a (Cut) yields $\vdash_m^{\omega+k+1} \supset C$.

2. Otherwise $C = \forall y_1 ... \forall y_p A(y_1, ..., y_p)$, and $\vdash_0^{\omega+2} \supset A(n_1, ..., n_p)$ holds for all $n_1, ..., n_p$ (cf. Lemmata 14.5, 14.6). From this we get $\vdash_0^{\omega+2+p} \supset \forall y_1 ... y_p A$.

Lemma 14.8.

$$\left.\begin{array}{l} \vdash_0^{\beta} \Delta, \Pi, \Gamma \supset Xt_0 \ \ \& \ \ \Gamma = \{\neg Xt_1, ..., \neg Xt_n\} \ \ \& \\ \Delta \subseteq \{\mathrm{Prog}_{\prec}(X)\} \cup \{\forall y \prec s Xy \to Xs : s \in Ter_0\} \ \ \& \\ \Pi \subseteq \{Xs : |s|_{\prec} \leq \alpha\} \end{array}\right\} \Longrightarrow |t_i|_{\prec} < \alpha + 2^{\beta} \text{ for some } i \in \{0, ..., n\}.$$

Proof by induction on β:

(Ax1) $Xs \in \Pi$ with $s^{\mathcal{N}} = t_0^{\mathcal{N}}$: Then $|t_0|_{\prec} = |s|_{\prec} \leq \alpha < \alpha + 2^{\beta}$.

$(\bot)$ $\vdash_0^{\beta_0} \Delta, \Pi, \Gamma, \neg Xt_0 \supset \bot$: L.14.1c $\Rightarrow \vdash_0^{\beta_0} \Delta, \Pi, \Gamma, \neg Xt_0 \supset Xt_0 \overset{\text{I.H.}}{\Rightarrow} |t_i|_{\prec} < \alpha + 2^{\beta_0}$ for some $i \in \{0, ..., n\}$.

$(\to l)_1$ $\vdash_0^{\beta_0} \Delta, \Pi, \Gamma \supset Xt_j$ with $j \in \{1, ..., n\}$: By I.H., $|t_i|_{\prec} < \alpha + 2^{\beta_0}$ for some $i \in \{1, ..., n\}$.

$(\to l)_2$ Assume (1) $\vdash_0^{\beta_0} \Delta, Xs, \Pi, \Gamma \supset Xt_0$ and (2) $\vdash_0^{\beta_0} \Delta, \Pi, \Gamma \supset \forall y \prec s Xy$:
We further assume (3) $\alpha + 2^{\beta_0} \leq |t_i|_{\prec}$ for $i = 1, ..., n$.
From (2) by L.14.2 and L.14.1b we obtain $\vdash_0^{\beta_0} \Delta, \Pi, \Gamma \supset X\underline{m}$ for all $m \prec s^{\mathcal{N}}$. Hence, by I.H. and (3), $|m|_{\prec} < \alpha + 2^{\beta_0}$ for all $m \prec s^{\mathcal{N}}$, i.e., $|s|_{\prec} \leq \alpha + 2^{\beta_0}$.
From (1) and $|s|_{\prec} \leq \alpha + 2^{\beta_0}$ by I.H. we obtain $|t_i|_{\prec} < (\alpha + 2^{\beta_0}) + 2^{\beta_0} \leq \alpha + 2^{\beta}$ for some $i \in \{0, ..., n\}$.

$(\forall l)$ $\vdash_0^{\beta_0} \forall y \prec t Xy \to Xt, \Delta, \Pi, \Gamma \supset C$: The claim follows immediately from the I.H.

As an immediate consequence from 14.8 we obtain

Theorem 14.9 (Boundedness). $\vdash_0^{\beta} \supset \mathrm{TI}_{\prec}(X) \implies \|\prec\| \leq 2^{\beta}$.

Proof:
$\vdash_0^{\beta} \supset \mathrm{Prog}_{\prec}(X) \to \forall x Xx \Rightarrow \vdash_0^{\beta} \mathrm{Prog}_{\prec}(X) \supset X\underline{n}$ for all $n \in \mathbb{N} \overset{14.8}{\Rightarrow} |n|_{\prec} < 2^{\beta}$ for all $n \in \mathbb{N} \Rightarrow \|\prec\| \leq 2^{\beta}$.

Theorem 14.10. $\mathrm{Z} \vdash \mathrm{TI}_{\prec}(X) \implies \|\prec\| < \varepsilon_0$.

Proof:
$Z \vdash \mathrm{TI}_{\prec}(X) \overset{14.7,14.4}{\Longrightarrow} \vdash_0^{\beta} \supset \mathrm{TI}_{\prec}(X)$ for some $\beta < \varepsilon_0 \overset{14.9}{\Rightarrow} \|\prec\| \leq 2^{\beta} < \varepsilon_0$.

Provability of transfinite induction in Z

In the following a, b, c, x, y, z denote natural numbers.

Definition of $b \prec' a$

$b \prec' a$ if, and only if, $a = \langle a_0, ..., a_n \rangle$ and one of the following cases holds

(i) $b = \langle a_0, ..., a_{k-1} \rangle$ with $k \leq n$,

(ii) $b = \langle a_0, ..., a_{k-1}, b_k, ..., b_m \rangle$ with $k \leq \min\{m, n\}$ and $b_k \prec' a_k$.

Lemma 14.11. $\mathrm{Z} \vdash x \prec' y \to y \prec' z \to x \prec' z$.

Inductive Definition of a set OT **of ordinal notations**

1. $0 \in \mathrm{OT}$,

2. $a_0, ..., a_n \in \mathrm{OT}$ & $a_n \preceq' \ldots \preceq' a_0 \implies \langle a_0, ..., a_n \rangle \in \mathrm{OT}$.

Definition $b \prec a \ :\Leftrightarrow \ a, b \in \mathrm{OT}$ & $b \prec' a$

Abbreviation: $\overline{F}(y) := \forall x(\,\forall z{\prec}x F(z) \ \to \ \forall z{\prec}x{*}\langle y\rangle\, F(z))$

Lemma 14.12. $\mathrm{Z} \vdash \mathrm{Prog}_{\prec}(F) \to \mathrm{Prog}_{\prec}(\overline{F})$

Proof (in Z):

Assume (1) $\mathrm{Prog}_{\prec}(F)$, (2) $\forall y{\prec}b\overline{F}(y)$, (3) $\forall z{\prec}aF(z)$. We have to prove $\forall z{\prec}\, a{*}\langle b\rangle F(z)$.

