An introduction to Kleene realizability

Alexandre Miquel

UNIVERSIDAD DE LA REPUBLICA URUGUAY

FACULTAD DE INGENIERIA

EQUIPO DE LÓGICA UDELAR

April 7th, 14th, 21th, IMERL

A disjunction without alternative

Theorem

At least one of the two numbers $e + \pi$ and $e\pi$ is transcendental

Proof

Reductio ad absurdum: Suppose $S = e + \pi$ and $P = e\pi$ are algebraic.
Then e, π are solutions of the polynomial with algebraic coefficients

$$X^2 - SX + P = 0$$

Hence e and π are algebraic. Contradiction.

- Proof does not say which of $e + \pi$ and/or $e\pi$ is transcendental
  (The problem of the transcendence of $e + \pi$ and $e\pi$ is still open.)
- Non constructivity comes from the use of reductio ad absurdum

An existence without a witness

Theorem

There are two irrational numbers a and b such that a^b is rational.

Proof

Either $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ or $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, by excluded middle. We reason by cases:

- If $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, take $a = b = \sqrt{2} \notin \mathbb{Q}$.
- If $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, take $a = \sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ and $b = \sqrt{2} \notin \mathbb{Q}$, since:

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^{(\sqrt{2}\times\sqrt{2})} = (\sqrt{2})^2 = 2 \in \mathbb{Q}$$

- Proof does not say which of $(\sqrt{2}, \sqrt{2})$ or $\left(\sqrt{2}^{\sqrt{2}}, \sqrt{2}\right)$ is solution
- Non constructivity comes from the use of excluded middle
- But there are constructive proofs, e.g.: $a = \sqrt{2}$ and $b = 2\log_2 3$

The first non constructive proof

- Historically, excluded middle and reductio ad absurdum are known since antiquity (Aristotle). But they were never used in an essential way until the end of the 19th century. Example:

Theorem

There exist transcendental numbers

Constructive proof, by Liouville 1844

The number $a = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0.110001000000\cdots$ is transcendental.

Non constructive proof, by Cantor 1874

Since $\mathbb{Z}[X]$ is denumerable, the set $\mathbb{A}$ of algebraic numbers is denumerable. But $\mathbb{R} \sim \mathfrak{P}(\mathbb{N})$ is not. Hence $\mathbb{R} \setminus \mathbb{A}$ is not empty and even uncountable.

Plan

Plan

Brouwer's intuitionism

Luitzen Egbertus Jan **Brouwer** (1881–1966)

1908: *The untrustworthiness of the principles of logic*

- Rejection of non constructive principles such as:
    - The law of excluded-middle ($A \vee \neg A$)
    - Reductio ad absurdum (deduce A from the absurdity of $\neg A$)
    - The Axiom of Choice, actually: only its strongest forms (Zorn)
- Principles of intuitionism:
    - Philosophy of the creative subject
    - Each mathematical objet is a construction of the mind.
      Proofs themselves are constructions (methods, rules...)
    - Rejection of Hilbert's formalism (no formal rules!)

Brouwer also made fundamental contributions to classical topology (fixed point theorem, invariance of the domain)... only to be accepted in the academia

Intuitionistic Logic (LJ)

Although Brouwer was deeply opposed to formalism, the rules of Intuitionistic Logic (LJ) were formalised by his student Arend **Heyting** (1898–1990)

1930: *The formal rules of intuitionistic logic*

1956: *Intuitionism. An introduction*

Intuitively:

- Constructions $A \wedge B$ and $\forall x\, A(x)$ keep their usual meaning, but constructions $A \vee B$ and $\exists x\, A(x)$ get a stronger meaning:
  - A proof of $A \vee B$ should implicitly decide which of A or B holds
  - A proof of $\exists x\, A(x)$ should implicitly construct x
- Implication $A \Rightarrow B$ has now a procedural meaning (cf later) and negation $\neg A$ (defined as $A \Rightarrow \bot$) is no more involutive

Technically: LJ $\subset$ LK (LK = classical logic)

Intuitionistic logic: what we keep / what we lose

- We keep the implications...

$$\begin{array}{rcll} A & \Rightarrow & \neg\neg A & \text{(Double negation)} \\ (A \Rightarrow B) & \Rightarrow & (\neg B \Rightarrow \neg A) & \text{(Contraposition)} \\ (\neg A \vee B) & \Rightarrow & (A \Rightarrow B) & \text{(Material implication)} \\ \neg A & \Leftrightarrow & \neg\neg\neg A & \text{(Triple negation)} \end{array}$$

  but converse implications are lost (but the last)

- De Morgan laws:

$$\begin{array}{rclcrcl} \neg(A \vee B) & \Leftrightarrow & \neg A \wedge \neg B & \qquad & \neg(A \wedge B) & \Leftarrow & \neg A \vee \neg B \\ \neg(\exists x\ A(x)) & \Leftrightarrow & \forall x\ \neg A(x) & \qquad & \neg(\forall x\ A(x)) & \Leftarrow & \exists x\ \neg A(x) \end{array}$$

- **Beware!** Do not confound the two rules:

$$\frac{A \vdash \bot}{\vdash \neg A} \quad \left(\begin{array}{l}\text{introduction rule of} \\ \text{negation, accepted,} \\ \text{cf proof of } \sqrt{2} \notin \mathbb{Q}\end{array}\right) \quad \text{and} \quad \frac{\neg A \vdash \bot}{\vdash A} \quad \left(\begin{array}{c}\text{Reductio ad} \\ \text{absurdum,} \\ \text{rejected}\end{array}\right)$$

Intuitionistic mathematics: what we keep / what we lose

In Algebra:

- We keep all basic algebra, but lose parts of spectral theory
- The theory of orders is almost entirely kept
- The same for combinatorics

In Topology:

- General topology needs to be entirely reformulated:
  topology without points, formal spaces

In Analysis:

- $\mathbb{R}$ still exists, but it is no more unique! (Depends on construction)
- Functions on compact sets do not reach their maximum
- We can reformulate Borel/Lebesgue measure & integral, using the suitable construction of $\mathbb{R}$ [Coquand'02]

A note on decidability

- Intuitionist mathematicians have nothing against statements of the form $A \lor \neg A$. They just need to be proved... constructively
  - LJ $\vdash$ $(\forall x, y \in \mathbb{N})(x = y \lor x \neq y)$ (equality is decidable on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$)
  - LJ $\nvdash$ $(\forall x, y \in \mathbb{R})(x = y \lor x \neq y)$ (equality is undecidable on $\mathbb{R}$, $\mathbb{C}$)
- More generally, the formula $(\forall \vec{x} \in S)\,(A(\vec{x}) \lor \neg A(\vec{x}))$

  is intended to mean: "Predicate/relation A is decidable on S"
- This intuitionistic notion of 'decidability' can be formally related to the mathematical (C.S.) notion of decidability using realizability
- **Variant:** Trichotomy
  - LJ $\vdash$ $(\forall x, y \in \mathbb{N})(x < y \lor x = y \lor x > y)$
  - LJ $\nvdash$ $(\forall x, y \in \mathbb{R})(x < y \lor x = y \lor x > y)$, but:
  - LJ $\vdash$ $(\forall x, y \in \mathbb{R})(x \neq y \Rightarrow x < y \lor x > y)$

The jungle of intuitionistic theories

- At the lowest levels of mathematics, intuitionism is well-defined:
  - LJ: Intuitionistic (predicate) logic
  - HA: Heyting Arithmetic (= intuitionistic arithmetic)
  - + some well-known extensions of HA (e.g. Markov principle)
- But as we go higher, definition is less clear. Two trends:
- **Predicative theories:** (Swedish school)
  - Bishop's constructive analysis
  - Martin-Löf type theories (MLTT)
  - Aczel's constructive set theory (CZF)
- **Impredicative theories:** (French school)
  - Girard's system F
  - Coquand-Huet's calculus of constructions
  - The Coq proof assistant
  - Intuitionistic Zermelo Fraenkel (IZF_R, IZF_C) [Myhill-Friedman 1973]

Brouwer's contribution to classical mathematics

Brouwer also made fundamental contributions to classical topology, especially in the theory of topological manifolds:

Theorem (Fixed point Theorem)

Any continuous function $f : B_n \to B_n$ has a fixed point $\quad (B_n = \text{unit ball of } \mathbb{R}^n)$

Theorem (Invariance of the domain)

Let $U \subseteq \mathbb{R}^n$ be an open set, and $f : U \to \mathbb{R}^n$ continuous.
Then $f(U)$ is open, and the function f is open.

Corollary (Topological invariance of dimension)

Let $U \subseteq \mathbb{R}^n$ and $V \subseteq \mathbb{R}^m$ be nonempty open sets.
If U and V are homeomorphic, then $n = m$.

