Dialectica and Hoare logic

Davide Barbarossa joint work with Thomas Powell

db2437@bath.ac.uk

https://davidebarbarossa12.github.io/

Department of Computer Science

UNIVERSITY OF BATH

Workshop on Programs from Proofs, Bath (UK)

16/09/2025

Table of contents

Let π be a formal proof of $\mathtt{x} : A \vdash B$

“A proof is an algorithm transporting evidence of the hypotheses to evidence of the conclusion”

Let π be a formal proof of $\mathtt{x} : A \vdash B$

“A proof is an algorithm transporting evidence of the hypotheses to evidence of the conclusion”

	Tarski	Type-Theory	Dialectica	(Classical) Realisability
extracted program $\pi^\bullet \in$	$\{\square\}$	STλC/STλμC/ F/MLTT/ Rocq/Lean/...	$\mathrm{T}/\mathrm{ST}\lambda\mathrm{C}^{\to,\times,+}/\ldots$	$\lambda_{\mathtt{callcc}}$
evidence $E(A)$	$\square$ or none	*normal* $\vdash \mathtt{M} : A$	$\vdash \mathtt{M} : W(A)$ s.t. $\vdash \forall \rho^{C(A)}.\ \mathtt{M} \perp_A \rho$	$\mathtt{M} \in \mathrm{PL}$ s.t. $\forall \rho \in C(A),\ M \perp \rho$
$E(A) \overset{[\![\pi]\!]}{\to} E(B)$	$\square \mapsto \square$	$\mathtt{M} \mapsto$ $\mathrm{nf}((\lambda \mathtt{x}.\pi^\bullet)\mathtt{M})$	$\mathtt{M} \mapsto$ $(\lambda \mathtt{x}.\pi^\bullet)\mathtt{M}$	$\mathtt{M} \mapsto$ $(\lambda \mathtt{x}.\pi^\bullet)\mathtt{M}$
why does it work	*soundness*	*sub. red. +SN+confl*	*adequacy*	*adequacy*
$\exists$ *proof*/$\exists$ *evidence*	$\Longleftrightarrow$	$\Longleftrightarrow$	$\not\Leftarrow, \Rightarrow$	$\not\Leftarrow, \Rightarrow$
Paradigm	*cl* (/)	*int/cl* (*pure/impure*)	*int* (*pure*)	*cl* (*impure*)

	Source $\to$ Target		
Gödel ('58)	$A \in \mathrm{HA}$	$\longmapsto$	$A_D\{w, c\} \in \mathbf{T}$
		such that	
	$\vdash_{\mathrm{HA}} A$	$\Longrightarrow$	$\vdash_{\mathbf{T}} A_D\{\mathtt{M}, c\}$ *for some* $\mathtt{M} \in \mathbf{T}$

Dialectica: overview

	Source $\rightarrow$ Target
Gödel ('58)	$A \in \mathrm{HA} \quad \longmapsto \quad A_D\{w, c\} \in \mathbf{T}$ *such that* $\vdash_{\mathrm{HA}} A \quad \Longrightarrow \quad \vdash_{\mathbf{T}} A_D\{\mathtt{M}, c\}$ *for some* $\mathtt{M} \in \mathbf{T}$
De Paiva ('91) + Pédrot ('15)	$A \in \Lambda \quad \longmapsto \quad W(A), C(A) \in \mathbf{P}$ $\mathtt{M} \in \Lambda \quad \longmapsto \quad \mathtt{M}^\bullet, \mathtt{M}_{\mathtt{x}} \in \mathbf{P}$ *(for* $\mathtt{x}$ *variable)* *such that* $\mathtt{x} : A \vdash_\Lambda \mathtt{M} : B \quad \Longrightarrow \quad \begin{cases} \mathtt{x} : W(A) \vdash_{\mathbf{P}} \mathtt{M}^\bullet : W(B) \\ \mathtt{x} : W(A) \vdash_{\mathbf{P}} \mathtt{M}_{\mathtt{x}} : C(B) \rightarrow \mathcal{M}[C(A)] \end{cases}$

$A \in \Lambda \longmapsto W(A),\ C(A) \in \mathbf{P}$

	α	$E \to F$
W	α_W	$W(E) \to W(F)$ $\times$ $W(E) \times C(F) \to \mathcal{M}[C(E)]$
C	α_C	$W(E) \times C(F)$

