Proof Mining

Lecture 3: Proof Interpretations

Paulo Oliva
Queen Mary University of London

Proof Society - Summer School

Swansea, 8-11 September 2019

Plan

Lecture 1: Incomplete Statements

Lecture 2: Proof Translations

Lecture 3: **Proof Interpretations**

Lecture 1 & 2 Recap

Incomplete statements can be strengthened by bounding or witnessing some of the quantifications

Complete

Goldbach conjecture. Every even interger greather than 2 can be expressed as the sum of two primes

Fermat's last theorem. No three positive integers a,b,c satisfy $a^n + b^n = c^n$, for $n > 2$

Incomplete

There are $a,b \in \mathbb{R}$ such that $a,b \notin \mathbb{Q}$ but $a^b \in \mathbb{Q}$

$\sqrt{2}$ is irrational

The set of primes is unbounded

Edelstein f.-point theorem. Any contractive $f : [0,1] \to [0,1]$ has at most one fixed point

Brouwer f.-point theorem. Any continuous $f : [0,1] \to [0,1]$ has a fixed point

$$\boxed{\vdash A \vee \neg A}$$

$$\dfrac{\dfrac{\dfrac{[A]_{\alpha}}{A \vee \neg A} \qquad [\neg(A \vee \neg A)]_{\gamma}}{\dfrac{\bot}{\neg A}\,\alpha}}{\dfrac{\bot}{A \vee \neg A}\,\text{PBC},\gamma}$$

$$\boxed{\vdash \neg\neg(A \vee \neg A)}$$

$$\dfrac{\dfrac{\dfrac{[A]_{\alpha}}{A \vee \neg A} \qquad [\neg(A \vee \neg A)]_{\gamma}}{\dfrac{\bot}{\neg A}\,\alpha}}{\dfrac{\bot}{\neg\neg(A \vee \neg A)}\,\to\text{I},\gamma}$$

Intuitionistic Logic
(ex falso quodlibet)

$$\dfrac{\dfrac{\vdots}{\bot}}{A}\ \text{EFQ}$$

Classical Logic
(proof by contraction)

$$\dfrac{\dfrac{\dfrac{[\neg A]_{\alpha}}{\vdots}}{\bot}}{A}\ \text{PBC},\ \alpha$$

Proposition (Gentzen 1933).

If CL proves $\Gamma \vdash A$ then IL proves $\Gamma^N \vdash A^N$ where

$$\begin{array}{lcllcl}
(A \wedge B)^N & \equiv & A^N \wedge B^N & (P)^* & \equiv & \neg\neg P \\
(A \vee B)^N & \equiv & \neg\neg(A^N \vee B^N) & (\forall x\, A)^N & \equiv & \forall x\, A^N \\
(A \to B)^N & \equiv & A^N \to B^N & (\exists x\, A)^N & \equiv & \neg\neg \exists x A^N
\end{array}$$

Comprehension

$$\exists f^{\mathbb{N}\to\mathbb{B}}\forall n^{\mathbb{N}}(fn \leftrightarrow A(n))$$

Let $T(n,n,u)$ be the statement that Turing machine with code n on input n will halt with computation u

