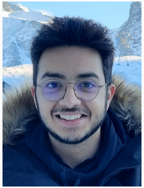
Interpolation and Quantifiers in Ortholattices



Sankalp Gambhir Simon Guilloud Viktor Kunčak

Laboratory For Automated Reasoning And Analysis

EPFL

Propositional Reasoning

- We rely extensively on propositional reasoning

Propositional Reasoning

- We rely extensively on propositional reasoning
- Validity checking — coNP-hard

Propositional Reasoning

- We rely extensively on propositional reasoning
- Validity checking — coNP-hard
- Can we do better?

Propositional Reasoning

- We rely extensively on propositional reasoning
- Validity checking — coNP-hard
- Can we do better?
- Abstractions?

Propositional Reasoning

- We rely extensively on propositional reasoning
- Validity checking — coNP-hard
- Can we do better?
- Abstractions?
  - Need: soundness

Propositional Reasoning

- We rely extensively on propositional reasoning
- Validity checking — coNP-hard
- Can we do better?
- Abstractions?
  - Need: soundness
  - Want: predictability, efficiency

Weakening Boolean Algebras

- Intuitionistic Logic

Weakening Boolean Algebras

- Intuitionistic Logic
  - Validity — PSPACE-Complete [1]

[1] Statman. *"Intuitionistic propositional logic is polynomial-space complete"*. In: TCS 1979

Weakening Boolean Algebras

- Intuitionistic Logic
  - Validity — PSPACE-Complete [1]
- Orthologic

[1] Statman. *"Intuitionistic propositional logic is polynomial-space complete"*. In: TCS 1979

Weakening Boolean Algebras

- Intuitionistic Logic
  - Validity — PSPACE-Complete [1]
- Orthologic
  - Validity — $O(n^2)$ time [2]

[1] Statman. *"Intuitionistic propositional logic is polynomial-space complete"*. In: TCS 1979
[2] Guilloud, Bucev, Milovančević, and Kunčak. *"Formula normalizations in verification"*. In: CAV 2023

Weakening Boolean Algebras

- Intuitionistic Logic
  - Validity — PSPACE-Complete [1]
- Orthologic
  - Validity — $O(n^2)$ time [2]

[1] Statman. *"Intuitionistic propositional logic is polynomial-space complete"*. In: TCS 1979
[2] Guilloud, Bucev, Milovančević, and Kunčak. *"Formula normalizations in verification"*. In: CAV 2023

Weakening Boolean Algebras

- Intuitionistic Logic
  - Validity — PSPACE-Complete [1]
- Orthologic
  - Validity — $O(n^2)$ time [2]

Propositional Logic	$\leftrightarrow$	Boolean Algebras
Intuitionistic Logic	$\leftrightarrow$	Heyting Algebras
Orthologic	$\leftrightarrow$	**Ortholattices**

[1] Statman. *"Intuitionistic propositional logic is polynomial-space complete"*. In: TCS 1979
[2] Guilloud, Bucev, Milovančević, and Kunčak. *"Formula normalizations in verification"*. In: CAV 2023

Ortholattices

Commutativity	$x \vee y = y \vee x$
Associativity	$x \vee (y \vee z) = (x \vee y) \vee z$
Reflexivity	$x \vee x = x$
One	$x \vee 1 = 1$
Zero	$x \vee 0 = x$
Double Negation	$\neg\neg x = x$
Excluded Middle	$x \vee \neg x = 1$
De Morgan	$x \vee (y \wedge z) = (x \vee y) \wedge (y \vee z)$
Distributivity	$x \vee (z \wedge y) = (x \vee z) \wedge (x \vee y)$

Ortholattices

Commutativity	$x \vee y = y \vee x$
Associativity	$x \vee (y \vee z) = (x \vee y) \vee z$
Reflexivity	$x \vee x = x$
One	$x \vee 1 = 1$
Zero	$x \vee 0 = x$
Double Negation	$\neg\neg x = x$
Excluded Middle	$x \vee \neg x = 1$
De Morgan	$x \vee (y \wedge z) = (x \vee y) \wedge (y \vee z)$
Distributivity **X**	$x \vee (z \wedge y) = (x \vee z) \wedge (x \vee y)$
Absorption	$x \vee (x \wedge y) = x$