... but these results use classical reasoning in an essential way,
and were never regarded as valid by Brouwer

What does it mean to be constructive for a theory? (1/2)

- There is no fixed criterion for a theory $\mathscr{T}$ to be constructive, but a mix of syntactical, semantical and philosophical criteria
- But it should fulfill at least the following 4 criteria:

(1) $\mathscr{T}$ should be recursive. Which means that the sets of axioms, derivations and theorems of $\mathscr{T}$ are all recursively enumerable

Note: This is already the case for standard classical theories: PA, ZF, ZFC, etc.

(2) $\mathscr{T}$ should be consistent: $\mathscr{T} \nvdash \bot$

(3) $\mathscr{T}$ should satisfy the disjunction property:

$$\text{If} \quad \mathscr{T} \vdash A \vee B, \quad \text{then} \quad \mathscr{T} \vdash A \quad \text{or} \quad \mathscr{T} \vdash B$$

(where A, B are closed)

(4) $\mathscr{T}$ should satisfy the numeric existence property:

$$\text{If} \quad \mathscr{T} \vdash (\exists x \in \mathbb{N})\, A(x), \quad \text{then} \quad \mathscr{T} \vdash A(n) \quad \text{for some } n \in \mathbb{N}$$

(where $A(x)$ only depends on x)

What does it mean to be constructive for a theory? (2/2)

- In most cases, we also require that:

  (5) $\mathscr{T}$ should satisfy the existence property (or witness property):

$$\text{If}\quad \mathscr{T} \vdash \exists x\, A(x),\quad \text{then}\quad \mathscr{T} \vdash A(t)\quad \text{for some closed term } t$$

(where $A(x)$ only depends on x)

Note: Needs to be adapted when the language of $\mathscr{T}$ has no closed term (e.g. set theory)

Theorem (Non constructivity of classical theories)

If a classical theory is recursive, consistent and contains Q, then it fulfills none of the disjunction and numeric existence properties

Note: Q = Robinson Arithmetic ($\subset$ PA), that is: the finitely axiomatized fragment of Peano Arithmetic (PA) with the only function symbols 0, s, $+$, $\times$, and where the induction scheme is replaced by the (much weaker) axiom $\forall x\,(x = 0 \lor \exists y\,(x = s(y)))$

Proof. From the hypotheses, Gödel's 1st incompleteness theorem applies, so we can pick a closed formula G such that $\mathscr{T} \nvdash G$ and $\mathscr{T} \nvdash \neg G$. We conclude noticing that:

$$\mathscr{T} \vdash G \lor \neg G \qquad \text{and} \qquad \mathscr{T} \vdash (\exists x \in \mathbb{N})\,((x = 1 \land G) \lor (x = 0 \land \neg G))$$

Why using LJ does not ensure constructivity (1/2)

- Constructivity is a semantical (and philosophical) criterion, that cannot be simply ensured by the use of intuitionistic logic (LJ)
- Indeed, some awkward axiomatizations in LJ may imply the excluded middle, and thus lead to non constructive theories. Some examples:
- **In intuitionistic arithmetic (HA):**
  - The axiom of well-ordering

$$(\forall S \subseteq \mathbb{N})\,[\exists x\,(x \in S) \ \Rightarrow\ (\exists x \in S)(\forall y \in S)\, x \leq y]$$

    implies the excluded middle; it is not constructive. In HA, induction (which is constructive) does not imply well-ordering

Why using LJ does not ensure constructivity (2/3)

- **In constructive analysis:** [Bishop 1967]
  - The axiom of trichotomy

    $$(\forall x, y \in \mathbb{R})\,(x < y \lor x = y \lor x > y)$$

    is not constructive. It has to be replaced by the axiom

    $$(\forall x, y \in \mathbb{R})\,(x \neq y \Rightarrow x < y \lor x > y)$$

    which is classically equivalent
  - The axiom of completeness

    > Each inhabited subset of $\mathbb{R}$ that has an upper bound in $\mathbb{R}$ has a least upper bound in $\mathbb{R}$

    implies excluded middle. It has to be restricted to the inhabited subsets $S \subseteq \mathbb{R}$ that are order located above, i.e., such that:

    For all $a < b$, either $(\forall x \in S)\,(x \leq b)$ or $(\exists x \in S)\,(x \geq a)$

Why using LJ does not ensure constructivity (3/3)

- **In Intuitionistic Set Theory:**
  - The classical formulation of the Axiom of Regularity

    $$\forall x\,(x \neq \varnothing \Rightarrow (\exists y \in x)(y \cap x \neq 0))$$

    implies excluded middle. It has to be replaced by the axiom scheme

    $$\forall x\,((\forall y \in x)\,A(y) \;\Rightarrow\; A(x)) \;\Rightarrow\; \forall x\,A(x)$$

    known as set induction, that is classically equivalent
  - The Axiom of Choice implies excluded middle [Diaconescu 1975]
- In all cases, the constructivity of a given intuitionistic theory $\mathscr{T}$ is justified by realizability techniques (for criteria (2)–(5))

Plan

The language of Arithmetic

First-order terms and formulas

FO-terms	e, e_1	$::=$	$x \mid f(e_1,\ldots,e_k)$ (f of arity k)
Formulas	A, B	$::=$	$e_1 = e_2 \mid \top \mid \bot \mid A \Rightarrow B$ $\mid A \land B \mid A \lor B \mid \forall x\, A \mid \exists x\, A$

- We assume given one k-ary function symbol f for each primitive recursive function of arity k: 0, s, $+$, $-$, $\times$, $\uparrow$, etc.
- Only one (binary) predicate symbol: $=$ (equality)
- Macros: $\neg A \ :=\ A \Rightarrow \bot, \quad A \Leftrightarrow B \ :=\ (A \Rightarrow B) \land (B \Rightarrow A)$
- **Syntactic worship:** Free & bound variables. Work up to α-conversion. Set of free variables: $FV(e)$, $FV(A)$. Substitution: $e\{x := e_0\}$, $A\{x := e_0\}$.

Choice of a deduction system

- There are many equivalent ways to present the deduction rules of intuitionistic (or classical) predicate logic:
  1. In the style of Hilbert (only formulas, no sequents)
  2. In the style of Gentzen (left & right rules)
  3. In the style of Natural Deduction (with or without sequents)

  Since these systems define the very same class of provable formulas[1] (for a given logic, LJ or LK), choice is just a matter of convenience

- Systems only based on formulas (Hilbert's, N.D. without sequents) are easier to define, but much more difficult to manipulate

- In what follows, we shall systematically use sequents

[1] In sequent-based systems, formulas are identified with sequents of the form $\vdash A$, that is: with sequents with 0 hypothesis (lhs) and 1 thesis (rhs)

Sequents

Definition (Sequent) [Gentzen 1934]

A sequent is a pair of finite lists of formulas written

$$A_1, \ldots, A_n \vdash B_1, \ldots, B_m \qquad (n, m \geq 0)$$

- $A_1, \ldots, A_n$ are the hypotheses (which form the subsequent)
- $B_1, \ldots, B_m$ are the theses (which form the consequent)
- $\vdash$ is the entailment symbol (that reads: 'entails')

Note: Some authors use finite multisets (of formulas) rather than finite lists, since the order is irrelevant, both in the subsequent and in the consequent

- Sequents are usually written $\Gamma \vdash \Delta$ (Γ, Δ finite lists of formulas)
- Intuitive meaning: $\bigwedge \Gamma \Rightarrow \bigvee \Delta$
- Empty sequent " $\vdash$ " represents contradiction
- **Syntactic worship:** Notations $FV(\Gamma)$, $\Gamma\{x := t\}$ extended to finite lists Γ

Rules of inference & systems of deduction

Formulas and sequents can be used as judgments. Each system of deduction is based on a set of judgments $\mathscr{J}$ (= a set of expressions asserting something)

- Given a set of judgments $\mathscr{J}$:

Definition (Rule of inference)

A rule of inference is a pair formed by a finite set of judgments $\{J_1, \ldots, J_n\} \subseteq \mathscr{J}$ and a judgment $J \in \mathscr{J}$, usually written

$$\frac{J_1 \quad \cdots \quad J_n}{J}$$

- $J_1, \ldots, J_n$ are the premises of the rule
- J is the conclusion of the rule

Definition (System of deduction)

A system of deduction is a set of inference rules

Derivable judgments (1/2)

Definition (Derivation)

Let $\mathscr{S}$ be a system of deduction based on some set of judgments $\mathscr{J}$.

1. Derivations (of judgments) in $\mathscr{S}$ are inductively defined as follows:

   If $d_1, \ldots, d_n$ are derivations of $J_1, \ldots, J_n$ in $\mathscr{S}$, respectively, and if $(\{J_1, \ldots, J_n\}, J)$ is a rule of $\mathscr{S}$, then

   $$d \;=\; \left\{ \frac{\begin{array}{c} \vdots\; d_1 \\ J_1 \end{array} \quad \cdots \quad \begin{array}{c} \vdots\; d_n \\ J_n \end{array}}{J} \right. \qquad \text{is a derivation of } J \text{ in } \mathscr{S}$$

2. A judgment J is derivable in $\mathscr{S}$ when there is a derivation of J in $\mathscr{S}$

- By definition, the set of derivable judgments of $\mathscr{S}$ is the smallest set of judgments that is closed under the rules in $\mathscr{S}$
- One also uses proof/provable for derivation/derivable

Derivable judgments (2/2)

- Two systems of deduction (based on the same set of judgments) are equivalent when the induce the same set of derivable judgments

Definition (Admissible rule)

A rule $R = (\{J_1, \ldots, J_n\}, J)$ is admissible in a system of deduction $\mathscr{S}$ when: $J_1, \ldots, J_n$ derivable in $\mathscr{S}$ implies J derivable in $\mathscr{S}$.

