Functional Interpretations

Paulo Oliva

Queen Mary, University of London, UK
(pbo@dcs.qmul.ac.uk)

Venice, 29 March 2005

Outline

Enriching mathematical theorems

- **Complete theorems**
- **Incomplete theorems**

Enriching mathematical theorems

- **Complete theorems**
  Universal statements
  E.g. Fermat's last theorem: $\forall n > 2 \forall x, y, z (x^n + y^n \neq z^n)$

- **Incomplete theorems**

Enriching mathematical theorems

- **Complete theorems**
  Universal statements
  E.g. Fermat's last theorem: $\forall n > 2 \forall x, y, z (x^n + y^n \neq z^n)$

- **Incomplete theorems**
  Existential statements
  E.g. Infinity of primes: $\forall n \exists p \geq n \, \mathrm{Prime}(p)$

Enriching mathematical theorems

- **Complete theorems**
  Universal statements
  E.g. Fermat's last theorem: $\forall n > 2 \forall x, y, z (x^n + y^n \neq z^n)$

- **Incomplete theorems**
  Existential statements
  E.g. Infinity of primes: $\forall n \exists p \geq n \, \mathrm{Prime}(p)$

- Use proof of incomplete theorem
  $\forall n (fn \geq n \wedge \mathrm{Prime}(fn))$

Enriching mathematical theorems

Theorem (A)

$\exists a \in \mathbb{I}\, (a^{\sqrt{2}} \in \mathbb{Q})$

Proof.

If $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ take $a = \sqrt{2}$

If $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ take $a = \sqrt{2}^{\sqrt{2}}$ □

Enriching mathematical theorems

Theorem (B)

$\forall f^{\mathbb{N}\to\mathbb{N}} \exists n^{\mathbb{N}} (fn = 0 \to \forall k (fk = 0))$

Proof.

Fix f

Let $n = \begin{cases} \min k (fk \neq 0) & \text{if } \exists k (fk \neq 0) \\ 0 & \text{otherwise} \end{cases}$ $\square$

Enriching mathematical theorems

Theorem (C)

Fix $n \in \mathbb{N}$. Each continuous function $f \in C[0,1]$ has a unique best approximating polynomial of degree n.

Lemma (Existence)

$\forall f \in C[0,1] \exists p \in P_n(||f - p|| =_{\mathbb{R}} dist(f, P_n))$

Lemma (Uniqueness)

$\forall f \in C[0,1] \forall p_0, p_1 \in P_n$
$(\wedge_{i=0}^{1} ||f - p_i|| =_{\mathbb{R}} dist(f, P_n) \to p_0 = p_1)$

Enriching mathematical theorems

Theorem (C)

Fix $n \in \mathbb{N}$. Each continuous function $f \in C[0,1]$ has a unique best approximating polynomial of degree n.

Lemma (Existence)

$\forall f \in C[0,1] \exists p \in P_n (||f - p|| =_{\mathbb{R}} dist(f, P_n))$

Lemma (Uniqueness)

$\forall f \in C[0,1] \forall p_0, p_1 \in P_n$
$(\forall k \, |||f - p_i|| - dist(f, P_n)| \leq 1/k \rightarrow \forall n \, ||p_0 - p_1|| \leq 1/n)$

Enriching mathematical theorems

Theorem (C)

Fix $n \in \mathbb{N}$. Each continuous function $f \in C[0,1]$ has a unique best approximating polynomial of degree n.

Lemma (Existence)

$\forall f \in C[0,1] \exists p \in P_n (||f - p|| =_{\mathbb{R}} dist(f, P_n))$

Lemma (Uniqueness)

$\forall f \in C[0,1] \forall p_0, p_1 \in P_n \forall n \exists k$
$(|||f - p_i|| - dist(f, P_n)| \leq 1/k \to ||p_0 - p_1|| \leq 1/n)$

Enriching mathematical theorems

Theorem (C)

Fix $n \in \mathbb{N}$. Each continuous function $f \in C[0,1]$ has a unique best approximating polynomial of degree n.

Lemma (Existence)

$$\forall f \in C[0,1] \exists p \in P_n (||f - p|| =_{\mathbb{R}} dist(f, P_n))$$

Lemma (Uniqueness)

$$\forall f \in C[0,1] \forall p_0, p_1 \in P_n \forall n \\ (|||f - p_i|| - dist(f, P_n)| \leq 1/\Phi(f, p_i, n) \to ||p_0 - p_1|| \leq 1/n)$$

Enriching mathematical theorems

Theorem (C)

Fix $n \in \mathbb{N}$. Each continuous function $f \in C[0,1]$ has a unique best approximating polynomial of degree n.

Lemma (Existence)

$$\forall f \in C[0,1] \exists p \in P_n(||f - p|| =_{\mathbb{R}} dist(f, P_n))$$

Lemma (Uniqueness)

$$\forall f \in C[0,1] \forall p_0, p_1 \in P_n \forall n \\ (|||f - p_i|| - dist(f, P_n)| \leq 1/\Phi(f, n) \rightarrow ||p_0 - p_1|| \leq 1/n)$$

Outline

1. Functional Interpretations
2. Three Applications
3. Conclusions

Functional interpretations

1. **Formalising statement**
   computational content
   based on representation of mathematical objects

2. **Formalising proof**
   qualitative results
   principles used in the proof

3. **Proof analysis**
   quantitative results
   theorem becomes complete

Functional interpretations

A functional interpretation of T in S consists of:

- A **formula mapping**

$$A \quad \mapsto \quad |A|^{\vec{x}}_{\vec{y}}$$

  - $\vec{x}$ marks the witnesses required by A (i.e. $\forall \vec{y} |A|^{\vec{t}}_{\vec{y}}$)
  - $\vec{y}$ marks the refutation of a given witness for A.

