Gödel's Dialectica Interpretation

Helmut Schwichtenberg

Mathematisches Institut der Universität München

Map 2007, 12. Jan. 2007, Leiden, Holland

Mathematics – Algorithms – Proofs

Here: $\tilde{\exists}$, weak (or "classical") existence.

Theorem (Euclid)

The gcd of two natural numbers is a linear combination of the two.

Proof.

The ideal (a_1, a_2) is principal, $= (d)$.
d is the gcd, and a linear combination of a_1, a_2. □

Gödel's Dialectica Interpretation (1958)

Theorem (Extraction)

$$\mathsf{KA}^{\omega} + (\mathrm{QF\text{-}\tilde{A}C}) + \cdots + \mathrm{Ax}^{-} \vdash \forall_y \tilde{\exists}_z B^{+}(y,z)$$

implies

$$\mathsf{KA}^{\omega} + \mathrm{Ax}^{-} \vdash \forall_y B^{+}(y, ty).$$

Notions used

- $\tilde{\exists}$ means $\neg\forall\neg$, and $\neg A := A \to \bot$.
- A^-: no positive content, $\tau^+(A) = \varepsilon$.
  B^+: no negative content, $\tau^-(B) = \varepsilon$.
- $(\mathrm{QF\text{-}\tilde{A}C})$: $\forall_x \tilde{\exists}_y A_0(x,y) \to \tilde{\exists}_f \forall_x A_0(x, fx)$.
- KA^ω = Kolmogorov arithmetic (1925), in finite types.

Positive and negative content of a formula A

$$\tau^+(P(\vec{s})) := \varepsilon \qquad \tau^-(P(\vec{s})) := \varepsilon,$$
$$\tau^+(\forall_{x^\rho} A) := \rho \Rightarrow \tau^+(A), \qquad \tau^-(\forall_{x^\rho} A) := \rho \otimes \tau^-(A),$$
$$\tau^+(\exists_{x^\rho} A) := \rho \otimes \tau^+(A), \qquad \tau^-(\exists_{x^\rho} A) := \tau^-(A).$$

and for implication

$$\tau^+(A \to B) := \big(\tau^+(A) \Rightarrow \tau^+(B)\big) \otimes \big(\tau^+(A) \Rightarrow \tau^-(B) \Rightarrow \tau^-(A)\big),$$
$$\tau^-(A \to B) := \tau^+(A) \otimes \tau^-(B).$$

Lemma (Characterization)

(a) $\tau^+(A) = \varepsilon$ *iff* A *without negative* $\forall$, *positive* $\exists$.

(b) $\tau^-(A) = \varepsilon$ *iff* A *without positive* $\forall$, *negative* $\exists$.

KA^ω

Kolmogorov arithmetic (1925), in finite types.

- Finite types: built from finitary base types by $\rho \Rightarrow \sigma$, $\rho \otimes \sigma$.
- Quantifiers range over the Scott-Ershov partial continuous functionals. Totality defined.
- $0 = 1$ for falsity, no negation.
- Formulas and types kept separate (no dependent types).
- $\mathcal{R}$ and Ind.
- $\vdash$ = natural deduction.

Proof of the extraction theorem

needs

- Gödel translation $A \mapsto \exists_x \forall_y |A|^x_y$.
- A more general formulation.

Theorem (Soundness)

Assume

$$\text{WE-KA}^\omega + \text{AC} + \text{IP}^- + \text{MP} + \text{Ax}^- \vdash A\,[u_i : C_i].$$

Pick $x_i^{\tau^+(C_i)}$ *and* $y^{\tau^-(A)}$. *Then we can find terms* $[\![M]\!]^+ =: t^{\tau^+(A)}$ *with* $y \notin \text{FV}(t)$ *and* $[\![M]\!]^-_i =: r_i^{\tau^-(C_i)}$:

$$\text{WE-KA}^\omega + \text{Ax}^- \vdash |A|^t_y\,[\bar{u}_i : |C_i|^{x_i}_{r_i}].$$

Proof: by induction on derivations terms.

