Light Monotone Dialectica

Extraction of moduli of uniform continuity for closed terms from Goedel's **T** of type $(\mathbb{N} \Rightarrow \mathbb{N}) \Rightarrow (\mathbb{N} \Rightarrow \mathbb{N})$

Mircea-Dan Hernest

Project LogiCal – Paris, France and GKLI – Munich, Germany

LFMTP'06 Talk in Seattle, 16 August 2006

Outline of this Talk

1. Introduction
   - A seemingly simple game-problem of discrete mathematics
   - Generalization and set-up for the Proof-theoretic machinery
2. Hereditarily Extensional Equality in computer system MinLog
   - Term system, majorizability and Hereditarily Extensional Equality
   - Weakly extensional monotonic Arithmetic for Göedel functionals
3. From Gödel's Dialectica to Light Monotone Dialectica
   - The pure Göedel's functional "Dialectica" interpretation
   - The Contraction Problem –> Achilles' heel for Dialectica !
   - The Light Monotone Dialectica majorant extraction
4. Conclusions and Future work
   - The human/computer outcome for our general game-problem
   - Computer really necessary? Implementing Monotone Dialectica
   - Work to be done –> the real "Light" Monotone Dialectica

A game-problem of discrete mathematics

1. Let $f, g, h : \mathbb{N} \mapsto \mathbb{N}$ s.t. h fixed & $\forall n \in \mathbb{N}.\, f(n) \leq h(n) \wedge g(n) \leq h(n)$

Given $k \in \mathbb{N}$ find $L \in \mathbb{N}$ s.t. $[\forall i \leq L.\, f(i) = g(i)] \Rightarrow [\forall j \leq k.\, f(j) = g(j)]$

2. Dummy answer $L :\equiv k$. Hence try to complicate the demand:

$$\forall f, g \leq_{\mathbb{N}\to\mathbb{N}} h.\, [\forall i \leq L.\, f(i) = g(i)] \Rightarrow [\forall j \leq k.\, f(f(j)) = g(g(j))]$$

3. Simple optimal answer $max\{k, h(0), \ldots, h(k)\}$. But what about:

$$\forall f, g \leq h.\, [\forall i \leq L.\, f(i) = g(i)] \Rightarrow [\forall j \leq k.\, f(f(f(j))) = g(g(g(j)))]$$

4. Temptation $max\{k, h(0), \ldots, h(k), h(h(0)), \ldots, h(h(k))\}$. False,

since $f(j) \leq h(j) \not\Rightarrow f(f(j)) \leq h(h(j))$, hence $f(f(0)) > h(h(j))$ possible.

5. How to solve this? And what about the fully general case?

$$\forall f, g \leq_{\mathbb{N}\to\mathbb{N}} h.\, [\forall i \leq L.\, f(i) = g(i)] \Rightarrow [\forall j \leq k.\, f^{(m)}(j) = g^{(m)}(j)]$$

Set-up for the Proof-theoretic machinery (1/2)

1. Extract moduli of uniform continuity for *closed* terms $\mathbf{t_m}$ of Goedel's **T** of type $(\mathbb{N} \Rightarrow \mathbb{N}) \Rightarrow (\mathbb{N} \Rightarrow \mathbb{N})$ where

$$\mathbf{t_m} \;:\equiv\; \lambda h^{\mathbb{N}\Rightarrow\mathbb{N}}, k^{\mathbb{N}} \,.\, \mathbf{R}_{\mathbb{N}\Rightarrow\mathbb{N}}(0)[\lambda p, q \,.\, h^{(m)}(p) + q](k+1)$$

2. Hence $\mathbf{t_m}(h,k) \;\equiv\; h^{(m)}(0) + h^{(m)}(1) + \ldots + h^{(m)}(k)$. How???

Let $\mathcal{P} :\equiv\; \vdash\; \forall f, g \,.\, [\forall i \,.\, f(i) =_{\mathbb{N}} g(i)] \;\Rightarrow\; [\forall j \,.\, \mathbf{t_m}(f,j) =_{\mathbb{N}} \mathbf{t_m}(g,j)]$

3. The above $\mathcal{P}$ is a Minimal Logic proof of (almost) $\mathbf{t_m} \approx \mathbf{t_m}$. We apply on $\mathcal{P}$ a Light Monotone Dialectica extraction in MinLog.
4. Gödel's Dialectica would give an exact realizer $\mathbf{t}'[f,g,j]$ for i s.t.