Functional interpretations

A functional interpretation of T in S consists of:

- A **formula mapping**

$$A \quad \mapsto \quad |A|^{\vec{x}}_{\vec{y}}$$

  - $\vec{x}$ marks the witnesses required by A (i.e. $\forall \vec{y} |A|^{\vec{t}}_{\vec{y}}$)
  - $\vec{y}$ marks the refutation of a given witness for A.

$$|\exists x \forall y A(x,y)|^{x}_{y} \equiv A(x,y)$$

$$|A \vee B|^{n} \equiv \text{if } (n = 0) \text{ then } A \text{ else } B$$

Functional interpretations

A functional interpretation of T in S consists of:

- A **formula mapping**

$$A \quad \mapsto \quad |A|^{\vec{x}}_{\vec{y}}$$

  - $\vec{x}$ marks the witnesses required by A (i.e. $\forall \vec{y} |A|^{\vec{t}}_{\vec{y}}$)
  - $\vec{y}$ marks the refutation of a given witness for A.

- A **proof mapping**

$$\mathrm{T} \vdash A \quad \mapsto \quad \mathrm{S} \vdash B,$$

for some B such that $B \rightarrow \exists \vec{x} \forall \vec{y} |A|^{\vec{x}}_{\vec{y}}$.

Functional interpretations

A functional interpretation of T in S consists of:

- A **formula mapping**

$$A \quad \mapsto \quad |A|^{\vec{x}}_{\vec{y}}$$

  - $\vec{x}$ marks the witnesses required by A (i.e. $\forall \vec{y} |A|^{\vec{t}}_{\vec{y}}$)
  - $\vec{y}$ marks the refutation of a given witness for A.

- A **proof mapping**

$$\mathrm{T} \vdash A \quad \mapsto \quad \mathrm{S} \vdash B,$$

for some B such that $B \to \exists \vec{x} \forall \vec{y} |A|^{\vec{x}}_{\vec{y}}$. (e.g. $B \equiv \forall \vec{y} |A|^{\vec{t}}_{\vec{y}}$)

Applications in proof theory

$$|\perp| \equiv \perp$$

$$\mathsf{T} \vdash \exists x \forall y |A|^x_y \to A' \qquad (\mathsf{S} \subseteq \mathsf{T})$$

$$\mathsf{S} \vdash \exists x \forall y |A|^x_y \to A$$

$$\mathsf{S} \not\vdash \exists x \forall y |A|^x_y$$

x in $\forall y |A|^x_y$ is content of A

Applications in proof theory

Consistency If S is consistent then T is consistent

$|\perp| \equiv \perp$

$\mathsf{T} \vdash \exists x \forall y |A|^x_y \to A' \qquad (\mathsf{S} \subseteq \mathsf{T})$

$\mathsf{S} \vdash \exists x \forall y |A|^x_y \to A$

$\mathsf{S} \nvdash \exists x \forall y |A|^x_y$

x in $\forall y |A|^x_y$ is content of A

Applications in proof theory

Consistency If S is consistent then T is consistent

$| \perp | \equiv \perp$

Closure T proves A then T proves A'

$\mathrm{T} \vdash \exists x \forall y |A|^x_y \to A'$ (S $\subseteq$ T)

$\mathrm{S} \vdash \exists x \forall y |A|^x_y \to A$

$\mathrm{S} \nvdash \exists x \forall y |A|^x_y$

x in $\forall y |A|^x_y$ is content of A

Applications in proof theory

Consistency	If S is consistent then T is consistent $\mid \bot \mid \equiv \bot$
Closure	T proves A then T proves A' $T \vdash \exists x \forall y \lvert A \rvert_y^x \rightarrow A'$ (S $\subseteq$ T)
Conservation	If T proves A then S proves A, for $A \in \Delta$ $S \vdash \exists x \forall y \lvert A \rvert_y^x \rightarrow A$

$S \nvdash \exists x \forall y |A|_y^x$

x in $\forall y |A|_y^x$ is content of A

Applications in proof theory

Consistency If S is consistent then T is consistent
$|\perp| \equiv \perp$

Closure T proves A then T proves A'
$\mathrm{T} \vdash \exists x \forall y |A|^x_y \to A'$ $\quad$ $(\mathrm{S} \subseteq \mathrm{T})$

Conservation If T proves A then S proves A, for A $\in \Delta$
$\mathrm{S} \vdash \exists x \forall y |A|^x_y \to A$

Independence T does not prove A
$\mathrm{S} \not\vdash \exists x \forall y |A|^x_y$

x in $\forall y |A|^x_y$ is content of A

Applications in proof theory

Consistency	If S is consistent then T is consistent $\lvert \perp \rvert \equiv \perp$
Closure	T proves A then T proves A' $T \vdash \exists x \forall y \lvert A\rvert^x_y \to A'$ (S $\subseteq$ T)
Conservation	If T proves A then S proves A, for $A \in \Delta$ $S \vdash \exists x \forall y \lvert A\rvert^x_y \to A$
Independence	T does not prove A $S \nvdash \exists x \forall y \lvert A\rvert^x_y$
Computation	Algorithm associated with proof of A x in $\forall y \lvert A\rvert^x_y$ is content of A