The Halting problem (known to be undecidable) is

$$A(n) \equiv \exists u T(n,n,u)$$

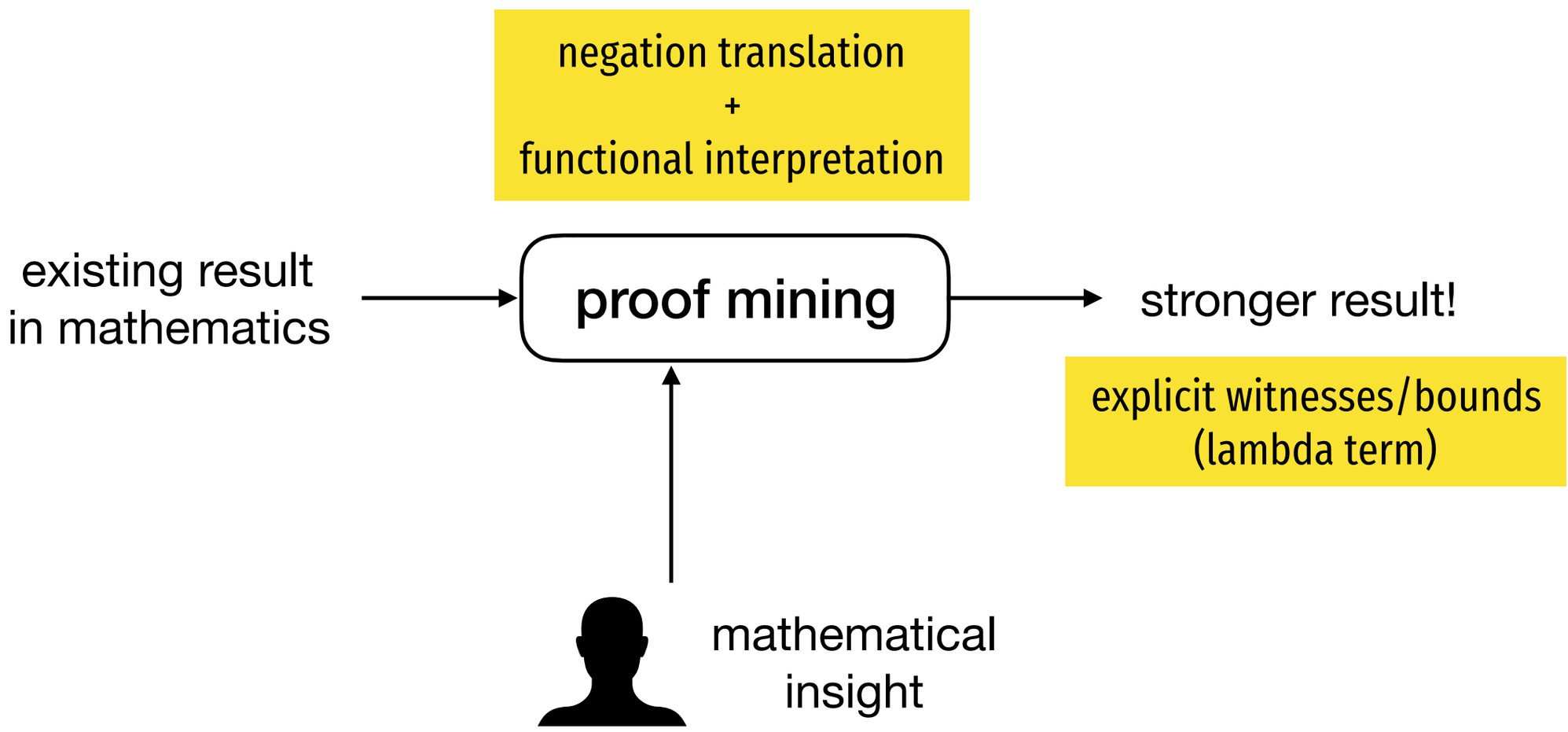
So clearly, the following (true) statement cannot be witnessed by a computable function f