Gödel translation

$$
\begin{aligned}
|P(\vec{s})|^r_s &:= P(\vec{s}),\\
|\forall_x A(x)|^r_s &:= |A(s0)|^{r(s0)}_{s1},\\
|\exists_x A(x)|^r_s &:= |A(r0)|^{r1}_{s},\\
|A \to B|^r_s &:= |A|^{s0}_{r1(s0)(s1)} \to |B|^{r0(s0)}_{s1}.
\end{aligned}
$$

For readability: write terms of a pair type in pair form. Then

$$
\begin{aligned}
|\forall_z A|^x_{z,y} &:= |A|^{xz}_{y},\\
|\exists_z A|^{z,x}_{y} &:= |A|^{x}_{y},\\
|A \to B|^{f,g}_{x,u} &:= |A|^{x}_{gxu} \to |B|^{fx}_{u}.
\end{aligned}
$$

Theorem (Euclid). Assume $0 < a_2$. There are k_1, k_2 such that $0 < |k_1 a_1 - k_2 a_2|$ and $\mathrm{Rem}(a_i, |k_1 a_1 - k_2 a_2|) = 0$ $(i = 1, 2)$.

Proof. There are k_1, k_2 such that $0 < |k_1 a_1 - k_2 a_2|$. The Minimum Principle with measure $|k_1 a_1 - k_2 a_2|$ gives k_1, k_2:

$$A(k_1, k_2) \quad (:= (0 < |k_1 a_1 - k_2 a_2|)), \tag{1}$$

$$\forall_{l_1, l_2}\big(|l_1 a_1 - l_2 a_2| < |k_1 a_1 - k_2 a_2| \to A(l_1, l_2) \to \bot\big). \tag{2}$$

Assume

$$\begin{aligned}\forall_{k_1, k_2}(0 < |k_1 a_1 - k_2 a_2| \to \mathrm{Rem}(a_1, |k_1 a_1 - k_2 a_2|) = 0 \to \\ \mathrm{Rem}(a_2, |k_1 a_1 - k_2 a_2|) = 0 \to \bot).\end{aligned} \tag{3}$$

Show $\bot$. Use (3) for k_1, k_2. Need $\mathrm{Rem}(a_i, |k_1 a_1 - k_2 a_2|) = 0$, by (1).

$$q := \mathrm{Quot}(a_1, |k_1 a_1 - k_2 a_2|), \quad r := \mathrm{Rem}(a_1, |k_1 a_1 - k_2 a_2|).$$

$$a_1 = q|k_1 a_1 - k_2 a_2| + r, \quad r < |k_1 a_1 - k_2 a_2| \quad (\text{use } 0 < |k_1 a_1 - k_2 a_2|).$$

From this $r = |\underbrace{\mathrm{Step}(a_1, a_2, k_1, k_2, q)}_{=: l_1} a_1 - \underbrace{q k_2}_{=: l_2} a_2| < |k_1 a_1 - k_2 a_2|$.

(2) for l_1, l_2 gives $A(l_1, l_2) \to \bot$. Hence $0 = |l_1 a_1 - l_2 a_2| = r$.

The Step function

Want

$$a_1 = q \cdot |k_1 a_1 - k_2 a_2| + r \rightarrow$$
$$r = |\mathrm{Step}(a_1, a_2, k_1, k_2, q) a_1 - q k_2 a_2|.$$

Let

$$\mathrm{Step}(a_1, a_2, k_1, k_2, q) := \begin{cases} q k_1 - 1 & \text{if } k_2 a_2 < k_1 a_1 \text{ and } 0 < q, \\ q k_1 + 1 & \text{otherwise.} \end{cases}$$

```
[n0,n1] [let pf7 ((Rec nat=>nat@@nat=>nat@@nat)([p3]0@0)
   ([n3,pf4,p5] [if (0<Lin n0 n1 p5 impb
                     Rem n0(Lin n0 n1 p5)=0 impb
                     Rem n1(Lin n0 n1 p5)=0 impb False)
      (pf4 [let p6 (Step n0 n1 p5(Quot n0(Lin n0 n1 p5))@
                   Quot n0(Lin n0 n1 p5)*right p5)
        [if (Lin n0 n1 p6<n3 impb
             0<Lin n0 n1 p6 impb False)
         (Quot n1(Lin n0 n1 p5)*left p5@
         Step n1 n0(right p5@left p5)
              (Quot n1(Lin n0 n1 p5)))
         p6]]) p5]) n1)
   [let p2 [if (0<n1 impb Rem n0 n1=0 impb False)
     (pf7(Step n0 n1(0@1)(Quot n0 n1)@Quot n0 n1))(0@1)]
    [if (0<Lin n0 n1 p2 impb
         Rem n0(Lin n0 n1 p2)=0 impb
         Rem n1(Lin n0 n1 p2)=0 impb False)
     (pf7(0@[if (0<n1) 0 2])) p2]]]
```

Future work

- Get more experience in unwinding classical proofs.
- Compare Gödel's Dialectica interpretation and its variants (Kohlenbach, Ferreira/Oliva) with refinements of the Dragalin-Friedman A-translation.