Formula translation

$$
\begin{array}{lcl}
|A_{\mathrm{at}}| & :\equiv & A_{\mathrm{at}} \\
|A \wedge B|^{x,v} & :\equiv & |A|^{x} \wedge |B|^{v} \\
|A \vee B|^{x,v,n} & :\equiv & |A|^{x} \vee_n |B|^{v} \\
|A \to B|^{f} & :\equiv & \forall x(|A|^{x} \to |B|^{fx}) \\
|\forall z A(z)|^{f} & :\equiv & \forall z |A(z)|^{fz} \\
|\exists z A(z)|^{x,z} & :\equiv & |A(z)|^{x}
\end{array}
$$

$$A \vee_n B :\equiv (n = 0 \to A) \wedge (n \neq 0 \to B)$$

Formula translation

$$
\begin{array}{lcl}
|A_{\mathrm{at}}| & :\equiv & A_{\mathrm{at}} \\
|A \wedge B|^{x,v} & :\equiv & |A|^{x} \wedge |B|^{v} \\
|A \vee B|^{x,v,n} & :\equiv & |A|^{x} \vee_n |B|^{v} \\
|A \to B|^{f}_{x} & :\equiv & |A|^{x} \to |B|^{fx} \\
|\forall z A(z)|^{f}_{z} & :\equiv & |A(z)|^{fz} \\
|\exists z A(z)|^{x,z} & :\equiv & |A(z)|^{x}
\end{array}
$$

$$A \vee_n B :\equiv (n = 0 \to A) \wedge (n \neq 0 \to B)$$

Formula translation

$$
\begin{array}{lcl}
|A_{\mathrm{at}}| & :\equiv & A_{\mathrm{at}} \\
|A \wedge B|^{x,v}_{y,w} & :\equiv & |A|^x_y \wedge |B|^v_w \\
|A \vee B|^{x,v,n}_{y,w} & :\equiv & |A|^x_y \vee_n |B|^v_w \\
|A \to B|^{f}_{x,w} & :\equiv & |A|^x_y \to |B|^{fx}_w \\
|\forall z A(z)|^{f}_{y,z} & :\equiv & |A(z)|^{fz}_y \\
|\exists z A(z)|^{x,z}_{y} & :\equiv & |A(z)|^{x}_y
\end{array}
$$

$$A \vee_n B :\equiv (n = 0 \to A) \wedge (n \neq 0 \to B)$$

Formula translation

$$
\begin{array}{lcl}
|A_{\mathrm{at}}| & :\equiv & A_{\mathrm{at}} \\
|A \wedge B|^{x,v}_{y,w} & :\equiv & |A|^x_y \wedge |B|^v_w \\
|A \vee B|^{x,v,n}_{y,w} & :\equiv & |A|^x_y \vee_n |B|^v_w \\
|A \to B|^f_{x,w} & :\equiv & \forall y |A|^x_y \to |B|^{fx}_w \\
|\forall z A(z)|^f_{y,z} & :\equiv & |A(z)|^{fz}_y \\
|\exists z A(z)|^{x,z}_y & :\equiv & |A(z)|^x_y
\end{array}
$$

$$A \vee_n B :\equiv (n = 0 \to A) \wedge (n \neq 0 \to B)$$

Formula translation

$$
\begin{array}{lcl}
|A_{\mathrm{at}}| & :\equiv & A_{\mathrm{at}} \\
|A \wedge B|^{x,v}_{y,w} & :\equiv & |A|^x_y \wedge |B|^v_w \\
|A \vee B|^{x,v,n}_{y,w} & :\equiv & |A|^x_y \vee_n |B|^v_w \\
|A \rightarrow B|^{f,g}_{x,w} & :\equiv & \forall y \sqsubset gxw |A|^x_y \rightarrow |B|^{fx}_w \\
|\forall z A(z)|^f_{y,z} & :\equiv & |A(z)|^{fz}_y \\
|\exists z A(z)|^{x,z}_y & :\equiv & |A(z)|^x_y
\end{array}
$$

$$
A \vee_n B :\equiv (n = 0 \rightarrow A) \wedge (n \neq 0 \rightarrow B)
$$

Formula translation (parametrised)

$$
\begin{array}{lcl}
|A_{\mathrm{at}}| & :\equiv & A_{\mathrm{at}} \\
|A \wedge B|^{x,v}_{y,w} & :\equiv & |A|^x_y \wedge |B|^v_w \\
|A \vee B|^{x,v,n}_{y,w} & :\equiv & |A|^x_y \vee_n |B|^v_w \\
|A \to B|^{f,g}_{x,w} & :\equiv & \forall y \sqsubset gxw |A|^x_y \to |B|^{fx}_w \\
|\forall z A(z)|^{f}_{y,z} & :\equiv & |A(z)|^{fz}_y \\
|\exists z A(z)|^{x,z}_{y} & :\equiv & |A(z)|^x_y
\end{array}
$$