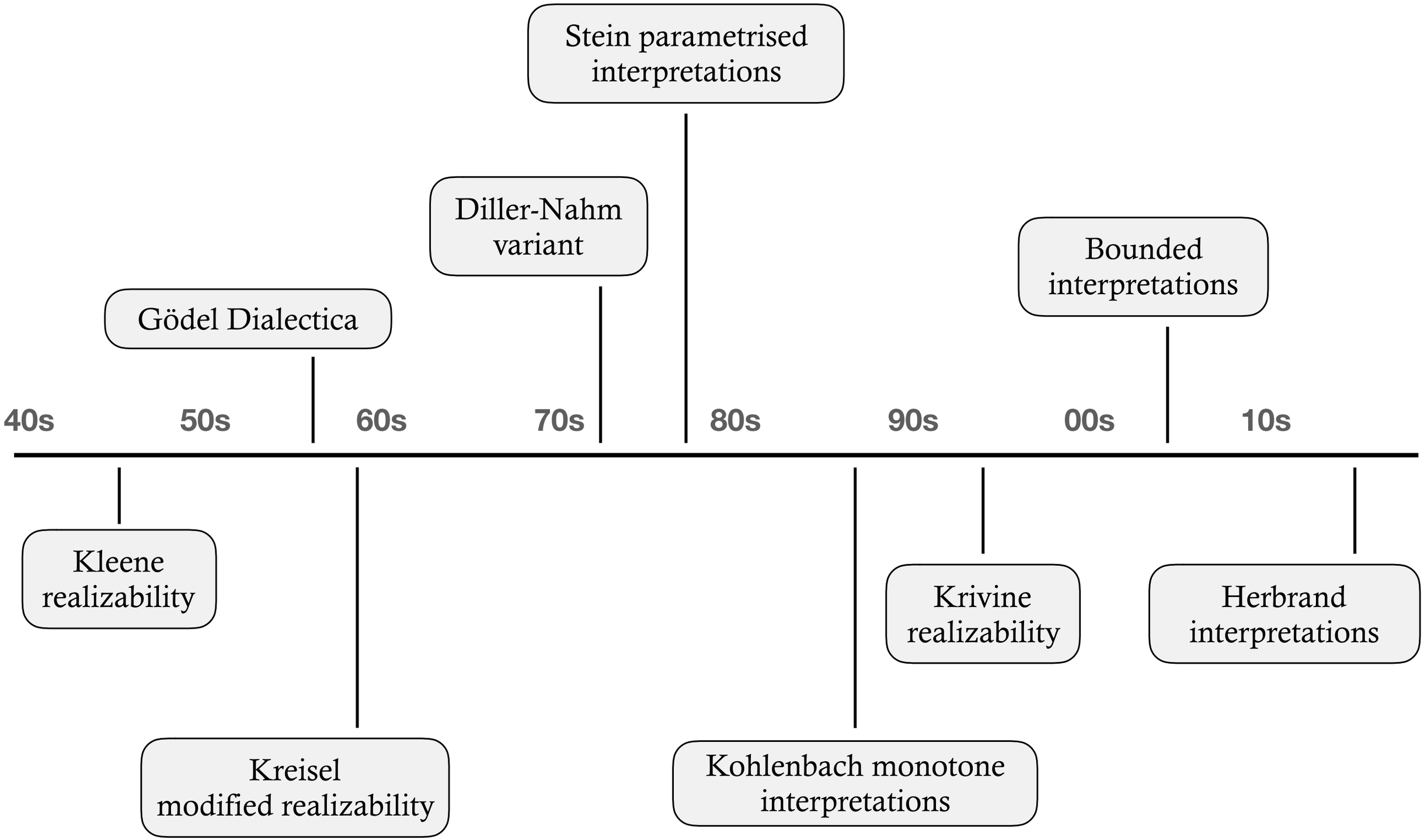
$$\exists f^{\mathbb{N}\to\mathbb{B}}\forall n^{\mathbb{N}}(fn \leftrightarrow \exists u T(n,n,u))$$

