

# Tutorial on Proof Theory

(with emphasis on proof mining)

## Lecture 3: Proof Interpretations

Paulo Oliva

Queen Mary University of London

*Days in Logic 2020*

Lisbon, 30 Jan - 1 Feb 2020

## Introduction Rules

$$\frac{\frac{\Gamma}{\vdots}}{A(x)} \quad x \notin \text{FV}(\Gamma)}{\forall x A(x)}$$

$$\frac{\vdots}{A(t)}{\exists x A(x)}$$

## Elimination Rules

$$\frac{\vdots}{\forall x A(x)}{A(t)}$$

$$\frac{\frac{\vdots}{\exists x A(x)} \quad \frac{[A(x)]}{\vdots}}{C} \quad x \notin \text{FV}(C)$$

$$\frac{\vdots}{A} \\ \hline A \vee B$$

$$\frac{\vdots}{A(t)} \\ \hline \exists x A(x)$$

$$\frac{\vdots}{\perp} \\ \hline A$$

**ML + EFQ** is called intuitionistic logic **IL**

**Proposition** (Disjunction property).

If IL proves  $A \vee B$  then either IL proves  $A$  or IL proves  $B$

**Proposition** (Existence property).

If IL proves  $\exists x A(x)$  then IL proves  $A(t)$  for some term  $t$

# Slash Translation

$$\Gamma | P \equiv \Gamma \vdash P$$

$$\Gamma | A \wedge B \equiv (\Gamma | A) \wedge (\Gamma | B)$$

$$\Gamma | A \vee B \equiv (\Gamma | A) \vee (\Gamma | B)$$

$$\Gamma | A \rightarrow B \equiv ((\Gamma | A) \rightarrow (\Gamma | B)) \wedge \Gamma \vdash A \rightarrow B$$

$$\Gamma | \forall x A \equiv \forall t (\Gamma | A[t/x]) \wedge \Gamma \vdash \forall x A$$

**Thm 1:** Assume  $\Gamma \vdash \Gamma$ . If  $\Gamma \vdash A$  then  $\Gamma | A$

**Thm 2:**  $\Gamma | A$  implies  $\Gamma \vdash A$

**Cor:** If  $\vdash A \vee B$  then either  $\vdash A$  or  $\vdash B$

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

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

$$\frac{\frac{\frac{[A]_\alpha}{A \vee \neg A} \quad [\neg(A \vee \neg A)]_\gamma}{\perp} \alpha}{\frac{A \vee \neg A \quad [\neg(A \vee \neg A)]_\gamma}{\perp} \text{PBC, } \gamma}$$

$$\frac{\frac{\frac{[A]_\alpha}{A \vee \neg A} \quad [\neg(A \vee \neg A)]_\gamma}{\perp} \alpha}{\frac{A \vee \neg A \quad [\neg(A \vee \neg A)]_\gamma}{\perp} \rightarrow\text{I, } \gamma} \neg\neg(A \vee \neg A)$$