Ortholattices

- incomplete but sound approximation for Boolean algebras
- quadratic-time normalization procedure
- found use recently in formula caching for verification [3]
- as well as in interactive theorem proving [4]

[3] Guilloud, Bucev, Milovančević, and Kunčak. *"Formula normalizations in verification"*. In: CAV 2023
[4] Guilloud, Gambhir, and Kunčak. *"LISA - A Modern Proof System"*. In: ITP 2023

Contributions

- Proof System for Quantified Orthologic (QOL)
- Failure of Quantifier Elimination
- Failure of Refutation-based Interpolation
- Proof of Implicational Interpolation

Moving to a Sequent Calculus

Sequent

$$\gamma_1, \gamma_2, ... \vdash \delta_1, \delta_2, ...$$

Moving to a Sequent Calculus

Sequent

$$\gamma_1, \gamma_2, ... \vdash \delta_1, \delta_2, ...$$

Proof rules

$$\frac{}{\phi \vdash \phi} \text{ Hypothesis} \qquad\qquad \frac{\Gamma \vdash \phi \qquad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi} \text{ RightAnd}$$

From Ortholattices to Orthologic

Intuitionistic logic — at most one formula on the right-hand side of the sequent

$$\gamma_1, \gamma_2, ... \vdash \psi$$

From Ortholattices to Orthologic

Intuitionistic logic — at most one formula on the right-hand side of the sequent

$$\gamma_1, \gamma_2, ... \vdash \psi$$

Orthologic — at most two formulas in the entire sequent

$$\phi \vdash \psi$$

$$\phi, \psi \vdash$$

$$\vdash \phi, \psi$$

From Ortholattices to Orthologic

Intuitionistic logic — at most one formula on the right-hand side of the sequent

$$\gamma_1, \gamma_2, ... \vdash \psi$$

Orthologic — at most two formulas in the entire sequent

$$\phi \vdash \psi$$

$$\phi, \psi \vdash$$

$$\vdash \phi, \psi$$

For convenience, written with left/right annotations, e.g. ϕ^L, ψ^R

Orthologic — Proof Rules

$$\frac{}{\phi^L, \phi^R}\ \text{Hyp}$$

$$\frac{\Gamma, \psi^R \qquad \psi^L, \Delta}{\Gamma, \Delta}\ \text{Cut}$$

$$\frac{\Gamma}{\Gamma, \Delta}\ \text{Weaken}$$

$$\frac{\Gamma, \phi^L}{\Gamma, (\phi \wedge \psi)^L}\ \text{LeftAnd} \qquad \frac{\Gamma, \phi^R \qquad \Gamma, \psi^R}{\Gamma, (\phi \wedge \psi)^R}\ \text{RightAnd}$$

$$\frac{\Gamma, \phi^L \qquad \Gamma, \psi^L}{\Gamma, (\phi \vee \psi)^L}\ \text{LeftOr} \qquad \frac{\Gamma, \phi^R}{\Gamma, (\phi \vee \psi)^R}\ \text{RightOr}$$

$$\frac{\Gamma, \phi^R}{\Gamma, (\neg\phi)^L}\ \text{LeftNot} \qquad \frac{\Gamma, \phi^L}{\Gamma, (\neg\phi)^R}\ \text{RightNot}$$

Orthologic — Proof Search

- Proofs in orthologic are at most quadratic in size of the formula
- Proofs can be found in cubic-time in the presence of axioms[1]

[1] **Orthologic with Axioms**
Simon Guilloud, Viktor Kunčak
POPL 2024, 19 Jan Friday 16:50

Interpolation

Given that

$$A_{\bar{x},\bar{y}} \implies B_{\bar{y},\bar{z}}$$

Interpolation

Given that

$$A_{\bar{x},\bar{y}} \implies B_{\bar{y},\bar{z}}$$

find $I_{\bar{y}}$ such that $A_{\bar{x},\bar{y}} \implies I_{\bar{y}}$, and $I_{\bar{y}} \implies B_{\bar{y},\bar{z}}$.

Interpolation

Given that

$$A_{\bar{x},\bar{y}} \implies B_{\bar{y},\bar{z}}$$

find $I_{\bar{y}}$ such that $A_{\bar{x},\bar{y}} \implies I_{\bar{y}}$, and $I_{\bar{y}} \implies B_{\bar{y},\bar{z}}$.