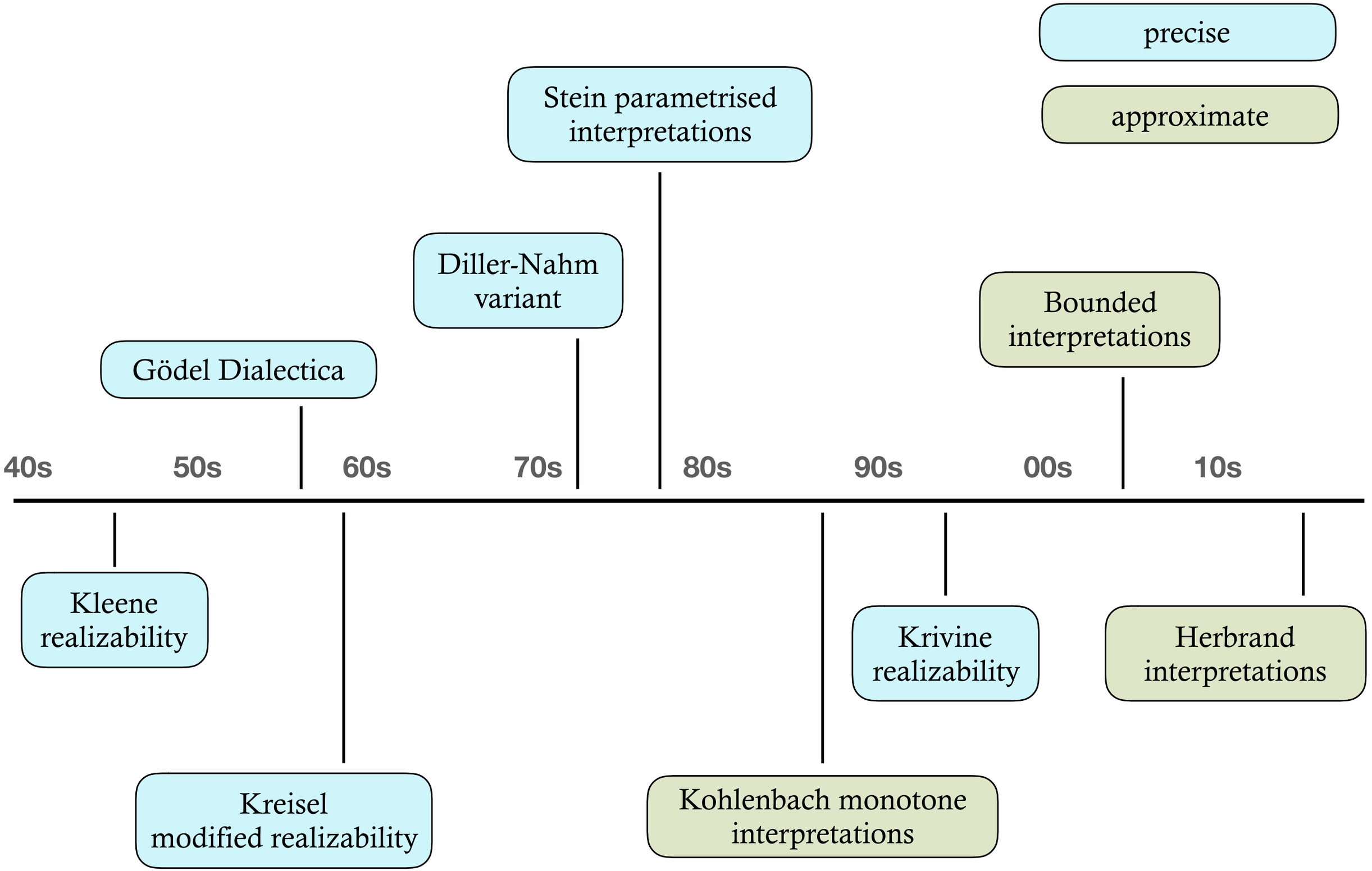
Today

- Functional interpretations
- Lambda calculus, system T
- Interpreting induction
- Interpreting choice and comprehension

Proof Mining




Stein parametrised interpretations
Diller-Nahm variant
Gödel Dialectica
Bounded interpretations
40s
50s
60s
70s
80s
90s
00s
10s
Kleene realizability
Kreisel modified realizability
Kohlenbach monotone interpretations
Krivine realizability
Herbrand interpretations


precise
approximate
Stein parametrised interpretations
Diller-Nahm variant
Gödel Dialectica
Bounded interpretations
40s
50s
60s
70s
80s
90s
00s
10s
Kleene realizability
Kreisel modified realizability
Kohlenbach monotone interpretations
Krivine realizability
Herbrand interpretations

Functional Interpretations

Lemma 1: $\forall p,q>0\left(\neg\text{Even}(p)\vee\neg\text{Even}(q)\to p^2\neq 2q^2\right)$

Lemma 2: $\forall x,y(x^2\neq y^2\to x\neq y)$

Theorem: $\forall p,q>0\left(\neg\text{Even}(p)\vee\neg\text{Even}(q)\to\frac{p}{q}\neq\sqrt{2}\right)$

Lemma 1^*: $\forall p,q>0\left(\neg\text{Even}(p)\vee\neg\text{Even}(q)\to|p^2-2q^2|\geq 1\right)$

Lemma 2^*: $\forall x,y,\delta(|x^2-y^2|\geq\delta\to|x-y|\geq\frac{\delta}{x+y})$

Theorem *: $\forall p,q>0\left(\neg\text{Even}(p)\vee\neg\text{Even}(q)\to|\frac{p}{q}-\sqrt{2}|\geq\frac{1}{pq+2q^2}\right)$

Lemma 1. $\exists x A(x) \to \exists y B(y)$ $\longrightarrow$ $\forall x(A(x) \to B(gx))$

Lemma 2. $\exists y B(y) \to \exists z C(z)$ $\longrightarrow$ $\forall y(B(y) \to C(hy))$

Theorem. $\exists x A(x) \to \exists z C(z)$

$$\dfrac{\dfrac{\exists x A(x) \quad \exists x A(x) \to \exists y B(y)}{\exists y B(y)} \qquad \exists y B(y) \to \exists z C(z)}{\exists z C(z)}$$

$A(x)$ $\longrightarrow$ $C(fx)$

f ?