From (3) and (2) by induction (on n) we obtain (4) $\forall n\forall\langle y_1, ..., y_n\rangle(y_1, ..., y_n \prec b \to \forall z{\prec}a{*}\langle y_1, ..., y_n\rangle F(z))$.

Now let $c \prec a{*}\langle b\rangle$. Then either $c \prec a$ or $c = a{*}\langle b_1, ..., b_n\rangle$ with $b_n \preceq ... \preceq b_1 \prec b$.

1. $c \prec a$: $F(c)$ follows from (3).

2. $c = a{*}\langle b_1, ..., b_n\rangle$ with $b_n \preceq ... \preceq b_1 \prec b$: Since $\prec'$ is transitive (cf. 14.11), we get $b_1, ..., b_n \prec b$ and then $\forall z \prec c\, F(z)$ by (4). Hence $F(c)$ by (1).

Lemma 14.13. $\mathrm{Z} \vdash \mathrm{TI}_{\prec}(\overline{F}, y) \to \mathrm{TI}_{\prec}(F, \langle y\rangle)$.

Proof (in Z):

Assume $\mathrm{Prog}_{\prec}(\overline{F}) \to \forall z \prec y\overline{F}(z)$ and $\mathrm{Prog}_{\prec}(F)$. By Lemma 4.12 we get $\mathrm{Prog}_{\prec}(\overline{F}) \wedge \forall z \prec y\overline{F}(z)$, hence $\overline{F}(y)$, and from this $\forall z \prec \langle y\rangle F(z)$, since $\mathrm{Z} \vdash \forall z\neg(z \prec 0)$.

Theorem 14.14. $\mathrm{Z} \vdash \mathrm{TI}_{\prec}(F, a)$, for each $a \in OT$.

Proof:

Let $c_0 := 0$, $c_{m+1} := \langle c_m\rangle$. Then $a \prec c_m$ for some m. By (meta-)induction on m we obtain $\mathrm{Z} \vdash \mathrm{TI}_{\prec}(F, c_m)$.

[Induction step: $\mathrm{Z} \vdash \mathrm{TI}_{\prec}(\overline{F}, c_m) \overset{4.13}{\Rightarrow} \mathrm{Z} \vdash \mathrm{TI}_{\prec}(F, c_{m+1})$]

Definition $o(0) := 0$, $o(\langle a_0, ..., a_n\rangle) := \omega^{o(a_0)} + \ldots + \omega^{o(a_k)}$

Lemma 4.15 o maps $(\mathrm{OT}, \prec)$ isomorphic onto $(\varepsilon_0, <)$.

Proof:

1. From the definition of $\prec'$ we get by induction on a: $a \not\prec' a$ and $\forall b(b \prec' a \vee a = b \vee a \prec' b)$.

2. $\forall a(o(a) < \varepsilon_0)$: trivial.

3. By induction on b we prove: $b \prec a \Rightarrow o(b) < o(a)$.

3.1. If $a = \langle a_0, ..., a_n\rangle$ and $b = \langle a_0, ..., a_{k-1}\rangle$ with $k \leq n$ then $o(b) < o(b) + \omega^{o(a_k)} + \ldots + \omega^{o(a_n)} = o(a)$.

3.2. If $a = \langle a_0, ..., a_n\rangle$, $b = \langle a_0, ..., a_{k-1}, b_k, ..., b_m\rangle$ with $k \leq \min\{m, n\}$, $b_k \prec a_k$, then by IH $o(b_m) \leq ... \leq o(b_k) < o(a_k)$ and thus $o(b) = \omega^{o(a_0)} + \ldots + \omega^{o(a_{k-1})} + \omega^{o(b_k)} + \ldots + \omega^{o(b_m)} < \omega^{o(a_0)} + \ldots + \omega^{o(a_k)} \leq o(a)$.

4. From 1. and 3. it follows that $o|_{\mathrm{OT}}$ is injective, and that $a, b \in \mathrm{OT}$ & $o(b) < o(a)$ implies $b \prec a$.

5. By induction on $\alpha < \varepsilon_0$ we prove $\exists a \in \mathrm{OT}(o(a) = \alpha)$: Let $\alpha \neq 0$. By 11.10a, 11.11a there are $\alpha_0 \geq ... \geq \alpha_n$ such that $\alpha = \omega^{\alpha_0} + \ldots + \omega^{\alpha_n}$ and $\alpha_0 < \alpha$ (the latter follows from $\alpha_0 \leq \omega^{\alpha_0} \leq \alpha < \varepsilon_0$). Now by IH there are $a_0, ..., a_n \in \mathrm{OT}$ with $\alpha_i = o(a_i)$. From $\alpha_n \leq ... \leq \alpha_0$ we obtain $a_n \preceq ... \preceq a_0$ by 4.

Hence $a := \langle a_0, ..., a_n\rangle \in \mathrm{OT}$ and $o(a) = \alpha$.

Corollary. $\prec$ is wellfounded with $|a|_\prec = \begin{cases} o(a) & \text{if } a \in \mathrm{OT} \\ 0 & \text{otherwise} \end{cases}$

Proof of $|a|_\prec = o(a)$: If $a \in \mathrm{OT}$ then $|a|_\prec = \sup\{|b|_\prec + 1 : b \prec a\} \overset{\mathrm{IH}}{=} \sup\{o(b)+1 : b \prec a\} \overset{4.15}{=} o(a)$.

Result.

Provability of transfinite induction in Z is characterized by the ordinal ε_0 in the following way:

(I) If $\lhd$ is an arithmetical wellfounded relation such that $\mathrm{Z} \vdash \mathrm{TI}_\lhd(X)$ then $\| \lhd \| < \varepsilon_0$.

(II) For each $\alpha < \varepsilon_0$ there exists a primitive recursive wellordering $\prec_\alpha$ of ordertype α such that $\mathrm{Z} \vdash \mathrm{TI}_{\prec_\alpha}(X)$. (For example: $m \prec_\alpha n :\Leftrightarrow m \prec n \prec a$, where $\prec$ is the above defined relation of ordertype ε_0, and $a \in \mathrm{OT}$ with $o(a) = \alpha$.)