- Focus search to relevant facts
- Better counterexamples
- Abstraction generalization [5]

[5] McMillan. "Interpolation and Model Checking." In: Handbook of Model Checking

Interpolation in Boolean Algebras

$$A_{\bar{x},\bar{y}} \implies B_{\bar{y},\bar{z}}$$

[6] D'Silva, Kroening, Purandare, and Weissenbacher. *"Interpolant Strength"*. In: VMCAI 2010

Interpolation in Boolean Algebras

$$A_{\bar{x},\bar{y}} \implies B_{\bar{y},\bar{z}}$$

With quantifiers, we get some interpolants for free:

- $I_1 : \exists \bar{x}. A_{\bar{x},\bar{y}}$
- $I_2 : \forall \bar{z}. B_{\bar{y},\bar{z}}$

[6] D'Silva, Kroening, Purandare, and Weissenbacher. *"Interpolant Strength"*. In: VMCAI 2010

Interpolation in Boolean Algebras

$$A_{\bar{x},\bar{y}} \implies B_{\bar{y},\bar{z}}$$

With quantifiers, we get some interpolants for free:

- $I_1 : \exists \bar{x}. A_{\bar{x},\bar{y}}$
- $I_2 : \forall \bar{z}. B_{\bar{y},\bar{z}}$

By quantifier elimination for Boolean algebras, the quantifier-free formulas $QE(I_1)$ and $QE(I_2)$ can be computed.

[6] D'Silva, Kroening, Purandare, and Weissenbacher. *"Interpolant Strength"*. In: VMCAI 2010

Interpolation in Boolean Algebras

$$A_{\bar{x},\bar{y}} \implies B_{\bar{y},\bar{z}}$$

With quantifiers, we get some interpolants for free:

- $I_1 : \exists \bar{x}. A_{\bar{x},\bar{y}}$
- $I_2 : \forall \bar{z}. B_{\bar{y},\bar{z}}$

By quantifier elimination for Boolean algebras, the quantifier-free formulas $QE(I_1)$ and $QE(I_2)$ can be computed.

Better: we get least and most general interpolants. [6]

[6] D'Silva, Kroening, Purandare, and Weissenbacher. *"Interpolant Strength"*. In: VMCAI 2010

Quantified Orthologic

We present the semantics of Quantified Orthologic (QOL) on complete ortholattices.

Quantified Orthologic

We present the semantics of Quantified Orthologic (QOL) on complete ortholattices.

- Greatest lower bound (universal quantification): $\bigwedge x.\phi$
- Least upper bound (existential quantification): $\bigvee x.\phi$

Quantified Orthologic

We present the semantics of Quantified Orthologic (QOL) on complete ortholattices.

- Greatest lower bound (universal quantification): $\bigwedge x.\phi$
- Least upper bound (existential quantification): $\bigvee x.\phi$

$$\frac{\Gamma, \phi[x := \gamma]^L}{\Gamma, (\bigwedge x.\phi)^L}\ \text{LeftForall} \qquad \frac{\Gamma, \phi[x := x']^R}{\Gamma, (\bigwedge x.\phi)^R}\ \text{RightForall}\ (x' \text{ not free in } \Gamma)$$

$$\frac{\Gamma, \phi[x := x']^L}{\Gamma, (\bigvee x.\phi)^L}\ \text{LeftExists}\ (x' \text{ not free in } \Gamma) \qquad \frac{\Gamma, \phi[x := \gamma]^R}{\Gamma, (\bigvee x.\phi)^R}\ \text{RightExists}$$

Quantified Orthologic

Theorem (Soundness)
For every sequent S, *if* $\vdash S$ *then* $\vDash S$.

Theorem (Completeness)
For every sequent S, *if* $\vDash S$ *then* $\vdash S$.

Quantified Orthologic

Theorem (Soundness)
For every sequent S, *if* $\vdash S$ *then* $\vDash S$.

Theorem (Completeness)
For every sequent S, *if* $\vDash S$ *then* $\vdash S$.

Inequalities correspond directly to sequents:

$$\gamma \leq \delta \iff \vdash (\gamma^L, \delta^R)$$

Quantifier Elimination

Given a formula ϕ with quantifiers, produce an equivalent quantifier-free formula $QE(\phi)$,

$$\phi \iff QE(\phi)$$

Quantifier elimination in Orthologic

Theorem
Quantified Orthologic does not admit quantifier elimination.