**Intuitionistic Logic**  
(ex falso quodlibet)

$$\frac{\vdots}{\perp} \text{EFQ}$$

**Classical Logic**  
(proof by contraction)

$$\frac{\frac{[\neg A]_\alpha}{\vdots}}{\perp} \text{PBC, } \alpha$$

**Proposition** (Gentzen 1933).

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

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

## Comprehension

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

---

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  $f$

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

# Plan

Lecture 1: Formal Proofs

Lecture 2: Proof Translations

Lecture 3: **Proof Interpretations**



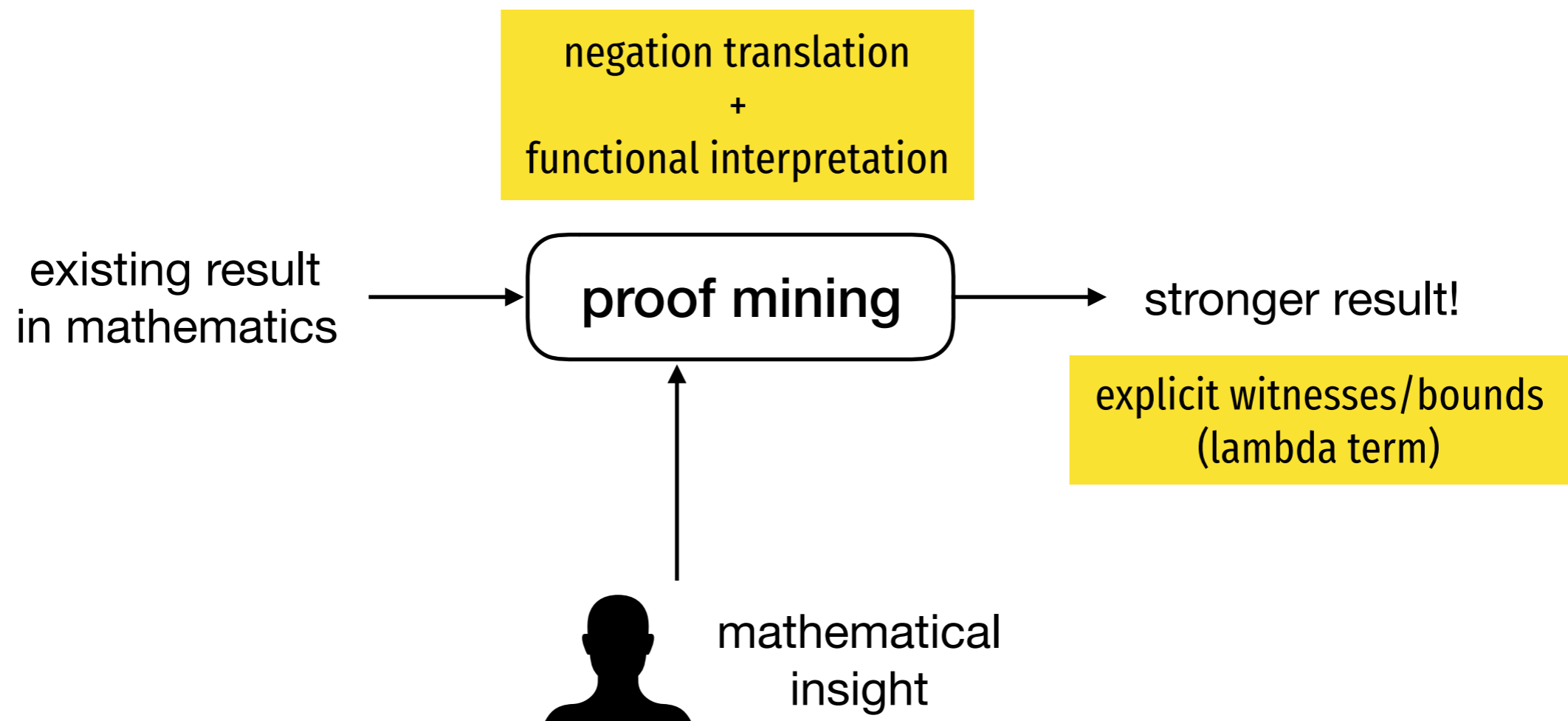
# Today

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

# Incomplete Statements

(opportunity for proof mining)

# Proof Mining



# Incomplete Statements

An **incomplete statement** contains a “positive” quantification which can be (non-trivially) bounded or witnessed precisely

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

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

Any continuous  $f : [0,1] \rightarrow [0,1]$  has a fixed point  
(Brouwer fixed-point theorem) ?

Any contractive  $f : [0,1] \rightarrow [0,1]$  has at most one fixed point  
(Edelstein fixed-point theorem) ?

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

**complete statement!**

$$\forall n (n \in \mathbb{N} \wedge n > 2 \rightarrow \neg \exists a, b, c \in \mathbb{N} (a^n + b^n = c^n))$$

equivalent to...

$$\forall n (n \in \mathbb{N} \wedge n > 2 \rightarrow \forall a, b, c \in \mathbb{N} (a^n + b^n \neq c^n))$$

**purely universal  
statement**

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

**complete statement!**

$$\forall n (n \in \mathbb{N} \wedge n \in \text{Even} \wedge n > 2 \rightarrow \exists p_1, p_2 \in \text{Prime} (n = p_1 + p_2))$$

existence without  
explicit witness!

**BUT**

$$\forall n (n \in \mathbb{N} \wedge n \in \text{Even} \wedge n > 2 \rightarrow \exists p_1, p_2 \leq n (p_1, p_2 \in \text{Prime} \wedge n = p_1 + p_2))$$

existence can be  
easily bounded

Any continuous  $f : [0,1] \rightarrow [0,1]$  has a fixed point  
(Brouwer fixed-point theorem)

**incomplete statement!**

$$\text{Cont}(f) \equiv \forall x^{[0,1]}, \varepsilon^{\mathbb{Q}^+} \exists \delta^{\mathbb{Q}^+} \forall y^{[0,1]} (|x - y| < \delta \rightarrow |fx - fy| < \varepsilon)$$

$$\forall f^{[0,1] \rightarrow [0,1]} (\text{Cont}(f) \rightarrow \exists x \in [0,1] (fx = x))$$

existence without  
explicit witness!

