Deciding entailment for cofibration languages

Robert Rose

jww Matthew Weaver and Dan Licata

HoTT 2023

Motivation

Cubical type theories[1,2,3] were invented to realize the potential of intensional Martin-Löf type theory to become a computational theory of *homotopy types* (or even *directed* homotopy types).

The standard semantics for cubical type theories are cubical presheaves, which serve as combinatorial models of (directed) homotopy theory. Witnesses of equality types are implemented as paths out of a special interval type, whose standard semantics is the representable cubical presheaf $\mathrm{Hom}(-, \mathsf{I})$:

$$0 \xrightarrow{x_1} 1$$

[1] Cyril Cohen et al. *Cubical Type Theory: a constructive interpretation of the univalence axiom*. 2016. arXiv: 1611.02108 [cs.LO].

[2] Carlo Angiuli et al. "Syntax and models of Cartesian cubical type theory". In: *Mathematical Structures in Computer Science* 31.4 (2021), pp. 424–468.

[3] Matthew Z. Weaver and Daniel R. Licata. "A Constructive Model of Directed Univalence in Bicubical Sets". In: *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*. LICS '20. Saarbrücken, Germany: Association for Computing Machinery, 2020, pp. 915–928.

Morphisms in I^n

We will focus on cube categories which have products, and so higher dimensional cubes are interpreted naturally as $\mathsf{I}^n = \underbrace{\mathsf{I}^1 \times \cdots \times \mathsf{I}^1}_{n\text{-times}}$.

For example, the non-degenerate 0- and 1-cubes in I^2 may be pictured as

$$\begin{tikzcd}
(0,1) \arrow[r, "{(x_1,1)}"] & (1,1) \\
(0,0) \arrow[u, "{(0,x_2)}"] \arrow[ur, "{(x_1,x_1)}"] \arrow[r, "{(x_1,0)}"'] & (1,0) \arrow[u, "{(1,x_2)}"']
\end{tikzcd}$$

Cofibration language

Cubical type theories include a specification of a cofibration language. The syntax will be that of a fragment of first-order equational logic.

Cofibration language

$$\begin{tikzcd}
(0,1) \arrow[r, "{(x_1,1)}"] & (1,1) \\
(0,0) \arrow[u, "{(0,x_2)}"] \arrow[ur, "{(x_1,x_1)}"] \arrow[r, "{(x_1,0)}"] & (1,0) \arrow[u, "{(1,x_2)}"']
\end{tikzcd}$$

For example, the upper left corner point is specified by the formula

$$(x_1 = 0) \wedge (x_2 = 1)$$

The boundary of the square is specified by

$$(x_1 = 0) \vee (x_1 = 1) \vee (x_2 = 0) \vee (x_2 = 1)$$

The 2-simplex below the diagonal is specified by $(x_1 = x_1 \vee x_2)$.

Cofibration language

In this talk, the terms of the cofibration language will be those suitable for formally describing elements in a free (distributive) lattice: they are generated by

- constants 0 and 1
- variables x_i, y_i, ...
- operations $\vee$ and $\wedge$

Formulas will be generated by

- $\perp$ and $\top$
- equations $(s = t)$ where s and t are terms
- connectives $\vee$ and $\wedge$
- the quantifier $\forall$

Semantics

We will view cofibration languages as fragments of the Mitchell-Bénabou language of the appropriate cubical presheaf topos. We will interpret them using the Kripke-Joyal semantics.

The image of the interpretation of formulas of the language is a subobject of Ω, known as the *cofibration classifier* Ψ.

Decision problem

Given cofibration formulas $\phi, \psi : \mathsf{I}^n \to \Omega$, is it the case that $\mathsf{I}^n \Vdash \phi \Rightarrow \psi$?
We will first consider this problem without $\forall$ in the formulas, and later with $\forall$.

