On the algorithmic structure of Dialectica realisers

Davide Barbarossa, Thomas Powell

Funded by: Imperative Programs from Proofs (EPSRC)

davide.barbarossa@ens-lyon.fr

https://davidebarbarossa12.github.io/

Laboratoire de l'Informatique du Parallélisme — ENS DE LYON

Department of Computer Science — UNIVERSITY OF BATH

CLS 2026, Paris (France)

25/02/2026

Table of contents

1. Dialectica in a nutshell
2. Dialectica Hoare Logic
3. Well-founded Loop and Classical Logic
4. Towards a Procedural Treatment of Dialectica
5. Conclusions

Dialectica in a nutshell

Gödel ('41/'58)	$A \in \mathrm{HA} \quad \longmapsto \quad \lvert A \rvert_c^w \in \mathbf{T}$ *such that* $\vdash_{\mathrm{HA}} A \quad \Longrightarrow \quad$ *there is* $\mathtt{M} \in \mathbf{T}$ *s.t.* $\vdash_{\mathbf{T}} \forall c. \lvert A \rvert_c^{\mathtt{M}}$

Dialectica in a nutshell

Gödel ('41/'58)	$A \in \mathrm{HA} \quad \longmapsto \quad |A|^w_c \in \mathbf{T}$ *such that* $\vdash_{\mathrm{HA}} A \quad \Longrightarrow \quad$ *there is* $\mathtt{M} \in \mathbf{T}$ *s.t.* $\vdash_{\mathbf{T}} \forall c. |A|^{\mathtt{M}}_c$
Kreisel (∼'50) Kohlenbach(∼90) ...	*Several variants and extensions (⇒ "Proof Mining")*

Dialectica in a nutshell

Gödel ('41/'58)	$A \in \mathrm{HA} \quad \longmapsto \quad \|A\|_c^w \in \mathbf{T}$ *such that* $\vdash_{\mathrm{HA}} A \quad \Longrightarrow \quad$ *there is* $\mathtt{M} \in \mathbf{T}$ *s.t.* $\vdash_{\mathbf{T}} \forall c. \|A\|_c^{\mathtt{M}}$
Kreisel (∼'50) Kohlenbach(∼90) …	*Several variants and extensions (⇒ "Proof Mining")*
De Paiva ('91)	*Dialectica Categories (and models of Linear Logic)*

Dialectica in a nutshell

Gödel ('41/'58)	$A \in \mathrm{HA} \longmapsto \lvert A\rvert^w_c \in \mathbf{T}$ *such that* $\vdash_{\mathrm{HA}} A \Longrightarrow$ *there is* $\mathtt{M} \in \mathbf{T}$ *s.t.* $\vdash_{\mathbf{T}} \forall c.\, \lvert A\rvert^{\mathtt{M}}_c$
Kreisel (∼'50) Kohlenbach(∼90) ...	*Several variants and extensions (⇒ "Proof Mining")*
De Paiva ('91)	*Dialectica Categories (and models of Linear Logic)*
Pédrot ('14)	$A \in \mathit{source} \longmapsto W(A), C(A) \in \mathit{target}$ $\mathtt{M} \in \mathit{source} \longmapsto \mathtt{M}^\bullet, \mathtt{M}_{\mathtt{x}} \in \mathit{target}$ *such that* $\mathtt{x} : A \vdash_{\mathit{source}} \mathtt{M} : B \Longrightarrow \begin{cases} \mathtt{x} : W(A) \vdash_{\mathit{target}} \mathtt{M}^\bullet : W(B) \\ \mathtt{x} : W(A) \vdash_{\mathit{target}} \mathtt{M}_{\mathtt{x}} : C(B) \to C(A) \end{cases}$

High-order Weak-Extensional Heyting-Arithmetic (WE-HA$^\omega$)

High-order Weak-Extensional Heyting-Arithmetic (WE-HA$^{\omega}$)

- PL of terms: Simply typed System **T** with ground type `nat`

High-order Weak-Extensional Heyting-Arithmetic (WE-HA$^\omega$)

- PL of terms: Simply typed System **T** with ground type `nat`
- Formulas: $\top, \bot, =_{\texttt{nat}}, \wedge, \vee, \rightarrow, \forall^X, \exists^X$ and $(t =_{X \to Y} s) := \forall^X x.(tx =_Y sx)$

$$(A \vee_{b^{\texttt{nat}}} B) := ((b =_{\texttt{nat}} 0) \rightarrow A) \wedge ((b \neq_{\texttt{nat}} 0) \rightarrow B)$$

High-order Weak-Extensional Heyting-Arithmetic (WE-HA$^\omega$)

- PL of terms: Simply typed System **T** with ground type `nat`
- Formulas: $\top, \bot, =_{\texttt{nat}}, \wedge, \vee, \rightarrow, \forall^X, \exists^X$ and $(t =_{X\rightarrow Y} s) := \forall^X x.(tx =_Y sx)$

$$(A \vee_{b^{\texttt{nat}}} B) := ((b =_{\texttt{nat}} 0) \rightarrow A) \wedge ((b \neq_{\texttt{nat}} 0) \rightarrow B)$$

- Axioms:

$$\textit{equality}$$
$$+$$
$$\textit{arithmetic}$$
$$+$$
$$(\texttt{if}\ b\ \texttt{then}\ s\ \texttt{else}\ t = s) \vee_b (\texttt{if}\ b\ \texttt{then}\ s\ \texttt{else}\ t = t)$$
$$+$$
$$(\texttt{rec}\ f\ g\ n = g) \vee_n (\texttt{rec}\ f\ g\ n = f\ (n-1)\ (\texttt{rec}\ f\ g\ (n-1)))$$

High-order Weak-Extensional Heyting-Arithmetic (WE-HA$^\omega$)