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

**incomplete statement!**

$$\text{Contractive}(f) \equiv \forall x, y \in [0,1] (|fx - fy| < |x - y|)$$

$$\forall f^{[0,1] \rightarrow [0,1]}$$

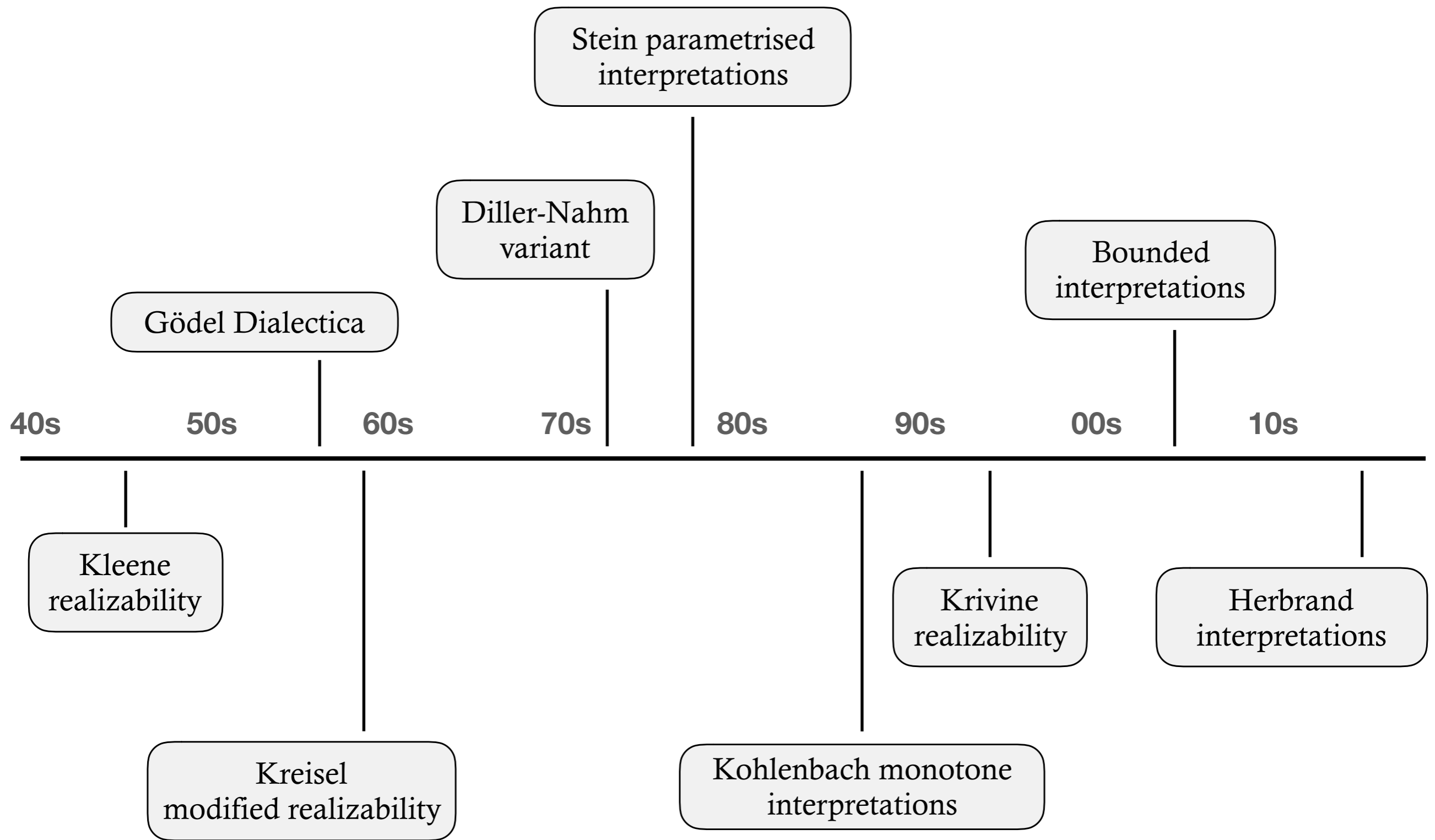
Contractive( $f$ )  $\rightarrow$