$$\forall f, g\, \forall j \,.\quad f(\mathbf{t}'[f,g,j]) =_{\mathbb{N}} g(\mathbf{t}'[f,g,j]) \;\Rightarrow\; \mathbf{t_m}(f,j) =_{\mathbb{N}} \mathbf{t_m}(g,j)$$

5. If $\widetilde{\mathbf{t}}$ *maj* $\lambda f, g, j \,.\, \mathbf{t}'$ then for $k \geq j$, $h^\star$ *maj* h and $h \geq f, g$ one has $(L :\equiv \widetilde{\mathbf{t}}(h^\star, h^\star, k)) \geq \mathbf{t}'[f,g,j]$ and therefore such an L is a solution:

$$\forall h \forall f, g \leq_{\mathbb{N}\to\mathbb{N}} h \forall k \,.\, [\forall i \leq L \,.\, f(i) = g(i)] \;\Rightarrow\; [\forall j \leq k \,.\, f^{(m)}(j) = g^{(m)}(j)]$$

Set-up for the Proof-theoretic machinery (2/2)

- Start from proof of *hereditarily extensional equality* of $\mathbf{t}$ to itself.
- Hence a proof of $\mathbf{t} \approx_{(\mathbb{N}\Rightarrow\mathbb{N})\Rightarrow(\mathbb{N}\Rightarrow\mathbb{N})} \mathbf{t}$ in system Z_0 of Berger-Buchholz-Schwichtenberg, the base logic of machine system MinLog.
- Hence a Minimal Logic proof without use of Extensionality Axiom.
- Two *extreme* approaches:
  1. First extract $\mathbf{t}'$ by Gödel's Dialectica and then majorize it via Howard's algorithm (Kohlenbach's PhD thesis, JSL paper '92).
  2. Directly extract $\widetilde{\mathbf{t}}$ by producing a majorant for the *closed* extracted term at each of the Dialectica recursion step (Kohlenbach '93).
- None of the two efficient on the computer. Solution: use an intermediate approach –> Extract partial majorants which are not necessarily closed terms, only simplify treatment of Contraction.
- Also use a Normalization during Extraction, i.e. NbE-normalize the extracted term of the conclusion of a Modus Ponens. (NdE)
- Huge impact of such Partial Evaluation. No solution without it!!

The term system – a lambda-variant of Göedel's **T**

1. All finite types generated from $\mathbb{N}$ and $\mathbb{B}$ by the rule $\sigma, \tau \mapsto (\sigma\tau)$
2. $tt^{\mathbb{B}}$, $ff^{\mathbb{B}}$ equality $=^{\mathbb{N}\mathbb{N}\mathbb{B}}$ and inequality $\geq^{\mathbb{N}\mathbb{N}\mathbb{B}}$, maximum $Max^{\mathbb{N}\mathbb{N}\mathbb{N}}$
3. $0^{\mathbb{N}}$ (zero), $Suc^{\mathbb{N}\mathbb{N}}$ (successor) and Gödel's recursor $\mathbf{R}_\tau^{\tau(\mathbb{N}\tau\tau)\mathbb{N}\tau}$

   $$And^{\mathbb{B}\mathbb{B}\mathbb{B}} \;:\equiv\; \lambda p, q\,.\,\mathbf{If}_{\mathbb{B}}\; p\; q\; ff \qquad Imp^{\mathbb{B}\mathbb{B}\mathbb{B}} \;:\equiv\; \lambda p, q\,.\,\mathbf{If}_{\mathbb{B}}\; p\; q\; tt$$

4. Combinators at all types are *defined* in terms of λ-abstraction:

   $$\Sigma \;:\equiv\; \lambda x, y, z\,.\,x\,z\,(y\,z) \qquad \Pi \;:\equiv\; \lambda x, y\,.\,x$$