Admissible rules are usually written

$$\frac{J_1 \quad \cdots \quad J_n}{J}$$

- Clearly: R admissible in $\mathscr{S}$ iff $\mathscr{S} \cup \{R\}$ equivalent to $\mathscr{S}$

- **Remark:** In practice, deduction systems are defined as finite sets of schemes of rules (that is: families of rules), that are still called rules. The notion of admissible rule immediately extends to schemes

A remark on implication

In logic, we have (at least) three symbols to represent implication:

- The implication symbol $\Rightarrow$, used in formulas. Represents a potential point for deduction, but not an actual deduction step
- The entailment symbol $\vdash$, used in sequents. Same thing as $\Rightarrow$, but in a sequent, that represents a formula under decomposition:

$$\begin{array}{rc} & A_1, \ldots, A_n \vdash B_1, \ldots, B_m \\ \approx & A_1 \wedge \cdots \wedge A_n \Rightarrow B_1 \vee \cdots \vee B_m \end{array}$$

  (So that $\vdash$ is a distinguished implication, closer to a point of deduction)

- The inference rule "$\overline{\qquad\qquad}$", used in rules & derivations. This symbol represents an actual deduction step:

$$\frac{P_1 \quad \cdots \quad P_n}{C} \qquad \left(\begin{array}{l}\text{From } P_1, \ldots, P_n \\ \text{deduce } C\end{array}\right)$$

On the meaning of sequents

- Sequents are not intended to enrich the expressiveness of a logical system; they are only intended to represent a state in a proof, or a formula under decomposition:

$$\Gamma \vdash \Delta \qquad \approx \qquad \bigwedge \Gamma \Rightarrow \bigvee \Delta$$

(With the conventions $\bigwedge \varnothing := \top$ and $\bigvee \varnothing := \bot$)

- **Formally:** In most (if not all[2]) systems in the literature, we have:

$$\Gamma \vdash \Delta \ \text{ derivable} \qquad \text{iff} \qquad \vdash \left(\bigwedge \Gamma \Rightarrow \bigvee \Delta\right) \ \text{ derivable}$$

This equivalence holds, at least:

  - In Gentzen's sequent calculus (LK)
  - In intuitionistic sequent calculus (LJ)
  - In intuitionistic/classical natural deduction (NJ/NK)
  - In Linear Logic (LL), replacing $\wedge$, $\vee$, $\top$, $\bot$, $\Rightarrow$ by $\otimes$, $⅋$, 1, $\bot$, $\multimap$

- **Exercise:** Check it for both systems NJ/NK presented hereafter

[2] The author knows no exception to this rule

Intuitionistic Natural Deduction (NJ)

- Intuitionistic Natural Deduction (NJ) is a deduction system based on asymmetric sequents of the form:

$$A_1, \ldots, A_n \vdash A \qquad \text{or:} \qquad \Gamma \vdash A$$

  These sequents are also called intuitionistic sequents

- Recall that: $\Gamma \vdash A$ has the same meaning as $\bigwedge \Gamma \Rightarrow A$

- System NJ has three kinds of (schemes of) rules:
  - Introduction rules, defining how to prove each connective/quantifier
  - Elimination rules, defining how to use each connective/quantifier
  - The Axiom rule, which is a conservation rule

- The Trimūrti of logic:

Introduction rules	=	Brahma
Elimination rules	=	Shiva
Axiom rule	=	Vishnu

Deduction rules of NJ (1/2)

- Rules for the intuitionistic propositional calculus:

$$
\begin{array}{lcc}
\text{(Axiom)} & \multicolumn{2}{c}{\dfrac{}{\Gamma \vdash A}\ {\scriptstyle A \in \Gamma}} \\[2ex]
(\Rightarrow) & \dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} & \dfrac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B} \\[2ex]
(\wedge) & \dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} & \dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \\[2ex]
(\vee) & \dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B} & \dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \\[2ex]
(\top) & \dfrac{}{\Gamma \vdash \top} & \text{(no elimination rule)} \\[2ex]
(\bot) & \text{(no introduction rule)} & \dfrac{\Gamma \vdash \bot}{\Gamma \vdash A}
\end{array}
$$

Deduction rules of NJ (2/2)

- Introduction & elimination rules for quantifiers:

$$(\forall)\qquad \frac{\Gamma\vdash A}{\Gamma\vdash\forall x\,A}\ {\scriptstyle x\notin FV(\Gamma)}\qquad\qquad \frac{\Gamma\vdash\forall x\,A}{\Gamma\vdash A\{x:=e\}}$$

$$(\exists)\qquad \frac{\Gamma\vdash A\{x:=e\}}{\Gamma\vdash\exists x\,A}\qquad\qquad \frac{\Gamma\vdash\exists x\,A\qquad \Gamma,A\vdash B}{\Gamma\vdash B}\ {\scriptstyle x\notin FV(\Gamma,B)}$$

- Introduction & elimination rules for equality:

$$(=)\qquad \frac{}{\Gamma\vdash e=e}\qquad\qquad \frac{\Gamma\vdash e_1=e_2\qquad \Gamma\vdash A\{x:=e_1\}}{\Gamma\vdash A\{x:=e_2\}}$$

- To get Classical Natural Deduction (NK), just replace

$$\frac{\Gamma\vdash\bot}{\Gamma\vdash A}\ \text{(ex falso quod libet)}\qquad \text{by}\qquad \frac{\Gamma,\neg A\vdash\bot}{\Gamma\vdash A}\ \text{(reductio ad absurdum)}$$

Basic properties of NJ/NK

- Admissible rules (both in NJ/NK):

$$\frac{\Gamma \vdash A}{\Gamma' \vdash A}\ \Gamma\subseteq\Gamma' \ \text{(Monotonicity)} \qquad \frac{\Gamma \vdash A}{\Gamma\{x := e\} \vdash A\{x := e\}}\ \text{(Substitutivity)}$$

where $\Gamma \subseteq \Gamma'$ means: for all A, $A \in \Gamma$ implies $A \in \Gamma'$

- From Monotonicity, we deduce (both in NJ/NK):

$$\frac{\Gamma \vdash A}{\sigma\Gamma \vdash A}\ \text{(Permutation)} \qquad \frac{\Gamma \vdash A}{\Gamma, B \vdash A}\ \text{(Weakening)} \qquad \frac{\Gamma, B, B \vdash A}{\Gamma, B \vdash A}\ \text{(Contraction)}$$

- We write $\Gamma \vdash_{\mathrm{NJ}} A$ for: '$\Gamma \vdash A$ is derivable in NJ' (the same for NK)

Proposition (Inclusion NJ $\subseteq$ NK)

If $\Gamma \vdash_{\mathrm{NJ}} A$, then $\Gamma \vdash_{\mathrm{NK}} A$

The axioms of first-order arithmetic

The axioms of first-order arithmetic are the following closed formulas:

- Defining equations of all primitive recursive function symbols:

$$\forall x\,(x+0=x) \qquad \forall x\,(x\times 0=0)$$
$$\forall x\,\forall y\,(x+s(y)=s(x+y)) \qquad \forall x\,\forall y\,(x\times s(y)=x\times y+x)$$
$$\forall x\,(\mathrm{pred}(0)=0) \qquad \forall x\,(x-0=0)$$
$$\forall x\,(\mathrm{pred}(s(x))=x) \qquad \forall x\,\forall y\,(x-s(y))=\mathrm{pred}(x-y)$$

etc.

- Peano axioms:

(P3) $\forall x\,\forall y\,(s(x)=s(y)\Rightarrow x=y)$

(P4) $\forall x\,\neg(s(x)=0)$

(P5) $\forall\vec{z}\,[A(\vec{z},0)\wedge\forall x\,(A(\vec{z},x)\Rightarrow A(\vec{z},s(x)))\Rightarrow\forall x\,A(\vec{z},x)]$

for all formulas $A(\vec{z},x)$ whose free variables occur among $\vec{z},x$

This set of axioms is written Ax(HA) or Ax(PA)

Heyting Arithmetic (HA)

Definition (Heyting Arithmetic)

Heyting Arithmetic (HA) is the theory based on first-order intuitionistic logic (NJ) and whose set of axioms is Ax(HA). Formally:

$$\mathrm{HA} \vdash A \quad \equiv \quad \Gamma \vdash_{\mathrm{NJ}} A \quad \text{for some } \Gamma \subseteq \mathrm{Ax(HA)}$$

- Replacing NJ by NK, we get Peano Arithmetic (same axioms)
- When building proofs, it is convenient to integrate the axioms of HA in the system of deduction, by replacing the Axiom rule

$$\frac{}{\Gamma \vdash A}\ {\scriptstyle A \in \Gamma} \qquad \text{by} \qquad \frac{}{\Gamma \vdash A}\ {\scriptstyle A \in \Gamma \cup \mathrm{Ax(HA)}}$$

  The extended deduction system is then written HA

- **Question:** Is HA constructive?

