Proof Theory

Jaap van Oosten

Department of Mathematics, Utrecht University

May 25, 2011

Propositional rules of the sequent calculus; weak structural rules and Cut Rule:

$$\text{Exchange Left}\ \frac{\Gamma, A, B, \Pi \rightarrow \Delta}{\Gamma, B, A, \Pi \rightarrow \Delta}$$

$$\text{Exchange Right}\ \frac{\Gamma \rightarrow \Delta, A, B, \Lambda}{\Gamma \rightarrow \Delta, B, A, \Lambda}$$

$$\text{Contraction Left}\ \frac{A, A, \Gamma \rightarrow \Delta}{A, \Gamma \rightarrow \Delta}$$

$$\text{Contraction Right}\ \frac{\Gamma \rightarrow \Delta, A, A}{\Gamma \rightarrow \Delta, A}$$

$$\text{Weakening Left}\ \frac{\Gamma \rightarrow \Delta}{A, \Gamma \rightarrow \Delta}$$

$$\text{Weakening Right}\ \frac{\Gamma \rightarrow \Delta}{\Gamma \rightarrow \Delta, A}$$

$$\text{Cut Rule}\ \frac{\Gamma \rightarrow \Delta, A \qquad A, \Gamma \rightarrow \Delta}{\Gamma \rightarrow \Delta}$$

Propositional rules of the sequent calculus; logical rules:

$$\neg\ \text{Left}\ \frac{\Gamma \rightarrow \Delta, A}{\neg A, \Gamma \rightarrow \Delta}$$

$$\neg\ \text{Right}\ \frac{A, \Gamma \rightarrow \Delta}{\Gamma \rightarrow \Delta, \neg A}$$

$$\wedge\ \text{Left}\ \frac{A, B\Gamma \rightarrow \Delta}{A \wedge B, \Gamma \rightarrow \Delta}$$

$$\wedge\ \text{Right}\ \frac{\Gamma \rightarrow \Delta, A \qquad \Gamma \rightarrow \Delta, B}{\Gamma \rightarrow \Delta, A \wedge B}$$

$$\vee\ \text{Left}\ \frac{A, \Gamma \rightarrow \Delta \qquad B, \Gamma \rightarrow \Delta}{A \vee B, \Gamma \rightarrow \Delta}$$

$$\vee\ \text{Right}\ \frac{\Gamma \rightarrow \Delta, A, B}{\Gamma \rightarrow \Delta, A \vee B}$$

$$\supset\ \text{Left}\ \frac{\Gamma \rightarrow \Delta, A \qquad B, \Gamma \rightarrow \Delta}{A \supset B, \Gamma \rightarrow \Delta}$$

$$\supset\ \text{Right}\ \frac{A, \Gamma \rightarrow \Delta, B}{\Gamma \rightarrow \Delta, A \supset B}$$

Syntax of First-Order Logic

A *language* $\mathcal{L}$ is a collection of *function symbols* $f, g, \ldots$ and *Relation (or Predicate) Symbols* $R, P \ldots$, each with specified *arity*. There are two infinite sets of variables: the set BV of *bound variables* and the set FV of *free variables*.

The set of *semiterms* is defined inductively: every variable (of either kind) is a semiterm; if $t_1, \ldots, t_n$ are semiterms and f an n-ary function symbol, then $f(t_1, \ldots, t_n)$ is a semiterm.

The set of *semiformulas* is defined by: if $t_1, \ldots, t_n$ are semiterms and R is an n-ary predicate symbol, then $R(t_1, \ldots, t_n)$ is a semiformula; these semiformulas are called *atomic*.

If ϕ and ψ are semiformulas then so are $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \supset \psi)$ and $(\neg\phi)$.

If ϕ is a semiformula and x is a bound variable then $(\forall x \phi)$ and $(\exists x \phi)$ are semiformulas.

We speak of $\mathcal{L}$-semiterms, $\mathcal{L}$-semiformulas.

Semantics of First-Order Logic

An $\mathcal{L}$-structure $\mathcal{M}$ is a nonempty set M together with, for each n-ary function symbol f of $\mathcal{L}$, a function $f^{\mathcal{M}} : M^n \to M$ and for each n-ary relation (predicate) symbol R a subset $R^{\mathcal{M}}$ of M^n.

Given $\mathcal{M}$, an *object assignment* is a map $\sigma : \mathrm{BV} \cup \mathrm{FV} \to M$. If v is a variable (of either type) and $m \in M$, then $\sigma(m/v)$ is the object assignment which assigns m to v and coincides with σ on the other variables.

Define for each $\mathcal{L}$-semiterm t its value in $\mathcal{M}$ under σ, $t^{\mathcal{M}}[\sigma]$:
if t is a variable, then $t^{\mathcal{M}}[\sigma] = \sigma(t)$. If $t = f(t_1, \ldots, t_n)$ then (inductively) $t^{\mathcal{M}}[\sigma] = f^{\mathcal{M}}(t_1^{\mathcal{M}}[\sigma], \ldots, t_n^{\mathcal{M}}[\sigma])$.

Define for each $\mathcal{L}$-semiformula ϕ whether or not ϕ *is true in* $\mathcal{M}$ *under* σ, $\mathcal{M} \models \phi[\sigma]$:

If ϕ is atomic, $\phi = R(t_1, \ldots, t_n)$ then $\mathcal{M} \models \phi[\sigma]$ precisely if $(t_1^{\mathcal{M}}[\sigma], \ldots, t_n^{\mathcal{M}}[\sigma])$ is an element of $R^{\mathcal{M}}$.

$\mathcal{M} \models (\phi \wedge \psi)[\sigma]$ if both $\mathcal{M} \models \phi[\sigma]$ and $\mathcal{M} \models \psi[\sigma]$;

$\mathcal{M} \models (\phi \vee \psi)[\sigma]$ at least one of $\mathcal{M} \models \phi[\sigma]$ and $\mathcal{M} \models \psi[\sigma]$ holds;

$\mathcal{M} \models (\neg\phi)[\sigma]$ if $\mathcal{M} \not\models \phi[\sigma]$ (i.e., $\mathcal{M} \models \phi[\sigma]$ does *not* hold;

$\mathcal{M} \models (\phi \supset \psi)[\sigma]$ if $\mathcal{M} \models ((\neg\phi) \vee \psi)[\sigma]$.