5. $at^{\mathbb{B}}$ is the *unique* predicate symbol of $WeZ_m^{\exists}$ – one $\mathbb{B}$ argument
6. *Extensionally* defined equality and inequality (below $\sigma \in \{\mathbb{B}, \mathbb{N}\}$)

$$s =_{\mathbb{N}} t \;:\equiv\; at(=s\,t) \qquad s =_{\mathbb{B}} t \;:\equiv\; at(s) \leftrightarrow at(t)$$

$$s \geq_{\mathbb{N}} t \;:\equiv\; at(\geq s\,t) \qquad s \geq_{\mathbb{B}} t \;:\equiv\; at(t) \rightarrow at(s)$$

$$s =_{\sigma_1 \ldots \sigma_n \rightarrow \sigma} t \;:\equiv\; \forall x_1^{\sigma_1} \ldots x_n^{\sigma_n} \,(s\,x_1 \ldots x_n =_\sigma t\,x_1 \ldots x_n)$$

$$s \geq_{\sigma_1 \ldots \sigma_n \rightarrow \sigma} t \;:\equiv\; \forall x_1^{\sigma_1} \ldots x_n^{\sigma_n} \,(s\,x_1 \ldots x_n \geq_\sigma t\,x_1 \ldots x_n)$$

Majorizability and Hereditarily Extensional Equality (1)

$$x \; maj_{\mathbb{N}} \; y \quad :\equiv \quad x \geq_{\mathbb{N}} y \quad :\equiv \quad at(\geq x^{\mathbb{N}} \, y^{\mathbb{N}})$$

$$x \geq_{\sigma\tau} y \quad \equiv \quad \forall z^{\sigma} \, (xz \geq_{\tau} yz)$$

$$x \; maj_{\sigma\tau} \; y \quad :\equiv \quad \forall z_1^{\sigma}, z_2^{\sigma} \, (z_1 \; maj_{\sigma} \; z_2 \; \rightarrow \; xz_1 \; maj_{\tau} \; yz_2)$$

$0 \; maj_{\mathbb{N}} \; 0$, $Suc \; maj_{\mathbb{N}\mathbb{N}} \; Suc$, $\boxed{\Sigma \; maj \; \Sigma \,, \; \Pi \; maj \; \Pi \text{ and } \mathbf{R}^{M} \; maj \; \mathbf{R}}$

$$WeZ_m \; \vdash \; t^{\star} \; maj_{\sigma\tau} \; t \; \wedge \; s^{\star} \; maj_{\sigma} \; s \; \Longrightarrow \; t^{\star} s^{\star} \; maj_{\tau} \; ts$$

$$x \approx_{\mathbb{N}} y \quad :\equiv \quad x =_{\mathbb{N}} y \quad :\equiv \quad at(= x^{\mathbb{N}} \, y^{\mathbb{N}})$$

$$x =_{\sigma\tau} y \quad \equiv \quad \forall z^{\sigma} \, (xz =_{\tau} yz)$$

$$x \approx_{\sigma\tau} y \quad :\equiv \quad \forall z_1^{\sigma}, z_2^{\sigma} \, (z_1 \approx_{\sigma} z_2 \; \rightarrow \; xz_1 \approx_{\tau} yz_2)$$

$0 \approx_{\mathbb{N}} 0$, $Suc \approx_{\mathbb{N}\mathbb{N}} Suc$, $\boxed{\Sigma \approx \Sigma \,, \; \Pi \approx \Pi \text{ and } \mathbf{R} \approx \mathbf{R}}$

$$WeZ_m \; \vdash \; t^{\star} \approx_{\sigma\tau} t \; \wedge \; s^{\star} \approx_{\sigma} s \; \Longrightarrow \; t^{\star} s^{\star} \approx_{\tau} ts$$

System WeZ_m –> Implic. Introd. with Contraction

1. WeZ_m - Weakly extensional Minimal Arithmetic with $\geq$ and Max
2. Minimal Arith. $\Leftrightarrow$ Heyting Arith. in all finite types $HA^\omega \setminus \perp \to A$
3. WeZ_m - underlying Logic is Natural Deduction, not Hilbert-style!
4. $\dfrac{[u:\ A]\ \ldots\ /B}{A \to B} \to^+$, particular set of instances of A in the same parcel (assumption variable) u get discharged; If at least two A get discharged then one has *logical Contraction*; If moreover A contains at least one positive universal or a negative existential quantifier then one has a *computationally relevant Contraction*
5. Comp. Relevance relative to both Gödel and Monotone Dialectica

$$\{A_{\mathbf{D}}(z;\, T_i(\underline{z}, \underline{x}, y))\}_{i=1}^{n+1},\ \{C^i_{\mathbf{D}}(x_i;\, T_i(\underline{z}, \underline{x}, y))\}_{i=n+2}^{m} \vdash\ B_{\mathbf{D}}(T(\underline{z}, \underline{x});\, y)$$

Same tuple z produced by $2 \leq n+1 \leq m$ discharged instances of A

If $\{T_i\}_{i=1}^{n+1}$ non-null (A is Dialectica relevant) $\Rightarrow$ *Equalization* is a must!