Lemma 1. $\exists x A(x) \to \exists y B(y) \longrightarrow \forall x(A(x) \to B(gx))$

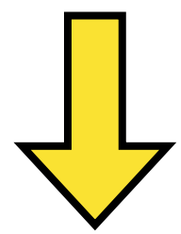
Lemma 2. $\exists y B(y) \to \exists z C(z) \longrightarrow \forall y(B(y) \to C(hy))$

Theorem. $\exists x A(x) \to \exists z C(z) \longrightarrow \forall x(A(x) \to C(h(gx)))$

$$\dfrac{\dfrac{[A(v)]_\alpha \quad \dfrac{\forall x(A(x) \to B(gx))}{A(v) \to B(gv)}}{B(gv)} \quad \dfrac{\forall y(B(y) \to C(hy))}{B(gv) \to C(h(gv))}}{\dfrac{\dfrac{C(h(gv))}{A(v) \to C(h(gv))}\,\alpha}{\forall x(A(x) \to C(h(gx)))}}$$

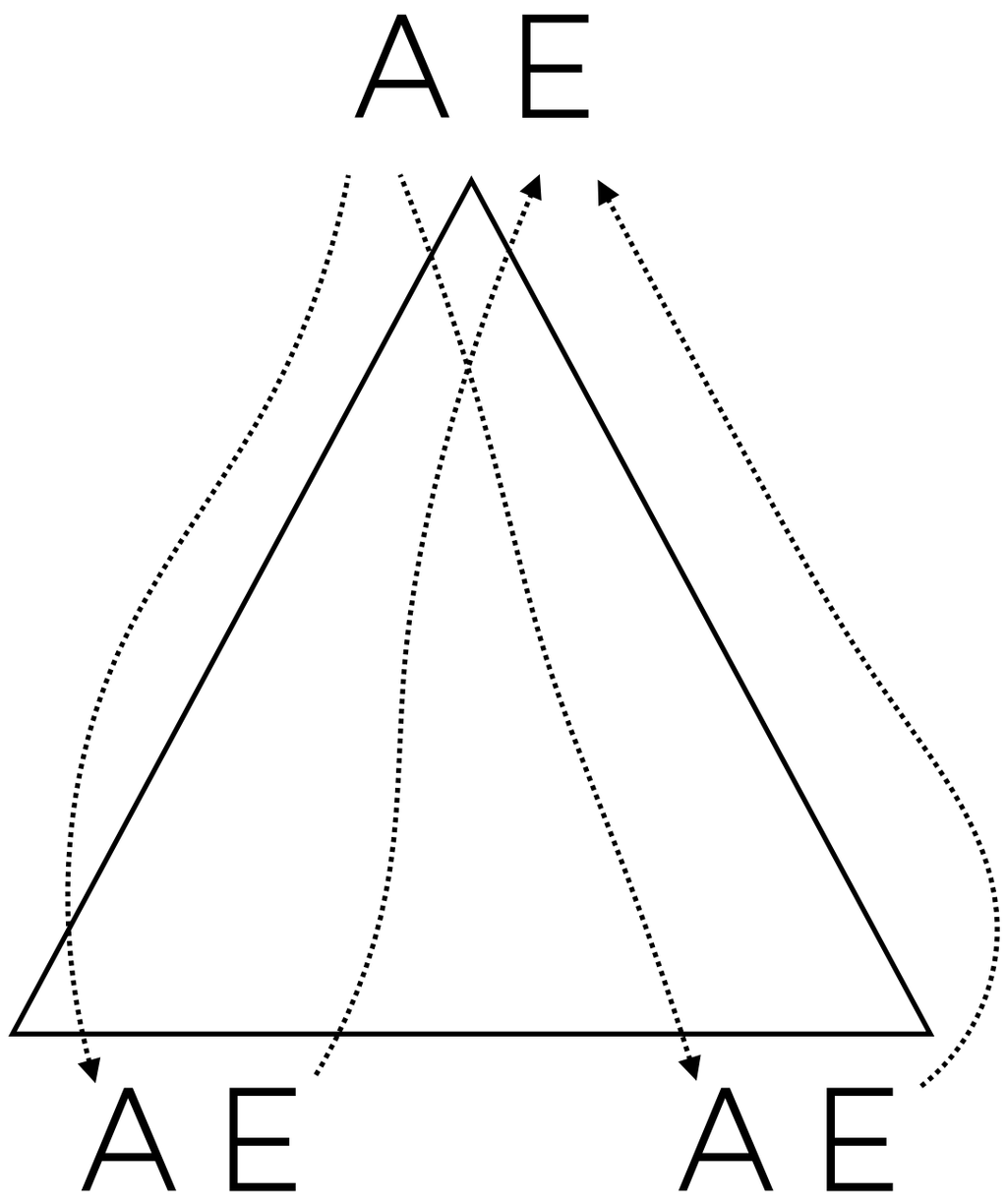
$$\dfrac{\dfrac{\exists x A(x) \quad \exists x A(x) \to \exists y B(y)}{\exists y B(y)} \qquad \exists y B(y) \to \exists z C(z)}{\exists z C(z)}$$

