Constructive Algebra

Daniel Wessel, Università di Verona, Dip.to di Informatica
Autumn School *Proof & Computation*
Fischbachau, September 16–22, 2018

github.com/danielwessel/pc18

Entailment relations

Entailment relations

Let S be a set, and let $\vdash \subseteq \mathrm{Fin}(S) \times \mathrm{Fin}(S)$.

$\vdash$ is an **entailment relation** if it is
reflexive, monotone, and transitive, i.e.,

$$\frac{U \between V}{U \vdash V}\,(\mathrm{R}) \qquad \frac{U \vdash V}{U, U' \vdash V, V'}\,(\mathrm{M}) \qquad \frac{U \vdash V, a \quad U, a \vdash V}{U \vdash V}\,(\mathrm{T})$$

Entailment relations

Let S be a set, and let $\vdash \subseteq \mathrm{Fin}(S) \times \mathrm{Fin}(S)$.

$\vdash$ is an **entailment relation** if it is
reflexive, monotone, and transitive, i.e.,

$$\frac{U \between V}{U \vdash V}\,(\mathrm{R}) \qquad \frac{U \vdash V}{U, U' \vdash V, V'}\,(\mathrm{M}) \qquad \frac{U \vdash V, a \quad U, a \vdash V}{U \vdash V}\,(\mathrm{T})$$

A **model** (or ideal element, point) of $\vdash$ is a subset α of S which "splits entailments", i.e.,

$$\frac{\alpha \supseteq U \quad U \vdash V}{\alpha \between V}$$

Semantics

Let $\mathrm{Spec}(\vdash)$ denote the class of models of $\vdash$.

Completeness theorem* (Scott)

The following are equivalent.

1. $U \vdash V$
2. $\forall \alpha \in \mathrm{Spec}(\vdash)\,(\,U \subseteq \alpha \;\rightarrow\; \alpha \between V\,)$

N.B.

Completeness implies excluded middle.

CT is classically equivalent to the prime ideal theorem.

The fundamental theorem: constructive semantics

Theorem (Cederquist, Coquand)

Every entailment relation $(S, \vdash)$ generates a distributive lattice L_S with a map $i : S \to L_S$ such that

$$U \vdash V \qquad \text{if and only if} \qquad \bigwedge_{a \in U} i(a) \leqslant \bigvee_{b \in V} i(b)$$

This i is *universal* among interpretations in distributive lattices:

$$\begin{tikzcd} (S, \vdash) \arrow[r, "i"] \arrow[dr, "\forall f"'] & L_S \arrow[d, dashed, "\exists ! g"] \\ & L \end{tikzcd}$$

Example: support of a ring

Consider the entailment relation of (proper) **prime ideal** of $\mathbf{R}$.

$$
\begin{aligned}
&\vdash 0\\
a &\vdash ab\\
a, b &\vdash a + b\\
ab &\vdash a, b\\
1 &\vdash
\end{aligned}
$$

Example: support of a ring

Consider the entailment relation of (proper) **prime ideal** of **R**.

$$
\begin{aligned}
&\vdash 0 && D(0) = 1 \\
a &\vdash ab && D(a) \leqslant D(ab) \\
a, b &\vdash a + b && D(a) \wedge D(b) \leqslant D(a + b) \\
ab &\vdash a, b && D(ab) \leqslant D(a) \vee D(b) \\
1 &\vdash && D(1) = 0
\end{aligned}
$$

Example: support of a ring

Consider the entailment relation of (proper) **prime ideal** of $\mathbf{R}$.

$$
\begin{aligned}
&\vdash 0 && D(0) = 1 \\
a &\vdash ab && D(a) \leqslant D(ab) \\
a, b &\vdash a + b && D(a) \wedge D(b) \leqslant D(a+b) \\
ab &\vdash a, b && D(ab) \leqslant D(a) \vee D(b) \\
1 &\vdash && D(1) = 0
\end{aligned}
$$

We get Joyal's lattice ("a notion of zero").
The dual of $\vdash$ yields the **universal support** on $\mathbf{R}$.

Vast applicability of entailment relations

- **Constructive algebra**
  e.g. Point-free spectra (Joyal, Coquand)
- **Proof theory**
  e.g. Szpilrajn's theorem (Negri–von Plato–Coquand)
- **Point-free topology**
  e.g. localic Hahn-Banach (Mulvey–Pelletier, Coquand)
- **Theoretical computer science**
  e.g. domain theory, resolution (Zhang–Rounds, Coquand)
- **Non-classical logic**
  e.g. many-valued logic (Scott)

Around Hilbert’s 17th problem

Example (Motzkin 1967)

$$M(x,y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$$
$$= \frac{x^2y^2(x^2+y^2+1)(x^2+y^2-2)^2 + (x^2-y^2)^2}{(x^2+y^2)^2}$$

But $M(x,y)$ cannot be written as a sum of squares of polynomials.

Sums of squares

Example (Motzkin 1967)

$$\begin{aligned} M(x,y) &= x^4y^2 + x^2y^4 + 1 - 3x^2y^2 \\ &= \frac{x^2y^2(x^2+y^2+1)(x^2+y^2-2)^2 + (x^2-y^2)^2}{(x^2+y^2)^2} \end{aligned}$$

But $M(x,y)$ cannot be written as a sum of squares of polynomials.