Semantics of First-Order Logic; continued

$\mathcal{M} \models (\exists x \phi)[\sigma]$ if for some $m \in M$, $\mathcal{M} \models \phi[\sigma(m/x)]$ holds;
$\mathcal{M} \models (\forall x \phi)[\sigma]$ if for all $m \in M$, $\mathcal{M} \models \phi[\sigma(m/x)]$ holds.
Note: whether or not $\mathcal{M} \models \phi[\sigma]$ depends only on the values of σ on the variables occurring in ϕ.
Subsemiformulas: ψ is a subsemiformula of ϕ if ψ occurs in the construction tree of ϕ (that is: ϕ is atomic and $\psi = \phi$, or $\phi = \neg\chi$ and $\psi = \phi$ or ψ is a subsemiformula of χ, etc.)
Quantifiers: these are $\forall x$ and $\exists x$; sometimes we use Qx if we mean either. Say an occurrence of variable v is *in the scope of* a quantifier Qx if this occurrence is in a subformula of form $Qx(\cdots)$.
An $\mathcal{L}$-*term* is a semiterm in which no bound variables occur.
An $\mathcal{L}$-*formula* is a semiformula such that every occurrence x of a bound variable is in the scope of a quantifier Qx.
An $\mathcal{L}$-*sentence* is an $\mathcal{L}$-formula without free variables.

Semantics of First-Order Logic; continued

For a sentence ϕ, whether or not $\mathcal{M} \models \phi[\sigma]$ does not depend on σ; we say $\mathcal{M} \models \phi$: "ϕ is true in $\mathcal{M}$", or "$\mathcal{M}$ satisfies ϕ".

Let Γ be a set of $\mathcal{L}$-sentences, ϕ an $\mathcal{L}$-sentence. We say $\Gamma \models \phi$ if every $\mathcal{M}$ which satisfies every element of Γ also satisfies ϕ.

Substitution: let t be a semiterm and v an occurrence of a variable in a semiformula ϕ. Then t is *freely substitutable* for v in ϕ, if for every bound variable x in t, v is not in the scope of a quantifier Qx. If that is the case, we can form the *substitution* $\phi(t/v)$ or simply $\phi(t)$. When we write $\phi(t)$ we always have a *specific* substitution in mind.

Sequent Calculus for First-Order Logic

Axioms: $A \to A$ for every atomic formula.

The propositional rules as before.

The quantifier rules:

$$\forall \text{ Left } \frac{A(t), \Gamma \to \Delta}{\forall x A(x), \Gamma \to \Delta}$$

$$\forall \text{ Right } \frac{\Gamma \to \Delta, A(b)}{\Gamma \to \forall x A(x)}$$

$$\exists \text{ Left } \frac{A(b), \Gamma \to \Delta}{\exists x A(x), \Gamma \to \Delta}$$

$$\exists \text{ Right } \frac{\Gamma \to \Delta, A(t)}{\Gamma \to \Delta, \exists x A(x)}$$

Here t is an arbitrary term, b in ($\forall$ Right) and ($\exists$ Left) is a free variable, the *eigenvariable* of the inference.

Theorem 2.4.2: Let P be an LK-proof of $\Gamma \to \Delta$ with every cut of depth $\leq d$. Then there is a cut-free LK-proof P^* of $\Gamma \to \Delta$ with

$$\|P^*\| < 2^{\|P\|}_{2d+2}$$

Lemma 2.4.2.1: Let P be an LK-proof of $\Gamma \to \Delta$ which ends in a cut of depth d, having all other cuts of depth $< d$. Then there is an LK-proof P^* of $\Gamma \to \Delta$ with all cuts of depth $< d$, such that

$$\|P^*\| < \|P\|^2$$

Lemma 2.4.2.2: Let P be an LK-proof of $\Gamma \to \Delta$ with all cuts of depth $\leq d$. Then there is an LK-proof P^* of $\Gamma \to \Delta$ with all cuts of depth $< d$, such that

$$\|P^*\| < 2^{2^{\|P\|}}$$

Exercises March 16, 2011

Exercise 1. Bring the following formulas in prenex normal form, and then in Skolem normal form:

$$\exists x\,(\exists y R(x,y,a) \supset \forall w R(x,w,a))$$
$$\forall u\,(\forall v S(u,v) \supset \exists w S(w,u))$$

Exercise 2. Bring the following formula in prenex normal form and then in Herbrand normal form:

$$\forall x \neg \exists y\,(B(y) \vee \neg C(x))$$

Sequent Calculus LJ for Intuitionistic Logic. Recall: in every sequent $\Gamma \to \Delta$, the cedent Δ consists of at most one formula!
Axioms: $A \to A$ for atomic formulas A

$$\text{Exch Left}\ \frac{\Gamma, A, B, \Pi \to \Delta}{\Gamma, B, A, \Pi \to \Delta}$$

$$\text{Contr Left}\ \frac{A, A, \Gamma \to \Delta}{A, \Gamma \to \Delta}$$

$$\text{Weak Left}\ \frac{\Gamma \to \Delta}{A, \Gamma \to \Delta}$$

$$\text{Weak Right}\ \frac{\Gamma \to}{\Gamma \to A}$$

$$\text{Cut}\ \frac{\Gamma \to A \qquad A, \Gamma \to \Delta}{\Gamma \to \Delta}$$

$$\neg\ \text{Left}\ \frac{\Gamma \to A}{\neg A, \Gamma \to}$$

$$\neg\ \text{Right}\ \frac{A, \Gamma \to}{\Gamma \to \neg A}$$

$$\wedge \text{ Left } \frac{A, B, \Gamma \rightarrow \Delta}{A \wedge B, \Gamma \rightarrow \Delta}$$

$$\wedge \text{ Right } \frac{\Gamma \rightarrow A \qquad \Gamma \rightarrow B}{\Gamma \rightarrow A \wedge B}$$

$$\vee \text{ Left } \frac{A, \Gamma \rightarrow \Delta \qquad B, \Gamma \rightarrow \Delta}{A \vee B, \Gamma \rightarrow \Delta}$$

$$\vee \text{ Right 1 } \frac{\Gamma \rightarrow A}{\Gamma \rightarrow A \vee B}$$

$$\vee \text{ Right 2 } \frac{\Gamma \rightarrow A}{\Gamma \rightarrow B \vee A}$$

$$\supset \text{ Left } \frac{\Gamma \rightarrow A \qquad B, \Gamma \rightarrow \Delta}{A \supset B, \Gamma \rightarrow \Delta}$$

$$\supset \text{ Right } \frac{A, \Gamma \rightarrow B}{\Gamma \rightarrow A \supset B}$$

$$\forall \text{ Left } \frac{A(t), \Gamma \rightarrow \Delta}{\forall x A x, \Gamma \rightarrow \Delta}$$

$$\forall \text{ Right } \frac{\Gamma \rightarrow A(b)}{\Gamma \rightarrow \forall x A x}$$

$$\exists \text{ Left } \frac{A(b), \Gamma \rightarrow \Delta}{\exists x A x, \Gamma \rightarrow \Delta}$$

$$\exists \text{ Right } \frac{\Gamma \rightarrow A(t)}{\Gamma \rightarrow \exists x A x}$$

Of course with the usual variable restrictions on ($\forall$ Right) and ($\exists$ Left).