Extensionality/Compatibility and Induction rules

$E_{\sigma,\tau} : \forall z^{\sigma\tau}, x^{\sigma}, y^{\sigma}.\ x =_{\sigma} y \rightarrow zx =_{\tau} zy$ – must be forbidden

$$\frac{\begin{array}{c} A_0 \\ \vdots \\ s =_{\sigma} t \end{array}}{B(s) \rightarrow B(t)}$$

$COMPAT_{\sigma}$ – with the restriction that all undischarged assumptions used in the proof of $s =_{\sigma} t$ (here denoted A_0) are quantifier-free

$$\frac{\begin{array}{cc} \emptyset & \emptyset \\ \vdots & \vdots \\ A(0) & \forall z\,(A(z) \rightarrow A(Sucz)) \end{array}}{\forall z\, A(z)}$$

IR_0 – equivalent to IA, IR in WeZ_m

$A(tt) \wedge A(ff) \ \rightarrow\ \forall p^{\mathbb{B}} A(p)$
(Boolean Induction Axiom)

$$\left.\begin{array}{l} \mathbf{R}_{\tau}\, x\, y\, 0 =_{\tau} x \\ \mathbf{R}_{\tau}\, x\, y\, (Sucz) =_{\tau} y(z, \mathbf{R}_{\tau}\, x\, y\, z) \end{array}\right\} : \mathtt{Ax}\mathbf{R}_{\tau}$$

Göedel's functional "Dialectica" interpretation

1. A translation of proofs which includes a translation of formulas.
2. $A(\underline{a}) \mapsto A^{\mathbf{D}} \equiv \exists \underline{x}\, \forall \underline{y}\, A_{\mathbf{D}}(\underline{x}; \underline{y}; \underline{a})$ with $\underline{a}$ all free vars of formula A
3. $A_{\mathbf{D}}$ is quantifier-free for Göedel's Dialectica, since decidability needed –> this no longer for Monotone setup $\Rightarrow$ *Bounded* Dialectica
4. Recursive syntactic translation from proofs in *Constructive Arithmetic* (or *Classical Arithmetic*, modulo the double-negation translation) to proofs in *Intuitionistic Arithmetic* such that positive occurrences of $\exists$ and negative occurrences of $\forall$ in the proof's conclusion get actually realized by terms in Gödel's **T**.
5. *Contraction Problem:* –> choose between a number of realizers according to a boolean term associated to the contraction formula; *Diller-Nahm:* –> postpone all choices to the very end by collecting all candidates and making a single final global choice; *Monotone Dialectica:* –> use a simple common upper bound (maximum majorant) of the candidates $\Longrightarrow$ extract *majorants*

The Light Dialectica interpretation of formulas

$$
\begin{aligned}
A^{\mathbf{D}} \quad &:\equiv \quad (A_{\mathbf{D}} :\equiv A) \text{ for prime formulas } A \\
(A \wedge B)^{\mathbf{D}} \quad &:\equiv \quad \exists \underline{x}, \underline{u} \, \forall \underline{y}, \underline{v} \, [\, (A \wedge B)_{\mathbf{D}} :\equiv A_{\mathbf{D}}(\underline{x}; \underline{y}; \underline{a}) \wedge B_{\mathbf{D}}(\underline{u}; \underline{v}; \underline{b}) \,] \\
(A \to B)^{\mathbf{D}} \quad &:\equiv \quad \exists \underline{Y}, \underline{U} \, \forall \underline{x}, \underline{v} \, [\, (A \to B)_{\mathbf{D}} :\equiv \\
&\qquad\qquad A_{\mathbf{D}}(\underline{x}; \underline{Y}(\underline{x}, \underline{v})) \to B_{\mathbf{D}}(\underline{U}(\underline{x}); \underline{v}) \,] \\
(\exists z A(z, \underline{a}))^{\mathbf{D}} \quad &:\equiv \quad \exists z^{\dagger}, \underline{x} \, \forall \underline{y} \, [\, (\exists z A(z, \underline{a}))_{\mathbf{D}}(z^{\dagger}, \underline{x}; \underline{y}; \underline{a}) :\equiv A_{\mathbf{D}}(\underline{x}; \underline{y}; z^{\dagger}, \underline{a}) \,] \\
(\overline{\exists} z A(z, \underline{a}))^{\mathbf{D}} \quad &:\equiv \quad \exists \underline{x} \, \forall \underline{y} \, [\, (\overline{\exists} z A(z, \underline{a}))_{\mathbf{D}}(\underline{x}; \underline{y}; \underline{a}) :\equiv \exists z \, A_{\mathbf{D}}(\underline{x}; \underline{y}; z, \underline{a}) \,] \\
(\forall z A(z, \underline{a}))^{\mathbf{D}} \quad &:\equiv \quad \exists \underline{X} \, \forall z^{\dagger}, \underline{y} \, [\, (\forall z A(z, \underline{a}))_{\mathbf{D}}(\underline{X}; z^{\dagger}, \underline{y}; \underline{a}) :\equiv A_{\mathbf{D}}(\underline{X}(z^{\dagger}); \underline{y}; z^{\dagger}, \underline{a} \\
(\overline{\forall} z A(z, \underline{a}))^{\mathbf{D}} \quad &:\equiv \quad \exists \underline{x} \, \forall \underline{y} \, [\, (\overline{\forall} z A(z, \underline{a}))_{\mathbf{D}}(\underline{x}; \underline{y}; \underline{a}) :\equiv \forall z \, A_{\mathbf{D}}(\underline{x}; \underline{y}; z, \underline{a}) \,]
\end{aligned}
$$