$$A \vee_n B :\equiv (n = 0 \to A) \wedge (n \neq 0 \to B)$$

Concrete instantiations

1958. Gödel's Dialectica interpretation
- *Relative consistency of* PA

1959. Kreisel's modified realizability
- *Independence results, unwinding proofs*

1974. Diller-Nahm variant of Dialectica interpretation
- *Solve contraction problem*

1978. Stein's family of functional interpretations
- *Relate modified realizability and Diller-Nahm's*

1992. Monotone functional interpretation
- *Proof mining*

Outline

1. Functional Interpretations
2. **Three Applications**
3. Conclusions

Sources of ineffectiveness

- Classical logic $A \vee \neg A$
- Countable choice $\forall n^{\mathbb{N}} \exists k^{\mathbb{N}} A(n,k) \rightarrow \exists f \forall n A(n, fn)$
  - $A \equiv$ recursive predicate
  - $A \equiv$ arithmetic predicates

Sources of ineffectiveness

- Classical logic $A \vee \neg A$
  (eliminated via negative translation)
- Countable choice $\forall n^{\mathbb{N}} \exists k^{\mathbb{N}} A(n,k) \to \exists f \forall n A(n, fn)$
  - $A \equiv$ recursive predicate
  - $A \equiv$ arithmetic predicates

Sources of ineffectiveness

- Classical logic $A \vee \neg A$
  (eliminated via negative translation)
- Countable choice $\forall n^{\mathbb{N}} \exists k^{\mathbb{N}} A(n,k) \to \exists f \forall n A(n, fn)$
  - $A \equiv$ recursive predicate
    (easy)
  - $A \equiv$ arithmetic predicates

Sources of ineffectiveness

- Classical logic $A \vee \neg A$
  (eliminated via negative translation)

- Countable choice $\forall n^{\mathbb{N}} \exists k^{\mathbb{N}} A(n,k) \to \exists f \forall n A(n, fn)$
  - $A \equiv$ recursive predicate
    (easy)
  - $A \equiv$ arithmetic predicates
    (hard)

Sources of ineffectiveness

- Classical logic $A \vee \neg A$
  (eliminated via negative translation)

- Countable choice $\forall n^{\mathbb{N}} \exists k^{\mathbb{N}} A(n,k) \rightarrow \exists f \forall n A(n, fn)$
  - $A \equiv$ recursive predicate
    (easy)

    weak König lemma
  - $A \equiv$ arithmetic predicates
    (hard)

Weak König Lemma

Every infinite finitely branching tree has an infinite path

Equivalent (over RCA_0) to Heine-Borel compactness

Formally:

$$\mathrm{WKL} \quad : \quad \forall f \left(\mathrm{bT}(f) \wedge \forall n \exists s^{\mathbb{B}^n}(s \in f) \to \exists \alpha^{\mathbb{B}^\omega} \forall n (\overline{\alpha} n \in f) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \left(\exists s^{\mathbb{B}^n}(s \in f^{\mathrm{bt}}) \to \exists \alpha^{\mathbb{B}^\omega} (\overline{\alpha} n \in f^{\mathrm{bt}}) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \exists \alpha^{\mathbb{B}^\omega} \forall n \left(\exists s^{\mathbb{B}^n}(s \in f^{\mathrm{bt}}) \to (\overline{\alpha} n \in f^{\mathrm{bt}}) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \exists \alpha \leq 1 \forall n \left(\exists s \leq t[n] A_0(s, f) \to A_0(\overline{\alpha} n, f) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \exists \alpha \leq 1 \forall n A_{\mathrm{b}}(f, \alpha, n)$$

$$\mathrm{WKL} \quad : \quad \exists \alpha_f \leq 1 \forall f, n A_{\mathrm{b}}(f, \alpha_f, n)$$

Weak König Lemma

Every infinite finitely branching tree has an infinite path

Equivalent (over RCA_0) to Heine-Borel compactness

Formally:

$$\mathrm{WKL} \quad : \quad \forall f \left(\mathrm{bT}(f) \wedge \forall n \exists s^{\mathbb{B}^n}(s \in f) \rightarrow \exists \alpha^{\mathbb{B}^\omega} \forall n (\overline{\alpha} n \in f) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \left(\forall n \exists s^{\mathbb{B}^n}(s \in f^{\mathrm{bt}}) \rightarrow \exists \alpha^{\mathbb{B}^\omega} \forall n (\overline{\alpha} n \in f^{\mathrm{bt}}) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \exists \alpha^{\mathbb{B}^\omega} \forall n \left(\exists s^{\mathbb{B}^n}(s \in f^{\mathrm{bt}}) \rightarrow (\overline{\alpha} n \in f^{\mathrm{bt}}) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \exists \alpha \leq 1 \forall n \left(\exists s \leq t[n] A_0(s, f) \rightarrow A_0(\overline{\alpha} n, f) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \exists \alpha \leq 1 \forall n A_{\mathrm{b}}(f, \alpha, n)$$

$$\mathrm{WKL} \quad : \quad \exists \alpha_f \leq 1 \forall f, n A_{\mathrm{b}}(f, \alpha_f, n)$$