- PL of terms: Simply typed System **T** with ground type `nat`
- Formulas: $\top, \bot, =_{\mathtt{nat}}, \wedge, \vee, \rightarrow, \forall^X, \exists^X$ and $(t =_{X \rightarrow Y} s) := \forall^X x.(tx =_Y sx)$

$$(A \vee_{b^{\mathtt{nat}}} B) := ((b =_{\mathtt{nat}} 0) \rightarrow A) \wedge ((b \neq_{\mathtt{nat}} 0) \rightarrow B)$$

- Axioms:

$$\begin{gathered} \textit{equality} \\ + \\ \textit{arithmetic} \\ + \\ (\mathbf{if}\ b\ \mathbf{then}\ s\ \mathbf{else}\ t = s) \vee_b (\mathbf{if}\ b\ \mathbf{then}\ s\ \mathbf{else}\ t = t) \\ + \\ (\mathbf{rec}\ f\ g\ n = g) \vee_n (\mathbf{rec}\ f\ g\ n = f\ (n-1)\ (\mathbf{rec}\ f\ g\ (n-1))) \end{gathered}$$

- Rules:

$$\begin{gathered} \textit{Intuitionistic Logic} \\ + \\ \frac{A_0 \rightarrow t = s \qquad A_0 \ \textit{quantifier free}}{A_0 \rightarrow B\{x := t\} \rightarrow B\{x := s\}} \end{gathered}$$

Dialectica for WE-HA$^\omega$ in WE-HA$^\omega$

$$\begin{array}{ccc} \textit{Formulas} & \longrightarrow & \textit{quant.-free Formulas} \times \vec{\mathbf{T}} \times \vec{\mathbf{T}} \\ A & \longmapsto & (\,|A|_c^w \quad , \quad W(A)\;,\; C(B)\,) \end{array}$$

Dialectica for WE-HA$^\omega$ in WE-HA$^\omega$

$$\begin{array}{ccc} \textit{Formulas} & \longrightarrow & \textit{quant.-free Formulas} \times \vec{\mathbf{T}} \times \vec{\mathbf{T}} \\ A & \longmapsto & (\,|A|^w_c \quad , \quad W(A)\;,\; C(B)\,) \end{array}$$

defined by:

$$\begin{array}{rcll} |A|^\emptyset_\emptyset & := & A & \textit{if } A \textit{ is atomic} \\ |A \wedge B|^{x,u}_{y,v} & := & |A|^x_y \wedge |B|^u_v & \\ |A \vee B|^{b^{\text{nat}},x,u}_{y,v} & := & |A|^x_y \vee_{b^{\text{nat}}} |B|^u_v & \\ |A \to B|^{f,F}_{x,v} & := & |A|^x_{Fxv} \to |B|^{fx}_v & \\ |\forall x.A|^f_{z,y} & := & |A\{x := z\}|^{fz}_y & \\ |\exists x.A|^{z,u}_y & := & |A\{x := z\}|^u_y & \end{array}$$

Dialectica for WE-HA$^\omega$ in WE-HA$^\omega$

$$\begin{array}{rcl} \textit{Formulas} & \longrightarrow & \textit{quant.-free Formulas} \times \vec{\mathbf{T}} \times \vec{\mathbf{T}} \\ A & \longmapsto & (\,|A|^w_c \quad , \quad W(A)\,,\, C(B)\,) \end{array}$$

Theorem (Soundness of Dialectica)

Let $\vdash_{\textit{WE-HA}^\omega} A$. *Then*

$$\vdash_{\textit{WE-HA}^\omega} \forall c.\,|A|^{\mathtt{a}}_c$$

where $\mathtt{a} \in \boldsymbol{T}$ *is "extracted" from the proof of* A

Dialectica for $\mathbf{WE\text{-}HA}^\omega$ in $\mathbf{WE\text{-}HA}^\omega$

$$\begin{array}{ccc} \textit{Formulas} & \longrightarrow & \textit{quant.-free Formulas} \times \vec{\mathbf{T}} \times \vec{\mathbf{T}} \\ A & \longmapsto & (\,|A|^w_c \;,\; W(A)\;,\; C(B)\,) \end{array}$$

Theorem (Soundness of Dialectica)

Let $\Delta \vdash_{WE\text{-}HA^\omega} A$. Then

$$\Delta' \vdash_{WE\text{-}HA^\omega} \forall c.\, |\Delta|^{\mathtt{d}}_c \Longrightarrow \Delta' \vdash_{WE\text{-}HA^\omega} \forall c.\, |A|^{\mathtt{a}}_c$$

where $\mathtt{a} \in \boldsymbol{T}$ is "extracted" from a proof of A

Dialectica for WE-HA$^\omega$ in WE-HA$^\omega$

$$\begin{array}{ccc} \textit{Formulas} & \longrightarrow & \textit{quant.-free Formulas} \times \vec{\mathbf{T}} \times \vec{\mathbf{T}} \\ A & \longmapsto & (\,|A|^w_c \;,\; W(A)\;,\; C(B)\,) \end{array}$$

Theorem (Soundness of Dialectica)

Gödel inductively defines a ***program transformation*** $(\_) \longmapsto (\_)^\bullet$ *which meets the following specification:*

If $\mathtt{x} : \Delta \vdash_{\textit{WE-HA}^\omega} \mathtt{M} : A$*, then:*

$$\Delta' \vdash_{\textit{WE-HA}^\omega} \forall c.\, |\Delta|^{\mathtt{d}}_c \implies \Delta' \vdash_{\textit{WE-HA}^\omega} \forall c.\, |A|^{\mathtt{M}^\bullet\{\mathtt{x}:=\mathtt{d}\}}_c$$