The Hydra game

A *hydra* is a finite unlabelled tree. By 0 we denote the hydra consisting of only one node.

Let σ be the rightmost head of a the hydra $h \neq 0$. If Hercules chops off this head the hydra h chooses an arbitrary number n and transforms itself into a new hydra $h[n]$ as follows (where τ is the node immediately below σ, h^- is h without σ, and $h^-|_\tau$ is the subtree of h^- with root τ):

Case 1: If τ is the root of h, then $h[n] := h^-$.

Case 2: Otherwise $h[n]$ arises from h^- by sprouting n replicas of $h^-|_\tau$ from the node immediately below τ.

A *hydra game* is a finite or infinite sequence $(h_i)_{i<\alpha}$ of hydras, such that $\forall i{+}1 < \alpha \exists n_i (h_{i+1} = h_i[n_i])$.

Theorem 14.16. Each hydra game terminates, i.e., $\forall h \forall (n_i)_{i<\omega} \exists k (h[n_0][n_1]...[n_k] = 0)$.

Theorem 14.17. $\mathrm{Z} \nvdash \forall h \forall (n_i)_{i<\omega} \exists k (h[n_0][n_1]...[n_k] = 0)$.

Proof of Theorem 14.16: To each hydra h we assign its Gödel number $\ulcorner h \urcorner$ as follows: $\ulcorner h \urcorner := \langle \ulcorner h_0 \urcorner, ..., \ulcorner h_{n-1} \urcorner\rangle$ where $h_0, ..., h_{n-1}$ are the immediate subtrees of h. Obviously the mapping $h \mapsto \ulcorner h \urcorner$ is a bijection from the set of all hydras onto $\mathbb{N}$. Therefore from now on we identify hydras and natural numbers.

The above operation $a \mapsto a[n]$ can be defined by primitive recursion as follows:

1. $\mathsf{tp}(0) := 0$, $0[n] := 0$.
2. If $a = \langle a_0, ..., a_m\rangle$ with $a_m = 0$ then $\mathsf{tp}(a) := 1$ and $a[n] := \langle a_0, ..., a_{m-1}\rangle$.
3. If $a = \langle a_0, ..., a_m\rangle$ with $\mathsf{tp}(a_m) = 1$ then $\mathsf{tp}(a) := \omega$ and $a[n] := \langle a_0, ..., a_{m-1}, \underbrace{a_m[0], ..., a_m[0]}_{n+1}\rangle$.
4. If $a = \langle a_0, ..., a_m\rangle$ with $\mathsf{tp}(a_m) = \omega$ then $\mathsf{tp}(a) := \omega$ and $a[n] := \langle a_0, ..., a_{m-1}, a_m[n]\rangle$.

Lemma 14.18. For each $a \neq 0$ one of the following two cases holds:

(i) $\mathsf{tp}(a) = 1$ & $o(a) = o(a[n]) + 1$ (for all n);

(ii) $\mathsf{tp}(a) = \omega$ & $o(a) = \sup_{n\in\omega} o(a[n])$ & $\forall n(o(a[n]) < o(a[n{+}1]))$.

From the Lemma it follows that $o(a[n]) < o(a)$ for each $a \neq 0$. This proves 14.16.

Proof of Theorem 14.17 (Unprovability of termination of the hydra game)

Abbreviation: Let $\lhd \subseteq \mathbb{N}\times\mathbb{N}$ be an arbitrary arithmetical relation.

$\mathrm{WF}_\lhd(G) :\equiv \forall x\exists! y G(x,y) \to \exists x, z_0, z_1(G(x,z_0) \wedge G(x{+}1, z_1) \wedge \neg z_1 \lhd z_0)$,

$\mathrm{WF}_\lhd(X) :\equiv \mathrm{WF}_\lhd(G)$ with $G(x,y) :\equiv \langle x,y\rangle \in X$.

$\mathrm{TI}_\lhd(F) :\equiv \mathrm{Prog}_\lhd(F) \to \forall x F$.

Lemma 14.19 $\mathrm{Z} \vdash \mathrm{WF}_\lhd(X) \iff \mathrm{Z} \vdash \mathrm{TI}_\lhd(X)$

Proof:

"$\Longrightarrow$": Assume $\mathrm{Z} \vdash \mathrm{WF}_\lhd(X)$; then also $\mathrm{Z} \vdash \mathrm{WF}_\lhd(G)$ for each formula $G(x,y)$.

Now we work "in Z": *Assumption:* $\mathrm{Prog}_\lhd(X) \wedge a \notin X$.

For suitable G we prove $\neg\mathrm{WF}_\lhd(G)$, i.e. $\forall i\exists! b G(i,b) \wedge \forall i, b_0, b_1(\, G(i,b_0) \wedge G(i{+}1, b_1) \to b_1 \lhd b_0\,)$.

$A(i,s) :\Leftrightarrow \forall j < i((s)_{j+1} \lhd (s)_j \wedge (s)_{j+1} \notin X \wedge \forall x \lhd (s)_j[x < (s)_{j+1} \to x \in X])$,

$G_a(i,b) :\Leftrightarrow \exists s((s)_0 = a \wedge (s)_i = b \wedge A(i,s))$.

(0) $A(i,s) \wedge A(i,\tilde{s}) \wedge (s)_0 = (\tilde{s})_0 \Rightarrow \forall j \leq i((s)_j = (\tilde{s})_j)$,

(1) G_a is function: cf. (0).

(2) G_a total: By induction on i we prove $\exists b\, G_a(i,b)$.
Induction step: $G_a(i,b_0) \overset{a\notin X}{\Rightarrow} b_0 \notin X \overset{\mathrm{Prog}_\lhd(X)}{\Longrightarrow} \exists b \lhd b_0(b \notin X) \Rightarrow \exists b_1\, G_a(i{+}1, b_1)$.

(3) $G_a(i,b_0) \wedge G_a(i{+}1,b_1) \Rightarrow b_1 \lhd b_0$.
Proof: $\exists s[\,(s)_0 = a \wedge (s)_i = b_0 \wedge A(i,s)] \wedge \exists\tilde{s}[\,(\tilde{s})_0 = a \wedge (\tilde{s})_{i+1} = b_1 \wedge A(i{+}1,\tilde{s})] \overset{(0)}{\Longrightarrow}$
$\Longrightarrow b_1 = (\tilde{s})_{i+1} \lhd (\tilde{s})_i = (s)_i = b_0$.