Here $\cdot \mapsto \cdot^{\dagger}$ is a mapping which assigns to every given variable z a completely new variable $z^{\dagger}$ which has the same type of z.

Exact realizer synthesis by Dialectica Interpretation

Extraction and Soundness Theorem: There exists an algorithm which, given at input a $WeZ^{\exists +}$ proof $\mathcal{P} : \{C^i\}_{i=1}^n \vdash A$ [hence of the conclusion formula A, from the *undischarged* assumption formulas $\{C^i\}_{i=1}^n$] will produce at output 1) the tuples of terms T and $\{T_i\}_{i=1}^n$ 2) the tuples of variables $\{x_i\}_{i=1}^n$ and y 3) the verifying proof

$$\mathcal{P}_{\mathbf{D}} : \{C^i_{\mathbf{D}}(x_i; T_i(\underline{x}, y))\}_{i=1}^n \vdash A_{\mathbf{D}}(T(\underline{x}); y)$$

– where $\underline{x} :\equiv x_1, \ldots, x_n$. Moreover,

1. variables $\underline{x}$ and y are all completely new (not occur in $\mathcal{P}$)
2. the free variables of T and $\{T_i\}_{i=1}^n$ are among the free variables of A and $\{C^i\}_{i=1}^n$ (this one names “the *free variable condition* (**FVC**) for programs extracted by the Dialectica Interpretation”)

[$\Rightarrow \underline{x}, y$ not occur free in the *extracted* terms $\{T_i\}_{i=1}^n$ and T]

Notice that: Terms T and $\{T_i\}_{i=1}^n$ are not necessarily closed !!!

Problem –> Implication Introduction with Contraction

$$\boxed{\dfrac{[u\,:\,A]\;\ldots\;/B}{A \to B}\to^+} \qquad n \geq 1,\quad \underline{z} \equiv \overbrace{z,\ldots,z}^{n+1} \text{ and } \underline{x} \equiv x_{n+2},\ldots,x_m :$$

$$\{A_{\mathbf{D}}(z;\,T_i(\underline{z},\underline{x},y))\}_{i=1}^{n+1},\ \{C^i_{\mathbf{D}}(x_i;\,T_i(\underline{z},\underline{x},y))\}_{i=n+2}^{m} \vdash\ B_{\mathbf{D}}(T(\underline{z},\underline{x});y)$$

1) Same tuple z produced by $n+1 \leq m$ discharged instances of A

2) <u>Case</u>: tuples $\{T_i\}_{i=1}^{n+1}$ are non-null! Recall that $A_{\mathbf{D}}$ is quantifier-free