Weak König Lemma

Every infinite finitely branching tree has an infinite path

Equivalent (over RCA_0) to Heine-Borel compactness

Formally:

$$\mathrm{WKL} \quad : \quad \forall f \left(\mathrm{bT}(f) \wedge \forall n \exists s^{\mathbb{B}^n} (s \in f) \to \exists \alpha^{\mathbb{B}^\omega} \forall n (\overline{\alpha} n \in f) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \left(\forall n \exists s^{\mathbb{B}^n} (s \in f^{\mathrm{bt}}) \to \exists \alpha^{\mathbb{B}^\omega} \forall n (\overline{\alpha} n \in f^{\mathrm{bt}}) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \exists \alpha^{\mathbb{B}^\omega} \forall n \left(\exists s^{\mathbb{B}^n} (s \in f^{\mathrm{bt}}) \to (\overline{\alpha} n \in f^{\mathrm{bt}}) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \exists \alpha \leq 1 \forall n \left(\exists s \leq t[n] A_0(s, f) \to A_0(\overline{\alpha} n, f) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \exists \alpha \leq 1 \forall n A_{\mathrm{b}}(f, \alpha, n)$$

$$\mathrm{WKL} \quad : \quad \exists \alpha_f \leq 1 \forall f, n A_{\mathrm{b}}(f, \alpha_f, n)$$

Weak König Lemma

Every infinite finitely branching tree has an infinite path

Equivalent (over RCA_0) to Heine-Borel compactness

Formally:

$$\mathrm{WKL} \quad : \quad \forall f \left(\mathrm{bT}(f) \wedge \forall n \exists s^{\mathbb{B}^n}(s \in f) \to \exists \alpha^{\mathbb{B}^\omega} \forall n (\overline{\alpha} n \in f) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \left(\forall n \exists s^{\mathbb{B}^n}(s \in f^{\mathrm{bt}}) \to \exists \alpha^{\mathbb{B}^\omega} \forall n (\overline{\alpha} n \in f^{\mathrm{bt}}) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \exists \alpha^{\mathbb{B}^\omega} \forall n \left(\exists s^{\mathbb{B}^n}(s \in f^{\mathrm{bt}}) \to (\overline{\alpha} n \in f^{\mathrm{bt}}) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \exists \alpha \leq 1 \forall n \left(\exists s \leq t[n] A_0(s, f) \to A_0(\overline{\alpha} n, f) \right)$$

$$\mathrm{WKL} \quad : \quad \forall f \exists \alpha \leq 1 \forall n A_{\mathrm{b}}(f, \alpha, n)$$

$$\mathrm{WKL} \quad : \quad \exists \alpha_f \leq 1 \forall f, n A_{\mathrm{b}}(f, \alpha_f, n)$$

Weak König Lemma

Every infinite finitely branching tree has an infinite path

Equivalent (over RCA_0) to Heine-Borel compactness

Formally:

$$\mathsf{WKL} \quad : \quad \forall f \left(\mathrm{bT}(f) \wedge \forall n \exists s^{\mathbb{B}^n}(s \in f) \rightarrow \exists \alpha^{\mathbb{B}^\omega} \forall n(\overline{\alpha}n \in f) \right)$$

$$\mathsf{WKL} \quad : \quad \forall f \left(\forall n \exists s^{\mathbb{B}^n}(s \in f^{\mathrm{bt}}) \rightarrow \exists \alpha^{\mathbb{B}^\omega} \forall n(\overline{\alpha}n \in f^{\mathrm{bt}}) \right)$$

$$\mathsf{WKL} \quad : \quad \forall f \exists \alpha^{\mathbb{B}^\omega} \forall n \left(\exists s^{\mathbb{B}^n}(s \in f^{\mathrm{bt}}) \rightarrow (\overline{\alpha}n \in f^{\mathrm{bt}}) \right)$$

$$\mathsf{WKL} \quad : \quad \forall f \exists \alpha \leq 1 \forall n \left(\exists s \leq t[n] A_0(s, f) \rightarrow A_0(\overline{\alpha}n, f) \right)$$

$$\mathsf{WKL} \quad : \quad \forall f \exists \alpha \leq 1 \forall n A_{\mathrm{b}}(f, \alpha, n)$$

$$\mathsf{WKL} \quad : \quad \exists \alpha_f \leq 1 \forall f, n A_{\mathrm{b}}(f, \alpha_f, n)$$

Weak König Lemma

Every infinite finitely branching tree has an infinite path

Equivalent (over RCA_0) to Heine-Borel compactness

Formally:

$$\mathsf{WKL} \quad : \quad \forall f \left(\mathrm{bT}(f) \wedge \forall n \exists s^{\mathbb{B}^n} (s \in f) \to \exists \alpha^{\mathbb{B}^\omega} \forall n (\overline{\alpha} n \in f) \right)$$

$$\mathsf{WKL} \quad : \quad \forall f \left(\forall n \exists s^{\mathbb{B}^n} (s \in f^{\mathrm{bt}}) \to \exists \alpha^{\mathbb{B}^\omega} \forall n (\overline{\alpha} n \in f^{\mathrm{bt}}) \right)$$

$$\mathsf{WKL} \quad : \quad \forall f \exists \alpha^{\mathbb{B}^\omega} \forall n \left(\exists s^{\mathbb{B}^n} (s \in f^{\mathrm{bt}}) \to (\overline{\alpha} n \in f^{\mathrm{bt}}) \right)$$

$$\mathsf{WKL} \quad : \quad \forall f \exists \alpha \leq 1 \forall n \left(\exists s \leq t[n] A_0(s, f) \to A_0(\overline{\alpha} n, f) \right)$$

$$\mathsf{WKL} \quad : \quad \forall f \exists \alpha \leq 1 \forall n A_{\mathrm{b}}(f, \alpha, n)$$

$$\mathsf{WKL} \quad : \quad \exists \alpha_f \leq 1 \forall f, n A_{\mathrm{b}}(f, \alpha_f, n)$$