Dialectica for WE-HA$^\omega$ in WE-HA$^\omega$

$$\begin{array}{ccc} \textit{Formulas} & \longrightarrow & \textit{quant.-free Formulas} \times \vec{\mathbf{T}} \times \vec{\mathbf{T}} \\ A & \longmapsto & (\,|A|_c^w \;,\; W(A)\,,\, C(B)\,) \end{array}$$

Theorem (Soundness of Dialectica)

Gödel inductively defines a ***program transformation*** $(\_) \longmapsto (\_)^\bullet$ *which meets the following specification:*

If $\mathtt{x} : \Delta \vdash_{\textit{WE-HA}^\omega} \mathtt{M} : A$, *then:*

$$\Delta' \vdash_{\textit{WE-HA}^\omega} \forall c.\, |\Delta|_c^{\mathtt{d}} \implies \Delta' \vdash_{\textit{WE-HA}^\omega} \forall c.\, |A|_c^{\mathtt{M}^\bullet\{\mathtt{x}:=\mathtt{d}\}}$$

– *If I add the logical principles in* Δ, *which computational principles should I add in* Δ' *in order to justify the former?*

– *Which is the theory* Δ *of formulas that are justifiable (in the empty* Δ'*)?*

Hoare Triple: $A\langle f\rangle B$

Intuition: f : state $\to$ state and it "justifies" $A \to B$

Hoare Triple: $A\langle f\rangle B$

Intuition: f : state $\to$ state and it "justifies" $A \to B$ in the sense of the formula

$$\forall^{\text{state}} s.(\, A\{x := s\} \to B\{x := fs\}\,)$$

Hoare Triple: $A\langle f\rangle B$

Intuition: f : state $\rightarrow$ state and it "justifies" $A \rightarrow B$ in the sense of the formula

$$\forall^{\text{state}} s. (\, A\{x := s\} \rightarrow B\{x := f s\}\,)$$

Theorem (Hoare Logic Soundness)

If the judgment $A\langle f\rangle B$ is derivable, then the formula above is provable (in some ambient theory, say WE-HA$^{\omega}$).

Hoare Triple: $A\langle f\rangle B$

Intuition: $f : \text{state} \to \text{state}$ and it "justifies" $A \to B$ in the sense of the formula

$$\forall^{\text{state}} s.(\, A\{x := s\} \to B\{x := fs\}\,)$$

Theorem (Hoare Logic Soundness)

If the judgment $A\langle f\rangle B$ is derivable, then the formula above is provable (in some ambient theory, say WE-HA$^\omega$).

Say A and B are quantifier-free. Then the above formula is:

$$\forall^{\text{state}} s.(\, A\{x := s\} \to B\{x := fs\}\,)$$

Hoare Triple: $A\langle f\rangle B$

Intuition: f : state → state and it "justifies" $A \to B$ in the sense of the formula

$$\forall^{\text{state}} s.(\, A\{x := s\} \to B\{x := fs\}\,)$$

Theorem (Hoare Logic Soundness)

If the judgment $A\langle f\rangle B$ is derivable, then the formula above is provable (in some ambient theory, say WE-HA$^\omega$).

Say A and B are quantifier-free. Then the above formula is:

$$\forall^{\text{state}} s.(\, |A\{x := s\}|^{\emptyset}_{\emptyset} \to |B\{x := fs\}|^{\emptyset}_{\emptyset}\,)$$

Hoare Triple: $A\langle f\rangle B$

Intuition: f : state $\to$ state and it "justifies" $A \to B$ in the sense of the formula

$$\forall^{\text{state}} s.(\, A\{x := s\} \to B\{x := fs\}\,)$$

Theorem (Hoare Logic Soundness)

If the judgment $A\langle f\rangle B$ is derivable, then the formula above is provable (in some ambient theory, say WE-HA$^{\omega}$).

Say A and B are quantifier-free. Then the above formula is:

$$\forall^{\text{state}} s.(\, |\exists^{\text{state}} x.A|^{s,\emptyset}_{\emptyset} \to |\exists^{\text{state}} x.B|^{fs,\emptyset}_{\emptyset}\,)$$

Hoare Triple: $A\langle f\rangle B$

Intuition: f : state $\to$ state and it "justifies" $A \to B$ in the sense of the formula

$$\forall^{\text{state}} s.(\, A\{x := s\} \to B\{x := fs\}\,)$$

Theorem (Hoare Logic Soundness)

If the judgment $A\langle f\rangle B$ is derivable, then the formula above is provable (in some ambient theory, say WE-HA$^\omega$).

Say A and B are quantifier-free. Then the above formula is:

$$\forall^{\text{state}} s.\ \left|\exists^{\text{state}} x.A \to \exists^{\text{state}} x.B\right|^{f,\emptyset}_{(s,\emptyset),\emptyset}$$

Hoare Triple: $A\langle f\rangle B$

Intuition: f : state $\to$ state and it "justifies" $A \to B$ in the sense of the formula

$$\forall^{\text{state}} s.(\, A\{x := s\} \to B\{x := fs\}\,)$$

Theorem (Hoare Logic Soundness)

If the judgment $A\langle f\rangle B$ is derivable, then the formula above is provable (in some ambient theory, say WE-HA$^\omega$).

Say A and B are quantifier-free. Then the above formula is:

$$\forall^{\text{state}} s.\ \left|\exists^{\text{state}} x.A \to \exists^{\text{state}} x.B\right|^{f,\emptyset}_{(s,\emptyset),\emptyset}$$

Let's take this seriously in all its generality:

$$A\,\langle \mathtt{f} \mid \mathtt{F}\rangle\, B := \forall s, v.\ |A \to B|^{\mathtt{f},\mathtt{F}}_{s,v}$$

for A, B any formulas. Intuition: $\langle \mathtt{f} \mid \mathtt{F}\rangle$ "justifies" $A \to B$.