Example

Does the following formula hold?

$$(v = z \vee u) \wedge (u \wedge v = u) \wedge (z = v \wedge z)$$
$$\Rightarrow$$
$$(w \wedge ((v \vee x) \wedge y) \vee (x \wedge z)) \vee (((y \wedge w) \vee (x \wedge y)) \wedge z)$$
$$=$$
$$(w \wedge x \wedge v) \vee (y \wedge ((w \wedge x) \vee ((x \vee z) \wedge w) \vee (w \wedge z) \vee (x \wedge v)))$$

Example

$$\begin{aligned}\phi &:= (u = z \vee t) \wedge (t \wedge u = t) \wedge (z = u \wedge z)\\ \psi &:= (w \wedge ((u \vee x) \wedge y) \vee (x \wedge z)) \vee (((y \wedge w) \vee (x \wedge y)) \wedge z)\\ &\quad = (w \wedge x \wedge u) \vee (y \wedge ((w \wedge x) \vee ((x \vee z) \wedge w)\\ &\qquad \vee (w \wedge z) \vee (x \wedge u)))\end{aligned}$$

According to the Kripke-Joyal semantics, $\phi \Rightarrow \psi$ holds iff for all $m \geq 0$ and morphisms $\alpha : \mathsf{I}^m \to \mathsf{I}^6$ whenever $\phi(\alpha)$ holds, $\psi(\alpha)$ holds.

Example

In particular, if this formula $\phi \Rightarrow \psi$ holds, then it holds when $m = 0$: e.g., when $\alpha = (0, 1, 0, 0, 1, 1)$. Such substitutions readily evaluate to equations between 0 and 1.

$$(1 = 1 \vee 0) \wedge (0 \wedge 1 = 0) \wedge (1 = 1 \wedge 1)$$
$$\Rightarrow$$
$$(0 \wedge ((1 \vee 0) \wedge 1) \vee (0 \wedge 1)) \vee (((1 \wedge 0) \vee (0 \wedge 1)) \wedge 1)$$
$$=$$
$$(0 \wedge 0 \wedge 1) \vee (1 \wedge ((0 \wedge 0) \vee ((0 \vee 1) \wedge 0) \vee (0 \wedge 1) \vee (0 \wedge 1)))$$

becomes

$$(1 = 1) \wedge (0 = 0) \wedge (1 = 1) \Rightarrow (0 = 0)$$

As it turns out, $\phi \Rightarrow \psi$ does hold for all such substitutions α, and in this case, this is enough to know that the formula holds.

Example

We get the same answer when we perform the minor translation to propositional logic (trading $=$ for $\Leftrightarrow$) and view α as a Boolean assignment:

$$(v \Leftrightarrow z \vee u) \wedge (u \wedge v \Leftrightarrow u) \wedge (z \Leftrightarrow v \wedge z)$$

$$\Rightarrow$$

$$(w \wedge ((v \vee x) \wedge y) \vee (x \wedge z)) \vee (((y \wedge w) \vee (x \wedge y)) \wedge z)$$

$$\Leftrightarrow$$

$$(w \wedge x \wedge v) \vee (y \wedge ((w \wedge x) \vee ((x \vee z) \wedge w) \vee (w \wedge z) \vee (x \wedge v)))$$

Reduction to UNSAT

Asking that this formula hold for all Boolean assignments is just to ask if it valid.

Such a reduction, if it were sound, would mean that the decision problem is efficiently reducible to UNSAT, the canonical problem of the complexity class coNP.

On the practical side, this would open the door to using modern SAT solving techniques in implementations of cubical type theories.

Unsound reduction

However, the simplistic effort at a reduction above easily fails in general. For example,

$$\top \Rightarrow (x = 0) \vee (x = 1)$$

does not hold in the Kripke-Joyal semantics, while

$$\top \Rightarrow (x \Leftrightarrow 0) \vee (x \Leftrightarrow 1)$$

is valid as a Boolean formula.

The counterexample is just $\alpha = \mathrm{id} : \mathsf{I}^1 \to \mathsf{I}^1$.