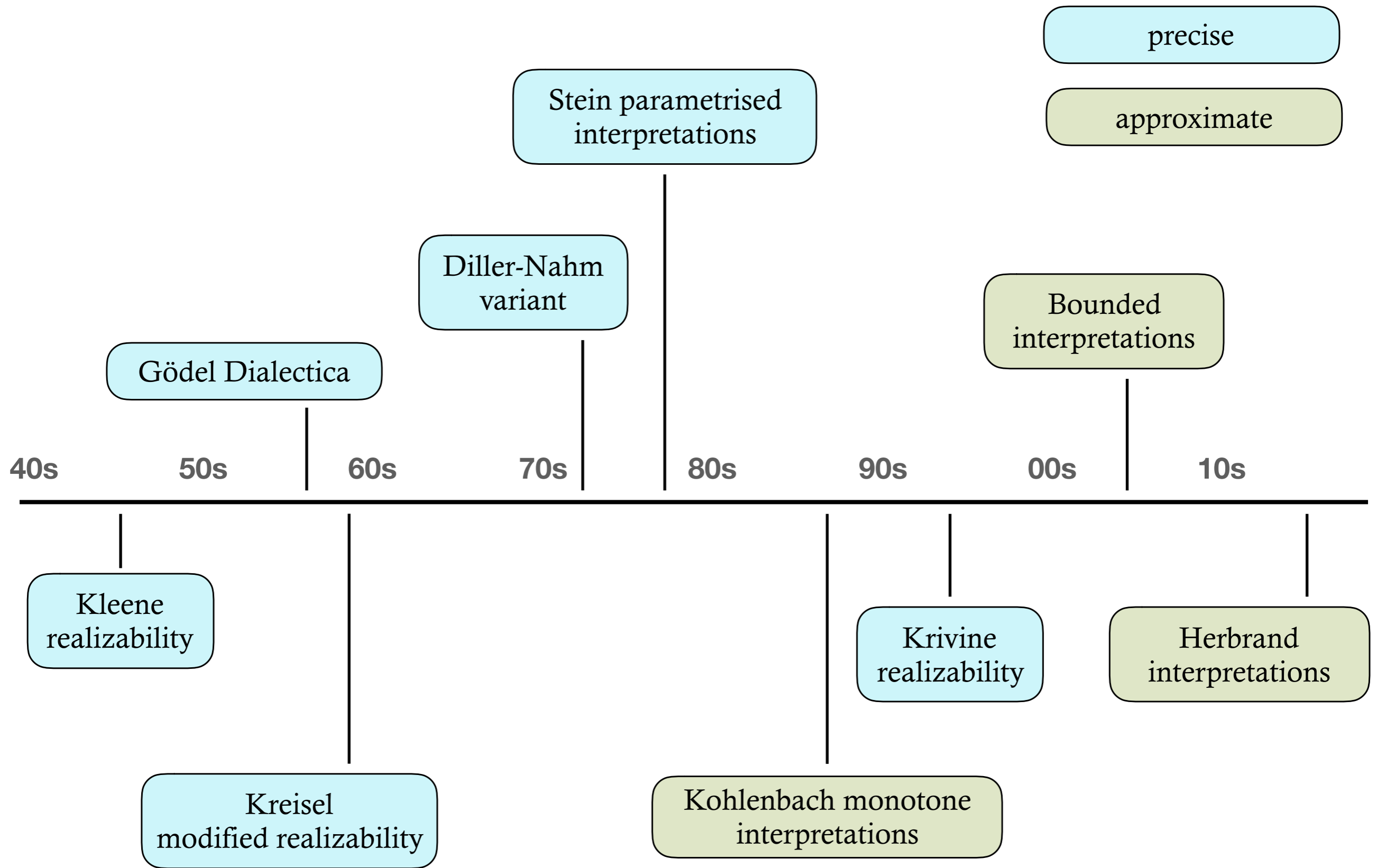
$$\forall x_1, x_2 (x_1 = fx_1 \wedge x_2 = fx_2 \rightarrow x_1 = x_2)$$

how close should  $x_i$  be to  $f(x_i)$   
to ensure  $x_1$  is close to  $x_2$ ?



# Functional Interpretations





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