Quantifier elimination in Orthologic

Theorem
Quantified Orthologic does not admit quantifier elimination.

Counterexample: $\phi = \bigvee x.(\neg x \wedge (y \vee x))$

Quantifier elimination in Orthologic

Theorem
Quantified Orthologic does not admit quantifier elimination.

Counterexample: $\phi = \bigvee x.(\neg x \wedge (y \vee x))$

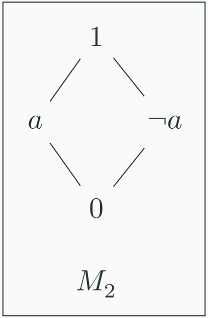
Quantifier elimination must contain only y: $0, 1, y, \neg y, ...$

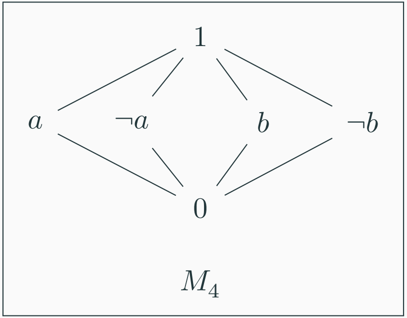
Quantifier elimination in Orthologic

Theorem
Quantified Orthologic does not admit quantifier elimination.

Counterexample: $\phi = \bigvee x.(\neg x \wedge (y \vee x))$

Quantifier elimination must contain only y: $0, 1, y, \neg y, \ldots$





Refutation-based Interpolation

Given two sequents γ and δ, and a proof of contradiction assuming γ and δ, find an interpolant sequent I, such that

- I can be deduced from γ alone

Refutation-based Interpolation

Given two sequents γ and δ, and a proof of contradiction assuming γ and δ, find an interpolant sequent I, such that

- I can be deduced from γ alone
- I and δ are inconsistent when assumed together

Refutation-based Interpolation

Given two sequents γ and δ, and a proof of contradiction assuming γ and δ, find an interpolant sequent I, such that

- I can be deduced from γ alone
- I and δ are inconsistent when assumed together
- $FV(I) \subset FV(\gamma) \cap FV(\delta)$

Refutation-based Interpolation

Given two sequents γ and δ, and a proof of contradiction assuming γ and δ, find an interpolant sequent I, such that

- I can be deduced from γ alone
- I and δ are inconsistent when assumed together
- $FV(I) \subset FV(\gamma) \cap FV(\delta)$

Refutation-based Interpolation

Given two sequents γ and δ, and a proof of contradiction assuming γ and δ, find an interpolant sequent I, such that

- I can be deduced from γ alone
- I and δ are inconsistent when assumed together
- $FV(I) \subset FV(\gamma) \cap FV(\delta)$

Theorem
Orthologic does not admit refutation-based interpolation.

Refutation-based Interpolation

Given two sequents γ and δ, and a proof of contradiction assuming γ and δ, find an interpolant sequent I, such that

- I can be deduced from γ alone
- I and δ are inconsistent when assumed together
- $FV(I) \subset FV(\gamma) \cap FV(\delta)$

Theorem
Orthologic does not admit refutation-based interpolation.

Counterexample:

$$\gamma : (z \vee \neg y) \wedge (\neg z \vee \neg y)^R$$

$$\delta : (x \wedge \neg y) \vee (\neg x \wedge \neg y)^R$$

Refutation-based Interpolation

Given two sequents γ and δ, and a proof of contradiction assuming γ and δ, find an interpolant sequent I, such that

- I can be deduced from γ alone
- I and δ are inconsistent when assumed together
- $FV(I) \subset FV(\gamma) \cap FV(\delta)$

Theorem
Orthologic does not admit refutation-based interpolation.

Counterexample:

$$\gamma : (z \vee \neg y) \wedge (\neg z \vee \neg y)^R$$
$$\delta : (x \wedge \neg y) \vee (\neg x \wedge \neg y)^R$$

No sequent I containing only y can be a refutation-based interpolant for this example.