Basic properties

- Given a function symbol f and a closed FO-terms e, we write:
  - $f^{\mathbb{N}}$ $(: \mathbb{N}^k \to \mathbb{N})$ the primitive recursive function associated to f
  - $e^{\mathbb{N}}$ $(\in \mathbb{N})$ the denotation of e in $\mathbb{N}$ (standard model)
- Since the system of axioms of HA provides the defining equations of all primitive recursive functions, we have:

Proposition (Computational completeness)

If $\mathbb{N} \models e_1 = e_2$, then $\mathrm{HA} \vdash e_1 = e_2$

Note: Converse implication amounts to the property of consistency

Corollary (Completeness for Σ^0_1-formulas)

If $\mathbb{N} \models \exists\vec{x}\,(e_1(\vec{x}) = e_2(\vec{x}))$, then $\mathrm{HA} \vdash \exists\vec{x}\,(e_1(\vec{x}) = e_2(\vec{x}))$

Note: Converse implication is the property of 1-consistency

- Gödel's 1st incompleteness theorem says that HA is not Π^0_1-complete

Plan

Background

- 1908. Brouwer: *The untrustworthiness of the principles of logic*
  (Principles of intuitionism)
- 1936. Church: *An unsolvable problem of elementary number theory*
  (Application of the λ-calculus to the *Entscheidungsproblem*)
- 1936. Turing: *On computable numbers, with an application to the Entscheidungsproblem*
  (Alternative solution to the *Entscheidungsproblem*, using Turing machines)
- 1936. Kleene: *λ-definability and recursiveness*
  (Definition of partial recursive functions)
- 1945. Kleene: *On the interpretation of intuitionistic number theory*
  (Introduction of realizability, as a semantics for HA)

Kleene realizability

1945. Kleene: *On the interpretation of intuitionistic number theory*

- Realizability in Heyting Arithmetic (HA)
- Definition of the realizability relation $n \Vdash A$
  - n = Gödel code of a partial recursive function
  - A = closed formula of HA
- **Theorem:** Every provable formula of HA is realized
  (But some unprovable formulas are realized too...)
- Application to the disjunction & existence properties

Remarks:

- Codes for partial recursive functions can be replaced by the elements of any partial combinatory algebra
- Here, we shall take closed terms of PCF (partially computable functions)

The language of realizers

Terms of PCF (= λ-calculus + primitive pairs & integers)

$$\begin{array}{llllllll} \textbf{Terms} & t, u & ::= & x & \mid & \lambda x\,.\,t & \mid & tu \\ & & \mid & \mathtt{pair} & \mid & \mathtt{fst} & \mid & \mathtt{snd} \\ & & \mid & 0 & \mid & \mathtt{S} & \mid & \mathtt{rec} \end{array}$$

Syntactic worship: Free & bound variables. Renaming. Work up to α-conversion. Set of free variables: $FV(t)$. Capture-avoiding substitution: $t\{x := u\}$

- **Notations:** $\langle t_1, t_2 \rangle \;:=\; \mathtt{pair}\; t_1\; t_2, \qquad \bar{n} \;:=\; \mathtt{S}^n\, 0 \quad (n \in \mathbb{N})$

Reduction rules

$$(\lambda x\,.\,t)\, u \;\succ\; t\{x := u\}$$

$$\begin{array}{lll} \mathtt{fst}\; \langle t_1, t_2 \rangle & \succ & t_1 \\ \mathtt{snd}\; \langle t_1, t_2 \rangle & \succ & t_2 \end{array} \qquad \begin{array}{rll} \mathtt{rec}\; t_0\; t_1\; 0 & \succ & t_0 \\ \mathtt{rec}\; t_0\; t_1\; (\mathtt{S}\, u) & \succ & t_1\; u\; (\mathtt{rec}\; t_0\; t_1\; u) \end{array}$$

- Grand reduction written $t \succ^* u$ (reflexive, transitive, context-closed)

Definition of the relation $t \Vdash A$

- **Recall:** For each closed FO-term e, we write $e^{\mathbb{N}}$ its denotation in $\mathbb{N}$

Definition of the realizability relation $t \Vdash A$ (t, A closed)

$$
\begin{array}{lcl}
t \Vdash e_1 = e_2 & \equiv & e_1^{\mathbb{N}} = e_2^{\mathbb{N}} \ \wedge \ t \succ^* 0 \\
t \Vdash \bot & \equiv & \bot \\
t \Vdash \top & \equiv & t \succ^* 0 \\
t \Vdash A \Rightarrow B & \equiv & \forall u \ (u \Vdash A \ \Rightarrow \ tu \Vdash B) \\
t \Vdash A \wedge B & \equiv & \exists t_1 \ \exists t_2 \ (t \succ^* \langle t_1, t_2 \rangle \ \wedge \ t_1 \Vdash A \ \wedge \ t_2 \Vdash B) \\
t \Vdash A \vee B & \equiv & \exists u \ ((t \succ^* \langle \bar{0}, u \rangle \ \wedge \ u \Vdash A) \ \vee \ (t \succ^* \langle \bar{1}, u \rangle \ \wedge \ u \Vdash B)) \\
t \Vdash \forall x \, A(x) & \equiv & \forall n \ (t \, \bar{n} \Vdash A(n)) \\
t \Vdash \exists x \, A(x) & \equiv & \exists n \ \exists u \ (t \succ^* \langle \bar{n}, u \rangle \ \wedge \ u \Vdash A(n))
\end{array}
$$

Lemma (closure under anti-evaluation)

If $t \succ^* t'$ and $t' \Vdash A$, then $t \Vdash A$

We now want to prove the

Theorem (Soundness)

If $\quad \mathrm{HA} \vdash A, \quad$ then $\quad t \Vdash A \quad$ for some closed PCF-term t

Outline of the proof:

- **Step 1:** Translating FO-terms into PCF-terms
- **Step 2:** Translating derivations of LJ into PCF-terms
- **Step 3:** Adequacy lemma
- **Step 4:** Realizing the axioms of HA
- **Final step:** Putting it all together

Step 1: Translating FO-terms into PCF-terms

Proposition (Compiling primitive recursive functions in PCF)

Each function symbol f is computed by a closed PCF-term f^*:

$$\text{If} \quad f^{\mathbb{N}}(n_1, \dots, n_k) = m, \quad \text{then} \quad f^*\ \bar{n}_1 \cdots \bar{n}_k\ \succ^*\ \bar{m}$$

Proof. Standard exercise of compilation. Examples:

$$\begin{array}{rcl} 0^* & := & 0 \\ s^* & := & \mathtt{S} \\ \mathrm{pred}^* & := & \lambda x\,.\,\mathtt{rec}\ 0\ (\lambda z, \_\,.\,z)\ x \end{array} \qquad \begin{array}{rcl} (+)^* & := & \lambda x, y\,.\,\mathtt{rec}\ x\ (\lambda\_, z\,.\,\mathtt{S}\,z)\ y \\ (\times)^* & := & \lambda x, y\,.\,\mathtt{rec}\ 0\ (\lambda\_, z\,.\,(+)^*\ z\ x)\ y \\ (-)^* & := & \lambda x, y\,.\,\mathtt{rec}\ x\ (\lambda\_, z\,.\,\mathrm{pred}^*\ z)\ y \end{array}$$

- Each FO-term e with free variables $x_1, \dots, x_k$ is translated into a closed PCF-term e^* with the same free variables, letting:

$$x^* \ :=\ x \qquad \text{and} \qquad \big(f(e_1, \dots, e_k)\big)^* \ :=\ f^*\ e_1^* \cdots e_k^*$$

Fact: If e is closed, then $e^*\ \succ^*\ \bar{n}$, where $n = e^{\mathbb{N}}$

Step 2: Translating derivations into PCF-terms (1/3)

- Every derivation $d : (A_1, \ldots, A_n \vdash B)$ is translated into a PCF-term d^* with free variables $x_1, \ldots, x_k, z_1, \ldots, z_n$, where:
  - $x_1, \ldots, x_k$ are the free variables of $A_1, \ldots, A_n, B$
  - $z_1, \ldots, z_n$ are proof variables associated to $A_1, \ldots, A_n$
- The construction of d^* follows the Curry-Howard correspondence:

$$\left(\frac{}{A_1, \ldots, A_n \vdash A_i}\right)^* := z_i \qquad \left(\frac{}{\Gamma \vdash \top}\right)^* := 0 \qquad \left(\frac{\begin{array}{c}\vdots\ d\\ \Gamma \vdash \bot\end{array}}{\Gamma \vdash A}\right)^* := \mathsf{any\_term}$$

$$\left(\frac{\begin{array}{c}\vdots\ d\\ \Gamma, A \vdash B\end{array}}{\Gamma \vdash A \Rightarrow B}\right)^* := \lambda z\,.\,d^* \qquad \left(\frac{\begin{array}{c}\vdots\ d_1\\ \Gamma \vdash A \Rightarrow B\end{array} \quad \begin{array}{c}\vdots\ d_2\\ \Gamma \vdash A\end{array}}{\Gamma \vdash B}\right)^* := d_1^* d_2^*$$