3) Since $\{T_i\}_{i=1}^{n+1}$ non-null $\implies$ their *equalization* is a *must*:

$$\mathbf{S} :\equiv \lambda \underline{x}, z, y\,.\,\mathbf{If}^n_\tau(\mathsf{t}^{\mathbf{D}}_A[z;\,T^1],\ldots,\mathsf{t}^{\mathbf{D}}_A[z;\,T^n],\,T_{n+1}(\underline{z},\underline{x},y),\,T^n,\ldots,T^1)$$

one can now cancell all $\{A_{\mathbf{D}}\}_{i=1}^{n+1}$ *by a single* $\to^+$ *in the verifying proof*

$$\{A_{\mathbf{D}}(z;\,\mathbf{S}(\underline{x},z,y))\}_{i=1}^{n+1},\ \{C^i_{\mathbf{D}}(x_i;\,S_i(\underline{x},z,y))\}_{i=n+2}^{m} \vdash\ B_{\mathbf{D}}(S(\underline{x},z);y)$$

$$\{C^i_{\mathbf{D}}(x_i;\,S_i(\underline{x},z,y))\}_{i=n+2}^{m} \vdash\ A_{\mathbf{D}}(z;\,\mathbf{S}(\underline{x},z,y)) \to B_{\mathbf{D}}(S(\underline{x},z);y)$$

The Light Monotone Dialectica program extraction

Majorant realizer synthesis by Light Monotone Dialectica

Theorem: There ex. an algorithm which, given at input a $WeZ_m^{\exists +}$ proof $\mathcal{P} : \{C^i(a_i)\}_{i=1}^n \vdash A(a')$ [hence of the conclusion formula A, whose free variables form the *tuple* a, from the *undischarged* assumption formulas $\{C^i\}_{i=1}^n$] it will produce at output the following ($\underline{a} :\equiv a_1, \ldots, a_n, a'$):

1. tuples of terms $\{T_i[\underline{a}]\}_{i=1}^n$ and $T[\underline{a}]$, with free variables among $\underline{a}$
2. the tuples of variables $\{x_i\}_{i=1}^n$ and y, all together with
3. the following verifying proof in $WeZ_m^{\exists}$ (below let $\underline{x} :\equiv x_1, \ldots, x_n$):

$$\vdash \exists Y_1, \ldots Y_n, X \,[\, \textstyle\bigwedge_{i=1}^n (\lambda \underline{a}.\, T_i) \; maj \; Y_i \wedge (\lambda \underline{a}.\, T) \; maj \; X \wedge \\ \forall \underline{a}, \underline{x}, y \,(\, \{\textstyle\bigwedge_{i=1}^n {C^i}_{\mathbf{D}}(x_i; Y_i(\underline{a}, \underline{x}, y); a_i)\} \rightarrow A_{\mathbf{D}}(X(\underline{a}, \underline{x}); y; a)\,)\,]$$

Variables $\underline{x}$ and y do not occur in $\mathcal{P}$ (they are all completely new)

$\Longrightarrow$ $\underline{x}$ and y do not occur free in the *extracted* terms $\{T_i\}_{i=1}^n$ and T.

Majorizability and Hereditarily Extensional Equality (2)

$$x \; maj_{\mathbb{N}} \; y \quad :\equiv \quad x \geq_{\mathbb{N}} y \quad :\equiv \quad at(\geq x^{\mathbb{N}} \, y^{\mathbb{N}})$$

$$x \geq_{\sigma\tau} y \quad \equiv \quad \forall z^{\sigma} \, (xz \geq_{\tau} yz)$$

$$x \; maj_{\sigma\tau} \; y \quad :\equiv \quad \forall z_1^{\sigma}, z_2^{\sigma} \, (z_1 \; maj_{\sigma} \; z_2 \; \rightarrow \; xz_1 \; maj_{\tau} \; yz_2)$$

$0 \; maj_{\mathbb{N}} \; 0$, $Suc \; maj_{\mathbb{NN}} \; Suc$, $\boxed{\Sigma \; maj \; \Sigma \,, \; \Pi \; maj \; \Pi \; \text{and} \; \mathbf{R}^M \; maj \; \mathbf{R}}$

$$WeZ_m \; \vdash \; t^{\star} \; maj_{\sigma\tau} \; t \; \wedge \; s^{\star} \; maj_{\sigma} \; s \; \Longrightarrow \; t^{\star} s^{\star} \; maj_{\tau} \; ts$$

$$x \approx_{\mathbb{N}} y \quad :\equiv \quad x =_{\mathbb{N}} y \quad :\equiv \quad at(= x^{\mathbb{N}} \, y^{\mathbb{N}})$$

$$x =_{\sigma\tau} y \quad \equiv \quad \forall z^{\sigma} \, (xz =_{\tau} yz)$$

$$x \approx_{\sigma\tau} y \quad :\equiv \quad \forall z_1^{\sigma}, z_2^{\sigma} \, (z_1 \approx_{\sigma} z_2 \; \rightarrow \; xz_1 \approx_{\tau} yz_2)$$