Theorem. If $\Gamma \to \Delta$ is provable in LJ from axioms only, then it has a cut-free proof.

Corollary. If $\to \exists x Ax$ is provable in LJ from axioms only, then there is a term t such that $\to A(t)$ is provable in LJ
If $\to A \vee B$ is provable in LJ from axioms only, then either $\to A$ or $\to B$ is provable.

Kripke structures for a language $\mathcal{L}$:

1. A partially ordered set P
2. For each $p \in P$ a nonempty set $D(p)$
3. For each $p \le q$ in P a function $f_{pq} : D(p) \to D(q)$
4. For every n-ary function symbol g of $\mathcal{L}$ and every $p \in P$ a function $[g]_p : D(p)^n \to D(p)$
5. For every n-ary relation symbol R of $\mathcal{L}$ and every $p \in P$ a subset $[R]_p \subset D(p)^n$

Subject to the following conditions:

a.f_{pp} is the identity function and for $p \le q \le r$ we have: $f_{pr} = f_{qr} \circ f_{pq}$

b. $f_{pq}([g]_p(x_1, \dots, x_n)) = [g]_q(f_{pq}(x_1, \dots, f_{pq}(x_n))$

c. $(x_1, \dots, x_n) \in [R]_p \;\Rightarrow\; (f_{pq}(x_1, \dots, f_{pq}(x_n)) \in [R]_q$

We get, for any term t of $\mathcal{L}$ with free variables $a_1, \ldots, a_n$ and every $p \in P$, a function

$$[t]_p : D(p)^n \to D(p)$$

which again satisfies:

$$f_{pq}([t]_p(x_1, \ldots, x_n)) = [t]_q(f_{pq}(x_1), \ldots, f_{pq}(x_n))$$

for all $x_1, \ldots, x_n \in D(p)$.

Define a relation $p \Vdash \phi[x_1, \ldots, x_n]$ for $p \in P$, ϕ an $\mathcal{L}$-formula with free variables $a_1, \ldots, a_n$ and $x_1, \ldots, x_n \in D(p)$:

$p \Vdash R(t_1, \ldots, t_m)[\vec{x}]$ iff $([t_1]_p(\vec{x}), \ldots, [t_m]_p(\vec{x})) \in [R]_p$
$p \Vdash t = s[\vec{x}]$ iff $[t]_p(\vec{x}) = [s]_p(\vec{x})$
$p \Vdash (\phi \wedge \psi)[\vec{x}]$ iff $p \Vdash \phi[\vec{x}]$ and $p \Vdash \psi[\vec{x}]$
$p \Vdash (\phi \vee \psi)[\vec{x}]$ iff $p \Vdash \phi[\vec{x}]$ or $p \Vdash \psi[\vec{x}]$
$p \Vdash (\phi \supset \psi)[\vec{x}]$ iff for all $q \geq p$, if $q \Vdash \phi[f_{pq}(\vec{x})]$ then $q \Vdash \psi[f_{pq}(\vec{x})]$
$p \Vdash (\neg\phi)[\vec{x}]$ iff for all $q \geq p$, $q \nVdash \phi[f_{pq}(\vec{x})]$
$p \Vdash (\exists y \phi)[\vec{x}]$ if for some $x' \in D(p)$, $p \Vdash \phi[x', \vec{x}]$
$p \Vdash (\forall y \phi)[\vec{x}]$ if for all $q \geq p$ and all $x' \in D(q)$, $q \Vdash \phi[x', f_{pq}(\vec{x})]$

Exercise: For all ϕ and $\vec{x}$ as above: if $p \Vdash \phi[\vec{x}]$ and $q \geq p$, then $q \Vdash \phi[f_{pq}(\vec{x})]$

Example. Let:

$P =$ 

with $D(0) = \{x\}$, $D(1) = \{x, \xi\}$ and f_{01} the inclusion.
Let $[A]_0 = \emptyset$, $[A]_1 = \{x\}$
$[B]_0 = \{(x, x)\}$, $[B]_1 = \{(x, x)\}$

Then $0 \Vdash \forall y(A(x) \vee B(x, y))$ since for all $\eta \in D(0)$, $\eta = x$ and $0 \Vdash B(x, x)$, and for all $\eta \in D(1)$, $1 \Vdash A(x) \vee B(x, \eta)$ since $1 \Vdash A(x)$.
However, $0 \nVdash A(x) \vee \forall y B(x, y)$: $0 \nVdash A(x)$ is clear, and $1 \nVdash B(x, \xi)$ so $0 \nVdash \forall y B(x, y)$.

We see that the implication

$$\forall y(A(x) \vee B(x, y)) \supset (A(x) \vee \forall y B(x, y))$$

is not valid in Kripke models.

A Kripke structure for propositional logic is just a partially ordered set P.

A *truth assignment* σ assigns to every propositional variable p a subset σ_p of P which satisfies: if $\xi \in \sigma_p$ and $\eta \geq \xi$, then $\eta \in \sigma_p$.

We then define the relation $\xi \Vdash A[\sigma]$:

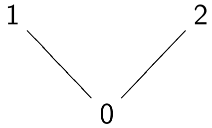
$\xi \Vdash p[\sigma]$ iff $\xi \in \sigma_p$

$\xi \Vdash A \wedge B$, $\xi \Vdash A \vee B$ as before

$\xi \Vdash \neg A$ iff for all $\eta \geq \xi$, $\eta \nVdash A$

$\xi \Vdash A \supset B$ iff for all $\eta \geq \xi$, if $\eta \Vdash A$ then $\eta \Vdash B$

Example: Let

$P =$ 

Let $\sigma_p = \{1\}, \sigma_q = \{2\}$.