Formal systems: Heyting arithmetic HA^ω

- Universal axioms for 0 and S
- Gödel's primitive recursion
- Induction rule

$$\frac{\vdash A(0) \qquad A(n) \vdash A(n+1)}{\vdash A(n)} \text{ (IND)}$$

- $\mathsf{PA}^\omega \equiv \mathsf{HA}^\omega + \mathsf{LEM}$

Formal systems: Others

System	Induction	Subsystem of
$\widehat{\mathrm{PA}}^{\omega}\restriction$	semi-decidable	
RCA_0	semi-decidable	$\widehat{\mathrm{PA}}^{\omega}\restriction + \mathrm{AC}_{\mathrm{qf}}$
PRA	decidable	
CPV^{ω}	NP	$\widehat{\mathrm{PA}}^{\omega}\restriction$
BTFA	NP	$\mathrm{CPV}^{\omega} + \mathrm{AC}_{\mathrm{qf}}$
PV	P	CPV^{ω}

Three results about WKL

Theorem (Friedman)

$\mathsf{RCA}_0 + \mathsf{WKL}$ *is* Π^0_2*-conservative over* PRA

Theorem (Ferreira)

$\mathsf{BTFA} + \mathsf{WKL}_{\mathsf{bd}}$ *is* Π^0_2*-conservative over* PV

Corollary (Ferreira)

Π^0_2*-theorems of* $\mathsf{BTFA} + \mathsf{WKL}_{\mathsf{qf}}$ *have poly-time realizers*

Three results about WKL

Theorem (Friedman)

$\mathrm{RCA}_0 + \mathrm{WKL}$ *is* Π^0_2*-conservative over* PRA

Effective version: Monotone functional interpretation

Theorem (Ferreira)

$\mathrm{BTFA} + \mathrm{WKL}_{\mathrm{bd}}$ *is* Π^0_2*-conservative over* PV

Corollary (Ferreira)

Π^0_2*-theorems of* $\mathrm{BTFA} + \mathrm{WKL}_{\mathrm{qf}}$ *have poly-time realizers*

Three results about WKL

Theorem (Friedman)

$\mathrm{RCA}_0 + \mathrm{WKL}$ *is* Π^0_2*-conservative over* PRA

Effective version: Monotone functional interpretation

Theorem (Ferreira)

$\mathrm{BTFA} + \mathrm{WKL}_{\mathrm{bd}}$ *is* Π^0_2*-conservative over* PV

Corollary (Ferreira)

Π^0_2*-theorems of* $\mathrm{BTFA} + \mathrm{WKL}_{\mathrm{qf}}$ *have poly-time realizers*

Effective version: Gödel's functional interpretation

Three results about WKL

Theorem (Friedman)

$\mathsf{RCA}_0 + \mathsf{WKL}$ *is* Π^0_2*-conservative over* PRA

Effective version: Monotone functional interpretation

Theorem (Ferreira)

$\mathsf{BTFA} + \mathsf{WKL}_{\mathsf{bd}}$ *is* Π^0_2*-conservative over* PV

Effective version: Bounded functional interpretation

Corollary (Ferreira)

Π^0_2*-theorems of* $\mathsf{BTFA} + \mathsf{WKL}_{\mathsf{qf}}$ *have poly-time realizers*

Effective version: Gödel's functional interpretation

1. Monotone functional interpretation

Theorem (Friedman)

$\widehat{\mathrm{PA}}^{\omega}\!\restriction + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}$ *is* Π^0_2*-conservative over* PRA

Proof (Kohlenbach'92).

$\square$

1. Monotone functional interpretation

Theorem (Friedman)

$\widehat{\mathrm{PA}}^{\omega}\!\restriction + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}$ *is* Π^0_2*-conservative over* PRA

Proof (Kohlenbach'92).

1. $\widehat{\mathrm{HA}}^{\omega}\!\restriction + \mathrm{MP} + \mathrm{AC}_{\mathrm{qf}} \vdash \exists \alpha_f \forall f, n A_{\mathrm{b}}(f, \alpha_f, n) \to \forall x \exists y A_0(x, y)$

□

1. Monotone functional interpretation

Theorem (Friedman)

$\widehat{\mathrm{PA}}^{\omega}\!\restriction + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}$ *is* Π^0_2*-conservative over* PRA

Proof (Kohlenbach'92).

1. $\widehat{\mathrm{HA}}^{\omega}\!\restriction + \mathrm{MP} + \mathrm{AC}_{\mathrm{qf}} \vdash \exists \alpha_f \forall f, n A_{\mathrm{b}}(f, \alpha_f, n) \to \forall x \exists y A_0(x, y)$
2. By m.f.i. there exists a monotone q such that $\widehat{\mathrm{HA}}^{\omega}\!\restriction \vdash \forall x (\exists \alpha_f \forall f, n \leq q[\alpha_f, x] A_{\mathrm{b}}(f, \alpha_f, n) \to \exists y A_0(x, y))$

□

1. Monotone functional interpretation

Theorem (Friedman)

$\widehat{\mathrm{PA}}^{\omega}\!\restriction + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}$ *is* Π^0_2*-conservative over* PRA

Proof (Kohlenbach'92).