So we have proved $\mathrm{Z} \vdash \mathrm{Prog}_\lhd(X) \wedge a \notin X \to \neg\mathrm{WF}_\lhd(G_a)$.

Hence $\mathrm{Z} \vdash \neg(\mathrm{Prog}_\lhd(X) \wedge a \notin X)$, i.e., $\mathrm{Z} \vdash \mathrm{Prog}_\lhd(X) \to a \in X$.

"$\Longleftarrow$": Assume $\mathrm{Z} \vdash \mathrm{TI}_\lhd(X)$. Then also $\mathrm{Z} \vdash \mathrm{TI}_\lhd(F)$ for any F.

Let $F(y) := \exists x(\langle x,y\rangle \in X) \to B$ with $B := \exists x, z_0, z_1(\langle x,z_0\rangle \in X \wedge \langle x{+}1, z_1\rangle \in X \wedge \neg(z_1 \lhd z_0))$.

Now we work "in Z": Assume $\forall x\exists y(\langle x,y\rangle \in X)$ and $\forall z \lhd y F(z)$ and $\langle x,y\rangle \in X$.

Then there exists z such that $\langle x{+}1, z\rangle \in X$.

If $\neg(z \lhd y)$ then $\langle x,y\rangle \in X \wedge \langle x{+}1,z\rangle \in X \wedge \neg(z \lhd y)$, thence B.

If $z \lhd y$ then $F(z)$ and $\exists x_1(\langle x_1, z\rangle \in X)$, thence B.

So we have proved: $\mathrm{Z} \vdash \forall x\exists y(\langle x,y\rangle \in X) \to \forall y(\forall z \lhd y F(z) \to F(y))$.

Together with $\mathrm{Z} \vdash \mathrm{TI}_\lhd(F)$ this yields $\mathrm{Z} \vdash \forall x\exists y(\langle x,y\rangle \in X) \to \forall y F(y)$, i.e.,

$\mathrm{Z} \vdash \forall x\exists y(\langle x,y\rangle \in X) \to \exists y\exists x(\langle x,y\rangle \in X) \to B$.

This yields $\mathrm{Z} \vdash \forall x\exists y(\langle x,y\rangle \in X) \to B$, i.e., $\mathrm{Z} \vdash \mathrm{WF}_\lhd(X)$.

Definition $b \prec_1 a \;:\Leftrightarrow\; a \neq 0 \;\&\; \exists i(b = a[i])$

Theorem 14.20

(a) $\prec_1$ is wellfounded and $\|\prec_1\| = \varepsilon_0$.

(b) $\mathrm{Z} \nvdash \mathrm{WF}_{\prec_1}(X)$.

Proof:

(a) From $\forall a \neq 0 \forall n(o(a[n]) < o(a))$, it follows that $\prec_1$ is wellfounded.

Now by $\prec_1$-induction on $a \in \mathbb{N}$ we obtain $o(a) = |a|_{\prec_1}$: $0 \neq a \overset{14.18}{\Rightarrow} o(a) = \sup_{n\in\omega}(o(a[n])+1) \overset{\mathrm{IH}}{=} \sup_{n\in\omega}(|a[n]|_{\prec_1}+1) = \sup\{|b|_{\prec_1}+1 : b \prec_1 a\} = |a|_{\prec_1}$. Hence $\varepsilon_0 = \sup\{|a|_{\prec_1}+1 : a \in \mathbb{N}\} = \|\prec_1\|$.

(b) $\varepsilon_0 = \|\prec_1\| \overset{4.10}{\Longrightarrow} \mathrm{Z} \nvdash \mathrm{TI}_{\prec_1}(X) \overset{4.19}{\Rightarrow} \mathrm{Z} \nvdash \mathrm{WF}_{\prec_1}(X)$.

Remark: Theorem 14.17 follows from 14.20b.

$\forall a \forall (n_i)_{i<\omega} \exists k(a[n_0][n_1]...[n_k] = 0) \;\Leftrightarrow$

$\forall (a_i)_{i<\omega}(\forall i(a_i = 0 \vee a_{i+1} \prec_1 a_i) \to \exists k(a_k = 0)) \;\Leftrightarrow$

$\forall x \exists! y(\langle x, y\rangle \in X) \wedge \forall x(\langle x, 0\rangle \in X \vee \forall z_0, z_1(\langle x, z_0\rangle \in X \wedge \langle x{+}1, z_1\rangle \in X \to z_1 \prec_1 z_0)) \to \exists x(\langle x, 0\rangle \in X)$.

By pure logic and $\forall y \neg(y \prec_1 0)$ the latter implies $\mathrm{WF}_{\prec_1}(X)$:

$\forall x \exists! y(\langle x, y\rangle \in X) \to \exists x([\langle x, 0\rangle \notin X \wedge \exists z_0, z_1(\langle x, z_0\rangle \in X \wedge \langle x{+}1, z_1\rangle \in X \wedge \neg(z_1 \prec_1 z_0))] \vee \langle x, 0\rangle \in X)$,

$\forall x \exists! y(\langle x, y\rangle \in X) \to \exists x, z_0, z_1(\langle x, z_0\rangle \in X \wedge \langle x{+}1, z_1\rangle \in X \wedge \neg(z_1 \prec_1 z_0))$.

15 Gödel's 2nd Incompleteness Theorem

Theorem (Gödel's 2nd Incompleteness Theorem)
If T is a recursively axiomatizable, consistent theory with $\mathrm{Z} \subseteq T$ then $T \nvdash \neg Prov_T(\ulcorner \bot \urcorner)$,
i.e., T does not prove its own consistency.

Here $Prov_T(x) := \exists y(Prf_\Phi(x,y) \approx 0)$, where Φ is a primitive recursive axiom system of T, and $Prf_\Phi \in \mathrm{PR}^2$ is the function symbol implicitely defined in the proof of Theorem 5.3 such that
$Prf_\Phi(a,b) = 0 \;\Leftrightarrow\; (a,b) \in \mathsf{Prf}_\Phi$.

We will obtain Gödel's 2nd Incompleteness Theorem as a Corollary from Theorems 15.1, 15.2 below.