Step 2: Translating derivations into PCF-terms (2/3)

$$\left(\dfrac{\begin{array}{cc}\vdots\, d_1 & \vdots\, d_2\\ \Gamma\vdash A & \Gamma\vdash B\end{array}}{\Gamma\vdash A\wedge B}\right)^{*} := \langle d_1^*, d_2^*\rangle$$

$$\left(\dfrac{\begin{array}{c}\vdots\, d\\ \Gamma\vdash A\wedge B\end{array}}{\Gamma\vdash A}\right)^{*} := \mathtt{fst}\ d^* \qquad \left(\dfrac{\begin{array}{c}\vdots\, d\\ \Gamma\vdash A\wedge B\end{array}}{\Gamma\vdash B}\right)^{*} := \mathtt{snd}\ d^*$$

$$\left(\dfrac{\begin{array}{c}\vdots\, d\\ \Gamma\vdash A\end{array}}{\Gamma\vdash A\vee B}\right)^{*} := \langle \bar{0}, d^*\rangle \qquad \left(\dfrac{\begin{array}{c}\vdots\, d\\ \Gamma\vdash B\end{array}}{\Gamma\vdash A\vee B}\right)^{*} := \langle \bar{1}, d^*\rangle$$

$$\left(\dfrac{\begin{array}{ccc}\vdots\, d & \vdots\, d_0 & \vdots\, d_1\\ \Gamma\vdash A\vee B & \Gamma, A\vdash C & \Gamma, B\vdash C\end{array}}{\Gamma\vdash C}\right)^{*} := \mathsf{match}\ d^*\ (\lambda z\,.\,d_0^*)\ (\lambda z\,.\,d_1^*)$$

writing $\quad \mathsf{match} \;:=\; \lambda x, x_0, x_1\,.\,\mathtt{rec}\ (x_0\,(\mathtt{snd}\,x))\ (\lambda\_,\_\,.\,x_1\,(\mathtt{snd}\,x))\ (\mathtt{fst}\,x)$

Step 2: Translating derivations into PCF-terms (3/3)

$$\left(\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma\vdash A\end{array}}{\Gamma\vdash\forall x\,A}\right)^* := \lambda x\,.\,d^* \qquad \left(\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma\vdash\forall x\,A\end{array}}{\Gamma\vdash A\{x:=e\}}\right)^* := d^*e^*$$

$$\left(\dfrac{\begin{array}{c}\vdots\ d\\ \Gamma\vdash A\{x:=e\}\end{array}}{\Gamma\vdash\exists x\,A}\right)^* := \langle e^*,d^*\rangle \qquad \left(\dfrac{\begin{array}{cc}\vdots\ d_1 & \vdots\ d_2\\ \Gamma\vdash\exists x\,A & \Gamma,A\vdash B\end{array}}{\Gamma\vdash B}\right)^* := \text{let }\langle x,z\rangle=d_1^*\text{ in }d_2^*$$

$$\left(\overline{\Gamma\vdash e=e}\right)^* := 0 \qquad \left(\dfrac{\begin{array}{cc}\vdots\ d_1 & \vdots\ d_2\\ \Gamma\vdash e_1=e_2 & \Gamma\vdash A\{x=e_1\}\end{array}}{\Gamma\vdash A\{x:=e_2\}}\right)^* := d_2^*$$

writing $\quad \text{let }\langle x,z\rangle=t\text{ in }u \;:=\; (\lambda y\,.\,(\lambda x,z\,.\,u)\,(\mathtt{fst}\;y)\,(\mathtt{snd}\;y))\;t$

Step 3: Adequacy lemma

Recall that in the definition of d^*, we assumed that each first-order variable x is also a PCF-variable. (Remaining PCF-variables z are used as proof variables.)

Definition (Valuation)

A valuation is a function ρ : FOVar $\to \mathbb{N}$. A valuation ρ may be applied:

- to a formula A; notation: $A[\rho]$ (result is a closed formula)
- to a PCF-term t; notation: $t[\rho]$ (result is a possibly open PCF-term)

Lemma (Adequacy)

Let $d : (A_1, \ldots, A_n \vdash B)$ be a derivation in NJ. Then:

- for all valuations ρ,
- for all realizers $t_1 \Vdash A_1[\rho], \ldots, t_n \Vdash A_n[\rho]$,

we have: $$d^*[\rho]\{z_1 := t_1, \ldots, z_n := t_n\} \Vdash B[\rho]$$

Proof: By induction on d, using that $\{t : t \Vdash B\}$ is closed under anti-evaluation

Step 4: Realizing the axioms of HA

Lemma (Realizing true Π^0_1-formulas)

Let $e_1(\vec{x})$, $e_2(\vec{x})$ be FO-terms depending on free variables $\vec{x}$.
If $\quad \mathbb{N} \models \forall \vec{x}\,(e_1(\vec{x}) = e_2(\vec{x}))$, then $\quad \lambda \vec{x}\,.\,\bar{0} \Vdash \forall \vec{x}\,(e_1(\vec{x}) = e_2(\vec{x}))$

- Since all defining equations of function symbols are Π^0_1:

Corollary

All defining equations of function symbols are realized

Lemma (Realizing Peano axioms)

$$\begin{array}{rcl} \lambda xyz\,.\,z & \Vdash & \forall x\,\forall y\,(s(x) = s(y) \Rightarrow x = y) \\ \text{any\_term} & \Vdash & \forall x\,(s(x) \neq 0) \\ \lambda \vec{z}\,.\,\mathtt{rec} & \Vdash & \forall \vec{z}\,[A(\vec{z},0) \Rightarrow \forall x\,(A(\vec{z},x) \Rightarrow A(\vec{z},s(x))) \Rightarrow \forall x\,A(\vec{z},x)] \end{array}$$

Final step: Putting it all together

Theorem (Soundness)

If $\quad \mathrm{HA} \vdash A, \quad$ then $\quad t \Vdash A \quad$ for some closed PCF-term t

Proof. Assume $\mathrm{HA} \vdash A$, so that there are axioms $A_1, \ldots, A_n$ and a derivation $d : (A_1, \ldots, A_n \vdash A)$ in LJ. Take realizers $t_1, \ldots, t_n$ of $A_1, \ldots, A_n$. By adequacy, we have $d^*\{z_1 := t_1, \ldots, z_n := t_n\} \Vdash A$.

Corollary (Consistency)

HA is consistent: $\quad \mathrm{HA} \nvdash \bot$

Proof. If $\mathrm{HA} \vdash \bot$, then the formula $\bot$ is realized, which is impossible by definition

- **Remark.** Since $\mathrm{HA} \subseteq \mathrm{PA}$ and PA is consistent (from the existence of the standard model), we already knew that HA is consistent

Σ_1^0-soundness and completeness

Proposition (Σ_1^0-soundness/completeness)

For every closed Σ_1^0-formula, the following are equivalent:

(1) $\mathrm{HA} \vdash \exists\vec{x}\,(e_1(\vec{x}) = e_2(\vec{x}))$ (formula is provable)

(2) $t \Vdash \exists\vec{x}\,(e_1(\vec{x}) = e_2(\vec{x}))$ for some t (formula is realized)

(3) $\mathbb{N} \models \exists\vec{x}\,(e_1(\vec{x}) = e_2(\vec{x}))$ (formula is true)

Proof. (1) $\Rightarrow$ (2) by soundness
(2) $\Rightarrow$ (3) by definition of $t \Vdash \exists\vec{x}\,(e_1(\vec{x}) = e_2(\vec{x}))$
(3) $\Rightarrow$ (1) by Σ_1^0-completeness

Corollary (Existence property for Σ_1^0-formulas)

If $\mathrm{HA} \vdash \exists\vec{x}\,(e_1(\vec{x}) = e_2(\vec{x}))$, then $\mathrm{HA} \vdash e_1(\vec{n}) = e_2(\vec{n})$ for some $\vec{n} \in \mathbb{N}$

Proof. Use (1) $\Rightarrow$ (3), and conclude by computational completeness

The halting problem

- Let h be the binary function symbol associated to the primitive recursive function $h^{\mathbb{N}} : \mathbb{N}^2 \to \mathbb{N}$ defined by

$$h^{\mathbb{N}}(n,k) \;=\; \begin{cases} 1 & \text{if Turing machine } n \text{ stops after } k \text{ evaluation steps} \\ 0 & \text{otherwise} \end{cases}$$