$0 \approx_{\mathbb{N}} 0$, $Suc \approx_{\mathbb{NN}} Suc$, $\boxed{\Sigma \approx \Sigma \,, \; \Pi \approx \Pi \; \text{and} \; \mathbf{R} \approx \mathbf{R}}$

$$WeZ_m \; \vdash \; t^{\star} \approx_{\sigma\tau} t \; \wedge \; s^{\star} \approx_{\sigma} s \; \Longrightarrow \; t^{\star} s^{\star} \approx_{\tau} ts$$

The WeZ_m proof at input & post-extraction ops.

1. Let $\mathbf{t}_\rho$ be a closed term of Gödel's **T**. Then $WeZ_m \vdash \mathbf{t} \approx_\rho \mathbf{t}$.
2. Let $\mathbf{t}_{(\mathbb{N}\to\mathbb{N})\to(\mathbb{N}\to\mathbb{N})}$ be a closed **T**-term. Since

$$WeZ_m \quad \vdash \quad \forall x^{\mathbb{N}\to\mathbb{N}}, y^{\mathbb{N}\to\mathbb{N}} \, [\, x =_{\mathbb{N}\to\mathbb{N}} y \; \leftrightarrow \; x \approx_{\mathbb{N}\to\mathbb{N}} y \,]$$

(due to weak extensionality + reflexivity) it immediately follows that

$$WeZ_m \quad \vdash \quad \forall x^{\mathbb{N}\to\mathbb{N}}, y^{\mathbb{N}\to\mathbb{N}} \, [\, x =_{\mathbb{N}\to\mathbb{N}} y \; \to \; \mathbf{t}(x) =_{\mathbb{N}\to\mathbb{N}} \mathbf{t}(y) \,]$$

3. Let $\mathbf{t}[\underline{a}]$ be a **T**-term with free vars $\underline{a}$. There exists a corresponding **T**-term $\mathbf{t}^\star[\underline{a}]$ such that $WeZ_m \vdash \lambda \underline{a} . \mathbf{t}^\star \; maj \; \lambda \underline{a} . \mathbf{t}$. <u>Very simple $\mathbf{t}^\star$ construction</u>: just replace each **R** in **t** with the corresponding $\mathbf{R}^M$.
4. If the type of a is $\mathbb{N} \to \rho$ then $a^M \; maj \; a$, hence $\mathbf{t}^\star[\underline{a^M}] \; maj \; \mathbf{t}[\underline{a}]$.
5. For a of type $\mathbb{N} \to \rho$ define $\boxed{a^M(k) \; :\equiv \; Max_\rho(a(0), \ldots, a(k))}$

MinLog computer output for our game-problem, $m = 3$

1. For $\mathbf{t}_3 \;:\equiv\; \lambda h^{\mathbb{N}\Rightarrow\mathbb{N}}, k^{\mathbb{N}} . \mathbf{R}_{\mathbb{N}\Rightarrow\mathbb{N}}(0)[\lambda p, q . h^{(3)}(p) + q](k+1)$ want

$$\forall f, g \leq h . [\forall i \leq L . f(i) = g(i)] \Rightarrow [\forall j \leq k . f(f(f(j))) = g(g(g(j)))]$$

2. The MinLog machine outputs in less than one minute:

$$\lambda h, k . max\{k, h(0) \ldots, h(k), max\{h(0) \ldots h(max\{h(0) \ldots h(k)\})\}\}$$

which immediately rewrites more humanly readable as

$$L^3 \;:\equiv\; \lambda h, k . max\{k, h(0), h(1), \ldots, h(max\{k, h(0), h(1), \ldots, h(k)\})\}$$

3. Recall that for $m = 2$ and $m = 1$ the (human) outcomes were

$$L^2 \;:\equiv\; \lambda h, k . max\{k, h(0), h(1), \ldots, h(k)\}$$
$$L^1 \;:\equiv\; \lambda h, k . k$$

Final human solution for our general game-problem

Pattern can be noticed (by the human!) in the solution of our problem for terms

$$\mathbf{t_m} \;:\equiv\; \lambda h, k \,.\, h^{(m)}(0) + \ldots + h^{(m)}(k)\,,$$

with $h^{(m)}(i) \;:\equiv\; h(h \ldots (h(i)))$ s.t. h appears m times on the right side.