Disjunction in the consequent

One difference between these two problems is that the second one has a disjunction (of formulas) on the right, while the first one does not. As it turns out, this is the only obstruction. For now, we record that

$$\mathsf{I}^n \Vdash \phi \Rightarrow (s = t)$$

iff

$$\text{for all } \beta : \mathsf{I}^0 \to \mathsf{I}^n, \mathsf{I}^n \Vdash \phi(\beta) \text{ implies } \mathsf{I}^n \Vdash (s = t)(\beta)$$

Transforming the consequent

Suppose we extend the formula to I^2 and shift the second equation?

$$\mathsf{I}^2 \not\models \top \Rightarrow (x_1 = 0) \vee (x_2 = 1)$$

because, for example, applying the formula to $\beta = (1, 0)$ yields $\perp$.

Analogously,

$$\top \Rightarrow (x_1 \Leftrightarrow 0) \vee (x_2 \Leftrightarrow 1)$$

is not valid as a Boolean formula, with $x_1 = 1$ and $x_2 = 0$ satisfying its negation.

The transformation C

Let $\psi : \mathsf{I}^n \to \Omega$. Let $a = \mathsf{lvs}(\psi)$ be the number of leaves in a formula ψ. We define a formula $\mathsf{C}_j : \mathsf{I}^{an} \to \Omega$:

$$
\begin{aligned}
\mathsf{C}_j(\psi_1 \vee \psi_2) &:= \mathsf{C}_j(\psi_1) \vee \mathsf{C}_{j+\mathsf{lvs}(\psi_1)}(\psi_2) \\
\mathsf{C}_j(\psi_1 \wedge \psi_2) &:= \mathsf{C}_j(\psi_1) \wedge \mathsf{C}_{j+\mathsf{lvs}(\psi_1)}(\psi_2) \\
\mathsf{C}_j\big((s = t)\big) &:= \big(s[x_{jn+1}/x_1, \ldots, x_{jn+n}/x_n] = t[x_{jn+1}/x_1, \ldots, x_{jn+n}/x_n]\big) \\
\mathsf{C}_j(\top) &:= \top \\
\mathsf{C}_j(\bot) &:= \bot
\end{aligned}
$$

We let $\mathsf{C}(\psi) := \mathsf{C}_0(\psi)$.

Example

Consider the problem

$$\phi := (x_1 = x_1 \vee x_2)$$
$$\psi := (x_1 = 1) \vee (x_1 = x_2) \vee (x_2 = 0)$$

Note that

$$\mathsf{I}^2 \not\Vdash \phi \Rightarrow \psi$$

because when $\alpha = (x_1 \vee x_2, x_2) : \mathsf{I}^2 \to \mathsf{I}^2$, we have

- $\mathsf{I}^2 \Vdash (x_1 = x_1 \vee x_2)(\alpha)$
- $\mathsf{I}^2 \not\Vdash (x_1 = 1)(\alpha)$
- $\mathsf{I}^2 \not\Vdash (x_1 = x_2)(\alpha)$
- $\mathsf{I}^2 \not\Vdash (x_2 = 0)(\alpha)$

Example

Consider the problem

$$\phi := (x_1 = x_1 \vee x_2)$$
$$\psi := (x_1 = 1) \vee (x_1 = x_2) \vee (x_2 = 0)$$

Specifically, when $\alpha = (x_1 \vee x_2, x_2) : \mathrm{I}^2 \to \mathrm{I}^2$, we have