Dialectica Hoare Logic (DHL)

Rules for deriving judgments $A \langle \mathtt{f} \mid \mathtt{F} \rangle B$, with $A, B \in \text{WE-HA}^\omega$ and $\mathtt{f}, \mathtt{F} \in \mathbf{T}$

Dialectica Hoare Logic (DHL)

Rules for deriving judgments $A\,\langle \mathtt{f} \mid \mathtt{F} \rangle\, B$, with $A, B \in \text{WE-HA}^{\omega}$ and $\mathtt{f}, \mathtt{F} \in \mathbf{T}$, such that

Theorem (Dialectica Hoare Logic Soundness)

If the judgment

$$A\,\langle \mathtt{f} \mid \mathtt{F} \rangle\, B$$

is derivable in DHL, then $\mathtt{f}, \mathtt{F}$ *justify* $A \to B$*, i.e.*

$$\vdash_{\textit{WE-HA}^{\omega}} \quad \forall s\, v.\ |A|^{s}_{\mathtt{F}sv} \to |B|^{\mathtt{f}s}_{v}\ .$$

Dialectica Hoare Logic (DHL)

Rules for deriving judgments $A \langle \mathtt{f} \,|\, \mathtt{F} \rangle B$, with $A, B \in \text{WE-HA}^\omega$ and $\mathtt{f}, \mathtt{F} \in \mathbf{T}$, such that

Theorem (Dialectica Hoare Logic Soundness)

If the judgment

$$A \langle \mathtt{f} \,|\, \mathtt{F} \rangle B$$

is derivable in DHL, then $\mathtt{f}, \mathtt{F}$ *justify* $A \to B$*, i.e.*

$$\vdash_{\mathit{WE\text{-}HA}^\omega} \quad \forall s\, v.\ |A|^{s}_{\mathtt{F}sv} \to |B|^{\mathtt{f}s}_{v}\ .$$

Usual Soundness Theorem by Gödel. But with the focus on programs $\mathtt{f}, \mathtt{F}$ and DHL as a specification system for them, instead of on formulas.

Dialectica Hoare Logic

$$\bot\ \langle a \mid - \rangle\ P \qquad P\ \langle - \mid \alpha \rangle\ \top \qquad P\ \langle \mathtt{I} \mid \mathtt{proj}_2 \rangle\ P \qquad \frac{P_\exists \to Q_\forall \in \mathrm{Ax}}{P_\exists\ \langle - \mid - \rangle\ Q_\forall} \qquad \frac{P_\exists\ \langle - \mid - \rangle\ Q_\forall}{P'_\exists\ \langle - \mid - \rangle\ Q'_\forall}\ \text{for}\ \frac{P_\exists \to Q_\forall}{P'_\exists \to Q'_\forall} \in \mathrm{Rule}$$

$$\frac{P\ \langle a, b \mid \alpha \rangle\ Q \wedge R}{P\ \langle b, a \mid \tilde{\alpha} \rangle\ R \wedge Q}\,p\wedge_R \qquad \frac{P \wedge Q\ \langle a \mid \alpha, \beta \rangle\ R}{Q \wedge P\ \langle \tilde{a} \mid \tilde{\beta}, \tilde{\alpha} \rangle\ R}\,p\wedge_L \qquad \frac{P\ \langle a, b \mid \alpha \rangle\ Q \vee_c R}{P\ \langle b, a \mid \tilde{\alpha} \rangle\ R \vee_{\bar{c}} Q}\,p\vee_R \qquad \frac{P \vee_c Q\ \langle a \mid \alpha, \beta \rangle\ R}{Q \vee_{\bar{c}} P\ \langle \tilde{a} \mid \tilde{\beta}, \tilde{\alpha} \rangle\ R}\,p\vee_L$$

$$\frac{P\ \langle a \mid \alpha \rangle\ Q}{P\ \langle a, b \mid \alpha_\pi \rangle\ Q \vee_0 R}\vee_R \qquad \frac{P\ \langle a \mid \alpha \rangle\ Q}{P \wedge R\ \langle a_\pi \mid \alpha_\pi, \beta \rangle\ Q}\wedge_L \qquad \frac{P\ \langle a, b \mid \alpha \rangle\ Q \wedge R}{P\ \langle a \mid \alpha_p \rangle\ Q}\wedge_R \qquad \frac{P \vee_0 R\ \langle a \mid \alpha, \beta \rangle\ Q}{P\ \langle a_p \mid \alpha_p \rangle\ Q}\vee_L$$

$$\frac{P \wedge \phi\ \langle a \mid \alpha \rangle\ R \quad Q \wedge \neg\phi\ \langle b \mid \beta \rangle\ R \quad \phi\ qf}{P \vee Q\ \langle \lambda x, y.\,\mathsf{if}\ \phi\ \mathsf{then}\ ax\ \mathsf{else}\ by \mid \alpha_\pi, \beta_\pi \rangle\ R}\,cond_L \qquad \frac{P\ \langle a \mid \alpha \rangle\ Q \quad P\ \langle b \mid \beta \rangle\ R}{P\ \langle a, b \mid \lambda x, v, w.\,\mathsf{if}\ |P|^x_{\alpha x v}\ \mathsf{then}\ \beta x w\ \mathsf{else}\ \alpha x v \rangle\ Q \wedge R}\,cond_R$$

$$\frac{P\ \langle a, b \mid \alpha \rangle\ Q \to R}{P \wedge Q\ \langle a \mid \alpha, b \rangle\ R}\,uncurry \qquad \frac{P \wedge Q\ \langle a \mid \alpha, \beta \rangle\ R}{P\ \langle a, \beta \mid \alpha \rangle\ Q \to R}\,curry \qquad \frac{P\ \langle a \mid \alpha \rangle\ Q \quad Q\ \langle b \mid \beta \rangle\ R}{P\ \langle \lambda x.b(a(x)) \mid \lambda x, w.\ \alpha x(\beta(ax)w) \rangle\ R}\,comp$$

