Realizability and Strong Normalization for Heyting Arithmetic with EM_1

Federico Aschieri
(joint work S. Berardi, G. Birolo)

Equipe Plume, LIP
ENS de Lyon

Toulouse, 24 Avril 2013

Proof Terms

- Variables: for terms $x, y, z, \ldots$, for individuals $\alpha, \beta, \ldots$

Proof Terms

- Variables: for terms $x, y, z, \ldots$, for individuals $\alpha, \beta, \ldots$
- Functions ($\rightarrow$):

$$\lambda x\, u \mid tu$$

Proof Terms

- Variables: for terms $x, y, z, \ldots$, for individuals $\alpha, \beta, \ldots$
- Functions ($\rightarrow$):

$$\lambda x\, u \mid tu$$

- Pairs ($\wedge$):

$$\langle u, v \rangle \mid \pi_0 u \mid \pi_1 u$$

Proof Terms

- Variables: for terms $x, y, z, \ldots$, for individuals $\alpha, \beta, \ldots$
- Functions ($\rightarrow$):

$$\lambda x\, u \mid tu$$

- Pairs ($\wedge$):

$$\langle u, v \rangle \mid \pi_0 u \mid \pi_1 u$$

- Sums ($\vee$):

$$\iota_0(u) \mid \iota_1(u) \mid u[x.v_1, y.v_2]$$

Proof Terms

- Variables: for terms $x, y, z, \ldots$, for individuals $\alpha, \beta, \ldots$
- Functions ($\rightarrow$):

$$\lambda x\, u \mid tu$$

- Pairs ($\wedge$):

$$\langle u, v \rangle \mid \pi_0 u \mid \pi_1 u$$

- Sums ($\vee$):

$$\iota_0(u) \mid \iota_1(u) \mid u[x.v_1, y.v_2]$$

- Products ($\forall$):

$$\lambda \alpha\, u \mid tn \quad (n \text{ individual})$$

Proof Terms

- Variables: for terms $x, y, z, \ldots$, for individuals $\alpha, \beta, \ldots$
- Functions ($\rightarrow$):
$$\lambda x\, u \mid tu$$
- Pairs ($\wedge$):
$$\langle u, v\rangle \mid \pi_0 u \mid \pi_1 u$$
- Sums ($\vee$):
$$\iota_0(u) \mid \iota_1(u) \mid u[x.v_1, y.v_2]$$
- Products ($\forall$):
$$\lambda\alpha\, u \mid tn \quad (n \text{ individual})$$
- Co-Products ($\exists$):
$$(n, t) \mid u[(\alpha, x).v] \quad (n \text{ individual})$$

Proof Terms(2)

- Numerals:

$$0, S0, SS0, \ldots$$

Proof Terms(2)

- Numerals:

$$0, S0, SS0, \ldots$$

- Recursion (Induction):

$$\mathsf{rec}\ u\ v\ t$$

Proof Terms (3)

(EM_1):

$$u \parallel_a v$$

Proof Terms (3)

(EM$_1$):

$$u \parallel_a v$$

Permutations:

$$(u \parallel_a v)w \mapsto uw \parallel_a vw$$

Proof Terms (3)

(EM$_1$):

$$u \parallel_a v$$

Permutations:

$$(u \parallel_a v)w \mapsto uw \parallel_a vw$$

$$\pi_i(u \parallel_a v) \mapsto \pi_i u \parallel_a \pi_i v$$

Proof Terms (3)

(EM_1):

$$u \parallel_a v$$

Permutations:

$$(u \parallel_a v)w \mapsto uw \parallel_a vw$$

$$\pi_i(u \parallel_a v) \mapsto \pi_i u \parallel_a \pi_i v$$

$$(u \parallel_a v)[x.w_1, y.w_2] \mapsto u[x.w_1, y.w_2] \parallel_a v[x.w_1, y.w_2]$$

Proof Terms (3)