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

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

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

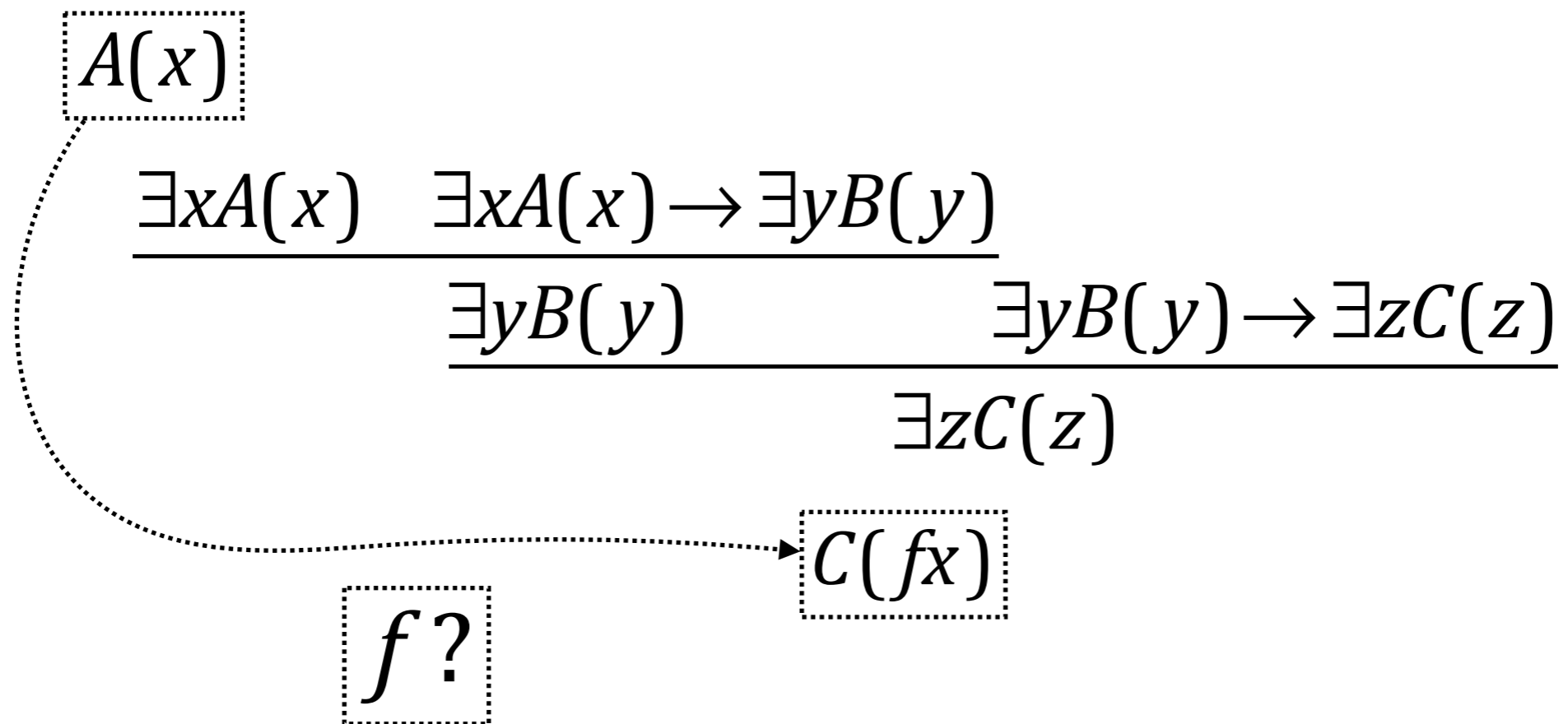
Lemma 2\*:  $\forall x, y, \delta (|x^2 - y^2| \geq \delta \rightarrow |x - y| \geq \frac{\delta}{x + y})$