$$\frac{P\ \langle a \mid \alpha \rangle\ Q(t)}{P\ \langle \lambda\_.t, a \mid \alpha \rangle\ \exists x\, Q(x)}\exists_R \qquad \frac{P(t)\ \langle a \mid \alpha \rangle\ Q}{\forall x\, P(x)\ \langle \lambda f.a(ft) \mid \lambda\_.t, \lambda f.\alpha(ft) \rangle\ Q}\forall_L$$

$$\frac{P(x)\ \langle a \mid \alpha \rangle\ Q}{\exists x\, P(x)\ \langle \lambda x.a \mid \lambda x.\alpha \rangle\ Q}\exists_L (x \notin Q) \qquad \frac{P\ \langle a \mid \alpha \rangle\ Q(x)}{P\ \langle \lambda y, x.ay \mid \lambda y, x.\alpha y \rangle\ \forall x\, Q(x)}\forall_R (x \notin P)$$

$$\frac{\exists x\, P(x)\ \langle a \mid \alpha \rangle\ Q}{P(t)\ \langle at \mid \alpha t \rangle\ Q}\,s_L \qquad \frac{P\ \langle a \mid \alpha \rangle\ \forall x\, Q(x)}{P\ \langle \lambda y.ayt \mid \lambda y, v.\alpha y t v \rangle\ Q(t)}\,s_R \qquad \frac{P_\forall\ \langle a, b \mid \alpha \rangle\ \exists x\, Q(x)}{P_\forall\ \langle b \mid \alpha \rangle\ Q(a)}\,\epsilon_R \qquad \frac{\forall x\, P_\forall(x)\ \langle - \mid \alpha, \beta \rangle\ Q_{qf}}{P_\forall(\alpha)\ \langle - \mid \beta \rangle\ Q_{qf}}\,\epsilon_L$$

$$\frac{P'\ \langle \mathtt{I} \mid \mathtt{proj}_2 \rangle\ P \quad P\ \langle a \mid \alpha \rangle\ Q \quad Q\ \langle \mathtt{I} \mid \mathtt{proj}_2 \rangle\ Q'}{P'\ \langle a \mid \alpha \rangle\ Q'}\,cons \qquad \frac{P\ \langle a \mid \alpha \rangle\ Q \quad a, \alpha = b, \beta}{P\ \langle b \mid \beta \rangle\ Q}\,ext \qquad \frac{P(x)\ \langle a(x) \mid \alpha(x) \rangle\ P(x+1)}{P(0)\ \langle \mathsf{rec}\ a \mid \mathsf{rec}^*\, a\, \alpha \rangle\ \forall x.\ P(x)}\,ind$$

Update WE-HA$^{\omega}$

Update WE-HA$^\omega$

- Term PL: $\cdots \mid \prec : X \to X \to \mathtt{nat}$
  $\mid \mathtt{whilerec}_{\phi,a} : (X \to U) \to (X \to U \to U) \to X \to U$
- Formulas: same as before
- Axioms: same as before + the following for $\phi\{x\}$ q.f.:

$$(\phi\{x := y\} \to ay \prec y) \to$$
$$\mathtt{whilerec}_{\phi,a}\, u\, F\, y =_U \mathtt{if}\ \phi\{x := y\}\ \mathtt{then}\ F\, y\, (\mathtt{whilerec}_{\phi,a}\, u\, F\, (ay))\ \mathtt{else}\ (uy)$$

- Rules: same as before + $\dfrac{\forall x. ((\forall y \prec x. A\{x := y\}) \to A)}{\forall x. A}$ *(w.-f. induction)*

Update WE-HA$^\omega$

- Term PL: $\cdots \mid \prec: X \to X \to \mathtt{nat}$
  $\mid \mathtt{whilerec}_{\phi,a} : (X \to U) \to (X \to U \to U) \to X \to U$
- Formulas: same as before
- Axioms: same as before + the following for $\phi\{x\}$ q.f.:

$$(\phi\{x := y\} \to ay \prec y) \to$$
$$\mathtt{whilerec}_{\phi,a}\, u\, F\, y =_U \mathtt{if}\ \phi\{x := y\}\ \mathtt{then}\ F\, y\, (\mathtt{whilerec}_{\phi,a}\, u\, F\, (ay))\ \mathtt{else}\ (uy)$$

- Rules: same as before + $\dfrac{\forall x. (\, (\forall y \prec x. A\{x := y\}) \to A\,)}{\forall x. A}$ *(w.-f. induction)*

Remark

The sugars

$$\begin{array}{rcllll} \mathtt{while}\, \phi\, \mathtt{do}\, a & := & \mathtt{whilerec}_{\phi,a} & \mathtt{I} & \mathtt{proj}_2 & : X \to X \\ \mathtt{while}^*\, \phi\, \mathtt{do}\, (a, \alpha) & := & \mathtt{whilerec}_{\phi,a} & \mathtt{proj}_2 & (\lambda x, f, v.\, \alpha x(fv)) & : X \to V \to V \end{array}$$

behave in WE-HA$^\omega$ like a usual *well-founded* while and a backward while, resp.