(EM$_1$):

$$u \parallel_a v$$

Permutations:

$$(u \parallel_a v)w \mapsto uw \parallel_a vw$$

$$\pi_i(u \parallel_a v) \mapsto \pi_i u \parallel_a \pi_i v$$

$$(u \parallel_a v)[x.w_1, y.w_2] \mapsto u[x.w_1, y.w_2] \parallel_a v[x.w_1, y.w_2]$$

$$(u \parallel_a v)[(\alpha, x).w] \mapsto u[(\alpha, x).w] \parallel_a v[(\alpha, x).w]$$

Proof Terms (4)

(EM_1):

$$u \parallel_a v$$

Proof Terms (4)

(EM$_1$):

$$u \parallel_a v$$

$$\mathsf{H}_a^{\forall\alpha \mathsf{P}}$$

$$\mathsf{W}_a^{\exists\alpha\neg \mathsf{P}}$$

(EM_1):

$$u \parallel_a v$$

$$\mathrm{H}_a^{\forall \alpha \mathrm{P}}$$

$$\mathrm{W}_a^{\exists \alpha \neg \mathrm{P}}$$

Exceptions:

$$(\mathrm{H}_a^{\forall \alpha \mathrm{P}}) n \mapsto \texttt{True}, \text{ if } \mathrm{P}[n/\alpha] = \texttt{True}$$

Proof Terms (4)

(EM_1):

$$u \parallel_a v$$

$$\mathsf{H}_a^{\forall \alpha \mathsf{P}}$$

$$\mathsf{W}_a^{\exists \alpha \neg \mathsf{P}}$$

Exceptions:

$$(\mathsf{H}_a^{\forall \alpha \mathsf{P}})n \mapsto \mathtt{True}, \text{ if } \mathsf{P}[n/\alpha] = \mathtt{True}$$

$$u \parallel_a v \mapsto u,$$

Proof Terms (4)

(EM_1):

$$u \parallel_a v$$

$$\mathsf{H}_a^{\forall \alpha \mathsf{P}}$$
$$\mathsf{W}_a^{\exists \alpha \neg \mathsf{P}}$$

Exceptions:

$$(\mathsf{H}_a^{\forall \alpha \mathsf{P}})n \mapsto \mathtt{True}, \text{ if } \mathsf{P}[n/\alpha] = \mathtt{True}$$

$$u \parallel_a v \mapsto u, \text{ (if } a \text{ does not occur free in } u\text{)}$$

Proof Terms (4)

(EM_1):

$$u \parallel_a v$$

$$\mathsf{H}_a^{\forall \alpha \mathsf{P}}$$

$$\mathsf{W}_a^{\exists \alpha \neg \mathsf{P}}$$

Exceptions:

$$(\mathsf{H}_a^{\forall \alpha \mathsf{P}})n \mapsto \mathtt{True}, \text{ if } \mathsf{P}[n/\alpha] = \mathtt{True}$$

$$u \parallel_a v \mapsto u, \text{ (if } a \text{ does not occur free in } u\text{)}$$

$$u \parallel_a v \mapsto v[a := n]$$

Proof Terms (4)

(EM_1):

$$u \parallel_a v$$

$$\mathsf{H}_a^{\forall\alpha\mathsf{P}}$$

$$\mathsf{W}_a^{\exists\alpha\neg\mathsf{P}}$$

Exceptions:

$$(\mathsf{H}_a^{\forall\alpha\mathsf{P}})n \mapsto \mathtt{True}, \text{ if } \mathsf{P}[n/\alpha] = \mathtt{True}$$

$$u \parallel_a v \mapsto u, \ (\text{if } a \text{ does not occur free in } u)$$

$$u \parallel_a v \mapsto v[a := n] := v[\mathsf{W}_a^{\exists\alpha\neg\mathsf{P}} := (n, \mathtt{True})]$$

Proof Terms (4)