Let T be a recursively axiomatizable consistent theory and $\mathcal{L} := \mathrm{L}(T)$.
Let Z be the axiom system of arithmetic, as introduced in §14 but without set variables. So, $\mathrm{L(Z)} = \mathcal{L}_0 = \mathrm{PR}$.
A Σ_1-*formula* is an $\mathcal{L}_0$-formula of the form $\exists x(s \approx t)$. Note that $Prov_T(x)$ is a Σ_1-formula.

Convention. Within formulas we often write $\ulcorner A \urcorner$ instead of $\underline{\ulcorner A \urcorner}$.

Theorem 15.1 (Gödel-Löb)
Assume that $\mathrm{Z} \subseteq T$, and that P is a 1-ary $\mathcal{L}$-formula satisfying the following *derivability conditions* for all $\mathcal{L}$-sentences A, B:

(D1) $T \vdash A \;\Rightarrow\; T \vdash P(\ulcorner A \urcorner)$,
(D2) $T \vdash P(\ulcorner A \to B \urcorner) \to P(\ulcorner A \urcorner) \to P(\ulcorner B \urcorner)$,
(D3) $T \vdash P(\ulcorner A \urcorner) \to P(\ulcorner P(\ulcorner A \urcorner) \urcorner)$.

Then for every $\mathcal{L}$-sentence A the following implication holds: $T \vdash P(\ulcorner A \urcorner) \to A \implies T \vdash A$.

Especially we have $T \nvdash \neg P(\ulcorner \bot \urcorner)$.

Proof:
Abbreviation: $\Box A := P(\ulcorner A \urcorner)$.
Let A be an $\mathcal{L}$-sentence with $T \vdash \Box A \to A$. Since every (primitive) recursive function is representable in Z (cf. Theorem 6.5 or the proof of 15.2a), the Fixpoint Lemma (Theorem 5.8) applies, and there exist an $\mathcal{L}$-sentence C such that $T \vdash C \leftrightarrow (\Box C \to A)$. Now we conclude:

(1) $T \vdash \Box C \to \Box\Box C \to \Box A$, [from $\vdash C \to \Box C \to A$ by (D1),(D2)]
(2) $T \vdash \Box C \to \Box A$, [from (1) and (D3) $\vdash \Box C \to \Box\Box C$]
(3) $T \vdash \Box C \to A$, [(2) and $\vdash \Box A \to A$]
(4) $T \vdash C$, [from (3) and $\vdash (\Box C \to A) \to C$]
(5) $T \vdash \Box C$, [(4),(D1)]
(6) $T \vdash A$. [(3),(5)]

Theorem 15.2.
(a) $\mathrm{Z} \vdash A$, for each *true* Σ_1-sentence A.
(b) $\mathrm{Z} \vdash Prov_T(\ulcorner A \to B \urcorner) \to Prov_T(\ulcorner A \urcorner) \to Prov_T(\ulcorner B \urcorner)$ for all $\mathcal{L}$-sentences A, B.
(c) If $\mathrm{Z} \subseteq T$ then $\mathrm{Z} \vdash A \to Prov_T(\ulcorner A \urcorner)$ for each Σ_1-sentence A.

Proof:

(a) Let $A = \exists x(s \approx t)$. Then there is an $a \in \mathbb{N}$ such that $s_x(\underline{a})^{\mathcal{N}} = t_x(\underline{a})^{\mathcal{N}}$. By L.15.3(Corollary) we get $\mathrm{Z} \vdash s_x(\underline{a}) \approx t_x(\underline{a})$ and then $\mathrm{Z} \vdash \exists x(s \approx t)$.

(b) One easily shows $\mathrm{Z} \vdash Prf_\Phi(\ulcorner A \to B \urcorner, y) \to Prf_\Phi(\ulcorner A \urcorner, z) \to Prf_\Phi(\ulcorner B \urcorner, y * z * \langle \ulcorner B \urcorner \rangle)$.
This implies the assertion.

(c) Roughly speaking, (c) is obtained by formalizing the proof of (a) in Z.

Proof of Gödel's 2nd Incompleteness Theorem:
Theorem 15.2 $\Rightarrow$ T and $P(x) := Prov_T(x)$ satisfy the conditions of Theorem 15.1 $\overset{15.1}{\Rightarrow}$ $T \nvdash \neg Prov_T(\ulcorner \bot \urcorner)$.

Lemma 15.3

For each $f \in \mathrm{PR}^n$ and all $a_1, ..., a_n, b \in \mathbb{N}$ we have: $f(a_1, ..., a_n) = b \implies \mathrm{Z} \vdash f\underline{a_1}...\underline{a_n} \approx \underline{b}$.

Proof by induction on the definition of f:

1. $\mathsf{S}(a) = b \Rightarrow \mathsf{S}\underline{a} = \underline{b} \Rightarrow \mathrm{Z} \vdash \mathsf{S}\underline{a} \approx \underline{b}$.

2. $\mathsf{C}^n_k(a_1, ..., a_n) = b \Rightarrow k = b \Rightarrow \mathrm{Z} \vdash \mathsf{C}^n_k\underline{a_1}...\underline{a_n} \approx \underline{b}$.

3. $\mathrm{I}^n_i(a_1, ..., a_n) = b \Rightarrow a_i = b \Rightarrow \mathrm{Z} \vdash \mathrm{I}^n_i\underline{a_1}...\underline{a_n} \approx \underline{b}$.

4. $f = (\circ h g_1 ... g_m)$ und $f(a) = b$:
Then $h(b_1, ..., b_m) = b$ with $b_1 := g_1(a), \ldots, b_m := g_m(a)$; and by I.H. we have
$\mathrm{Z} \vdash h\underline{b_1}...\underline{b_m} \approx \underline{b} \wedge g_1\underline{a} \approx \underline{b_1} \wedge \ldots \wedge g_m\underline{a} \approx \underline{b_m}$. From this we get $\mathrm{Z} \vdash f\underline{a} \approx hg_1\underline{a}...g_m\underline{a} \approx h\underline{b_1}...\underline{b_m} \approx \underline{b}$.

5. $f = (\mathsf{R}gh)$: Side induction on the last argument of f.

5.1. $f(a, 0) = b \Rightarrow g(a) = b \overset{\text{I.H.}}{\Rightarrow} \mathrm{Z} \vdash f\underline{a}0 \approx g\underline{a} \approx \underline{b}$.