$\mathtt{M} \in \Lambda \longmapsto \mathtt{M}^\bullet,\ \mathtt{M}_\mathtt{y} \in \mathbf{P}$

	$\mathtt{x}$	$\lambda\mathtt{x}.\mathtt{M}$	$\mathtt{PQ}$
$(\_)^\bullet$	$\mathtt{x}$	$\left\langle \begin{array}{c} \lambda\mathtt{x}.\mathtt{M}^\bullet \\ \lambda\pi.(\lambda\mathtt{x}.\mathtt{M}_\mathtt{x})\pi^1\pi^2 \end{array} \right\rangle$	$\mathtt{P}^{\bullet\,1}\mathtt{Q}^\bullet$
$(\_)_\mathtt{y}$	$\begin{cases} \lambda\pi.[\pi], & \mathtt{x} = \mathtt{y} \\ \lambda\pi.\emptyset, & \mathtt{y} \neq \mathtt{y} \end{cases}$	$\lambda\pi.(\lambda\mathtt{x}.\mathtt{M}_\mathtt{y})\pi^1\pi^2$	$\lambda\pi.\left(\begin{array}{c} \mathtt{P}_\mathtt{y}\langle \mathtt{Q}^\bullet, \pi\rangle \\ + \\ \mathtt{P}^{\bullet\,2}\langle \mathtt{Q}^\bullet, \pi\rangle \gg\!= \mathtt{Q}_y \end{array} \right)$

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

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

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

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

- Terms PL: Simply typed System **T** with ground type `nat`
- Formulas: Usual ones, they talk about numbers and high-order **T**-terms

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

- Terms PL: Simply typed System **T** with ground type `nat`
- Formulas: Usual ones, they talk about numbers and high-order **T**-terms
- Axioms:

$$\begin{gathered} \textit{equality} \\ + \\ PA \\ + \\ (\texttt{if}\ b\ \texttt{then}\ s\ \texttt{else}\ t = s) \vee_b (\texttt{if}\ b\ \texttt{then}\ s\ \texttt{else}\ t = t) \\ + \\ (\texttt{rec}\ z\, y\, n = y) \vee_n (\texttt{rec}\ z\, y\, n = z\,(n-1)\,(\texttt{rec}\ z\, y\,(n-1))) \end{gathered}$$

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

- Terms PL: Simply typed System **T** with ground type `nat`
- Formulas: Usual ones, they talk about numbers and high-order **T**-terms
- Axioms:

$$\begin{array}{c} \textit{equality} \\ + \\ PA \\ + \\ (\mathtt{if}\ b\ \mathtt{then}\ s\ \mathtt{else}\ t = s) \vee_b (\mathtt{if}\ b\ \mathtt{then}\ s\ \mathtt{else}\ t = t) \\ + \\ (\mathtt{rec}\ z\ y\ n = y) \vee_n (\mathtt{rec}\ z\ y\ n = z\ (n-1)\ (\mathtt{rec}\ z\ y\ (n-1))) \end{array}$$

- Rules:

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

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

$$\begin{array}{ccc} \textit{Formulas} & \longrightarrow & \textit{q.f.Formulas} \times \vec{\mathrm{Var}} \times \vec{\mathrm{Var}} \\ A & \longmapsto & (\,|A|\;,\,W(A)\,,\,C(B)\,), \qquad \textit{written } |A|^{W(A)}_{C(A)} \end{array}$$

defined by:

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

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

$$\begin{array}{ccc} \mathit{Formulas} & \longrightarrow & \mathit{q.f.Formulas} \times \vec{\mathrm{Var}} \times \vec{\mathrm{Var}} \\ A & \longmapsto & (\,|A|\;,\, W(A)\,,\, C(B)\,), \qquad \textit{written } |A|^{W(A)}_{C(A)} \end{array}$$

Theorem (Soundness of Dialectica)

$$\mathit{WE\text{-}HA}^\omega \vdash A \;\Rightarrow\; \mathit{WE\text{-}HA}^\omega \vdash \forall y.\, |A|^a_y$$