(EM_1):

$$u \parallel_a v$$

$$\mathsf{H}_a^{\forall \alpha \mathsf{P}}$$

$$\mathsf{W}_a^{\exists \alpha \neg \mathsf{P}}$$

Exceptions:

$$(\mathsf{H}_a^{\forall \alpha \mathsf{P}})n \mapsto \mathtt{True}, \text{ if } \mathsf{P}[n/\alpha] = \mathtt{True}$$

$$u \parallel_a v \mapsto u, \text{ (if } a \text{ does not occur free in } u\text{)}$$

$$u \parallel_a v \mapsto v[a := n] := v[\mathsf{W}_a^{\exists \alpha \neg \mathsf{P}} := (n, \mathtt{True})]$$

$$\text{(if } \mathsf{H}_a^{\forall \alpha \mathsf{P}} n \text{ occurs in } u \text{ and } \mathsf{P}[n/\alpha] = \mathtt{False}\text{)}$$

$$\frac{\Gamma, a : \forall\alpha^{\mathbb{N}}\mathsf{P} \vdash u : C \qquad \Gamma, a : \exists\alpha^{\mathbb{N}}\neg\mathsf{P} \vdash v : C}{\Gamma \vdash u \parallel_a v : C}$$

P atomic

Typing Rules

$$\frac{\Gamma, a : \forall\alpha^{\mathbb{N}}\mathsf{P} \vdash u : C \qquad \Gamma, a : \exists\alpha^{\mathbb{N}}\neg\mathsf{P} \vdash v : C}{\Gamma \vdash u \parallel_a v : C}$$

P atomic

$$\Gamma, a : \forall\alpha^{\mathbb{N}}\mathsf{P} \vdash \mathsf{H}_a^{\forall\alpha\mathsf{P}} : \forall\alpha^{\mathbb{N}}\mathsf{P}$$

Typing Rules

$$\frac{\Gamma, a : \forall\alpha^{\mathbb{N}}\mathsf{P} \vdash u : C \qquad \Gamma, a : \exists\alpha^{\mathbb{N}}\neg\mathsf{P} \vdash v : C}{\Gamma \vdash u \parallel_a v : C}$$

P atomic

$$\Gamma, a : \forall\alpha^{\mathbb{N}}\mathsf{P} \vdash \mathsf{H}_a^{\forall\alpha\mathsf{P}} : \forall\alpha^{\mathbb{N}}\mathsf{P}$$

$$\Gamma, a : \exists\alpha^{\mathbb{N}}\neg\mathsf{P} \vdash \mathsf{W}_a^{\exists\alpha\neg\mathsf{P}} : \exists\alpha^{\mathbb{N}}\neg\mathsf{P}$$

Logical Interpretation

$$\dfrac{\dfrac{\begin{matrix}\dfrac{\forall\alpha \mathsf{P}}{\underline{\mathsf{P}[n/\alpha]}} & \dfrac{\forall\alpha \mathsf{P}}{\underline{\mathsf{P}[m/\alpha]}} & \underline{\forall\alpha \mathsf{P}} \\ \vdots & \vdots & \vdots\end{matrix}}{C} \qquad \dfrac{\begin{matrix}\exists\alpha\neg \mathsf{P}\\ \vdots\end{matrix}}{C}}{C}$$

Logical Interpretation (2)

$$\dfrac{\dfrac{\begin{matrix}\dfrac{\forall\alpha P}{P[n/\alpha]} & \dfrac{\forall\alpha P}{P[m/\alpha]}\\ \vdots & \vdots\end{matrix}}{C} \qquad \dfrac{\begin{matrix}\exists\alpha\neg P\\ \vdots\end{matrix}}{C}}{C}$$

Converts to:

$$\dfrac{\begin{matrix}\dfrac{\Pi_0}{P[n/\alpha]} & \dfrac{\Pi_1}{P[m/\alpha]}\\ \vdots & \vdots\end{matrix}}{C}$$

Logical Interpretation (3)

$$
\dfrac{
  \dfrac{
    \begin{array}{cc}
      \dfrac{\dfrac{\forall\alpha \mathsf{P}}{\mathsf{P}[n/\alpha] = \texttt{False}}}{\vdots}
      &
      \dfrac{\dfrac{\forall\alpha \mathsf{P}}{\mathsf{P}[m/\alpha]}}{\vdots}
    \end{array}
  }{C}
  \qquad
  \dfrac{\begin{array}{c}\exists\alpha\neg \mathsf{P} \\ \vdots\end{array}}{C}
}{C}
$$