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

Lemma 1.  $\exists xA(x) \rightarrow \exists yB(y)$   $\longrightarrow$   $\forall x(A(x) \rightarrow B(gx))$

Lemma 2.  $\exists yB(y) \rightarrow \exists zC(z)$   $\longrightarrow$   $\forall y(B(y) \rightarrow C(hy))$

Theorem.  $\exists xA(x) \rightarrow \exists zC(z)$



$$\boxed{\text{Lemma 1. } \exists x A(x) \rightarrow \exists y B(y)} \longrightarrow \boxed{\forall x (A(x) \rightarrow B(gx))}$$

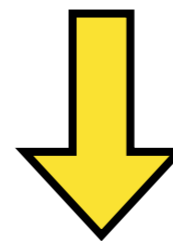
$$\boxed{\text{Lemma 2. } \exists y B(y) \rightarrow \exists z C(z)} \longrightarrow \boxed{\forall y (B(y) \rightarrow C(hy))}$$

$$\boxed{\text{Theorem. } \exists x A(x) \rightarrow \exists z C(z)} \longrightarrow \boxed{\forall x (A(x) \rightarrow C(h(gx)))}$$

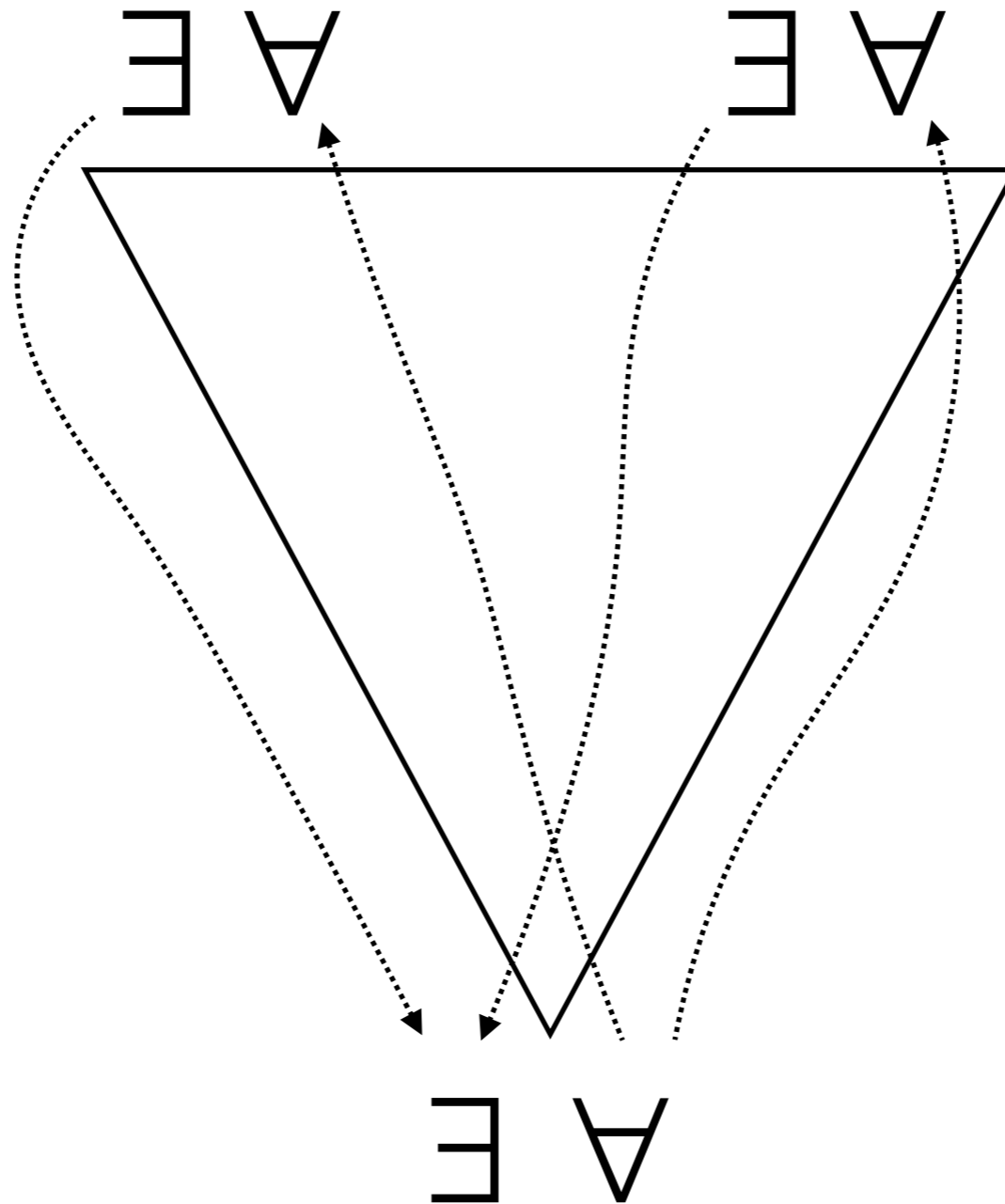
$$\frac{[A(v)]_{\alpha} \quad \frac{\forall x (A(x) \rightarrow B(gx))}{A(v) \rightarrow B(gv)}}{B(gv)} \quad \frac{\forall y (B(y) \rightarrow C(hy))}{B(gv) \rightarrow C(h(gv))}}{\frac{C(h(gv))}{A(v) \rightarrow C(h(gv))} \quad \alpha}{\forall x (A(x) \rightarrow C(h(gx)))}$$