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

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

$$\begin{array}{ccc} \textit{Formulas} & \longrightarrow & \textit{q.f.Formulas} \times \overrightarrow{\mathrm{Var}} \times \overrightarrow{\mathrm{Var}} \\ A & \longmapsto & (\,|A|\,,\, W(A)\,,\, C(B)\,), \qquad \textit{written } |A|^{W(A)}_{C(A)} \end{array}$$

Theorem (Soundness of Dialectica)

If WE-HA$^\omega_\Delta \supseteq$ WE-HA$^\omega$ proves the Dialectica of Δ, then:

$$\Delta + \textit{WE-HA}^\omega \vdash A \;\Rightarrow\; \textit{WE-HA}^\omega_\Delta \vdash \forall y.\,|A|^a_y$$

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

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

$$
\begin{array}{ccc}
\mathit{Formulas} & \longrightarrow & \mathit{q.f.Formulas} \times \overrightarrow{\mathrm{Var}} \times \overrightarrow{\mathrm{Var}} \\
A & \longmapsto & (\,|A|\;,\, W(A)\,,\, C(B)\,), \qquad \mathit{written}\ |A|^{W(A)}_{C(A)}
\end{array}
$$

Theorem (Soundness of Dialectica)

If WE-HA$^\omega_\Delta \supseteq$ WE-HA$^\omega$ proves the Dialectica of Δ, then:

$$\Delta + \textit{WE-HA}^\omega \vdash M : A \;\Rightarrow\; \textit{WE-HA}^\omega_\Delta \vdash \forall y.\, |A|^{M^\bullet}_y$$

where $(\_) \longmapsto (\_)^\bullet$ is the program transformation defined before

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

$$\begin{array}{ccc} \mathit{Formulas} & \longrightarrow & \mathit{q.f.Formulas} \times \vec{\mathrm{Var}} \times \vec{\mathrm{Var}} \\ A & \longmapsto & (\,|A|\ , W(A)\,, C(B)\,), \qquad \textit{written } |A|^{W(A)}_{C(A)} \end{array}$$

Theorem (Adequacy of Dialectica)

If $d \Vdash \Delta$*, then:*

$$\Delta \vdash M : A \;\Rightarrow\; M^\bullet\{d\} \Vdash A$$

where $(\_\,) \longmapsto (\_\,)^\bullet$ ***is the program transformation defined before***

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

First intuition: $f : A \to B$.

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

First intuition: $f : A \to B$. More precise intuition: it stands for the formula

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

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$^\omega$). So, second intuition: $f \Vdash_{Hoare} A \to B$.

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

First intuition: $f : A \to B$. More precise intuition: it stands for the formula

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

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$^\omega$). So, second intuition: $f \Vdash_{Hoare} A \to B$.

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

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

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

First intuition: $f : A \to B$. More precise intuition: it stands for the formula

$$\forall^{\mathrm{State}} s.(\, A \to B\{s := f s\}\,)$$

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$^\omega$). So, second intuition: $f \Vdash_{Hoare} A \to B$.

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

$$\forall^{\mathrm{State}} s.\,|\exists x.A \to \exists x.B|^{f,\emptyset}_{(s,\emptyset),\emptyset}$$

Let's take this seriously in all its generality:

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

for A, B any formula. Intuition: $\langle f \mid F\rangle \Vdash_{Dialectica} A \to B$.

Dialectica Hoare Logic (DHL)

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

Theorem (Dialectica Hoare Logic Soundness)

If the judgment

$$A \langle f \mid F \rangle B$$

is derivable in DHL, then

$$\textit{WE-HA}^\omega \quad \vdash \quad \forall s\, v.\ |A|^{s}_{Fsv} \to |B|^{fs}_{v}\,.$$

Dialectica Hoare Logic (DHL)

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

Theorem (Dialectica Hoare Logic Soundness)

If the judgment

$$A\,\langle f \mid F\rangle\,B$$

is derivable in DHL, then

$$\textit{WE-HA}^\omega \quad \vdash \quad \forall s\, v.\ |A|^{s}_{Fsv} \to |B|^{fs}_{v}\,.$$

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

See also De Paiva's thesis and Pédrot's thesis!