Then $0 \not\Vdash ((p \supset q) \vee (q \supset p))[\sigma]$

Theorem. Both for propositional and first-order logic, the intuitionistic sequent calculus is sound and complete for Kripke models.

Exercises, March 30:

1. Find a cut-free LJ-proof of the intuitionistic sequent $\neg\neg\neg A \to \neg A$; and also one for $\to \neg\neg(A \vee \neg A)$

2. Find Kripke countermodels for the following statements:

a. $((p \supset q) \supset p) \supset p$

b. $(\phi \supset \exists x \psi(x)) \supset \exists x(\phi \supset \psi(x))$ (x not in ϕ)

In general, one can get by, when constructing Kripke models for statements not involving equalitiy axioms, with structures where, for $p \leq q$, $D(p) \subseteq D(q)$.
For propositional logic, one can take the poset P to be a *finite tree*.

Some additional exercises:

3. Let P be a partially ordered set with a least element. Show that the following two conditions are equivalent:
a. For any truth assignment, for every $\xi \in P$,
$\xi \Vdash ((p \supset q) \vee (q \supset p))$
b. P is a linear order.

4. Let P be a partially ordered set. Prove that the following two statements are equivalent:
a. For every Kripke structure for a language $\mathcal{L}$ on P and for every $\mathcal{L}$-sentence ϕ which is LK-valid, we have $p \Vdash \neg\neg\phi$ for every $p \in P$
b. For every $p \in P$ there is an element $q \geq p$ such that q is maximal in P.

For a hint: see next page

Hint for Exercise 4 of previous page:
For the direction b⇒a, note that if p is a maximal element in the partially ordered set of a Kripke structure for a language $\mathcal{L}$, then $p \Vdash \phi$ for every classically valid (i.e., LK-valid) $\mathcal{L}$-sentence ϕ.

For the other direction, let $\mathcal{L}$ be the language $\{<\}$ of orders; let

$$D(p) \ = \ \{q \in P \mid q \leq p\}$$

(with f_{pq} the inclusion) and $<$ interpreted as the order on $D(p)$ inherited from P.

Consider the $\mathcal{L}$-sentence ϕ:

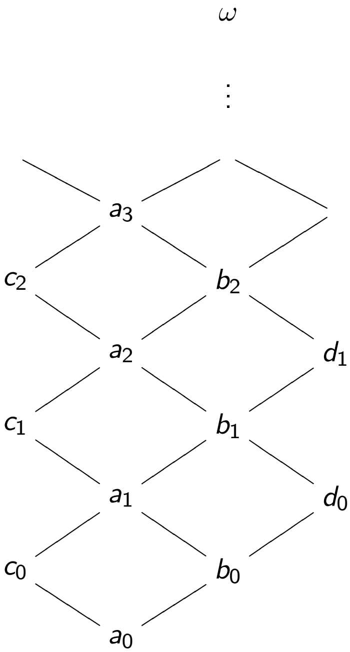
$$\forall x \exists y (x < y) \vee \exists x \forall y \neg (x < y)$$

and show that $p \Vdash \phi$ precisely when p is a maximal element in P.

Some scattered facts about intuitionistic logic:
1. Let $(\cdot)^-$ be the negative (Gödel-Gentzen) translation. Then it is easy to prove by induction, that for propositional formulas ϕ, $\mathrm{LJ} \vdash (\phi)^- \leftrightarrow \neg\neg\phi$. Combining this with the theory on p. 67, we get *Glivenko's Theorem*: for any propositional formula A, $\mathrm{LK} \vdash A$ if and only if $\mathrm{LJ} \vdash \neg\neg A$. Warning: this does *not* hold for all first-order formulas A!

Modulo LK-provable equivalence, there are exactly 2^{2^n} formulas in the n propositional variables $p_1, \ldots, p_n$.

Intuitionistically, the situation is more complicated: modulo LJ-provable equivalence, there are infinitely many formulas in one propositional variable p. These (equivalence classes of) formulas constitute a lattice: the *Rieger-Nishimura lattice* or the *free Heyting algebra on one generator*:



with

$$\omega = p \supset p$$
$$a_0 = p \wedge \neg p$$
$$b_0 = p$$
$$c_0 = \neg p$$
$$d_i = c_i \supset a_i$$
$$c_{i+1} = d_i \supset b_i$$
$$a_{i+1} = c_i \vee b_i$$
$$b_{i+1} = a_{i+1} \vee d_i$$

Proof of the second statement of 1.2.7.2: let a relation be Δ_1-defined by $I\Delta_0$; then it is Δ_0-defined by $I\Delta_0$ and $I\Delta_0$ proves the equivalence between the two definitions.
Since R is Δ_1-defined there are formulas $\forall\vec{x}\psi(\vec{x},\vec{y})$ and $\exists\vec{v}\chi(\vec{v},\vec{y})$ (with $\psi,\chi \in \Delta_0$) which both define R, and

$$\begin{array}{ll} (1) & I\Delta_0 \vdash \forall\vec{y}(\forall\vec{x}\psi(\vec{x},\vec{y}) \supset \exists\vec{v}\chi(\vec{v},\vec{y})) \\ (2) & I\Delta_0 \vdash \forall\vec{y}(\exists\vec{v}\chi(\vec{v},\vec{y}) \supset \forall\vec{x}\psi(\vec{x},\vec{y})) \end{array}$$

From (1) we get $I\Delta_0 \vdash \forall\vec{y}\exists\vec{x}\exists\vec{v}(\psi(\vec{x}.\vec{y}) \supset \chi(\vec{v},\vec{y}))$, hence by Parikh's Theorem we get a term $t(\vec{y})$ such that

$$(3) \quad I\Delta_0 \vdash \forall\vec{y}\exists\vec{x} \leq t(\vec{y})\exists\vec{v} \leq t(\vec{y})(\psi(\vec{x},\vec{y}) \supset \chi(\vec{v},\vec{y}))$$

We conclude:

$$I\Delta_0 \vdash \forall\vec{y}(\forall\vec{x} \leq t(\vec{y})\psi(\vec{x},\vec{y}) \supset \exists\vec{v} \leq t(\vec{y})\chi(\vec{v},\vec{y}))$$

Then $\forall\vec{x} \leq t(\vec{y})\psi(\vec{x},\vec{y})$ is a Δ_0-formula defining R.