5.2. Let $f(a, c{+}1) = b$. Then $h(a, c, d) = b$ with $d := f(a, c)$. By I.H. and S.I.H. from this we get
$\mathrm{Z} \vdash h\underline{a}\,\underline{c}\,\underline{d} \approx \underline{b}$ and $\mathrm{Z} \vdash f\underline{a}\,\underline{c} \approx \underline{d}$; hence $\mathrm{Z} \vdash f\underline{a}\,\underline{c{+}1} \approx f\underline{a}\mathsf{S}\underline{c} \approx h\underline{a}\,\underline{c}\,f\underline{a}\,\underline{c} \approx \underline{b}$.

Corollary. If t is a closed PR-term then $\mathrm{Z} \vdash t \approx \underline{b}$ for $b := t^{\mathcal{N}}$.

A generalization of Gödel's 2nd Incompleteness Theorem

Let T^* be a recursively axiomatizable theory and $\mathcal{L}^* := \mathrm{L}(T^*)$. We do not require that $\mathcal{L}_0 \subseteq \mathcal{L}^*$.

Definition

An *interpretation of* Z *in* T^* consists of a 1-ary $\mathcal{L}^*$-formula N and a mapping $A \mapsto A^N$, which assigns to each $\mathcal{L}_0$-formula A an $\mathcal{L}^*$-formula A^N such that the following holds:

(I1) $\bot^N = \bot$, $(A \to B)^N = A^N \to B^N$, $(\forall x A)^N = \forall x(N(x) \to A^N)$; $\mathrm{FV}(A^N) = \mathrm{FV}(A)$;

(I2) $\mathrm{Z} \vdash A$ & $\mathrm{FV}(A) = \emptyset \implies T^* \vdash A^N$.

The interpretation is called *strong* if in addition we have

(I3) $\mathrm{Z} \vdash Prov_{\mathrm{Z}}(\ulcorner A \urcorner) \to Prov_{T^*}(\ulcorner A^N \urcorner)$, for each $\mathcal{L}_0$-sentence A,

(I4) There is a primitive recursive function g such that $g(\ulcorner A \urcorner) = \ulcorner A^N \urcorner$, for each $\mathcal{L}_0$-sentence A.

Theorem 15.4

If T^* is a recursively axiomatizable, consistent theory, and $A \mapsto A^N$ a strong interpretation of Z in T^*, then $T^* \nvdash \neg Prov_{T^*}(\ulcorner \bot \urcorner)^N$.

Proof:

Let $T := \{A : A \text{ an } \mathcal{L}_0\text{-sentence with } T^* \vdash A^N\}$ and $P(x) := Prov_{T^*}(gx)$.

(1) $T \vdash A$ & A an $\mathcal{L}_0$-sentence $\Rightarrow$ $T^* \vdash A^N$, i.e. $A \in T$.

Proof: By assumption there are $A_1, ..., A_n \in T$ with $A_1 \to \ldots \to A_n \to A$ is logically valid.
From this we get by (I1),(I2) $T^* \vdash A_1^N \to \ldots \to A_n^N \to A^N$ and $T^* \vdash A_i^N$ $(i = 1, ..., n)$, hence $T^* \vdash A^N$.

(2) T consistent. [Proof: $T \vdash \bot \overset{(1)}{\Rightarrow} T^* \vdash \bot^N$. $\bot^N = \bot$.]

(3) $\mathrm{Z} \subseteq T$. [Proof: $A \in \mathrm{Z} \overset{(I2)}{\Rightarrow} T^* \vdash A^N$ & A $\mathcal{L}_0$-sentence $\Rightarrow$ $A \in T$.]

(D1) $T \vdash A \overset{(1)}{\Rightarrow} T^* \vdash A^N \overset{15.2a}{\Rightarrow} \mathrm{Z} \vdash P(\ulcorner A \urcorner)$.

(D2) From $\mathrm{Z} \vdash Prov_{T^*}(\ulcorner A^N \to B^N \urcorner) \to Prov_{T^*}(\ulcorner A^N \urcorner) \to Prov_{T^*}(\ulcorner B^N \urcorner)$ [15.2b] and $\ulcorner A^N \to B^N \urcorner =$
$= \ulcorner (A \to B)^N \urcorner = g(\ulcorner A \to B \urcorner)$, $\ulcorner A^N \urcorner = g(\ulcorner A \urcorner)$, $\ulcorner B^N \urcorner = g(\ulcorner A \urcorner)$ we get $\mathrm{Z} \vdash P(\ulcorner A \to B \urcorner) \to P(\ulcorner A \urcorner) \to P(\ulcorner B \urcorner)$.

(D3) $B := P(\ulcorner A \urcorner)$ is a Σ_1-sentence. Hence $\mathrm{Z} \vdash B \to Prov_{\mathrm{Z}}(\ulcorner B \urcorner)$ (by 15.2c), which by (I3) yields $\mathrm{Z} \vdash B \to Prov_{T^*}(\ulcorner B^N \urcorner)$ and then $\mathrm{Z} \vdash B \to P(\ulcorner B \urcorner)$ by (I4).

Theorem 15.1 $\Rightarrow$ $T \nvdash \neg P(\ulcorner \bot \urcorner)$ $\Rightarrow$ $\neg Prov_{T^*}(\ulcorner \bot \urcorner) \notin T$ $\Rightarrow$ $T^* \nvdash \neg Prov_{T^*}(\ulcorner \bot \urcorner)^N$.

Towards a proof of Theorem 15.2c

For $q \in \mathcal{L}_0 \cup \textsc{Vars} \cup \{\bot, \to, \forall, \approx\}$ let $\hat{q} := \underline{SN(q)}$.

For PR-terms $t_0, ..., t_{n-1}$ the PR-Term $\langle\!|t_0, ..., t_{n-1}|\!\rangle$ is defined as follows:
$\langle\!|\rangle := 0$, $\quad \langle\!|t_0, ..., t_n|\!\rangle := \mathsf{S}\pi t_0 \langle\!|t_1, ..., t_n|\!\rangle$.

Note: For closed PR-terms $t_0, ..., t_{n-1}$ we have $\langle\!|t_0, ..., t_{n-1}|\!\rangle^{\mathcal{N}} = \langle t_0^{\mathcal{N}}, ..., t_{n-1}^{\mathcal{N}} \rangle$.