$$\begin{aligned}
\widetilde{t_1}(h,k) &\equiv k \\
\widetilde{t_2}(h,k) &\equiv max\{k, h(0), \ldots, h(\widetilde{t_1}(h,k))\} \\
\widetilde{t_3}(h,k) &\equiv max\{k, h(0), \ldots, h(\widetilde{t_2}(h,k))\} \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Immediate inference of the generic (recursive) solution for $m \in \mathbb{N}$:

$$\widetilde{t_{m+1}}(h,k) \quad\equiv\quad max\{k, h(0), \ldots, h(\widetilde{t_m}(h,k))\}$$

Verify that $\widetilde{\mathbf{t_m}}$ is the optimal modulus of uniform continuity for $\mathbf{t_m}$!

Now an easy exercise for the human ! $\Longrightarrow$ See my PhD thesis :)

Was the Computer really necessary?

1. Maybe not, but what if the problem were more complex/tedious ?
2. Certainly helpful for preventing the human error ! Effectively !

Implementing Monotone Dialectica

1. The "light" variant of Monotone Dialectica is the result of our implementation effort ! Many operations which are "easy" for the human (mathematician) are not really that easy for the machine !
2. On the computer, the Goal is to produce programs in normal form !
3. Hence improve the Nbe-normalization by its own Partial Evaluation $\Longrightarrow$ Normalization during Extraction (NdE) $\Longleftrightarrow$ NbE-normalize the term extracted for the conclusion of each Modus Ponens .
4. Only majorize at Contraction $\Longrightarrow$ produce a partial majorant which is transformed at the end by replacing each $\mathbf{R}$ with its corresp. $\mathbf{R}^M$.
5. Why? Well, some of the $\mathbf{R}$ may be eliminated during the partial NbE-normalization ... Also use the more clever $\mathbf{R}^M$, with just 1 $\mathbf{R}$.

A lot of Work to be done . . .

1. Completely formalize and explore the limits of *Normalization during Extraction* (NdE) $\Rightarrow$ generic optimization for $(\mathbf{t_n}..(\mathbf{t_2}(\mathbf{t_1}\mathbf{t_0}))..)$
2. Completely formalize these ad-hoc optimizations of the computer implementation of Monotone Dialectica and combine with the "light" optimization brought by the use of quantifiers without comp. content
3. We suspect that the use of these *ncm* quantifiers may eliminate some of the comput. contractions in the Hered. Ext. Eq. extraction ! This game-problem is already solved for a very particular case only !
4. Find other more interesting $\mathbf{T}$-terms $\mathbf{t_m}$, for which the modulus of uniform continuity is far more difficult to find !
5. Find other more interesting examples for the *Proof Mining* by the Light (monotone) Dialectica on the Computer !
6. Improve the human-interaction side of our Dialectica extraction modules in MinLog, in order to render "MinLog for Dialectica" as an indispensable computer tool even for the more pure mathematically oriented Proof Mining !

Short List of related Papers I

U. Kohlenbach.
Proof Interpretations and the Computational Content of Proofs.
Lecture Course, latest version in the author's web page.

U. Kohlenbach and P. Oliva.
Proof Mining: a systematic way of analysing proofs in Mathematics.
Proc. of the Steklov Inst. of Mathem., 242:136–164, 2003.

U. Kohlenbach.
Pointwise hereditary majorization and some applications.
Arch. Math. Logic, 31:227–241, 1992.

U. Kohlenbach.
Analysing proofs in Analysis.
In *Logic: from Foundations to Applications, Keele, 1993*, European Logic Colloquium, pages 225–260. Oxford University Press, 1996.

Short List of related Papers II

- M.-D. Hernest.
  Light Dialectica program extraction from a classical Fibonacci proof Proceedings of DCM@ICALP'06, ENTCS (2007), 10pp.
- M.-D. Hernest. Light Functional Interpretation.
  CSL 2005 - In *LNCS* 3634 pp. 477 – 492, July 2005.
- M.-D. Hernest and U. Kohlenbach.
  A complexity analysis of functional interpretations.
  Theoretical Computer Science, 338(1-3):200–246, 2005.
- U. Berger.
  Uniform Heyting Arithmetic.
  Annals of Pure and Applied Logic, 133(1-3):125–148, 2005.
- U. Berger, W. Buchholz, and H. Schwichtenberg.
  Refined program extraction from classical proofs.
  Annals of Pure and Applied Logic, 114:3–25, 2002.