Converts to:

$$
\dfrac{
  \begin{array}{c}
    \dfrac{\dfrac{\sqcap}{\neg \mathsf{P}[n/\alpha]}}{\exists\alpha\neg \mathsf{P}} \\
    \vdots
  \end{array}
}{C}
$$

$$t \Vdash A$$

Realizability

$$t \Vdash A$$

t may contain free hypotheses $H_a^{\forall \alpha P}$

Realizability (2)

- $t \Vdash A \to B$ if and only if for all u, if $u \Vdash A$, then $tu \Vdash B$

Realizability (2)

- $t \Vdash A \rightarrow B$ if and only if for all u, if $u \Vdash A$, then $tu \Vdash B$
- $t \Vdash A \wedge B$ if and only if $\pi_0 t \Vdash A$ and $\pi_1 t \Vdash B$

Realizability (2)

- $t \Vdash A \to B$ if and only if for all u, if $u \Vdash A$, then $tu \Vdash B$
- $t \Vdash A \wedge B$ if and only if $\pi_0 t \Vdash A$ and $\pi_1 t \Vdash B$
- $t \Vdash \forall \alpha^{\mathbb{N}} A$ if and only if for every numeral n, $tn \Vdash A[n/\alpha]$

Realizability (3)

- $t \Vdash A \vee B$ if and only if one of the following holds:

  i) $t = \iota_0(u)$ and $u \Vdash A$ or $t = \iota_1(u)$ and $u \Vdash B$;

- $t \Vdash A \vee B$ if and only if one of the following holds:

  i) $t = \iota_0(u)$ and $u \Vdash A$ or $t = \iota_1(u)$ and $u \Vdash B$;

  ii) $t = u \parallel_a v$ and $u \Vdash A \vee B$ and $v[a := m] \Vdash A \vee B$ for every numeral m;
  ($v[a := m] = v[\mathsf{W}_a^{\exists\alpha\neg\mathsf{P}} := (m, \mathsf{H}_a^{\forall\alpha.\alpha=0}\mathsf{S0})]$ if m is not a witness for P)

Realizability (3)

- $t \Vdash A \vee B$ if and only if one of the following holds:

  i) $t = \iota_0(u)$ and $u \Vdash A$ or $t = \iota_1(u)$ and $u \Vdash B$;

  ii) $t = u \parallel_a v$ and $u \Vdash A \vee B$ and $v[a := m] \Vdash A \vee B$ for every numeral m;
  ($v[a := m] = v[\mathsf{W}_a^{\exists\alpha\neg\mathsf{P}} := (m, \mathsf{H}_a^{\forall\alpha.\alpha=0}\mathsf{S0})]$ if m is not a witness for P)

  iii) $t \notin \mathsf{NF}$ is neutral and for all t', $t \mapsto t'$ implies $t' \Vdash A \vee B$.

Realizability (3)

- $t \Vdash A \vee B$ if and only if one of the following holds:

  i) $t = \iota_0(u)$ and $u \Vdash A$ or $t = \iota_1(u)$ and $u \Vdash B$;

  ii) $t = u \parallel_a v$ and $u \Vdash A \vee B$ and $v[a := m] \Vdash A \vee B$ for every numeral m;
  ($v[a := m] = v[\mathsf{W}_a^{\exists\alpha\neg \mathsf{P}} := (m, \mathsf{H}_a^{\forall\alpha.\alpha=0}\mathsf{S}0)]$ if m is not a witness for P)

  iii) $t \notin \mathsf{NF}$ is neutral and for all t', $t \mapsto t'$ implies $t' \Vdash A \vee B$.

- $t \Vdash \exists\alpha^{\mathrm{N}} A$ if and only if one of the following holds:

  i) $t = (n, u)$ for some numeral n and $u \Vdash A[n/\alpha]$;

Realizability (3)

- $t \Vdash A \vee B$ if and only if one of the following holds:

  i) $t = \iota_0(u)$ and $u \Vdash A$ or $t = \iota_1(u)$ and $u \Vdash B$;

  ii) $t = u \parallel_a v$ and $u \Vdash A \vee B$ and $v[a := m] \Vdash A \vee B$ for every numeral m;
  ($v[a := m] = v[\mathrm{W}_a^{\exists\alpha\neg\mathrm{P}} := (m, \mathrm{H}_a^{\forall\alpha.\alpha=0}\mathrm{S0})]$ if m is not a witness for P)

  iii) $t \notin$ NF is neutral and for all t', $t \mapsto t'$ implies $t' \Vdash A \vee B$.