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

functional interpretations perform such proof transformations



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

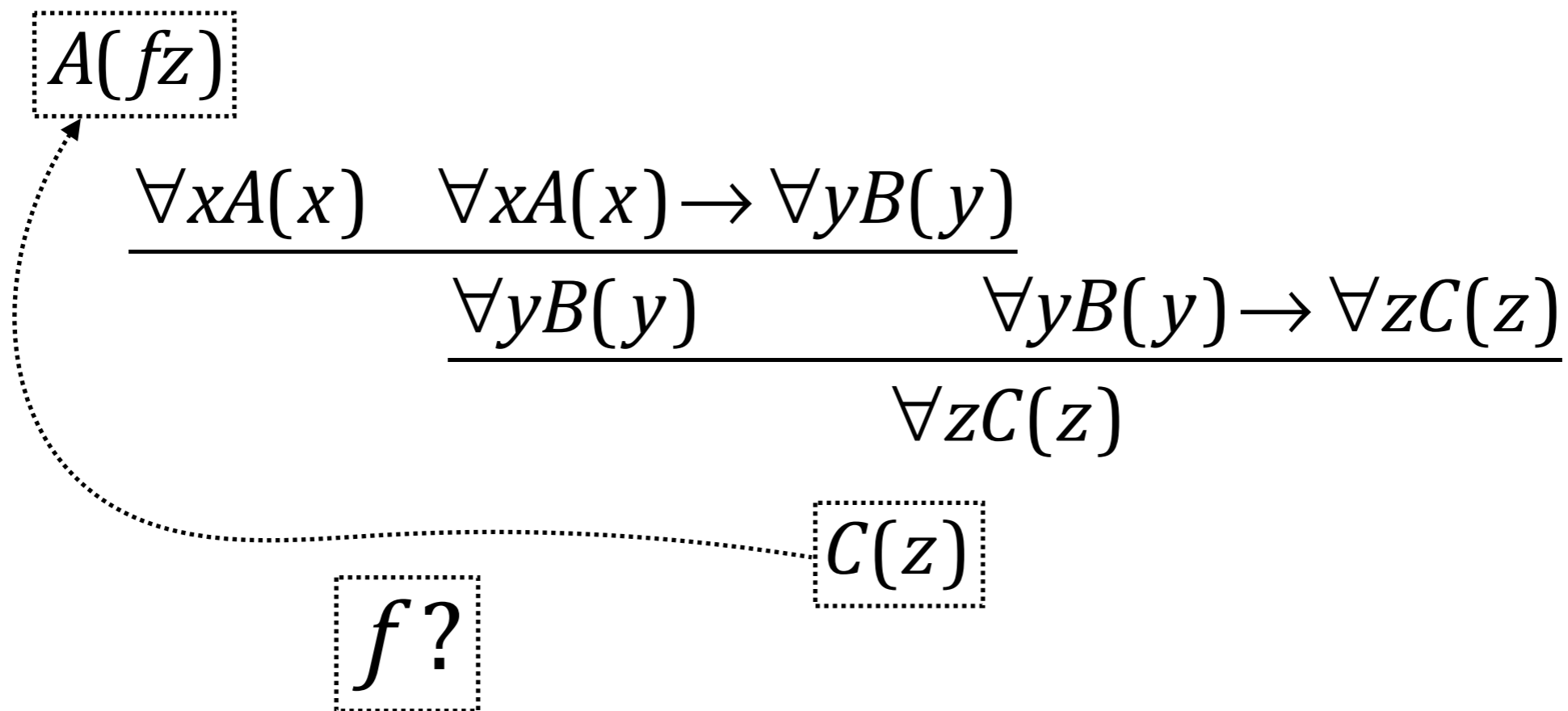




Lemma 1.  $\forall xA(x) \rightarrow \forall yB(y) \longrightarrow \forall y(A(gy) \rightarrow B(y))$

Lemma 2.  $\forall yB(y) \rightarrow \forall zC(z) \longrightarrow \forall z(B(hz) \rightarrow C(z))$

Theorem.  $\forall xA(x) \rightarrow \forall zC(z)$



$$\boxed{\text{Lemma 1. } \forall x A(x) \rightarrow \forall y B(y)} \longrightarrow \boxed{\forall y (A(gy) \rightarrow B(y))}$$

$$\boxed{\text{Lemma 2. } \forall y B(y) \rightarrow \forall z C(z)} \longrightarrow \boxed{\forall z (B(hz) \rightarrow C(z))}$$

$$\boxed{\text{Theorem. } \forall x A(x) \rightarrow \forall z C(z)} \longrightarrow \boxed{\forall z (A(g(hz)) \rightarrow C(z))}$$

$$\begin{array}{c}
 [A(g(hz))]_{\alpha} \quad \frac{\forall y (A(gy) \rightarrow B(y))}{A(g(hz)) \rightarrow B(hz)} \quad \frac{\forall z (B(hz) \rightarrow C(z))}{B(hz) \rightarrow C(z)} \\
 \hline
 B(hz) \quad \frac{C(z)}{A(g(hz)) \rightarrow C(z)} \quad \alpha \\
 \hline
 \forall z (A(g(hz)) \rightarrow C(z))
 \end{array}$$

# Gödel's Dialectica Interpretation

# ÜBER EINE BISHER NOCH NICHT BENÜTZTE ERWEITERUNG DES FINITEN STANDPUNKTES

von Kurt GÖDEL, Princeton

Dialectica, vol. 12, 1958

$$|A \wedge B|_{y,w}^{x,v} \equiv |A|_y^x \wedge |B|_w^v$$

$$|A \vee B|_{y,w}^{x,v,b} \equiv (b=0 \wedge |A|_y^x) \vee (b \neq 0 \wedge |B|_w^v)$$

$$|A \rightarrow B|_{x,w}^{f,g} \equiv |A|_{g(x,w)}^x \rightarrow |B|_w^{f(x)}$$

$$|\forall z A(z)|_{y,z}^f \equiv |A(\mathbf{z})|_y^{f(\mathbf{z})}$$

$$|\exists z A(z)|_y^{x,z} \equiv |A(\mathbf{z})|_y^x$$

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

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

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

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

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

assumption used twice (contraction)

$$\frac{[A(0)]_{\alpha} \quad \frac{\forall n(A(n) \rightarrow A(n+1))}{A(0) \rightarrow A(1)}}{A(1)} \quad \frac{\forall n(A(n) \rightarrow A(n+1))}{A(1) \rightarrow A(2)}}{A(2)}$$

Is there an a single  $a$  such that:

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

Is there an a single  $a$  such that:

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

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

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

Works, but... a bit of a hack

# Diller-Nahm Variant



# Diller-Nahm Interpretation

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

precise witnesses for positive existential,  
approximating set for negative universals

Is there a finite set  $S$  such that:

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

Yes!

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

Indeed:

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

# Interpreting Induction

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

By induction hypothesis we have:

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

So witness for conclusion is:

$$k := fn(f(n-1)(\dots(f 0 k_0))) = \text{Rec } n k_0 f$$

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

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

Gödel system T  
= lambda calculus + Rec

Choice, Compactness, etc...