Another important remark: let T be any arithmetical theory and f a function. Then if f is Σ_1-defined by T, it is in fact Δ_1-defined:

For, suppose the Σ_1-formula $\exists\vec{z}A_f(\vec{x},\vec{z},y)$ defines the relation $f(\vec{x})=y$, with $A_f \in \Delta_0$.
Then since $T \vdash \forall\vec{x}\exists!y\exists\vec{z}A_f(\vec{x},\vec{z},y)$ we have:

$$T \vdash \forall\vec{x},y(\exists\vec{z}A_f(\vec{x},\vec{z},y) \leftrightarrow \forall\vec{z}\forall w(A_f(\vec{x},\vec{z},w) \supset w=y))$$

so the Π_1-formula $\forall\vec{z}\forall w(A_f(\vec{x},\vec{z},w) \supset w=y)$ also defines f.

Exercises.

1. Express by a Δ_0-formula ϕ that "there exist unique a and b such that $y = ax + b$ and $b < x$", and prove that

$$I\Delta_0 \vdash \forall x > 0 \forall y \phi$$

2.a) Give a formula ϕ such that $\exists! x \exists! y \phi$ is true but $\exists! y \exists! x \phi$ is false.

b) Define a quantifier $\exists!(a, b)$ for " there is a unique pair (a, b)", and show that $\exists!(a, b)$ is not equivalent to $\exists! a \exists! b$.

Exercises for section 1.2.

1. Prove that in $I\Delta_0$ the following sentence is provable:

$$\forall xa \exists z \, [\forall k (1 \le k \le \mathrm{Len}(x) \supset \beta(k,x) = \beta(k,z)) \\ \wedge \beta(\mathrm{Len}(x)+1, z) = a \,]$$

2. Prove: $B\Sigma_{n+1} \Rightarrow I\Sigma_n$ and $I\Pi_n \Leftrightarrow L\Sigma_n$.
3. The *Ackermann function* is defined by:

$$\begin{aligned} A(0,n) &= n+1 \\ A(m+1,0) &= A(m,1) \\ A(m+1,n+1) &= A(m, A(m+1,n)) \end{aligned}$$

Prove that the graph of the Ackermann function is Δ_1-definable by $I\Sigma_1$.
4. Prove that $2^{x-1} > x^2$ for all $x \ge 7$. Conclude from this that $|x|^2 < x$ whenever $x > 36$.

Exercises about Gödel's Incompleteness Theorems. We work with PA. In the exercises below you may assume that $\mathbb{N}$ is a model of PA. When we say 'true', we mean: true in $\mathbb{N}$.
Let G be the Gödel sentence: so $\mathrm{PA} \vdash G \leftrightarrow \neg\exists x \mathrm{Prf}(x, \overline{\ulcorner G \urcorner})$, where $\mathrm{Prf}(x, y)$ is a Δ_1-formula representing the relation: "y is the Gödel number of a formula and x is a Gödel number of a proof in PA of that formula".

1. Prove that G is true.
2. Prove that $\mathrm{PA} \nvdash G$.
3. Prove that $\mathrm{PA} \nvdash \neg G$.

Elements of Partial Recursive Function Theory

Definition. A *partial function* $\mathbb{N}^k \rightharpoonup \mathbb{N}$ is a function $U \xrightarrow{f} \mathbb{N}$ where $U \subseteq \mathbb{N}^k$. We write $\mathrm{dom}(f)$ for U. We also write $f(\vec{x})\downarrow$ ("$f(\vec{x})$ is defined") for: $\vec{x} \in \mathrm{dom}(f)$.

Definition. A partial function $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ is defined by *minimization* from a partial function $g : \mathbb{N}^{k+1} \rightharpoonup \mathbb{N}$ if

$$\begin{aligned} \mathrm{dom}(f) \quad = \quad & \{\vec{x} \mid \exists y\, [g(\vec{x}, y) = 0 \text{ and} \\ & \forall i \leq y\, (\vec{x}, i) \in \mathrm{dom}(g)]\} \end{aligned}$$

and for all $\vec{x} \in \mathrm{dom}(f)$, $f(\vec{x})$ is the least such y.
We write: $f(\vec{x}) \simeq \mu y.g(\vec{x}, y) = 0$.
Between expressions involving partial functions, the symbol "$\simeq$" means: the LHS is defined precisely when the RHS is, and they denote the same value if defined.

Definition. The class of *partial recursive functions* is the least class of partial functions which contains all primitive recursive functions and is closed under composition and minimization.

If $f_1, \ldots, f_k$ are n-ary partial recursive functions and g is k-ary partial recursive, then the composition of g and $f_1, \ldots, f_k$ is the n-ary partial function h, defined by

$$h(\vec{x}) \;\simeq\; g(f_1(\vec{x}), \ldots, f_k(\vec{x}))$$

Here $\vec{x} \in \mathrm{dom}(h)$ if and only if $\vec{x} \in \bigcap_{i=1}^{k} \mathrm{dom}(f_i)$ and $(f_1(\vec{x}), \ldots, f_k(\vec{x})) \in \mathrm{dom}(g)$.

Theorem [Normal Form Theorem; Kleene] There are primitive recursive functions T^k, for each $k > 0$, and U, satisfying the following:
For every partial recursive function $f : \mathbb{N}^k \to \mathbb{N}$ there is a number e such that for all $\vec{x} \in \mathbb{N}^k$:

- $\vec{x} \in \mathrm{dom}(f) \;\Leftrightarrow\; \exists y\, T^k(e, \vec{x}, y) = 0$
- $f(\vec{x}) \;\simeq\; U(\mu y. T^k(e, \vec{x}, y) = 0)$

In view of the Normal Form Theorem, we write $\varphi_e^{(k)}$ for f, and we call e an *index* for the partial recursive function f.