Dialectica with While

Add to DHL the rule:

$$\frac{\exists x.\,(P_\forall(x) \wedge \phi(x)) \ \langle a \,|\, \alpha\rangle \ \exists x.P_\forall(x) \qquad \forall x.\,(\phi(x) \to ax \prec x)}{\exists x.P_\forall(x)\,\langle\, \texttt{while}\,\phi\ \texttt{do}\ a \,|\, \texttt{while}^*\,\phi\,\texttt{do}\,(a,\alpha)\rangle\ \exists x.\,(P_\forall(x) \wedge \neg\phi(x))}$$

Theorem

Dialectica Hoare Logic Soundness keeps holding, i.e. the $\texttt{f}, \texttt{F}$ *(now with possible loops) in* $A\,\langle \texttt{f} \,|\, \texttt{F}\rangle\, B$ *still justify* $A \to B$ *(now with well-founded induction).*

A minimum principle: $\exists x.\, \theta \vdash \exists x.\, (\theta \wedge \forall y \prec x. \neg\, \theta(y))$

with $\prec$ well-founded and $\theta\{x^X\}$ quantifier-free.

$$
\dfrac{\dfrac{\dfrac{\dfrac{\overline{\theta \wedge \phi_g \,\langle - \mid - \rangle\, \theta(gx)}}{\theta \wedge \phi_g \,\langle gx \mid - \rangle\, \exists x.\, \theta}\ \exists_R}{\exists x.\, (\theta \wedge \phi_g)\,\langle g \mid - \rangle\, \exists x.\, \theta}\ \exists_L \qquad \forall x.\, (\phi_g \to gx \prec x)}{\exists x.\, \theta \,\langle \texttt{while}\ \phi_g\ \texttt{do}\ g \mid - \rangle\, \exists x.\, (\theta \wedge \neg\phi_g)}\ \mathit{while}}{\dfrac{\exists x.\, \theta \,\langle \lambda x, g.(\texttt{while}\ \phi_g\ \texttt{do}\ g)x \mid - \rangle\, \forall g \exists x.\, (\theta \wedge \neg\phi_g)}{\exists x.\, \theta \,\langle \lambda x, g.(\texttt{while}\ \phi_g\ \texttt{do}\ g)x \mid - \rangle\, \neg\neg\exists x.\, (\theta \wedge \forall y \prec x.\, \neg\theta(y))}\ N}\ \forall_R
$$

with $\phi_g := gx \prec x \wedge \theta(gx)$.

Idea: trial-and-error. (Appears very often in proof mining).

Fix fresh sets of commands $\overrightarrow{Comm}, \overleftarrow{Comm}$ of new types $S \to S$ and $S \to T \to T$. LOOP_D := IMP with commands from above and *without* variable allocation:

$$C ::= \texttt{skip} \mid \langle c \mid \gamma \rangle \mid C; C \mid \texttt{if}\ \phi\ \texttt{then}\ C\ \texttt{else}\ C \mid \texttt{while}\ \phi\ \texttt{do}\ C$$

Fix fresh sets of commands $\overrightarrow{Comm}, \overleftarrow{Comm}$ of new types $S \to S$ and $S \to T \to T$.
$\mathrm{LOOP}_D :=$ IMP with commands from above and *without* variable allocation:

$$C ::= \texttt{skip} \mid \langle c \mid \gamma \rangle \mid C; C \mid \texttt{if } \phi \texttt{ then } C \texttt{ else } C \mid \texttt{while } \phi \texttt{ do } C$$

Define a translation $\mathrm{LOOP}_D \to \mathbf{T}^{S \to S} \times \mathbf{T}^{S \to T \to T}$ as:

LOOP_D	$(\_)^+$	$(\_)^-$
$\langle c \mid \gamma \rangle$	c	γ
$\texttt{skip}$	$\texttt{I}$	$\texttt{proj}_2$
$C_1; C_2$	$\lambda x.\, C_2^+(C_1^+ x)$	$\lambda x, w.\ C_1^- x(C_2^-(C_1^+ x)w)$
$\texttt{if } \phi \texttt{ then } C_1 \texttt{ else } C_2$	$\lambda s.\texttt{if } \phi(s) \texttt{ then } C_1^+ s \texttt{ else } C_2^+ s$	$\lambda s, t.\texttt{if } \phi(s) \texttt{ then } C_1^- st \texttt{ else } C_2^- st$
$\texttt{while } \phi \texttt{ do } C$	$\texttt{while } \phi \texttt{ do } C^+$	$(\texttt{while}^* \phi \texttt{ do } C^+), C^-$

"Hoare Logic" for LOOP_D

$$\frac{}{[P]\,\texttt{skip}\,[P]} \qquad \frac{P(s,\gamma st) \to Q(cs,t) \in \text{Ax}}{[P]\,\langle c \mid \gamma\rangle\,[Q]} \qquad \frac{[P]\,C_1\,[Q] \quad [Q]\,C_2\,[R]}{[P]\,C_1; C_2\,[R]}$$

$$\frac{[P \wedge \phi(s)]\,C_1\,[R] \quad [Q \wedge \neg\phi(s)]\,C_2\,[R]}{[P \vee_{\phi(s)} Q]\,\texttt{if}\ \phi(s)\ \texttt{then}\ C_1\ \texttt{else}\ C_2\,[R]} \qquad \frac{[P \wedge \phi(s)]\,C\,[P] \quad \phi(s)(s) \to C^+ s \prec s}{[P]\,\texttt{while}\ \phi(s)\ \texttt{do}\ C\,[P \wedge \neg\phi(s)]}$$

$$\frac{P' \to P \quad [P]\,C\,[Q] \quad Q \to Q'}{[P']\,C\,[Q']}$$

"Hoare Logic" for LOOP$_D$

$$\frac{}{[P]\,\texttt{skip}\,[P]} \qquad \frac{P(s,\gamma st) \to Q(cs,t) \in \mathrm{Ax}}{[P]\,\langle c \,|\, \gamma\rangle\,[Q]} \qquad \frac{[P]\,C_1\,[Q] \quad [Q]\,C_2\,[R]}{[P]\,C_1; C_2\,[R]}$$

$$\frac{[P \wedge \phi(s)]\,C_1\,[R] \quad [Q \wedge \neg\phi(s)]\,C_2\,[R]}{[P \vee_{\phi(s)} Q]\,\texttt{if}\;\phi(s)\;\texttt{then}\;C_1\;\texttt{else}\;C_2\,[R]} \qquad \frac{[P \wedge \phi(s)]\,C\,[P] \quad \phi(s)(s) \to C^+ s \prec s}{[P]\,\texttt{while}\;\phi(s)\;\texttt{do}\;C\,[P \wedge \neg\phi(s)]}$$

$$\frac{P' \to P \quad [P]\,C\,[Q] \quad Q \to Q'}{[P']\,C\,[Q']}$$

Theorem (Soundness wrt Dialectica)