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

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

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

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

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

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

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

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

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

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 + $\dfrac{\forall x. \left((\forall y \prec x. A\{x := y\}) \to A \right)}{\forall x. A}$

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 + $\dfrac{\forall x. (\, (\forall y \prec x. A\{x := y\}) \to A\,)}{\forall x. A}$

Remark

The sugars

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

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.

$$\exists x.\, \theta \vdash \exists x.\, (\theta \wedge \forall y \prec x. \neg\, \theta(y))$$

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

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

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 type $S \to S$ and $S \to T \to T$, and consider
$\mathrm{LOOP}_D :=$ IMP with commands from above and *without* variable allocation:

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

Fix fresh sets of commands $\overrightarrow{Comm}, \overleftarrow{Comm}$ of type $S \to S$ and $S \to T \to T$, and consider
$\mathrm{LOOP}_D :=$ 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 $\mathrm{LOOP}_D \to \mathbf{T}^{S \to S} \times \mathbf{T}^{S \to T \to T}$:

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

Hoare Logic for LOOP_D

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

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

$$\frac{P'(s,t) \to P(s,t) \quad [P]\,C\,[Q] \quad Q(s,t) \to Q'(s,t)}{[P']\,C\,[Q']}$$

where the formulas and their provability are wrt the ambient WE-HA$^\omega$.

Theorem (Soundness wrt Dialectica)

Let P, Q quantifier free with only one variable s^S and one t^T. Let $[P]\,C\,[Q]$ be sugar for $\exists s \forall t. P\ \langle C^+ \mid C^- \rangle\ \exists s \forall t. Q$. Then the rules above are sound wrt Dialectica, and so WE-HA$^\omega \vdash \forall s, v.\ P\{t := C^- st\} \to Q\{s := C^+ s\}$.

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

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

$$\frac{}{s, \mathtt{skip} \vec{\Downarrow} s, \epsilon, \epsilon} \qquad \frac{}{s, \langle c \mid \gamma \rangle \vec{\Downarrow} cs, s :: \epsilon, \gamma :: \epsilon} \qquad \frac{s, C_1 \vec{\Downarrow} s', \sigma, \Gamma \quad s', C_2 \vec{\Downarrow} s'', \sigma', \Gamma'}{s, C_1; C_2 \vec{\Downarrow} s'', \sigma' :: \sigma, \Gamma' :: \Gamma}$$

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

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

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

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

Big-step Operational semantics of LOOP$_D$

Forward OS: $s, C \overset{\rightarrow}{\Downarrow} s', \sigma, \Gamma$

Backward OS: $\sigma, \Gamma, t \overset{\leftarrow}{\Downarrow} \sigma', \Gamma', t'$

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

Suppose that $\text{WE-HA}^\omega \vdash \forall s(\phi(s) \to C^+ s \prec s)$ *for all* $\texttt{while}\,\phi\,\texttt{do}\,C$ *of* $LOOP_D$. *Then for any* $s : S$ *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 any* $t : T$, $\rho : S^*$ *and* $\Delta : (S \to T \to T)^*$,
$$\sigma :: \rho, \Gamma :: \Delta, t \overset{\leftarrow}{\Downarrow} \rho, \Delta, (C^- st).$$

Dialectica can be used to implement (high-order) Automatic Differentiation: discovered by Kerjean and Pédrot!

Variable allocation? Concurrency? More?

Variable allocation? Concurrency? More?

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

Variable allocation? Concurrency? More?

- Think of S and T as partial HEAP $\to \mathbb{N}$ in WE-HA$^\omega$. Then we should/would 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 in parallel 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?** Don't know !

Variable allocation? Concurrency? More?

- Think of S and T as partial HEAP $\to \mathbb{N}$ in WE-HA$^\omega$. Then we should/would 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 in parallel 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?** Don't know !
- 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?**

Variable allocation? Concurrency? More?

- Think of S and T as partial HEAP $\to \mathbb{N}$ in WE-HA$^\omega$. Then we should/would 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 in parallel 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?** Don't know !
- 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?** (see Horatio's talk)

Variable allocation? Concurrency? More?

- Think of S and T as partial HEAP $\to \mathbb{N}$ in WE-HA$^\omega$. Then we should/would 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 in parallel 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?** Don't know !
- 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?** (see Horatio's talk)

Thank you!