- $t \Vdash \exists\alpha^{\mathrm{N}} A$ if and only if one of the following holds:

  i) $t = (n, u)$ for some numeral n and $u \Vdash A[n/\alpha]$;

  ii) $t = u \parallel_a v$ and $u \Vdash \exists\alpha^{\mathrm{N}} A$ and $v[a := m] \Vdash \exists\alpha^{\mathrm{N}} A$ for every numeral m

  iii) $t \notin$ NF is neutral and for all t', $t \mapsto t'$ implies $t' \Vdash \exists\alpha^{\mathrm{N}} A$.

Realizability (4)

$t \Vdash \mathsf{P}$ if and only if one of the following holds:

i) $t \in \mathsf{NF}$ and $\mathsf{P} = \mathtt{False}$ implies t contains a subterm $\mathsf{H}_a^{\forall\alpha\mathsf{Q}} n$ with $\mathsf{Q}[n/\alpha] = \mathtt{False}$;

Realizability (4)

$t \Vdash$ P if and only if one of the following holds:

i) $t \in$ NF and P $=$ `False` implies t contains a subterm $\mathsf{H}_a^{\forall \alpha \mathsf{Q}} n$ with $\mathsf{Q}[n/\alpha] =$ `False`;

ii) $t = u \parallel_a v$ and $u \Vdash$ P and $v[a := m] \Vdash$ P for every numeral m;

$t \Vdash \mathsf{P}$ if and only if one of the following holds:

i) $t \in \mathsf{NF}$ and $\mathsf{P} = \mathtt{False}$ implies t contains a subterm $\mathsf{H}_a^{\forall \alpha \mathsf{Q}} n$ with $\mathsf{Q}[n/\alpha] = \mathtt{False}$;

ii) $t = u \parallel_a v$ and $u \Vdash \mathsf{P}$ and $v[a := m] \Vdash \mathsf{P}$ for every numeral m;

iii) $t \notin \mathsf{NF}$ is neutral and for all t', $t \mapsto t'$ implies $t' \Vdash \mathsf{P}$

$$\mathrm{HA} + \mathrm{EM}_1 \vdash t : A \implies t \Vdash A$$

Soundness, Strong Normalization, Witness Extraction

$$\mathsf{HA} + \mathsf{EM}_1 \vdash t : A \implies t \Vdash A$$

$$t \Vdash A \implies t \in \mathsf{SN}$$

Soundness, Strong Normalization, Witness Extraction

$$\mathsf{HA} + \mathsf{EM}_1 \vdash t : A \implies t \Vdash A$$

$$t \Vdash A \implies t \in \mathsf{SN}$$

$$t \Vdash \exists \alpha \mathsf{P} \implies t \mapsto^* (n, u) \wedge \mathsf{P}[n/\alpha]$$

Disjunction Property and Existence Property

EM_1^-(Q atomic) :

$$\frac{\Gamma, a : \forall \alpha^{\mathbb{N}} \mathsf{P} \vdash u : \exists \beta\, \mathsf{Q} \qquad \Gamma, a : \exists \alpha^{\mathbb{N}} \neg \mathsf{P} \vdash v : \exists \beta\, \mathsf{Q}}{\Gamma \vdash u \parallel_a v : \exists \beta\, \mathsf{Q}}$$

$$\mathsf{HA} + \mathsf{EM}_1^- \vdash A \vee B \implies \mathsf{HA} + \mathsf{EM}_1^- \vdash A \text{ or } \mathsf{HA} + \mathsf{EM}_1^- \vdash B$$

$$\mathsf{HA} + \mathsf{EM}_1^- \vdash \exists \alpha A \implies \mathsf{HA} + \mathsf{EM}_1^- \vdash A(n)$$