Let $\nu \in \mathrm{PR}^1$ such that $\mathrm{Z} \vdash \nu\mathbf{0} \approx \underline{\ulcorner \mathbf{0} \urcorner} \wedge \nu\mathsf{S}x \approx \langle\!|\hat{\mathsf{S}}, \nu x|\!\rangle$.
Then $\nu(n) = \ulcorner \underline{n} \urcorner$ for all $n \in \mathbb{N}$.

Definition

A formula is called *simple*, if it is build up from atomic $\mathcal{L}_0$-formulas and closed $\mathcal{L}_0$-formulas of the shape $\forall x A$ by means of $\to$. $\mathcal{L}_0$-terms and simple formulas are called *simple expressions*.

q is used as syntactic variable for symbols from $\mathcal{L}_0 \cup \{\bot, \to, \approx\}$.

Let $\mathsf{Sub}_n^* \in \mathrm{PR}^{n+2}$ such that $\mathsf{Sub}_n^*(\ulcorner u \urcorner, \ulcorner t_0 \urcorner, ..., \ulcorner t_n \urcorner) = \ulcorner u_{v_0,...,v_n}(t_0, ..., t_n) \urcorner$.

($\mathsf{Sub}_n^*(a, \vec{c})$ shall be defined by recursion on a, similarly as $\mathsf{Sub}(a, c_1, c_2)$ in §5.)

Definition of $[u]$

For each simple expression u we define a PR-term $[u]$ as follows:
1. $[x] := \nu x$, 2. $[qu_1...u_n] := \langle\!|\hat{q}, [u_1], ..., [u_n]|\!\rangle$, 3. $[\forall x A] := \underline{\ulcorner \forall x A \urcorner}$.

Remark: $\mathrm{FV}([u]) = \mathrm{FV}(u)$.

Note:
If u is a simple expression with $\mathrm{FV}(u) \subseteq \{v_0, ..., v_n\}$ then $[u]^{\mathcal{N}}[v_0/a_0, \ldots, v_n/a_n] = \ulcorner u_{v_0,...,v_n}(\underline{a_0}, ..., \underline{a_n}) \urcorner$.
Especially $[u]^{\mathcal{N}} = \ulcorner u \urcorner$ if $\mathrm{FV}(u) = \emptyset$.

The following Lemma is stated without proof.

Lemma 15.5.

(a) If u is a simple expression with $\mathrm{FV}(u) \subseteq \{v_0, ..., v_n\}$, then
$\mathrm{Z} \vdash [u] \approx \mathsf{Sub}^*_n \ulcorner u \urcorner \nu v_0 \dots \nu v_n$.

(b) $\mathrm{Z} \vdash Prov_T(\langle\!\langle \hat{\to}, x, y \rangle\!\rangle) \to Prov_T(x) \to Prov_T(y)$.

(c) $\mathrm{Z} \vdash Prov_T(z) \to Prov_T(\mathsf{Sub}^*_n z\, \nu v_0 \dots \nu v_n)$.

Lemma 15.6. If u is a simple expression, and t is a term $\underline{k}$, x or $\mathsf{S}x$, then $\mathrm{Z} \vdash [u_y(t)] \approx [u]_y(t)$.

Proof by induction on u:

1. $u \in \textsc{Vars} \setminus \{y\}$ or $u = \forall x A$: trivial.

2. $u = y$: $[u_y(t)] = [t]$, $[u]_y(t) = \nu t$.

2.1. $t = \underline{k}$: $[\underline{k}]^{\mathcal{N}} = \ulcorner \underline{k} \urcorner = \nu(k) \overset{15.3(\mathrm{Cor.})}{\Longrightarrow} \vdash [\underline{k}] \approx \underline{\nu(k)} \approx \nu \underline{k}$.

2.2. $t = \mathsf{S}x$: $\vdash [\mathsf{S}x] \approx \langle\!\langle \hat{\mathsf{S}}, \nu x \rangle\!\rangle \approx \nu \mathsf{S}x$.

2.3. $t = x$: $[x] = \nu x$.

3. $u = q u_1 ... u_n$: $\vdash [u(y/t)] \approx \langle\!\langle \hat{q}, [u_1(y/t)], ..., [u_n(y/t)] \rangle\!\rangle \overset{\mathrm{IH}}{\approx} \langle\!\langle \hat{q}, [u_1](y/t), ..., [u_n](y/t) \rangle\!\rangle \approx [u](y/t)$.

Lemma 15.7. For simple formulas $A_1, ..., A_m, B$:

$\mathrm{Z} \vdash A_1 \to \dots \to A_m \to B \implies \mathrm{Z} \vdash Prov_T([A_1]) \to \dots \to Prov_T([A_m]) \to Prov_T([B])$

Proof: Abbreviation: $\mathsf{P}(x) := Prov_T(x)$.

(1) $\mathrm{Z} \vdash A \,\&\, A$ simple $\implies \mathrm{Z} \vdash \mathsf{P}([A])$.

Proof: $\mathrm{Z} \vdash A \Rightarrow T \vdash A \overset{15.2\mathrm{a}}{\Rightarrow} \mathrm{Z} \vdash \mathsf{P}(\ulcorner A \urcorner) \overset{15.5\mathrm{c}}{\Rightarrow} \mathrm{Z} \vdash \mathsf{P}(\mathsf{Sub}^*_n \ulcorner A \urcorner \nu v_0 \dots \nu v_n) \overset{15.5\mathrm{a}}{\Rightarrow} \mathrm{Z} \vdash \mathsf{P}([A])$.

(2) $\mathrm{Z} \vdash \mathsf{P}([A_1 \to \dots \to A_m \to B]) \to \mathsf{P}([A_1]) \to \dots \to \mathsf{P}([A_m]) \to \mathsf{P}([B])$, for simple $A_1, ..., A_m, B$.

Proof by induction on m:

1. $m = 0$: trivial. 2. $m > 0$: Let $C := A_2 \to ... \to A_m \to B$.

By 15.5b we then have $\mathrm{Z} \vdash \mathsf{P}([A_1 \to \dots \to A_m \to B]) \to \mathsf{P}([A_1]) \to \mathsf{P}([C])$.