Restrict the above rules to quantifier-free formulas with only one variable s^S *and one* t^T*.*
If $[P]\,C\,[Q]$ *is derivable then DHL derives* $\exists^S s \forall^T t.P \;\langle C^+ \,|\, C^- \rangle\; \exists^S s \forall^T t.Q$ *and so*

$$\vdash_{\mathit{WE\text{-}HA}^\omega} \forall s,t.\,\big(P\{t := C^- st\} \to Q\{s := C^+ s\}\big)$$

Big-step Operational semantics of LOOP$_D$

Big-step Operational semantics of $\mathbf{LOOP}_D$

Forward OS: $\mathbf{T}^S \times \mathbf{LOOP}_D \vec{\Downarrow} \; \mathbf{T}^S \times (\mathbf{T}^S)^* \times (\mathbf{T}^{S\to T\to T})^*$

$$\frac{}{s, \texttt{skip} \vec{\Downarrow} s, [\,], [\,]} \qquad \frac{}{s, \langle c \,|\, \gamma \rangle \vec{\Downarrow} cs, s :: [\,], \gamma :: [\,]} \qquad \frac{s, C_1 \vec{\Downarrow} s', \sigma, \Gamma \quad s', C_2 \vec{\Downarrow} s'', \sigma', \Gamma'}{s, C_1 ; C_2 \vec{\Downarrow} s'', \sigma' :: \sigma, \Gamma' :: \Gamma}$$

$$\frac{\phi(s) \quad s, C_1 \vec{\Downarrow} s', \sigma, \Gamma}{s, \texttt{if } \phi \texttt{ then } C_1 \texttt{ else } C_2 \vec{\Downarrow} s', \sigma, \Gamma} \qquad \frac{\neg\phi(s) \quad s, C_2 \vec{\Downarrow} s', \sigma, \Gamma}{s, \texttt{if } \phi \texttt{ then } C_1 \texttt{ else } C_2 \vec{\Downarrow} s', \sigma, \Gamma}$$

$$\frac{\neg\phi(s)}{s, \texttt{while } \phi \texttt{ do } C \vec{\Downarrow} s, [\,], [\,]} \qquad \frac{\phi(s) \quad s, C \vec{\Downarrow} s', \sigma, \Gamma \quad s' \prec s \quad s', \texttt{while } \phi \texttt{ do } C \vec{\Downarrow} s'', \sigma', \Gamma'}{s, \texttt{while } \phi \texttt{ do } C \vec{\Downarrow} s'', \sigma' :: \sigma, \Gamma' :: \Gamma}$$

Big-step Operational semantics of $\mathbf{LOOP}_D$

Forward OS: $\mathbf{T}^S \times \mathbf{LOOP}_D \vec{\Downarrow} \ \mathbf{T}^S \times (\mathbf{T}^S)^* \times (\mathbf{T}^{S \to T \to T})^*$

$$\frac{}{s, \texttt{skip} \vec{\Downarrow} s, [], []} \qquad \frac{}{s, \langle c \,|\, \gamma \rangle \vec{\Downarrow} cs, s :: [], \gamma :: []} \qquad \frac{s, C_1 \vec{\Downarrow} s', \sigma, \Gamma \quad s', C_2 \vec{\Downarrow} s'', \sigma', \Gamma'}{s, C_1; C_2 \vec{\Downarrow} s'', \sigma' :: \sigma, \Gamma' :: \Gamma}$$

$$\frac{\phi(s) \quad s, C_1 \vec{\Downarrow} s', \sigma, \Gamma}{s, \texttt{if}\ \phi\ \texttt{then}\ C_1\ \texttt{else}\ C_2 \vec{\Downarrow} s', \sigma, \Gamma} \qquad \frac{\neg\phi(s) \quad s, C_2 \vec{\Downarrow} s', \sigma, \Gamma}{s, \texttt{if}\ \phi\ \texttt{then}\ C_1\ \texttt{else}\ C_2 \vec{\Downarrow} s', \sigma, \Gamma}$$

$$\frac{\neg\phi(s)}{s, \texttt{while}\ \phi\ \texttt{do}\ C \vec{\Downarrow} s, [], []} \qquad \frac{\phi(s) \quad s, C \vec{\Downarrow} s', \sigma, \Gamma \quad s' \prec s \quad s', \texttt{while}\ \phi\ \texttt{do}\ C \vec{\Downarrow} s'', \sigma', \Gamma'}{s, \texttt{while}\ \phi\ \texttt{do}\ C \vec{\Downarrow} s'', \sigma' :: \sigma, \Gamma' :: \Gamma}$$

Backward OS: $(\mathbf{T}^S)^* \times (\mathbf{T}^{S \to T \to T})^* \times \mathbf{T}^T \overleftarrow{\Downarrow} \ (\mathbf{T}^S)^* \times (\mathbf{T}^{S \to T \to T})^* \times \mathbf{T}^T$

$$\frac{}{\sigma, \Gamma, t \overleftarrow{\Downarrow} \sigma, \Gamma, t} \qquad \frac{}{s :: \sigma, \gamma :: \Gamma, t \overleftarrow{\Downarrow} \sigma, \Gamma, \gamma s t} \qquad \frac{\sigma, \Gamma, t \overleftarrow{\Downarrow} \sigma', \Gamma', t' \quad \sigma', \Gamma', t' \overleftarrow{\Downarrow} \sigma'', \Gamma'', t''}{\sigma, \Gamma, t \overleftarrow{\Downarrow} \sigma'', \Gamma'', t''}$$