- $\mathrm{I}^2 \Vdash (x_1 = x_1 \vee x_2)(\alpha)$
- $\mathrm{I}^2 \nVdash (x_1 = 1)(\alpha)$ because $\mathrm{I}^2 \nVdash (x_1 = 1)(\alpha\beta_1)$ where $\beta_1 = (0, 0)$
- $\mathrm{I}^2 \nVdash (x_1 = x_2)(\alpha)$ because $\mathrm{I}^2 \nVdash (x_1 = x_2)(\alpha\beta_2)$ where $\beta_2 = (1, 0)$
- $\mathrm{I}^2 \nVdash (x_2 = 0)(\alpha)$ because $\mathrm{I}^2 \nVdash (x_1 = 1)(\alpha\beta_3)$ where $\beta_3 = (0, 1)$

Now we combine α and the β_i: $\beta = (\alpha\beta_1, \alpha\beta_2, \alpha\beta_3)$. Given that

$$\mathrm{C}(\psi) := (x_1 = 1) \vee (x_3 = x_4) \vee (x_5 = 0)$$

we have that $\mathrm{I}^6 \nVdash C(\psi)(\beta)$

Reduction

Let $\psi : \mathsf{I}^n \to \Omega$, let $a = \mathsf{lvs}(\psi)$, and let $\phi : \mathsf{I}^{an} \to \Omega$.

$$\mathsf{I}^{an} \Vdash \phi \Rightarrow \mathsf{C}(\psi)$$
$$\text{iff}$$
$$\text{for all } \beta : \mathsf{I}^0 \to \mathsf{I}^{an}, \mathsf{I}^0 \Vdash \phi(\beta) \text{ implies } \mathsf{I}^0 \Vdash \mathsf{C}(\psi)(\beta)$$

The top-to-bottom direction is trivial. The last slide exemplifies the contrapositive of the bottom-to-top direction.

Validity preservation

Let $\psi : \mathsf{I}^n \to \Omega$, and let $a = \mathsf{lvs}(\psi)$.

$$\mathsf{I}^n \Vdash \top \Rightarrow \psi$$

iff

$$\mathsf{I}^{an} \Vdash \top \Rightarrow \mathsf{C}(\psi)$$

The transformation A

Our goal now is to transform formulas in antecedent position.

Let $\phi : \mathsf{I}^n \to \Omega$, and let $a \geq 0$. We define $A(\phi) : \mathsf{I}^{an} \to \Omega$ by

$$
\begin{aligned}
\mathsf{A}(\phi_1 \vee \phi_2) &:= \mathsf{A}(\phi_1) \vee \mathsf{A}(\phi_2) \\
\mathsf{A}(\phi_1 \wedge \phi_2) &:= \mathsf{A}(\phi_1) \wedge \mathsf{A}(\phi_2) \\
\mathsf{A}\left((s = t)\right) &:= \bigwedge_{0 \leq j \leq a} \left(s[x_{jn+1}/x_1, \ldots, x_{jn+n}/x_n] = t[x_{jn+1}/x_1, \ldots, x_{jn+n}/x_n]\right) \\
\mathsf{A}(\bot) &:= \bot \\
\mathsf{A}(\top) &:= \top
\end{aligned}
$$

Example

Consider the problem:

$$\phi := (x_1 = 0) \vee (x_1 = 1)$$
$$\psi := (x_1 = 0) \vee (x_1 = 1)$$

Note the different effects of A and C:

$$\mathsf{A}(\phi) := ((x_1 = 0) \wedge (x_2 = 0)) \vee ((x_1 = 1) \wedge (x_2 = 1))$$
$$\mathsf{C}(\psi) := (x_1 = 0) \vee (x_2 = 1)$$

Validity preservation

$$\mathsf{I}^{n} \Vdash \phi \Rightarrow \psi$$

iff

$$\mathsf{I}^{an} \Vdash \mathsf{A}(\phi) \Rightarrow \mathsf{C}(\psi)$$

Main reduction (without $\forall$)

$$\mathsf{I}^n \Vdash \phi \Rightarrow \psi$$

iff

$$\text{for all } \beta : \mathsf{I}^0 \to \mathsf{I}^{an}, \mathsf{I}^0 \Vdash \mathsf{A}(\phi)(\beta) \text{ implies } \mathsf{I}^0 \Vdash \mathsf{C}(\psi)(\beta)$$

Reducing the latter problem to UNSAT is little more than a change of notation and prefixing a $\neg$.