## Comprehension

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

---

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  $f$

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

# Comprehension

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

---

## Approach I

1. Apply double negation translation

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

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

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

---

## Approach II

1. Notice that  $f$  can be easily "bounded"

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

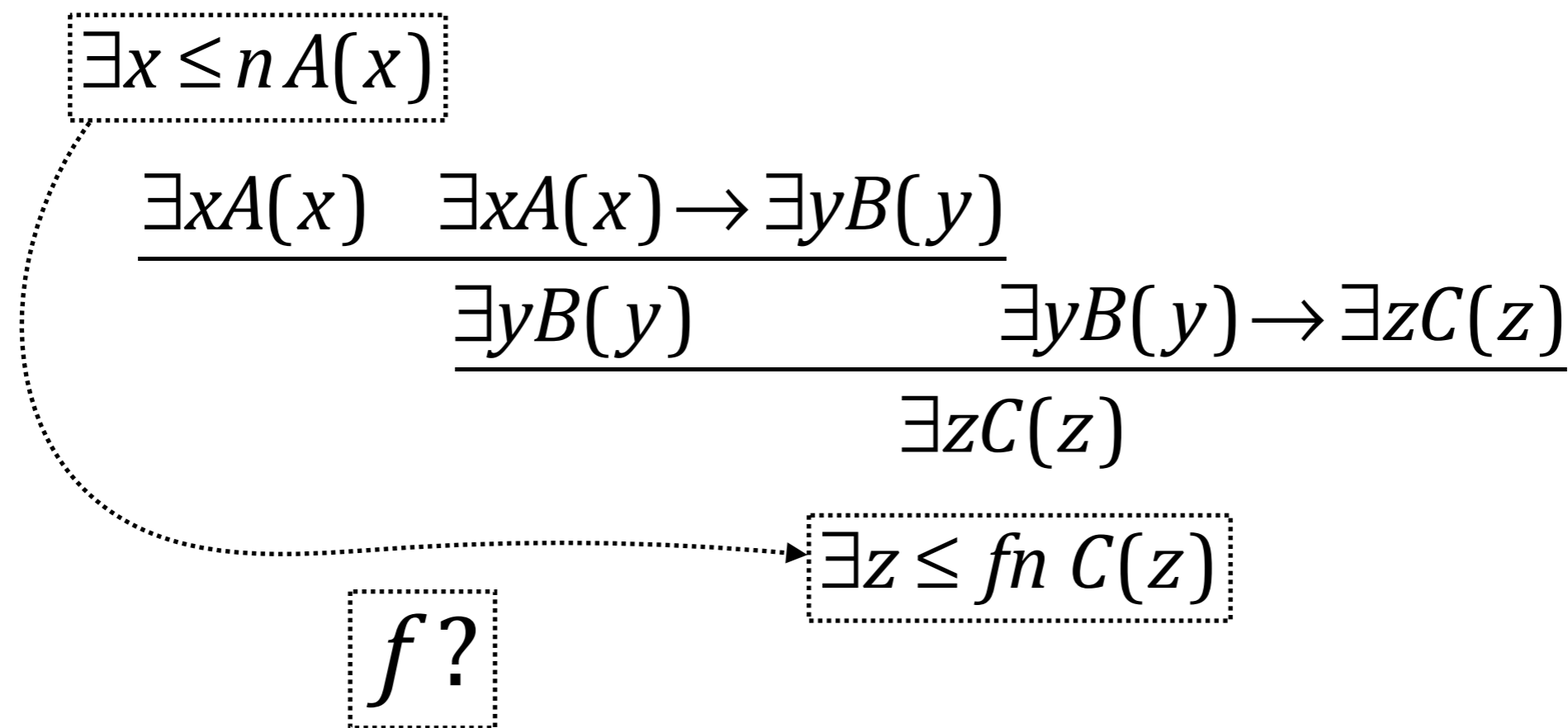
2. Work with "approximate" functional interpretations

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

$$\boxed{\text{Lemma 1. } \exists x A(x) \rightarrow \exists y B(y)} \longrightarrow \boxed{\exists x \leq n A(x) \rightarrow \exists y \leq gn B(y)}$$

$$\boxed{\text{Lemma 2. } \exists y B(y) \rightarrow \exists z C(z)} \longrightarrow \boxed{\exists y \leq n B(y) \rightarrow \exists z \leq hn C(z)}$$

$$\boxed{\text{Theorem. } \exists x A(x) \rightarrow \exists z C(z)} \longrightarrow \boxed{\exists x \leq n A(x) \rightarrow \exists z \leq h(gn) C(z)}$$



Lemma 1. $\exists x A(x) \rightarrow \exists y B(y)$	→	$\exists x \leq n A(x) \rightarrow \exists y \leq gn B(y)$
Lemma 2. $\exists y B(y) \rightarrow \exists z C(z)$	→	$\exists y \leq n B(y) \rightarrow \exists z \leq hn C(z)$
Theorem. $\exists x A(x) \rightarrow \exists z C(z)$	→	$\exists x \leq n A(x) \rightarrow \exists z \leq h(gn) C(z)$

$\exists x \leq n A(x)$	$\exists x \leq n A(x) \rightarrow \exists y \leq gn B(y)$	$\exists y \leq n B(y) \rightarrow \exists z \leq hn C(z)$
$\exists y \leq gn B(y)$	$\exists y \leq gn B(y) \rightarrow \exists z \leq h(gn) C(z)$	$\exists z \leq h(gn) C(z)$

# Approximate Interpretation


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

 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