Big-step Operational semantics of LOOP$_D$

Theorem (Forward+Backward OS = Backpropagation in LOOP$_D$)

Restrict LOOP$_D$ to only terminating (in WE-HA$^\omega$) while loops.
Let C be a command. Then:
For all $s : S$ there exist $\sigma : S^*$ and $\Gamma : (S \to T \to T)^*$ such that

1. $$s, C \overset{\rightarrow}{\Downarrow} (C^+ s), \sigma, \Gamma$$
2. *for all $t : T$,*
$$\sigma, \Gamma, t \overset{\leftarrow}{\Downarrow} [], [], (C^- s t).$$

Dialectica can be used to implement high-order backprop (discovered by Kerjean, Pédrot)

To go further

To go further

- Think of S and T as partial HEAP $\to \mathbb{N}$ in WE-HA$^{\omega}$. Then we should be able to have a **variable allocation Dialectica-Hoare rule?**

To go further

- Think of S and T as partial HEAP $\to \mathbb{N}$ in WE-HA$^\omega$. Then we should be able to have a **variable allocation Dialectica-Hoare rule?**
- The following rule is admissible in DHL:

$$\frac{P_1 \, \langle a \,|\, \alpha \rangle \, Q_1 \quad P_2 \, \langle b \,|\, \beta \rangle \, Q_2}{P_1 \wedge P_2 \;\; \langle a, b \,|\, \alpha, \beta \rangle \;\; Q_1 \wedge Q_2}$$

  Here, a, α and b, β operate on disjoint variables. So **frame rule?**

$$\frac{P_1 \, \langle a \,|\, \alpha \rangle \, Q_1 \quad P_2 \, \langle b \,|\, \beta \rangle \, Q_2}{P_1 * P_2 \;\; \langle a, \alpha \rangle \,||\, \langle b, \beta \rangle \;\; Q_1 * Q_2}$$

- **Dialectica for Bunched/Separation Logic?**

To go further

- Think of S and T as partial HEAP $\to \mathbb{N}$ in WE-HA$^\omega$. Then we should be able to have a **variable allocation Dialectica-Hoare rule?**
- The following rule is admissible in DHL:

$$\frac{P_1 \, \langle a \,|\, \alpha \rangle \, Q_1 \quad P_2 \, \langle b \,|\, \beta \rangle \, Q_2}{P_1 \wedge P_2 \;\; \langle a, b \,|\, \alpha, \beta \rangle \;\; Q_1 \wedge Q_2}$$

  Here, a, α and b, β operate on disjoint variables. So **frame rule?**

$$\frac{P_1 \, \langle a \,|\, \alpha \rangle \, Q_1 \quad P_2 \, \langle b \,|\, \beta \rangle \, Q_2}{P_1 * P_2 \;\; \langle a, \alpha \rangle \,||\, \langle b, \beta \rangle \;\; Q_1 * Q_2}$$

- **Dialectica for Bunched/Separation Logic?**
- Proof-mining = *quantitative results from qualitative ones*. The algorithmic idea is often by trial-and-error, like our `while` ϕ `do` a: **make this formal?**

To go further

- Think of S and T as partial HEAP $\to \mathbb{N}$ in WE-HA$^\omega$. Then we should be able to have a **variable allocation Dialectica-Hoare rule?**
- The following rule is admissible in DHL:

$$\frac{P_1 \langle a \,|\, \alpha \rangle Q_1 \quad P_2 \langle b \,|\, \beta \rangle Q_2}{P_1 \wedge P_2 \;\; \langle a, b \,|\, \alpha, \beta \rangle \;\; Q_1 \wedge Q_2}$$

Here, a, α and b, β operate on disjoint variables. So **frame rule?**

$$\frac{P_1 \langle a \,|\, \alpha \rangle Q_1 \quad P_2 \langle b \,|\, \beta \rangle Q_2}{P_1 * P_2 \;\; \langle a, \alpha \rangle \,||\, \langle b, \beta \rangle \;\; Q_1 * Q_2}$$

- **Dialectica for Bunched/Separation Logic?**
- Proof-mining = *quantitative results from qualitative ones*. The algorithmic idea is often by trial-and-error, like our `while` ϕ `do` a: **make this formal?**
- **Libraries for Computer-Assisted Dialectica realisers extraction?**

To go further

- Think of S and T as partial HEAP $\to \mathbb{N}$ in WE-HA$^\omega$. Then we should be able to have a **variable allocation Dialectica-Hoare rule?**
- The following rule is admissible in DHL:

$$\frac{P_1 \langle a \,|\, \alpha \rangle Q_1 \quad P_2 \langle b \,|\, \beta \rangle Q_2}{P_1 \wedge P_2 \ \langle a, b \,|\, \alpha, \beta \rangle \ Q_1 \wedge Q_2}$$

Here, a, α and b, β operate on disjoint variables. So **frame rule?**

$$\frac{P_1 \langle a \,|\, \alpha \rangle Q_1 \quad P_2 \langle b \,|\, \beta \rangle Q_2}{P_1 * P_2 \ \langle a, \alpha \rangle \,||\, \langle b, \beta \rangle \ Q_1 * Q_2}$$

- **Dialectica for Bunched/Separation Logic?**
- Proof-mining = *quantitative results from qualitative ones*. The algorithmic idea is often by trial-and-error, like our `while` ϕ `do` a: **make this formal?**
- **Libraries for Computer-Assisted Dialectica realisers extraction?**

Thank you!