- Write $\quad H(x) \;:=\; \exists y\,(H(x,y)=1)$ (halting predicate)

Proposition

The formula $\quad \forall x\,(H(x) \vee \neg H(x)) \quad$ is not realized

Proof. Let $t \Vdash \forall x\,(H(x) \vee \neg H(x))$, and put $u := \lambda x\,.\,\mathtt{fst}\,(t\,x)$. We check that:

- For all $n \in \mathbb{N}$, either $\quad u\,\bar{n} \succ^* \bar{0} \quad$ or $\quad u\,\bar{n} \succ^* \bar{1}$
- If $\quad u\,\bar{n} \succ^* \bar{0}, \quad$ then $H(n)$ is realized, so that Turing machine n halts
- If $\quad u\,\bar{n} \succ^* \bar{1}, \quad$ then $H(n)$ is not realized so that Turing machine n loops

Therefore, the program u solves the halting problem, which is impossible

EM is not derivable in HA

- By soundness we get: $\quad \mathrm{HA} \nvdash \forall x\,(H(x) \vee \neg H(x)).\quad$ Hence:

Theorem (Unprovability of EM)

The law of excluded middle (EM) is not provable in HA

- **Remark:** We actually proved that the open instance $\quad H(x) \vee \neg H(x)$ of EM is not provable in HA. On the other hand we can prove (classically) that each closed instance of EM is realizable:

Proposition (Realizing closed instances of EM)

For each closed formula A, the formula $\quad A \vee \neg A \quad$ is realized

Proof. Using meta-theoretic EM (in the model), we distinguish two cases:

- Either A is realized by some term t. $\quad$ Then $\langle \bar{0}, t\rangle \Vdash A \vee \neg A$
- Either A is not realized. $\quad$ Then $t \Vdash \neg A$ (t any), hence $\langle \bar{1}, t\rangle \Vdash A \vee \neg A$

- But this proof is not accepted by intuitionists $\qquad$ (uses meta-theoretic EM)

Unprovable, but realizable (1/3)

- We have already seen that the Halting Problem

(HP) $$\forall x\,(H(x) \vee \neg H(x))$$

is not realized. Therefore:

Proposition

any_term $\Vdash \neg$HP, but: HA $\nvdash \neg$HP (since: PA $\nvdash \neg$HP)

Proof. Since HP is not realized, its negation is realized by any term. On the other hand we have PA $\nvdash \neg$HP (since PA $\vdash$ HP), so that HA $\nvdash \neg$HP

- **Morality:**
  - PA takes position for the excluded middle
  - HA actually takes no position (for or against) the excluded middle. In practice, it is 100% compatible with classical logic
  - Kleene realizability takes position against excluded middle. Many realized formulas (such as $\neg$HP) are classically false

Unprovable, but realizable (2/3)

- Recall that all true Π^0_1-formulas are realized:

If $\mathbb{N} \models \forall\vec{x}\,(e_1(\vec{x}) = e_2(\vec{x}))$, then $\lambda\vec{x}\,.\,\bar{0} \Vdash \forall\vec{x}\,(e_1(\vec{x}) = e_2(\vec{x}))$

- But Gödel undecidable formula G is a true Π^0_1-formula. Therefore:

Proposition

$\lambda z\,.\,\bar{0} \Vdash G$, but: $\text{HA} \nvdash G$ (since: $\text{PA} \nvdash G$)

Remarks:

- Like $\neg$HP, the formula G is realized but not provable
- Unlike $\neg$HP, the formula G is classically true

Unprovable, but realizable (3/3)

- Markov Principle (MP) is the following scheme of axioms:

$$\forall x\,(A(x) \vee \neg A(x)) \Rightarrow \neg\neg\exists x\,A(x) \Rightarrow \exists x\,A(x)$$

- Obviously: $\mathsf{PA} \vdash \mathsf{MP}$

Proposition (MP is realized)

$$t_{\mathsf{MP}} \Vdash \forall x\,(A(x) \vee \neg A(x)) \Rightarrow \neg\neg\exists x\,A(x) \Rightarrow \exists x\,A(x)$$

where

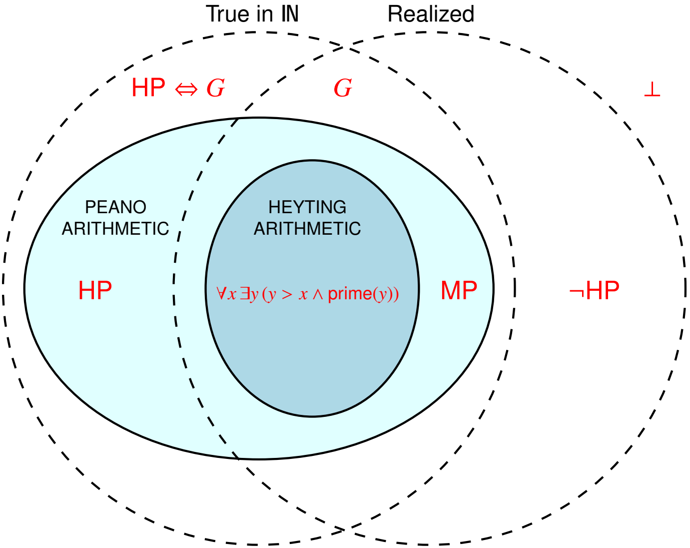
$$\begin{array}{rcl} t_{\mathsf{MP}} & := & \lambda z\_\,.\,\mathbf{Y}\,(\lambda rx\,.\,\text{if } \mathtt{fst}\,(z\,x) = 0 \text{ then } \langle x, \mathtt{snd}\,(z\,x)\rangle \text{ else } r\,(\mathtt{S}\,x)) \\ \mathbf{Y} & := & \lambda f\,.\,(\lambda x\,.\,f\,(x\,x))\,(\lambda x\,.\,f\,(x\,x)) \end{array}$$

- Using modified realizability, one can show: $\mathsf{HA} \nvdash \mathsf{MP}$ [Kreisel]

- We have the strict inclusions:

$$\mathsf{HA} \subset \mathsf{HA} + \mathsf{MP} \subset \mathsf{PA}$$

To sum up


True in $\mathbb{N}$
Realized
HP $\Leftrightarrow G$
G
$\perp$
PEANO ARITHMETIC
HEYTING ARITHMETIC
HP
$\forall x\, \exists y\, (y > x \wedge \mathrm{prime}(y))$
MP
$\neg$HP

Towards the disjunction and existence properties

Proposition (Semantic disjunction & existence properties)

1. If $\mathrm{HA} \vdash A \vee B$, then A is realized or B is realized
2. If $\mathrm{HA} \vdash \exists x\, A(x)$, then $A(n)$ is realized for some $n \in \mathbb{N}$

Proof. From main Theorem & definition of realizability:

1. If $\mathrm{HA} \vdash A \vee B$, then $t \Vdash A \vee B$ for some t, so that:
   either $t \succ^* \langle \bar{0}, u\rangle$ for some $u \Vdash A$, or $t \succ^* \langle \bar{1}, u\rangle$ for some $u \Vdash B$
2. If $\mathrm{HA} \vdash \exists x\, A(x)$, then $t \Vdash \exists x\, A(x)$ for some t, so that:
   $t \succ^* \langle \bar{n}, u\rangle$ for some $n \in \mathbb{N}$ and $u \Vdash A(n)$

- This weak forms of the disjunction & existence properties are now widely accepted as criteria of constructivity
- To prove the strong form, we need to introduce glued realizability

Glued realizability (1/3)

- Let $\mathcal{P}$ be a set of closed formulas such that:
  - $\mathcal{P}$ contains all theorems of HA
  - $\mathcal{P}$ is closed under modus ponens: $(A \Rightarrow B) \in \mathcal{P},\ A \in \mathcal{P} \ \Rightarrow\ B \in \mathcal{P}$

Definition of the relation $t \Vdash_{\mathcal{P}} A$ (t, A closed)

$$
\begin{array}{lcl}
t \Vdash_{\mathcal{P}} e_1 = e_2 & \equiv & e_1^{\mathbb{N}} = e_2^{\mathbb{N}} \ \wedge\ t \succ^* 0 \\
t \Vdash_{\mathcal{P}} \bot & \equiv & \bot \\
t \Vdash_{\mathcal{P}} \top & \equiv & t \succ^* 0 \\
t \Vdash_{\mathcal{P}} A \Rightarrow B & \equiv & \forall u\,(u \Vdash_{\mathcal{P}} A \ \Rightarrow\ tu \Vdash_{\mathcal{P}} B) \ \wedge\ (A \Rightarrow B) \in \mathcal{P} \\
t \Vdash_{\mathcal{P}} A \wedge B & \equiv & \exists t_1\,\exists t_2\,(t \succ^* \langle t_1, t_2\rangle \ \wedge\ t_1 \Vdash_{\mathcal{P}} A \ \wedge\ t_2 \Vdash_{\mathcal{P}} B) \\
t \Vdash_{\mathcal{P}} A \vee B & \equiv & \exists u\,((t \succ^* \langle \bar{0}, u\rangle \ \wedge\ u \Vdash_{\mathcal{P}} A) \ \vee\ (t \succ^* \langle \bar{1}, u\rangle \ \wedge\ u \Vdash_{\mathcal{P}} B)) \\
t \Vdash_{\mathcal{P}} \forall x\, A(x) & \equiv & \forall n\,(t\,\bar{n} \Vdash_{\mathcal{P}} A(n)) \ \wedge\ (\forall x\, A(x)) \in \mathcal{P} \\
t \Vdash_{\mathcal{P}} \exists x\, A(x) & \equiv & \exists n\,\exists u\,(t \succ^* \langle \bar{n}, u\rangle \ \wedge\ u \Vdash_{\mathcal{P}} A(n))
\end{array}
$$

- Plain realizability $=$ case where $\mathcal{P}$ contains all closed formulas

Glued realizability (2/3)

Theorem [Kleene'45]

1. If $t \Vdash_{\mathcal{P}} A$, then $A \in \mathcal{P}$
2. If $\mathrm{HA} \vdash A$, then $t \Vdash_{\mathcal{P}} A$ for some PCF-term t

Proof.