Theorem The system of indices for partial recursive functions has the following properties:

a) For every k-ary partial recursive f there are infinitely many indices e such that $f = \varphi_e^{(k)}$

b) (S_n^m-Theorem) There are primitive recursive functions S_n^m for each $n > 0$, $m > 0$, such that for each $e, x_1, \ldots, x_m, y_1, \ldots, y_n$:

$$\varphi_{S_n^m(e,x_1,\ldots,x_m)}(y_1, \ldots, y_n) \simeq \varphi_e^{(m+n)}(x_1, \ldots, x_m, y_1, \ldots, y_n)$$

c) For each $k > 0$ the partial function

$$e, x_1, \ldots, x_k \mapsto \varphi_e^{(k)}(x_1, \ldots, x_k)$$

is partial recursive.

Theorem [Recursion Theorem; Kleene] Let $F : \mathbb{N}^{k+1} \rightharpoonup \mathbb{N}$ be a partial recursive function. Then there is an index e such that for all $\vec{x} \in \mathbb{N}^k$:

$$\varphi_e^{(k)}(\vec{x}) \simeq F(\vec{x}, e)$$

Corollary. The partial recursive functions are closed under primitive recursion: if $g : \mathbb{N}^k \rightharpoonup \mathbb{N}$ and $h : \mathbb{N}^{k+2} \rightharpoonup \mathbb{N}$ are partial recursive and $f : \mathbb{N}^{k+1} \rightharpoonup \mathbb{N}$ is defined by

$$\begin{array}{rcl} f(\vec{x}, 0) & \simeq & g(\vec{x}) \\ f(\vec{x}, y+1) & \simeq & h(\vec{x}, f(\vec{x}, y), y) \end{array}$$

then f is partial recursive. Here $(\vec{x}, y) \in \mathrm{dom}(f)$ if and only if $\vec{x} \in \mathrm{dom}(g)$ and for all $i < y$,

$$(\vec{x}, f(\vec{x}, i), i) \in \mathrm{dom}(h)$$

Proof. Let $\mathrm{sg}(y)$ be the primitive recursive function such that $\mathrm{sg}(0) = 0$ and $\mathrm{sg}(y + 1) = 1$; and let $\overline{\mathrm{sg}}(y) = 1 \dot{-} \mathrm{sg}(y)$.
Let γ be an index for g and ι an index for h. Consider the partial function $F(\vec{x}, y, e)$, given by

$$\overline{\mathrm{sg}}(y) \cdot \varphi_\gamma^{(k)}(\vec{x}) + \mathrm{sg}(y) \cdot \varphi_\iota^{(k+2)}(\vec{x}, \varphi_e^{(k+1)}(\vec{x}, y \dot{-} 1), y \dot{-} 1)$$

Then F is partial recursive. By the recursion theorem, there is an index e such that for all $\vec{x}, y$,

$$\varphi_e^{(k+1)}(\vec{x}, y) \;\simeq\; F(\vec{x}, y, e)$$

It follows, that $\varphi_e^{(k+1)}(\vec{x}, y) \simeq f(\vec{x}, y)$.

Corollary [The "Halting Problem"; Turing] There is no partial recursive function f such that for all e and $x_1, \ldots, x_k$ we have: $f(e, \vec{x}) = 0$ if $\vec{x} \in \mathrm{dom}(\varphi_e^{(k)})$, and $f(e, \vec{x}) = 1$ otherwise.

Proof. Suppose such f exists. Let g be a partial recursive function such that $\mathrm{dom}(g) = \mathbb{N} - \{0\}$ (for example, $g(x) \simeq \mu y . x \cdot y > 1$). By the recursion theorem, let e be an index such that for all $\vec{x}$,

$$\varphi_e^{(k)}(\vec{x}) \ \simeq \ g(f(e, \vec{x}))$$

Then $\vec{x} \in \mathrm{dom}(\varphi_e^{(k)}) \ \Leftrightarrow \ f(e, \vec{x}) \neq 0 \ \Leftrightarrow \ \vec{x} \notin \mathrm{dom}(\varphi_e^{(k)})$; a contradiction.

Heyting Arithmetic

Heyting Arithmetic (HA) is the intuitionistic version of Peano Arithmetic. The language and axioms are the same:

1) $S(x) \neq 0$
2) $S(x) = S(y) \supset x = y$
3) $x + 0 = x$
4) $x + S(y) = S(x + y)$
5) $x \cdot 0 = 0$
6) $x \cdot S(y) = x \cdot y + x$
7) $\phi(0) \wedge \forall x(\phi(x) \supset \phi(S(x))) \supset \forall x \phi(x)$ for all ϕ

But the logic is given by the calculus LJ.

Although the logic of HA is intuitionistic, one can still prove instances of the 'Law of Excluded Middle':
$\mathrm{HA} \vdash \forall xy(x = y \vee \neg(x = y))$
$\mathrm{HA} \vdash \forall xy(x < y \vee x = y \vee x > y)$
where the order $<$ is defined as: $x < y \equiv \exists z(x + S(z) = y)$
These things are proved by induction.
In general, $\mathrm{HA} \vdash \phi \vee \neg\phi$ when ϕ is a Δ_0-formula.

We wish to define a nontrivial interpretation of HA into classical, ordinary mathematics. We cannot use an ordinary model, because then $\phi \vee \neg\phi$ would be true for *all* formulas.

Realizability (Kleene; 1945) In the following, we assume that $x, y \mapsto \langle x, y\rangle$ is a primitive recursive bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, with primitive recursive inverse $x \mapsto ((x)_0, (x)_1)$. So every number x is regarded as code of an ordered pair.

Consider a formula $\phi(u_1, \ldots, u_n)$ with free variables $u_1, \ldots, u_n$. For a number e and an n-tuple of numbers $k_1, \ldots, k_n$, we define what it means that

$$e \text{ realizes } \phi[k_1, \ldots, k_n]$$

by induction on the formula ϕ

e realizes $\phi[k_1, \ldots, k_n]$ if and only if $\mathbb{N} \models \phi[k_1, \ldots, k_n]$, if ϕ is an atomic formula

e realizes $(\phi \wedge \psi)[k_1, \ldots, k_n]$ if and only if $(e)_0$ realizes $\phi[k_1, \ldots, k_n]$ and $(e)_1$ realizes $\psi[k_1, \ldots, k_n]$

e realizes $(\phi \vee \psi)[k_1, \ldots, k_n]$ if and only if *either* $(e)_0 = 0$ and $(e)_1$ realizes $\phi[k_1, \ldots, k_n]$, *or* $(e)_0 \neq 0$ and $(e)_1$ realizes $\psi[k_1, \ldots, k_n]$

e realizes $(\phi \supset \psi)[k_1, \ldots, k_n]$ if and only if for each number a such that a realizes $\phi[k_1, \ldots, k_n]$, we have $\varphi_e(a)\downarrow$ and $\varphi_e(a)$ realizes $\psi[k_1, \ldots, k_n]$

e realizes $(\neg\phi)[k_1, \ldots, k_n]$ if and only if no number realizes $\phi[k_1, \ldots, k_n]$

e realizes $(\exists x \phi)[k_1, \ldots, k_n]$ if and only if $(e)_1$ realizes $\phi[(e)_0, k_1, \ldots, k_n]$

e realizes $(\forall x \phi)[k_1, \ldots, k_n]$ if and only if for each number m, $\varphi_e(m)\downarrow$ and $\varphi_e(m)$ realizes $\phi[m, k_1, \ldots, k_n]$