Universal quantifier

Because our indexing category has products and our variables have representable type, the interpretation of $\forall$ in the Kripke-Joyal semantics is remarkably efficient: given $\phi : \mathsf{I}^n \times \mathsf{I}^p \to \Omega$, and letting y be a variable of type I^p,

$$\mathsf{I}^n \Vdash \forall y.\phi \text{ iff } \mathsf{I}^n \times \mathsf{I}^p \Vdash \phi$$

We extend A and C so that they preserve $\forall$ and ignore the bound variables.

Main reduction (with $\forall$)

Let $\mathsf{A}(\phi)', \mathsf{C}(\psi)' : \mathsf{I}^{an} \times \mathsf{I}^{p} \to \Omega$ denote the formulas $\mathsf{A}(\phi)$ and $\mathsf{C}(\psi)$ after interpreting $\forall$.

$$\mathsf{I}^{n} \Vdash \phi \Rightarrow \psi$$

$$\text{iff}$$

$$\text{for all } \beta : \mathsf{I}^{0} \to \mathsf{I}^{an}, \text{ either } \mathsf{I}^{0} \nVdash \mathsf{A}(\phi)(\beta) \text{ or } \mathsf{I}^{0} \Vdash \mathsf{C}(\psi)(\beta)$$

$$\text{iff}$$

$$\text{for all } \beta : \mathsf{I}^{0} \to \mathsf{I}^{an}, \text{ either } \mathsf{I}^{p} \nVdash \mathsf{A}(\phi)'(\beta) \text{ or } \mathsf{I}^{p} \Vdash \mathsf{C}(\psi)'(\beta)$$

$$\text{iff}$$

$$\text{for all } \beta : \mathsf{I}^{0} \to \mathsf{I}^{an}, \text{ either}$$

$$\text{there exists } \gamma : I^{0} \to I^{p} \text{ such that } \mathsf{I}^{0} \nVdash \mathsf{A}(\phi)'(\beta, \gamma), \text{ or}$$

$$\text{for all } \gamma : I^{0} \to I^{p}, \mathsf{I}^{p} \Vdash \mathsf{C}(\psi)'(\beta, \gamma)$$

Classification

The final sentence —

$$\text{for all } \beta : \mathsf{I}^0 \to \mathsf{I}^{an}, \text{ either}$$
$$\text{there exists } \gamma : I^0 \to I^p \text{ such that } \mathsf{I}^0 \not\Vdash \mathsf{A}(\phi)'(\beta,\gamma), \text{ or}$$
$$\text{for all } \gamma : I^0 \to I^p, \mathsf{I}^p \Vdash \mathsf{C}(\psi)'(\beta,\gamma)$$

— naturally reduces to a ∀∃-formula of quantified Boolean logic.

Conversely, there's an efficient reduction of valid ∀∃-formulas in CNF to entailments in the cofibration language (specifically, entailments of $\bot$).

Proposition

The entailment problem for the cofibration language of presheaves over the fpt for distributive lattices is Π_2^{poly}*-complete.*

Classification

The cofibration languages of CCHM[4] and ABCFHL[5] interpret (efficiently) into a less expressive fragment of the Mitchell-Bénabou language. This pays dividends in terms of their run-time complexity.

Proposition

The entailment problem for the CCHM cofibration language is coNP-complete.

Proposition

The entailment problem for the ABCFHL cofibration language is coNP-complete.

[4] Cyril Cohen et al. *Cubical Type Theory: a constructive interpretation of the univalence axiom*. 2016. arXiv: 1611.02108 [cs.LO].

[5] Carlo Angiuli et al. "Syntax and models of Cartesian cubical type theory". In: *Mathematical Structures in Computer Science* 31.4 (2021), pp. 424–468.

Thank you!