1. $\widehat{\mathrm{HA}}^{\omega}\!\restriction + \mathrm{MP} + \mathrm{AC}_{\mathrm{qf}} \vdash \exists \alpha_f \forall f, n A_{\mathrm{b}}(f, \alpha_f, n) \to \forall x \exists y A_0(x, y)$
2. By m.f.i. there exists a monotone q such that $\widehat{\mathrm{HA}}^{\omega}\!\restriction \vdash \forall x (\exists \alpha_f \forall f, n \leq q[\alpha_f, x] A_{\mathrm{b}}(f, \alpha_f, n) \to \exists y A_0(x, y))$
3. By monotonicity of q $\widehat{\mathrm{HA}}^{\omega}\!\restriction \vdash \forall x (\exists \alpha_f \forall f, n \leq q[1, x] A_{\mathrm{b}}(f, \alpha_f, n) \to \exists y A_0(x, y))$

□

1. Monotone functional interpretation

Theorem (Friedman)

$\widehat{\mathrm{PA}}^{\omega}\!\restriction + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}$ *is* Π^0_2*-conservative over* PRA

Proof (Kohlenbach'92).

1. $\widehat{\mathrm{HA}}^{\omega}\!\restriction + \mathrm{MP} + \mathrm{AC}_{\mathrm{qf}} \vdash \exists \alpha_f \forall f, n A_{\mathrm{b}}(f, \alpha_f, n) \to \forall x \exists y A_0(x, y)$
2. By m.f.i. there exists a monotone q such that $\widehat{\mathrm{HA}}^{\omega}\!\restriction \vdash \forall x (\exists \alpha_f \forall f, n \leq q[\alpha_f, x] A_{\mathrm{b}}(f, \alpha_f, n) \to \exists y A_0(x, y))$
3. By monotonicity of q $\widehat{\mathrm{HA}}^{\omega}\!\restriction \vdash \forall x (\exists \alpha_f \forall f, n \leq q[1, x] A_{\mathrm{b}}(f, \alpha_f, n) \to \exists y A_0(x, y))$
4. $\widehat{\mathrm{HA}}^{\omega}\!\restriction \vdash \forall x \exists \alpha_f \forall f, n \leq q[1, x] A_{\mathrm{b}}(f, \alpha_f, n)$

□

2. Dialectica interpretation

Corollary (Ferreira)

Π^0_2*-theorems of* $\mathrm{CPV}^\omega + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}_{\mathrm{qf}}$ *have poly-time realizers*

Proof (Oliva'03).

$\square$

2. Dialectica interpretation

Corollary (Ferreira)

Π^0_2*-theorems of* $\mathrm{CPV}^\omega + \mathrm{AC_{qf}} + \mathrm{WKL_{qf}}$ *have poly-time realizers*

Proof (Oliva'03).

1. $\mathrm{CPV}^\omega + \mathrm{AC_{qf}} \overset{N+D}{\mapsto} \mathrm{IPV}^\omega$ (Cook/Urquhart'92)

□

2. Dialectica interpretation

Corollary (Ferreira)

Π^0_2*-theorems of* $\mathrm{CPV}^\omega + \mathrm{AC_{qf}} + \mathrm{WKL_{qf}}$ *have poly-time realizers*

Proof (Oliva'03).

1. $\mathrm{CPV}^\omega + \mathrm{AC_{qf}} \overset{N+D}{\mapsto} \mathrm{IPV}^\omega$ (Cook/Urquhart'92)
2. Realizer for $(\mathrm{WKL_{qf}})^D$ using $(w_z :\equiv Wz)$

$$\mathcal{B}(z) = \begin{cases} z & \text{if } |Y\hat{w}_z| \leq |w_z| \text{ or } |w_z| \neq |z| \\ \mathcal{B}(z*1) & \text{otherwise,} \end{cases}$$

□

2. Dialectica interpretation

Corollary (Ferreira)

Π^0_2*-theorems of* $\mathrm{CPV}^\omega + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}_{\mathrm{qf}}$ *have poly-time realizers*

Proof (Oliva'03).

1. $\mathrm{CPV}^\omega + \mathrm{AC}_{\mathrm{qf}} \overset{N+D}{\mapsto} \mathrm{IPV}^\omega$ (Cook/Urquhart'92)
2. Realizer for $(\mathrm{WKL}_{\mathrm{qf}})^D$ using $(w_z :\equiv Wz)$

$$\mathcal{B}(z) = \begin{cases} z & \text{if } |Y\hat{w}_z| \leq |w_z| \text{ or } |w_z| \neq |z| \\ \mathcal{B}(z * 1) & \text{otherwise,} \end{cases}$$

3. Type 1 terms of $\mathrm{IPV}^\omega + \mathcal{B}$ are poly-time

□

3. Bounded functional interpretation

Theorem (Ferreira)

$\mathrm{CPV}^{\omega} + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}_{\mathrm{bd}}$ *is* Π^0_2*-conservative over* PV

Proof (Ferreira/Oliva'05).