Main Theorem (Kleene)
1. For every sentence ϕ such that $\mathrm{HA} \vdash \phi$, there is a number e such that e realizes ϕ.
2. There is a Π_1-formula $\forall n \psi(m, n)$ such that the sentence

$$\forall m \, [\forall n \psi(m, n) \vee \neg \forall n \psi(m, n)]$$

is not realized by any number.

Hence, realizability is a nontrivial interpretation of HA.

We shall start by looking at point 2.

Definition. An *almost negative* formula is a formula which contains $\vee$ and $\exists$ only between (viz. before) Δ_0-formulas. Note, that every Δ_0-formula is almost negative.

Theorem on Almost Negative Formulas. Let ϕ be an almost negative formula with free variables $u_1, \ldots, u_n$.
1. There is a partial recursive function t_ϕ of n variables such that for all n-tuples $k_1, \ldots, k_n$ we have: if $\mathbb{N} \models \phi[k_1, \ldots, k_n]$ then $t_\phi(k_1, \ldots, k_n)$ is defined and realizes $\phi[k_1, \ldots, k_n]$
2. If a number e realizes $\phi[k_1, \ldots, k_n]$ then $\mathbb{N} \models \phi[k_1, \ldots, k_n]$

This theorem is proved by induction on the structure of ϕ. First a Lemma:

Δ_0-**Lemma** For every Δ_0-formula $\phi(u_1, \ldots, u_n)$ there is a primitive recursive function s_ϕ such that for all n-tuples $k_1, \ldots, k_n$ the following hold:
1. If $\mathbb{N} \models \phi[\vec{k}]$ then $(s_\phi(\vec{k}))_0 = 0$ and $(s_\phi(\vec{k}))_1$ realizes $\phi[\vec{k}]$
2. If $\mathbb{N} \not\models \phi[\vec{k}]$ then $(s_\phi(\vec{k}))_0 \neq 0$

Proof: Exercise!

Proof of the Theorem on Almost Negative Formulas: we define the partial recursive functions t_ϕ by recursion on the structure of ϕ, and we prove at the same time properties 1 and 2 by simultaneous induction on ϕ.
For atomic ϕ, let $t_\phi(\vec{k}) = 0$. The proof of 1 and 2 is by definition.
For $\exists x\phi$ with $\phi \in \Delta_0$ we put $t_{\exists x\phi}(\vec{k}) \simeq \langle a, b\rangle$, where

$$\begin{aligned} a &= \mu y.(s_\phi(y, \vec{k}))_0 = 0 \\ b &= (s_\phi(a, \vec{k}))_1 \end{aligned}$$

Here s_ϕ is the primitive recursive function from the Δ_0-Lemma.
For $\phi \wedge \psi$ we put

$$t_{\phi\wedge\psi}(\vec{k}) \simeq \langle t_\phi(\vec{k}), t_\psi(\vec{k})\rangle$$

For $\phi \supset \psi$: Let e be an index such that for all $\vec{k}, m$, $\varphi_e^{(n+1)}(\vec{k}, m) \simeq t_\psi(\vec{k})$. Then put

$$t_{\phi \supset \psi}(\vec{k}) = S_1^n(e, \vec{k})$$

where S_1^m is from the S_n^m-Theorem.
Proof of 1 and 2 in this case: First, suppose $\mathbb{N} \models (\phi \supset \psi)[\vec{k}]$. We always have $t_{\phi \supset \psi}(\vec{k})\downarrow$ since S_1^n is primitive recursive. Suppose m realizes $\phi[\vec{k}]$. Then $\mathbb{N} \models \phi[\vec{k}]$ by induction hypothesis, so $\mathbb{N} \models \psi[\vec{k}]$ by assumption. Hence by induction hypothesis $t_\psi(\vec{k})$ is defined and realizes $\psi[\vec{k}]$, but $t_\psi(\vec{k})$ is just the partial recursive function with index $t_{\phi \supset \psi}(\vec{k})$, applied to m. We conclude that $t_{\phi \supset \psi}(\vec{k})$ realizes $(\phi \supset \psi)[\vec{k}]$, as desired.
Conversely, suppose m realizes $(\phi \supset \psi)[\vec{k}]$. Suppose $\mathbb{N} \models \phi[\vec{k}]$. Then $t_\phi(\vec{k})$ is defined and realizes $\phi[\vec{k}]$, hence $\varphi_m^{(n)}(t_\phi(\vec{k}))$ is defined and realizes $\psi[\vec{k}]$. By induction hypothesis, $\mathbb{N} \models \psi[\vec{k}]$. We conclude that $\mathbb{N} \models (\phi \supset \psi)[\vec{k}]$.

For $\forall x\phi$, let e be an index such that for all $m, \vec{k}$, $\varphi_e^{(n+1)}(\vec{k}, m) \simeq t_\phi(m, \vec{k})$. Put

$$t_{\forall x\phi}(\vec{k}) \simeq S_1^n(e, \vec{k})$$

Convince yourself that this works (Exercise!). This finishes the proof of the Theorem on Almost Negative Formulas.