Further by I.H.: $\mathrm{Z} \vdash \mathsf{P}([C]) \to \mathsf{P}([A_2]) \to \dots \to \mathsf{P}([A_m]) \to \mathsf{P}([B])$.

Now the Lemma is obtained as follows:

$\mathrm{Z} \vdash A_1 \to \dots \to A_m \to B \overset{(1)}{\Rightarrow} \mathrm{Z} \vdash \mathsf{P}(A_1 \to \dots \to A_m \to B) \overset{(2)}{\Rightarrow} \mathrm{Z} \vdash \mathsf{P}([A_1]) \to \dots \to \mathsf{P}([A_m]) \to \mathsf{P}([B])$.

Lemma 15.8

$\mathrm{Z} \vdash f x_1 ... x_n \approx y \to Prov_T([f x_1 ... x_n \approx y])$, for each function symbol $f \in \mathrm{PR}^n$.

Proof by induction on the definition of f:

1. $f = \mathsf{C}^n_k$:

(1) $\vdash f\vec{x} \approx \underline{k}$,

(2) $\vdash \mathsf{P}([f\vec{x} \approx \underline{k}])$, [(1), 15.7]

(3) $\vdash \underline{k} \approx y \to [f\vec{x} \approx \underline{k}] \approx [f\vec{x} \approx y]_y(\underline{k}) \approx [f\vec{x} \approx y]$, [15.6]

(4) $\vdash f\vec{x} \approx y \to \mathsf{P}([f\vec{x} \approx y])$ [(1),(2),(3)]

2. $f = \mathrm{I}^n_i$: as 1.

3. $f = \mathsf{S}$:

(1) $\vdash \mathsf{P}([fx \approx \mathsf{S}x])$, [15.7]

(2) $\vdash \mathsf{S}x \approx y \to [fx \approx \mathsf{S}x] \approx [fx \approx y]_y(\mathsf{S}x) \approx [fx \approx y]$, [15.6]

4. $f = (\circ h g_1 ... g_m)$:

(1) $\vdash \mathsf{P}([g_1\vec{x} \approx y_1]) \to \ldots \to \mathsf{P}([g_m\vec{x} \approx y_m])$, [15.7]

(2) $\vdash g_i\vec{x} \approx y_i \to \mathsf{P}([g_i\vec{x} \approx y_i])$, [I.H.]

(3) $\vdash hy_1...y_m \approx y \to \mathsf{P}([hy_1...y_m \approx y])$, [I.H.]

(4) $\vdash g_1\vec{x} \approx y_1 \to \ldots \to g_m\vec{x} \approx y_m \to hy_1...y_m \approx y \to \mathsf{P}([f\vec{x} \approx y])$, [(1),(2),(3)]

(5) $\vdash hg_1\vec{x} \ldots g_m\vec{x} \approx y \to \mathsf{P}([f\vec{x} \approx y])$, [(4) with $g_i\vec{x}$ in place of y_i]

5. $f = (\mathsf{R}gh)$:

Let $t := [f\vec{x}z \approx y]$. We will prove $\vdash \mathsf{P}(t_{z,y}(0, f\vec{x}0))$ and $\vdash \mathsf{P}(t_{z,y}(z, f\vec{x}z)) \to \mathsf{P}(t_{z,y}(\mathsf{S}z, f\vec{x}\mathsf{S}z))$.

By (formal) induction from this we obtain $\vdash \mathsf{P}(t_{z,y}(z, f\vec{x}z))$ and then $\vdash f\vec{x}z \approx y \to \mathsf{P}(t)$.

5.1. (1) $\vdash \mathsf{P}([g\vec{x} \approx y]) \to \mathsf{P}([f\vec{x}0 \approx y])$, [15.7]

(2) $\vdash g\vec{x} \approx y \to \mathsf{P}([g\vec{x} \approx y])$, [I.H.]

(3) $\vdash t_z(0) \approx [f\vec{x}0 \approx y]$, [15.6]

(4) $\vdash g\vec{x} \approx y \to \mathsf{P}(t_z(0))$, [(1),(2),(3)]

(5) $\vdash \mathsf{P}(t_{z,y}(0, f\vec{x}0))$. [(4) with $f\vec{x}0$ in place of y]

5.2. (1') $\vdash \mathsf{P}([h\vec{x}zw \approx y]) \to \mathsf{P}([f\vec{x}z \approx w]) \to \mathsf{P}([f\vec{x}\mathsf{S}z \approx y])$, [15.7]

(2') $\vdash h\vec{x}zw \approx y \to \mathsf{P}([h\vec{x}zw \approx y])$, [I.H.]

(3') $\vdash t_y(w) \approx [f\vec{x}z \approx w] \wedge t_z(\mathsf{S}z) \approx [f\vec{x}\mathsf{S}z \approx y]$, [15.6]

(4') $\vdash h\vec{x}zw \approx y \to \mathsf{P}(t_y(w)) \to \mathsf{P}(t_z(\mathsf{S}z))$, [(1'),(2'),(3')]

(5') $\vdash \mathsf{P}(t_{z,y}(z, f\vec{x}z)) \to \mathsf{P}(t_{z,y}(\mathsf{S}z, f\vec{x}\mathsf{S}z))$. [(4') with $f\vec{x}z$, $f\vec{x}\mathsf{S}z$ in place of w, y]

Proof of 15.2c ($\mathrm{Z} \vdash A \to Prov_T(\ulcorner A \urcorner)$, for each Σ_1-sentence A):

Let $g \in \mathrm{PR}^1$ such that $\mathrm{Z} \vdash \exists x(gx \approx 0) \leftrightarrow A$.

(1) $Z \vdash gx \approx 0 \to A$, [obvious]

(2) $Z \vdash \mathsf{P}([gx{\approx}0]) \to \mathsf{P}([A])$, [(1), 15.7]

(3) $Z \vdash [gx{\approx}0] \approx [gx{\approx}y]_y(0)$, [15.6]

(4) $Z \vdash gx \approx 0 \to \mathsf{P}([gx{\approx}y]_y(0))$, [15.8]

(5) $Z \vdash gx \approx 0 \to \mathsf{P}([A])$, [(2),(3),(4)]

(6) $Z \vdash \exists x(gx \approx 0) \to \mathsf{P}(\ulcorner A \urcorner)$, [(5), $\vdash [A] \approx \ulcorner A \urcorner$]