functional interpretations perform such proof transformations



$$\dfrac{[A(v)]_\alpha \quad \dfrac{\forall x(A(x) \to B(gx))}{A(v) \to B(gv)}}{\dfrac{B(gv) \qquad B(gv) \to C(h(gv))}{\dfrac{C(h(gv))}{A(v) \to C(h(gv))}\,\alpha}} \qquad \dfrac{\forall y(B(y) \to C(hy))}{B(gv) \to C(h(gv))}$$

$$\forall x(A(x) \to C(h(gx)))$$


A E
A E
A E

Lemma 1. $\forall x A(x) \to \forall y B(y)$ $\longrightarrow$ $\forall y(A(gy) \to B(y))$

Lemma 2. $\forall y B(y) \to \forall z C(z)$ $\longrightarrow$ $\forall z(B(hz) \to C(z))$

Theorem. $\forall x A(x) \to \forall z C(z)$

$$\dfrac{\dfrac{\forall x A(x) \quad \forall x A(x) \to \forall y B(y)}{\forall y B(y)} \qquad \forall y B(y) \to \forall z C(z)}{\forall z C(z)}$$

$A(fz)$

$C(z)$

$f\,?$

Lemma 1. $\forall x A(x) \to \forall y B(y)$ $\longrightarrow$ $\forall y(A(gy) \to B(y))$

Lemma 2. $\forall y B(y) \to \forall z C(z)$ $\longrightarrow$ $\forall z(B(hz) \to C(z))$

Theorem. $\forall x A(x) \to \forall z C(z)$ $\longrightarrow$ $\forall z(A(g(hz)) \to C(z))$

$$\dfrac{\dfrac{[A(g(hz)]_{\alpha} \quad \dfrac{\forall y(A(gy) \to B(y))}{A(g(hz)) \to B(hz)}}{B(hz)} \qquad \dfrac{\forall z(B(hz) \to C(z))}{B(hz) \to C(z)}}{\dfrac{\dfrac{C(z)}{A(g(hz)) \to C(z)}\,\alpha}{\forall z(A(g(hz)) \to C(z))}}$$

Gödel's Dialectica Interpretation

ÜBER EINE BISHER NOCH NICHT BENÜTZTE ERWEITERUNG DES FINITEN STANDPUNKTES

von Kurt Gödel, Princeton

Dialectica, vol. 12, 1958

$$
\begin{aligned}
|A \wedge B|^{x,v}_{y,w} &\equiv |A|^{x}_{y} \wedge |B|^{v}_{w} \\
|A \vee B|^{x,v,b}_{y,w} &\equiv (b{=}0 \wedge |A|^{x}_{y}) \vee (b \neq 0 \wedge |B|^{v}_{w}) \\
|A \to B|^{f,g}_{x,w} &\equiv |A|^{x}_{g(x,w)} \to |B|^{f(x)}_{w} \\
|\forall z\, A(z)|^{f}_{y,z} &\equiv |A(z)|^{f(z)}_{y} \\
|\exists z\, A(z)|^{x,z}_{y} &\equiv |A(z)|^{x}_{y}
\end{aligned}
$$

Theorem (Gödel'58). If HA $\vdash A$ then there exists a term t of system T such that T $\vdash |A|^{t}_{y}$

$$
\begin{aligned}
|A \wedge B|^{x,v}_{y,w} &\equiv |A|^{x}_{y} \wedge |B|^{v}_{w} \\
|A \vee B|^{x,v,b}_{y,w} &\equiv (b{=}0 \wedge |A|^{x}_{y}) \vee (b \neq 0 \wedge |B|^{v}_{w}) \\
|A \to B|^{f,g}_{x,w} &\equiv |A|^{x}_{g(x,w)} \to |B|^{f(x)}_{w} \\
|\forall z\, A(z)|^{f}_{y,z} &\equiv |A(z)|^{f(z)}_{y} \\
|\exists z\, A(z)|^{x,z}_{y} &\equiv |A(z)|^{x}_{y}
\end{aligned}
$$