1. By a straightforward induction on A
2. Same proof as for plain realizability. Extracted program t is the same as before (definitions of $f \mapsto f^*$, $e \mapsto e^*$, $d \mapsto d^*$ unchanged). Only change appears in the statement & proof of Adequacy (step 3), that uses $\Vdash_{\mathcal{P}}$ rather than $\Vdash$.

- **To sum up:** For each set of closed formulas $\mathcal{P}$ that contains all theorems of HA and that is closed under modus ponens:

$$\text{provable in HA} \quad \subseteq \quad \mathcal{P}\text{-realized} \quad \subseteq \quad \mathcal{P}$$

Glued realizability (3/3)

- **Particular case:** $\mathcal{P} = \mathrm{HA}$: (= set of theorems of HA)

Proposition

$\mathrm{HA} \vdash A$ iff $t \Vdash_{\mathrm{HA}} A$ for some closed PCF-term t

- From this we deduce:

Corollary (Disjunction/existence properties)

1. If $\mathrm{HA} \vdash A \lor B$, then $\mathrm{HA} \vdash A$ or $\mathrm{HA} \vdash B$
2. If $\mathrm{HA} \vdash \exists x\, A(x)$, then $\mathrm{HA} \vdash A(n)$ for some $n \in \mathbb{N}$

Proof. Same proof as before, using the fact that $\mathrm{HA} \vdash A$ iff A is HA-realized

Program extraction

Proposition (Provably total functions are recursive)

If $\mathrm{HA} \vdash \forall\vec{x}\,\exists y\, A(\vec{x}, y)$ (i.e. the relation $A(\vec{x}, y)$ is provably total in HA), then there exists a total recursive function $\phi : \mathbb{N}^k \to \mathbb{N}$ such that:

$$\mathrm{HA} \vdash A(\vec{n}, \phi(\vec{n})) \qquad \text{for all } \vec{n} = (n_1, \ldots, n_k) \in \mathbb{N}^k$$

Proof. Let d be a derivation of A in HA, and d^* the corresponding closed PCF-term (constructed in Steps 1, 2, 4). We take $\phi := \lambda\vec{x}\,.\,\mathtt{fst}\,(d^*\,\vec{x})$

- **Note:** The relation $A(\vec{x}, y)$ may not be functional. In this case, the extracted program $\phi := \lambda\vec{x}\,.\,\mathtt{fst}\,(d^*\,\vec{x})$ associated to the derivation d chooses one output $\phi(\vec{n})$ for each input $\vec{n} \in \mathbb{N}^k$
- **Optimizing extracted program ϕ:** Using modified realizability [Kreisel], we can ignore all sub-proofs corresponding to Harrop formulas:

Harrop formulas

$$H \quad ::= \quad e_1 = e_2 \quad | \quad \top \quad | \quad \bot \quad | \quad H_1 \wedge H_2 \quad | \quad A \Rightarrow H \quad | \quad \forall x\, H$$

Plan

Kleene's original presentation (1/2)

- Kleene did not consider closed PCF-terms as realizers, but natural numbers, used as Gödel codes for partial recursive functions
- Definition of realizability parameterized by:
  - A recursive injection $\langle\cdot,\cdot\rangle : \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ (pairing)
  - An enumeration $(\phi_n)_{n\in\mathbb{N}}$ of all partial recursive functions of arity 1
- Kleene application: $n\cdot p \;:=\; \phi_n(p)$ (partial operation)
- **Realizability relation:** $n \Vdash A$ ($n\in\mathbb{N}$, A closed formula)

Theorem

If $\mathrm{HA}\vdash A$, then $n\Vdash A$ for some $n\in\mathbb{N}$

- As before, we can also realize many unprovable formulas, such as the negation of the Halting Problem ($\neg$HP), Gödel undecidable formula G and Markov Principle (MP), as well as Church's Thesis (CT) (cf later)

Kleene's original presentation (2/2)

Definition of the realizability relation $n \Vdash A$ $\quad (n \in \mathbb{N},\ A \text{ closed})$

$$
\begin{array}{lcl}
n \Vdash e_1 = e_2 & \equiv & e_1^{\mathbb{N}} = e_2^{\mathbb{N}} \ \wedge\ n = 0 \\
n \Vdash \bot & \equiv & \bot \\
n \Vdash \top & \equiv & n = 0 \\
n \Vdash A \Rightarrow B & \equiv & \forall p\ (p \Vdash A \ \Rightarrow\ n \cdot p \Vdash B) \\
n \Vdash A \wedge B & \equiv & \exists n_1\ \exists n_2\ (n = \langle n_1, n_2 \rangle \ \wedge\ n_1 \Vdash A \ \wedge\ n_2 \Vdash B) \\
n \Vdash A \vee B & \equiv & \exists m\ ((n = \langle 0, m \rangle \ \wedge\ m \Vdash A) \ \vee\ (n = \langle 1, m \rangle \ \wedge\ m \Vdash B)) \\
n \Vdash \forall x\, A(x) & \equiv & \forall p\ (n \cdot p \Vdash A(p)) \\
n \Vdash \exists x\, A(x) & \equiv & \exists p\ \exists m\ (n = \langle p, m \rangle \ \wedge\ m \Vdash A(p))
\end{array}
$$

- Proof of Main Theorem is essentially the same as before. But:
  - We need to work with Hilbert's system for LJ (rather than with NJ)
  - Gödel codes induce a lot of code obfuscation...
- As before, we can define glued realizability, prove the disjunction & existence properties, extract program from proofs, etc.

Church's Thesis (CT)

- Let h' be the ternary function symbol associated to the primitive recursive function $h'^{\mathbb{N}} : \mathbb{N}^3 \to \mathbb{N}$ defined by

$$h'^{\mathbb{N}}(n,p,k) \;=\; \begin{cases} s(r) & \text{if Turing machine } n \text{ applied to } p \text{ stops after} \\ & k \text{ evaluation steps and returns } r \\ 0 & \text{otherwise} \end{cases}$$

and put: $\qquad x \cdot y = z \quad := \quad \exists k\,(h'(x,y,k) = s(z))$

- Church's Thesis (CT) internalizes in the language of HA the fact that every provably total function is recursive:

$$\text{(CT)} \qquad \forall x\, \exists y\, A(x,y) \;\Rightarrow\; \exists n\, \forall x\, \exists y\, (n \cdot x = y \wedge A(x,y))$$

- Clearly: $\quad \mathrm{PA} \vdash \neg\mathrm{CT}$ $\qquad$ (take $A(x,y) \;:=\; (H(x) \wedge y = 1) \vee (\neg H(x) \wedge y = 0)$)

Proposition

CT is realized by some $n \in \mathbb{N}$ $\quad$ (although $\quad \mathrm{HA} \nvdash \mathrm{CT}$)

Towards partial combinatory algebras

Idea: To define a language of realizers, we need a set $\mathcal{A}$ whose elements behave as partial functions on $\mathcal{A}$, and that is 'closed under λ-abstraction'

Definition (Partial applicative structure – PAS)

A partial applicative structure (PAS) is a set $\mathcal{A}$ equipped with a partial function $(\cdot) : \mathcal{A} \times \mathcal{A} \rightharpoonup \mathcal{A}$, called application

Notation: $abc = (a \cdot b) \cdot c$, etc. (application is left-associative)

- **Intuition:** Each element a of a partial applicative structure $\mathcal{A}$ represents a partial function on $\mathcal{A}$: $(b \mapsto ab) : \mathcal{A} \rightharpoonup \mathcal{A}$
- A PAS is combinatorialy complete when it contains enough elements to represent all closed λ-terms (Formal definition given later)

Definition (Partial combinatory algebra – PCA)

A partial combinatory algebra (PCA) is a combinatorially complete PAS

Combinatorial completeness (1/3)

Let $\mathcal{A}$ be a partial applicative structure

Definition ($\mathcal{A}$-expressions)