Implicational Interpolation for Ortholattices

Given two ortholattice formulas γ and δ, such that $\gamma \leq \delta$ wrt laws of OL, an implicational interpolant is a formula I such that

- $\gamma \leq I$
- $I \leq \delta$
- $FV(I) \subset FV(\gamma) \cap FV(\delta)$

Implicational Interpolation for Ortholattices

Given a provable sequent Γ, Δ, an implicational interpolant is a formula I such that

- Γ, I^R
- I^L, Δ
- $FV(I) \subset FV(\Gamma) \cap FV(\Delta)$

Implicational Interpolation for Ortholattices

Given a provable sequent Γ, Δ, an implicational interpolant is a formula I such that

- Γ, I^R
- I^L, Δ
- $FV(I) \subset FV(\Gamma) \cap FV(\Delta)$

Theorem
Orthologic admits implicational interpolation.

Implicational Interpolation for Ortholattices

Given a provable sequent Γ, Δ, an implicational interpolant is a formula I such that

- Γ, I^R
- I^L, Δ
- $FV(I) \subset FV(\Gamma) \cap FV(\Delta)$

Theorem
Orthologic admits implicational interpolation.

- linear-time in size of the proof
- thus quadratic-time in size of the sequent

Theorem
Orthologic admits implicational interpolation.

Proof.
Base case:

Implicational Interpolation for Ortholattices

Theorem
Orthologic admits implicational interpolation.

Proof.
Base case:

$$\frac{}{\phi^L, \phi^R}\ \text{Hyp}$$

Implicational Interpolation for Ortholattices

Theorem
Orthologic admits implicational interpolation.

Proof.
Base case:

$$\frac{}{\phi^L, \phi^R}\ \text{Hyp}$$

Interpolant is $I = \phi$, and we trivially have proofs of ϕ^L, I^R and I^L, ϕ^R. $\square$

Implicational Interpolation for Ortholattices

Theorem
Orthologic admits implicational interpolation.

Proof.
Inductive case:

Implicational Interpolation for Ortholattices

Theorem
Orthologic admits implicational interpolation.

Proof.
Inductive case:

$$\frac{\Gamma, \phi^L}{\Gamma, \phi \wedge \psi^L}\ \textsf{LeftAnd}$$

Implicational Interpolation for Ortholattices

Theorem
Orthologic admits implicational interpolation.

Proof.
Inductive case:

$$\frac{\Gamma, \phi^L}{\Gamma, \phi \wedge \psi^L} \text{ LeftAnd}$$

Inductive hypothesis: there is an interpolant C for Γ, ϕ^L, such that there are proofs of

$$\Gamma, C^R \qquad\qquad C^L, \phi^L$$

Theorem
Orthologic admits implicational interpolation.

Proof.
Inductive case:

$$\frac{\Gamma, \phi^L}{\Gamma, \phi \wedge \psi^L} \text{ LeftAnd}$$

Inductive hypothesis: there is an interpolant C for Γ, ϕ^L, such that there are proofs of

$$\Gamma, C^R \qquad\qquad C^L, \phi^L$$

We have the interpolant $I = C$ inductively, and OL proofs of interpolation:

$$\frac{\Gamma, C^R}{\Gamma, C^R} \qquad\qquad \frac{C^L, \phi^L}{C^L, \phi \wedge \psi^L} \text{ LeftAnd}$$

Orthologic — Conclusions and Future

Starting with

- Orthologic, weakening of classical propositional logic
- Sound and complete proof system

We show

- Semantics of Quantified Orthologic
- Absence of quantifier elimination
- Absence of refutation-based interpolation
- Existence of implicational interpolation

References

[1] Richard Statman. **"Intuitionistic propositional logic is polynomial-space complete."** In: *Theoretical Computer Science* 9.1 (1979), pp. 67–72. ISSN: 0304-3975. DOI: https://doi.org/10.1016/0304-3975(79)90006-9. URL: https://www.sciencedirect.com/science/article/pii/0304397579900069.

[2] Simon Guilloud, Mario Bucev, Dragana Milovančević, and Viktor Kunčak. **"Formula normalizations in verification."** In: *International Conference on Computer Aided Verification*. Springer. 2023, pp. 398–422.

[3] Simon Guilloud, Sankalp Gambhir, and Viktor Kunčak. **"LISA - A Modern Proof System."** In: *14th International Conference on Interactive Theorem Proving (ITP 2023)*. Ed. by Adam Naumowicz and René Thiemann. Vol. 268. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023, 17:1–17:19. ISBN: 978-3-95977-284-6. DOI: 10.4230/LIPIcs.ITP.2023.17. URL: https://drops.dagstuhl.de/