To finish the proof of Part 2 of the Main Theorem: let $\psi(e, m, y)$ be a Δ_1-formula which represents the relation: $T^1(e, m, y) \neq 0$. So $\forall y\psi(e, m, y)$ is an almost negative formula which represents the relation: $\varphi_e^{(1)}(m)$ is undefined.
Suppose k realizes the sentence

$$\forall em[\forall y\psi(e, m, y) \vee \neg\forall y\psi(e, m, y)]$$

Then for all e, m, $\phi_k^{(2)}(e, m)$ is defined and:

$$\begin{array}{lcl} (\varphi_k^{(2)}(e, m))_0 = 0 & \Rightarrow & (\varphi_k^{(2)}(e, m))_1 \text{ realizes } \forall y\psi(e, m, y) \\ (\varphi_k^{(2)}(e, m))_0 \neq 0 & \Rightarrow & (\varphi_k^{(2)}(e, m))_1 \text{ realizes } \neg\forall y\psi(e, m, y) \end{array}$$

Then by the Theorem on Almost Negative Formulas we have: $\varphi_e^{(1)}(m)$ is defined, precisely if $(\varphi_k^{(2)}(e, m))_0 \neq 0$. But this contradicts the unsolvability of the Halting Problem.
This proves part 2 of the Main Theorem.

Proof sketch of Part 1 of the Main Theorem: if $\mathrm{HA} \vdash \phi$ then there is a number e such that e realizes ϕ.
This is done by induction on HA-proofs. One needs to check the axioms and rules of intuitionistic predicate logic, and the arithmetical axioms.
Starting with the induction axiom:

$$\forall \vec{y}[\phi(0,\vec{y}) \wedge \forall x(\phi(x,\vec{y}) \supset \phi(Sx,\vec{y})) \supset \forall x\phi(x,\vec{y})]$$

Since the partial recursive functions are closed under primitive recursion we can find an index e such that for all $\vec{k}, d, m$

$$\begin{array}{rcl} \varphi_e^{(n+2)}(\vec{k},d,0) & = & (d)_0 \\ \varphi_e^{(n+2)}(\vec{k},d,m+1) & \simeq & \Psi((d)_1, m, \varphi_e^{(n+2)}(\vec{k},d,m)) \end{array}$$

where $\Psi(a,b,c) \simeq \varphi^{(1)}_{\varphi_a^{(1)}(b)}(c)$.
Let f be such that $\varphi_f^{(n+2)}(e,\vec{k},d) = S_1^{n+1}(e,\vec{k},d)$.
Now suppose d realizes $\phi(0,\vec{k}) \wedge \forall m(\phi(m,\vec{k}) \supset \phi(S(m),\vec{k}))$, so $(d)_0$ realizes $\phi(0,\vec{k})$ and $(d)_1$ realizes $\forall m(\phi(m,\vec{k}) \supset \phi(S(m),\vec{k}))$.
One now proves that $\varphi_f^{(n+2)}(e,\vec{k},d)$ realizes $\forall m\phi(m,\vec{k})$.

Hence, $S_1^{n+1}(f, e, \vec{k})$ realizes

$$[\phi(0, \vec{k}) \wedge \forall m(\phi(m, \vec{k}) \supset \phi(S(m), \vec{k})) \supset \forall m \phi(m, \vec{k})]$$

So if $\varphi_{e'}^{(n)}(\vec{k}) = S_1^{n+1}(f, e, \vec{k})$ then e' realizes

$$\forall \vec{k}\, [\cdots]$$

The rest of the proof consists in verifying realizability for the other axioms of HA (this is easy) and the axioms and rules of intuitionistic predicate logic.
For this, a "Hilbert-type" proof system (instead of a sequent calculus) is most convenient. We omit this, but leave as
Exercise Verify realizability for the rule

$$\frac{B \supset A(x)}{B \supset \forall x A(x)}$$

with x not free in B. That is: suppose $B, A(x)$ are $\mathcal{L}_{\mathrm{HA}}$-formulas. Show that there is a partial recursive function F, such that for every a with the property that for every k, $\varphi_a(k)$ is defined and realizes $B \supset A(x)[k]$, $F(a)$ is defined and realizes $B \supset \forall x A(x)$.

A variation of realizability: $\vdash$-realizability

e $\vdash$-realizes $\phi[\vec{k}]$ iff $\mathbb{N} \models \phi[\vec{k}]$, for ϕ atomic

e $\vdash$-realizes $(\phi \wedge \psi)[\vec{k}]$ iff $(e)_0$ $\vdash$-realizes $\phi[\vec{k}]$ and $(e)_1$ $\vdash$-realizes $\psi[\vec{k}]$

e $\vdash$-realizes $\phi \vee \psi[\vec{k}]$ iff either $(e)_0 = 0$ and $(e)_1$ $\vdash$-realizes $\phi[\vec{k}]$, or $(e)_0 \neq 0$ and $(e)_1$ $\vdash$-realizes $\psi[\vec{k}]$

e $\vdash$-realizes $\phi \supset \psi[\vec{k}]$ if $\mathrm{HA} \vdash \phi(\vec{k}) \supset \psi(\vec{k})$ and for every a such that a $\vdash$-realizes $\phi[\vec{k}]$, $\varphi_e(a)$ is defined and realizes $\psi[\vec{k}]$

e $\vdash$-realizes $(\exists x \phi)[\vec{k}]$ iff $(e)_1$ $\vdash$-realizes $\phi[(e)_0, \vec{k}]$

e $\vdash$-realizes $(\forall x \phi)[\vec{k}]$ iff $\mathrm{HA} \vdash \forall x \phi(x, \vec{k})$ and for every m, $\varphi_e(m)$ is defined and $\vdash$-realizes $\phi[m, \vec{k}]$

Again we have:

$$\text{If HA} \vdash \phi \text{ then for some } e,\ e \vdash\text{-realizes } \phi$$

But also:

$$\text{If } e \vdash\text{-realizes } \phi[\vec{k}] \text{ then HA} \vdash \phi(\vec{k})$$

We obtain the following *derived rules for HA*:
1. If $\mathrm{HA} \vdash A \vee B$ then $\mathrm{HA} \vdash A$ or $\mathrm{HA} \vdash B$
(Disjunction Property for HA)
2. If $\mathrm{HA} \vdash \exists x A(x)$ then for some number m, $\mathrm{HA} \vdash A(m)$
(Existence Property of HA)
3. If $\mathrm{HA} \vdash \forall x \exists y A(x, y)$ then for some number e,

$$\mathrm{HA} \vdash \forall x \exists y (T^1(e, x, y) = 0 \wedge A(x, U(y)))$$

(assuming function symbols for T and U conservatively added to HA, with axioms about their behaviour)
which states: "every total relation contains the graph of a total recursive function". This is called *Church's Rule* for HA.
Exercise Show that there is no Church's Rule for PA.