Combinatory terms over $\mathcal{A}$ (or $\mathcal{A}$-expressions) are defined by:

$$\mathcal{A}\textbf{-expressions} \qquad t, u \quad ::= \quad x \quad | \quad a \quad | \quad tu \qquad (a \in \mathcal{A})$$

Syntactic worship: Free variables $FV(t)$, substitution $t\{x := u\}$

- **Remark:** Set of $\mathcal{A}$-expr. $=$ free magma generated by $A \uplus \mathrm{Var}$
- We define a (partial) interpretation function $t \mapsto t^{\mathcal{A}}$ from the set of closed $\mathcal{A}$-expressions to $\mathcal{A}$, using the inductive definition:

$$a^{\mathcal{A}} = a \qquad\qquad (tu)^{\mathcal{A}} = t^{\mathcal{A}} \cdot u^{\mathcal{A}}$$

- Notations:

$t\downarrow$	when	$t^{\mathcal{A}}$ is defined
$t\uparrow$	when	$t^{\mathcal{A}}$ is undefined
$t \cong u$	when	either $t, u\uparrow$ or $t, u\downarrow$ and $t^{\mathcal{A}} = u^{\mathcal{A}}$

Combinatorial completeness (2/3)

Definition (Combinatorial completeness)

A partial applicative structure $\mathcal{A}$ is combinatorially complete when for each $\mathcal{A}$-term $t(x_1, \ldots, x_n)$ with free variables among $x_1, \ldots, x_n$ $(n \geq 1)$, there exists $a \in \mathcal{A}$ such that for all $a_1, \ldots, a_n \in \mathcal{A}$:

1. $a a_1 \cdots a_{n-1} \downarrow$
2. $a a_1 \cdots a_n \cong t(a_1, \ldots, a_n)$

Notation: $a \; = \; (x_1, \ldots, x_n \mapsto t(x_1, \ldots, x_n))^{\mathcal{A}}$ (not unique, in general)

Theorem (Combinatorial completeness)

A partial applicative structure $\mathcal{A}$ is combinatorially complete iff there are two elements $\mathbf{K}, \mathbf{S} \in \mathcal{A}$ s.t. for all $a, b, c \in \mathcal{A}$:

1. $\mathbf{K}ab\downarrow$ and $\mathbf{K}ab = a$
2. $\mathbf{S}ab\downarrow$ and $\mathbf{S}abc \cong ac(bc)$

Combinatorial completeness (3/3)

- **Condition is necessary:** by combinatorial completeness, take

$$\mathbf{K} \;=\; (x, y \mapsto x)^{\mathcal{A}} \quad \text{and} \quad \mathbf{S} \;=\; (x, y, z \mapsto xz(yz))^{\mathcal{A}}$$

- To prove that condition is sufficient, use combinators $\mathbf{K}, \mathbf{S} \in \mathcal{A}$ to define λ-abstraction on the set of $\mathcal{A}$-expressions:

Definition of $\lambda x\,.\,t$:

$$\begin{array}{lcl@{\qquad}lcll} \lambda x\,.\,x & := & \mathbf{SKK} & \lambda x\,.\,y & := & \mathbf{K}\,y & \text{if } y \not\equiv x \\ \lambda x\,.\,a & := & \mathbf{K}\,a & \lambda x\,.\,tu & := & \mathbf{S}\,(\lambda x\,.\,t)\,(\lambda x\,.\,u) & \end{array}$$

By construction we have $FV(\lambda x\,.\,t) = FV(t) \setminus \{x\}$, and for each $\mathcal{A}$-expression $t(x)$ that depends (at most) on x:

$$\lambda x\,.\,t(x)\downarrow \qquad \text{and} \qquad (\lambda x\,.\,t(x))\,a \;\cong\; t(a) \quad \text{for all } a \in \mathcal{A}$$

- **Condition is sufficient:** if $\mathbf{K}, \mathbf{S} \in \mathcal{A}$ exist, put

$$(x_1, \ldots, x_n \mapsto t(x_1, \ldots, x_n))^{\mathcal{A}} \;:=\; (\lambda x_1 \cdots x_n\,.\,t(x_1, \ldots, x_n))^{\mathcal{A}}$$

Examples of partial combinatory algebras

Definition (Partial combinatory algebra – PCA)

A partial combinatory algebra (PCA) is a combinatorially complete PAS

- Examples of total combinatory algebras:
  - The set of closed λ-terms quotiented by β-conversion
  - The set of closed PCF-terms quotiented by β-conversion
  - The free magma generated by constants $\mathbf{K}, \mathbf{S}$ and quotiented by the relations $\mathbf{K}\,a\,b = a$, $\mathbf{S}\,a\,b\,c = ac(bc)$ (Combinatory Logic)
- Examples of (really) partial combinatory algebras:
  - The set of closed λ-terms in normal form, equipped with the partial application defined by: $t \cdot u = \mathrm{NF}(tu)$
  - $\mathbb{N}$ equipped with Kleene application: $n \cdot p = \phi_n(p)$

Using partial combinatory algebras

- Using combinatory completeness, we can encode all constructs of PCF in any partial combinatory algebra $\mathcal{A}$, for example:

  - $\mathtt{pair} \;:=\; (\lambda xyz\,.\,zxy)^{\mathcal{A}}$
  - $\mathtt{fst} \;:=\; (\lambda z\,.\,z\,(\lambda xy\,.\,x))^{\mathcal{A}}$
  - $\mathtt{snd} \;:=\; (\lambda z\,.\,z\,(\lambda xy\,.\,y))^{\mathcal{A}}$
  - $\mathtt{0} \;:=\; (\lambda xf\,.\,x)^{\mathcal{A}}\ (= \mathbf{K})$
  - $\mathtt{succ} \;:=\; (\lambda nxf\,.\,f\,n)^{\mathcal{A}}$ [Parigot]
  - $\mathbf{Y} \;:=\; (\lambda f\,.\,(\lambda x\,.\,f\,(x\,x))\,(\lambda x\,.\,f\,(x\,x)))^{\mathcal{A}}$ [Church]
  - $\mathtt{rec} \;:=\; (\lambda x_0 x_1\,.\,\mathbf{Y}\,(\lambda rn\,.\,n\,x_0\,(\lambda z\,.\,x_1\,z\,(r\,z))))^{\mathcal{A}}$

- Using these constructions, we can define the relation or realizability $a \Vdash A$, where $a \in \mathcal{A}$ and A is a closed formula (exercise)

- Main Theorem holds in all PCA $\mathcal{A}$ (exercise), and depending on the choice of $\mathcal{A}$, we can realize more or less formulas

Where do the combinators $\mathbf{K}, \mathbf{S}$ come from?

- Through the CH correspondence, the types of combinators $\mathbf{K} = \lambda xy\,.\,x$ and $\mathbf{S} = \lambda xyz\,.\,xz(yz)$ correspond to the axioms of Hilbert deduction for minimal propositional logic:

$$\begin{array}{lcl@{\quad:\quad}l} \mathbf{K} & = & \lambda xy\,.\,x & A \Rightarrow B \Rightarrow A \\ \mathbf{S} & = & \lambda xyz\,.\,xz(yz) & (A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C \end{array}$$

Hilbert deduction for LJ

- **Rules:**

$$\frac{\vdash A \Rightarrow B \quad \vdash A}{\vdash B} \qquad \frac{\vdash A \Rightarrow B}{\vdash A \Rightarrow \forall x\, B}\ {\scriptstyle x \notin FV(A)} \qquad \frac{\vdash A \Rightarrow B}{\vdash \exists x\, A \Rightarrow B}\ {\scriptstyle x \notin FV(B)}$$

- **Axioms:**

$$A \Rightarrow B \Rightarrow A \qquad (A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C$$

$$A \Rightarrow B \Rightarrow A \land B \qquad A \land B \Rightarrow A \qquad A \land B \Rightarrow B \qquad \top \qquad \bot \Rightarrow A$$

$$A \Rightarrow A \lor B \qquad B \Rightarrow A \lor B \qquad (A \Rightarrow C) \Rightarrow (B \Rightarrow C) \Rightarrow A \lor B \Rightarrow C$$

$$\forall x\, A \Rightarrow A\{x := e\} \qquad A\{x := e\} \Rightarrow \exists x\, A$$

Extensions and variants

- **Extensions:**
  - To second- & higher-order arithmetic [Troelstra]
  - To intuitionistic & constructive set theories:
    - IZF_R, IZF_C [Myhill-Friedman 1973, McCarty 1984]
    - CZF [Aczel 1977]
- **Variants:**
  - Modified realizability [Kreisel]
  - Techniques of reducibility candidates [Tait, Girard, Parigot]
- **Categorical realizability:**
  - Strong connections with topoi [Scott, Hyland, Johnstone, Pitts]
- **Realizability for classical logic:**
  - Kleene realizability via a negative translation [Kohlenbach]
  - Classical realizability in PA2, in ZF [Krivine 1994, 2001–2013]