$$A = \sqrt{2} \notin \mathbb{Q} \qquad |A|^{f}_{p,q} \equiv |\frac{p}{q} - \sqrt{2}| > f(p,q)$$

$$A = \forall n \exists p \in \mathbb{P}(p > n) \qquad |A|^{f}_{n} \equiv fn \in \mathbb{P} \wedge fn \geq n$$

$$\boxed{\forall n(A(n)\to A(n+1))\vdash A(0)\to A(2)}$$

assumption used twice (contraction)

$$\dfrac{[A(0)]_{\alpha}\qquad \dfrac{\forall n(A(n)\to A(n+1))}{A(0)\to A(1)}}{A(1)}\qquad \dfrac{\forall n(A(n)\to A(n+1))}{A(1)\to A(2)}$$

$$A(2)$$

Is there an a single a such that:

$$\boxed{A(a)\to A(a+1)\vdash A(0)\to A(2)}$$

Is there an a single a such that:

$$\boxed{A(a) \to A(a+1) \vdash A(0) \to A(2)}$$

In fact there is, when the formulas are “decidable”

$$a := \left\{ \begin{array}{ll} 0 & \text{if } \neg(A(0) \to A(1)) \\ 1 & \text{otherwise} \end{array} \right\}$$

Works, but… a bit of a hack

Diller-Nahm Variant

Diller-Nahm Interpretation

$$
\begin{aligned}
|A \wedge B|^{x,v}_{y,w} &\equiv |A|^{x}_{y} \wedge |B|^{v}_{w} \\
|A \vee B|^{x,v,b}_{y,w} &\equiv (b{=}0 \wedge |A|^{x}_{y}) \vee (b \neq 0 \wedge |B|^{v}_{w}) \\
|A \to B|^{f,g}_{x,w} &\equiv \forall y \in g(x,w)\, |A|^{x}_{y} \to |B|^{f(x)}_{w} \\
|\forall z\, A(z)|^{f}_{y,z} &\equiv |A(z)|^{f(z)}_{y} \\
|\exists z\, A(z)|^{x,z}_{y} &\equiv |A(z)|^{x}_{y}
\end{aligned}
$$

precise witnesses for positive existential,
approximating set for negative universals

Is there an a finite set S such that:

$$\boxed{\forall a \in S(A(a) \to A(a+1)) \vdash A(0) \to A(2)}$$

Yes!

$$\boxed{S := \{0,1\}}$$

Indeed:

$$\boxed{\forall a \in \{0,1\}(A(a) \to A(a+1)) \vdash A(0) \to A(2)}$$

Interpreting Induction

$$\frac{\exists k A(0,k) \quad \forall n^{\mathbb{N}}(\exists k A(n,k) \to \exists k A(n+1,k))}{\forall n^{\mathbb{N}} \exists k A(n,k)}$$

By induction hypothesis we have:

$$A(0,k_0) \quad \text{and} \quad \forall n^{\mathbb{N}}(A(n,k) \to A(n+1, fnk))$$

So witness for conclusion is:

$$k := fn(f(n-1)(\ldots(f\,0k_0)) = \mathrm{Rec}\, n\, k_0\, f$$

$$\mathrm{Rec}\ 0\ k_0\ f\ =\ k_0$$

$$\mathrm{Rec}\ (n+1)\ k_0\ f = f\ n\ (\mathrm{Rec}\ n\ k_0\ f)$$

Gödel system T
=
lambda calculus + Rec

Choice, Compactness, etc…

Comprehension

$$\exists f^{\mathbb{N}\to\mathbb{B}}\forall n^{\mathbb{N}}(fn \leftrightarrow A(n))$$

Let $T(n,n,u)$ be the statement that Turing machine with code n on input n will halt with computation u

The Halting problem (known to be undecidable) is

$$A(n) \equiv \exists u T(n,n,u)$$

So clearly, the following (true) statement cannot be witnessed by a computable function f

$$\exists f^{\mathbb{N}\to\mathbb{B}}\forall n^{\mathbb{N}}(fn \leftrightarrow \exists u T(n,n,u))$$

Comprehension

$$\exists f^{\mathbb{N}\to\mathbb{B}}\forall n^{\mathbb{N}}(fn \leftrightarrow A(n))$$

Approach I

1. Apply double negation translation

$$\neg\neg\exists f^{\mathbb{N}\to\mathbb{B}}\forall n^{\mathbb{N}}(fn \leftrightarrow A^{N}(n))$$

2. Extend system T so as to be able to witness this

   E.g. system T + recursion on well-founded trees

   (bar recursion)

"Life offers a cruel choice: you can be right or happy. Not both."