□

3. Bounded functional interpretation

Theorem (Ferreira)

$\mathrm{CPV}^\omega + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}_{\mathrm{bd}}$ *is* Π^0_2*-conservative over* PV

Proof (Ferreira/Oliva'05).

1. $\mathrm{IPV}^\omega + \mathrm{MP} + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}_{\mathrm{bd}} \vdash A$

□

3. Bounded functional interpretation

Theorem (Ferreira)

$\mathrm{CPV}^{\omega} + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}_{\mathrm{bd}}$ *is* Π^0_2*-conservative over* PV

Proof (Ferreira/Oliva'05).

1. $\mathrm{IPV}^{\omega} + \mathrm{MP} + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}_{\mathrm{bd}} \vdash A$
2. $\mathrm{WKL}_{\mathrm{bd}}$ follows from $\mathrm{BCC}_{\mathrm{bd}}$
   $\mathrm{BCC}_{\mathrm{bd}} \ : \ \forall b \exists f \leq t \forall x \leq b A_{\mathrm{b}}(x, f) \rightarrow \exists f \leq t \forall x A_{\mathrm{b}}(x, f)$

□

3. Bounded functional interpretation

Theorem (Ferreira)

$\mathrm{CPV}^\omega + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}_{\mathrm{bd}}$ *is* Π^0_2*-conservative over* PV

Proof (Ferreira/Oliva'05).

1. $\mathrm{IPV}^\omega + \mathrm{MP} + \mathrm{AC}_{\mathrm{qf}} + \mathrm{WKL}_{\mathrm{bd}} \vdash A$
2. $\mathrm{WKL}_{\mathrm{bd}}$ follows from $\mathrm{BCC}_{\mathrm{bd}}$
   $\mathrm{BCC}_{\mathrm{bd}} \; : \; \forall b \exists f \leq t \forall x \leq b A_{\mathrm{b}}(x, f) \to \exists f \leq t \forall x A_{\mathrm{b}}(x, f)$
3. $\mathrm{IPV}^\omega \vdash (\mathrm{BCC}_{\mathrm{bd}})^B$

□

Different approaches

1. Weakened
2. Interpreted by functional
3. Interpreted by interpretation

Outline

What about other proof-theoretic techniques?

Proof theory tools

Other ways to give computational meaning to proofs:

- Herbrand's theorem
- Cut elimination
- Formuale-as-types isomorphism

Herbrand's theorem

$$\exists x A(x)$$

$$\Big\downarrow \textit{Herb.thm.}$$

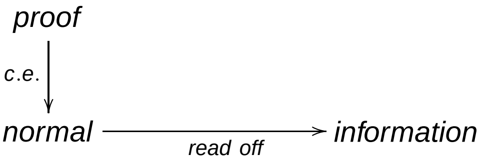
$$A(t_0) \vee \ldots \vee A(t_n)$$

Herbrand's theorem

$$\begin{array}{ccc} \exists x A(x) & \xrightarrow{\textit{neg. trans.}} & \neg\forall x \neg A(x) \\ \Big\downarrow \textit{Herb.thm.} & & \Big\downarrow \textit{f.i.} \\ A(t_0) \vee \ldots \vee A(t_n) & \xleftarrow{\textit{norm.} + \textit{cases}} & \neg\neg A(t) \end{array}$$

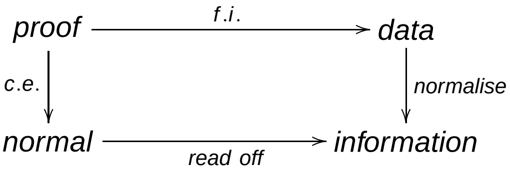
- Kohlenbach/Gerhardy'05
  Proof of Herbrand's theorem via Dialectica interpretation

Cut elimination



- **Cut elimination**
  normalises the proof, information can be easily read off

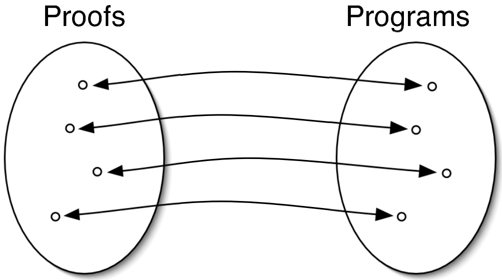
Cut elimination



- **Cut elimination**
  normalises the proof, information can be easily read off
- **Functional interpretations**
  get raw data from original proof, normalise to get info

Formulae-as-types isomorphism

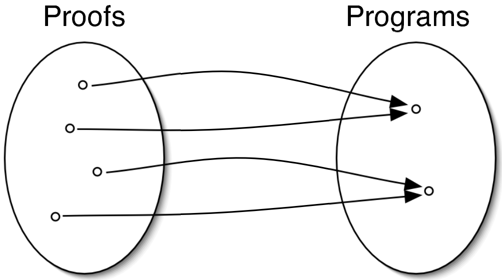
Formulae-as-types isomorphism



Program corresponds to proof

Formulae-as-types isomorphism

Functional interpretation



Program captures “essence” of proof!

Summary

- Uses
  - proof-theoretic results
  - unwind of proofs, proof mining
- Characteristics
  - *modular*: applicable to real-life proofs
  - *adaptable*: many variations, different uses
  - *context*: classical proofs, analysis