- Albert J. Bernstein

Precise

$$f(x)=\left\{\begin{array}{ll} 0 & \text{if } \exists u.T(x,x,u) \\ 1 & \text{if } \forall u.\neg T(x,x,u) \end{array}\right\}$$

precise

but

non-computable

Approximate

$$f(x)=\{0,\ 1\}$$

approximate

but

computable

Comprehension

$$\exists f^{\mathbb{N}\to\mathbb{B}}\forall n^{\mathbb{N}}(fn \leftrightarrow A(n))$$

Approach II

1. Notice that f can be easily "bounded"

$$\exists f^{\mathbb{N}\to\mathbb{B}} \leq 1\forall n^{\mathbb{N}}(fn \leftrightarrow A^{N}(n))$$

2. Work with "approximate" functional interpretations

   E.g. Monotone, bounded, Herbrand, … interpretations

Lemma 1. $\exists x A(x) \to \exists y B(y)$ $\longrightarrow$ $\exists x \leq n\, A(x) \to \exists y \leq gn B(y)$

Lemma 2. $\exists y B(y) \to \exists z C(z)$ $\longrightarrow$ $\exists y \leq n B(y) \to \exists z \leq hn C(z)$

Theorem. $\exists x A(x) \to \exists z C(z)$ $\longrightarrow$ $\exists x \leq n\, A(x) \to \exists z \leq h(gn)\, C(z)$

$\exists x \leq n\, A(x)$

$$\frac{\exists x A(x) \quad \exists x A(x) \to \exists y B(y)}{\exists y B(y)} \qquad \frac{\exists y B(y) \to \exists z C(z)}{\exists z C(z)}$$

f ? : $\exists z \leq fn\ C(z)$

Lemma 1. $\exists x A(x) \to \exists y B(y)$ $\longrightarrow$ $\exists x \leq n\, A(x) \to \exists y \leq gn B(y)$

Lemma 2. $\exists y B(y) \to \exists z C(z)$ $\longrightarrow$ $\exists y \leq n B(y) \to \exists z \leq hn C(z)$

Theorem. $\exists x A(x) \to \exists z C(z)$ $\longrightarrow$ $\exists x \leq n\, A(x) \to \exists z \leq h(gn) C(z)$

$$\dfrac{\dfrac{\exists x \leq n A(x) \quad \exists x \leq n A(x) \to \exists y \leq gn B(y)}{\exists y \leq gn B(y)} \qquad \dfrac{\exists y \leq n B(y) \to \exists z \leq hn C(z)}{\exists y \leq gn B(y) \to \exists z \leq h(gn) C(z)}}{\exists z \leq h(gn) C(z)}$$

Approximate Interpretation

$$
\begin{aligned}
|A \wedge B|^{x,v}_{y,w} &\equiv |A|^{x}_{y} \wedge |B|^{v}_{w} \\
|A \vee B|^{x,v}_{y,w} &\equiv |A|^{x}_{y} \vee |B|^{v}_{w} \\
|A \to B|^{f,g}_{x,w} &\equiv \forall y \in g(x,w)\, |A|^{x}_{y} \to |B|^{f(x)}_{w} \\
|\forall z^{\mathbb{N}} A(z)|^{f}_{y,a} &\equiv \forall z \leq a\, |A(z)|^{f(a)}_{y} \\
|\exists z^{\mathbb{N}} A(z)|^{x,a}_{y} &\equiv \exists z \leq a\, |A(z)|^{x}_{y}
\end{aligned}
$$

P. Oliva, **Unifying functional interpretations**, NDJFL, 47 (2), 2006

G. Ferreira and P. Oliva, **Funct. inter. of intuitionistic linear logic**, CSL, 2009

M.D. Hernest and P. Oliva, **Hybrid functional interpretations**, CiE, 2008

P. Oliva, **Modified realizability interpretation of classical linear logic**, LICS 2007

G. Ferreira and P. Oliva, **Functional interpretations of intuitionistic linear logic**, Logical Methods in Computer Science, 7(1), 2011

J. Gaspar and P. Oliva, **Proof interpretations with truth**, MLQ, 56(6):591-610, 2010

P. Oliva, **Kreisel's modified realizability and recent variants**, to appear

B. Dinis and P. Oliva, **Parametrised functional interpretations**, in preparation