Hilbert's 17th problem

Suppose that $f \in \mathbb{R}[x_1, \ldots, x_n]$ is nonnegative at all points of $\mathbb{R}^n$.
Is f a finite sum of squares of rational functions?

Artin gave an affirmative answer.

Sums of squares

"[Artin's] method was as remarkable as the result. It was perhaps the first triumph of what is sometimes called 'abstract' algebra."

Richard Brauer
Emil Artin

Artin's key observation
The totally positive elements of a field are precisely the sums of squares.

Ordered rings

An order $\leqslant$ of a ring $\mathbf{R}$ is **compatible** if, for all $a, b, c \in \mathbf{R}$,

$$\begin{aligned} a \leqslant b &\to a + c \leqslant b + c \\ 0 \leqslant a \wedge 0 \leqslant b &\to 0 \leqslant ab \end{aligned}$$

Positive cones $P \subseteq \mathbf{R}$ determine the compatible orders:

$$\begin{aligned} P \cap -P &= 0 \\ P \cdot P &\subseteq P \\ P + P &\subseteq P \\ P \cup -P &= \mathbf{R} \end{aligned}$$

Orders as ideal objects

Let **R** be an **integral ring**, i.e., such that, for all $a \in \mathbf{R}$,

$$a = 0 \lor \forall b \in \mathbf{R} \, (\, ab = 0 \;\rightarrow\; b = 0 \,)$$

Let $\vdash$ be generated by all instances of

$$\begin{aligned} a, -a &\vdash \\ a, b &\vdash ab \\ a, b &\vdash a + b \\ &\vdash a, -a \qquad \text{for } a \neq 0 \end{aligned}$$

Orders as ideal objects

Proposition

Let $U \in \mathrm{Fin}(\mathbf{R})$. The following are equivalent.

1. $U \vdash$
2. There are $a_0, \dots, a_n \in (U)$ and $x_0, \dots, x_n \in \mathbf{R} \setminus \{ 0 \}$ s.t.

$$\sum_{i=0}^{n} a_i x_i^2 = 0$$

where (U) is the multiplicative monoid generated by U.

Proof strategy.

Abbreviate the second item by $\mathsf{Inc}(U)$.

Show that

(i) $\mathsf{Inc}(U)$ implies $U \vdash$

(ii) Inc is monotone

(iii) Inc obeys

$$\frac{U \vdash V \quad \forall b \in V\, \mathsf{Inc}(W, b)}{\mathsf{Inc}(U, W)}$$

where $U \vdash V$ is an initial entailment. $\square$

Corollary

Let $\mathbf{K}$ be a non-trivial discrete field.

The following are equivalent.

1. $\vdash$ **collapses**, i.e., $\emptyset \vdash \emptyset$
2. -1 is a sum of squares

Sums of squares

Corollary

Let $\mathbf{K}$ be a non-trivial discrete field.

The following are equivalent.

1. $\vdash$ **collapses**, i.e., $\emptyset \vdash \emptyset$
2. -1 is a sum of squares

Corollary

Let $\mathbf{K}$ be a discrete formally real field and let $0 \neq a \in \mathbf{K}$.

The following are equivalent.

1. a is **totally positive**, i.e., $\vdash a$
2. a is a sum of squares.

Corollary

Let $\mathbf{K}$ be a **factorial field**, and let $f \in \mathbf{K}[X]$ be irreducible and of odd degree. Let $\vdash$ and $\vdash_f$ be the entailment relations of total order of $\mathbf{K}$ and $\mathbf{K}[X]/\langle f \rangle$, respectively.

Then $\vdash$ and $\vdash_f$ **collapse simultaneously**.

Classically, this means that every odd-degree extension of a formally real field is formally real.

Proof.

By induction on the degree of f, following the classical proof. $\square$

Perspectives

- Orderability criteria for groups.
  E.g., **Levi's theorem**: "An abelian group is orderable iff it is torsion-free" in terms of collapse.

- Ordered groups and topology.
  E.g., **Sikora's theorem**: "The space of compatible orders of $\mathbb{Z}^n$, where $n > 1$, is a Cantor space" by Stone duality.

- **Extendability** criteria for partial orders.
  E.g., Serre's theorem on extension of partial orders of fields.

- **Archimedean** property requires an infinitary disjunction.
  How can we deal with this?

Generalized entailment relations

Let S be a set, and let $\vdash \subseteq \mathrm{Fin}(S) \times \mathrm{Pow}(S)$.
$\vdash$ is a **generalized entailment relation** if it is
reflexive and transitive:

$$\frac{U \between V}{U \vdash V}\,(\mathrm{R}) \qquad \frac{U \vdash V \quad \forall b \in V\,(\,U', b \vdash W\,)}{U, U' \vdash W}\,(\mathrm{T})$$

Perspectives:

- (T) can be eliminated for inductively generated entrels.
- Generalized entrels interpret conservatively in frames.
- We can now describe, e.g., maximal and minimal spectra.

References I

[CC00] Jan Cederquist and Thierry Coquand. "Entailment relations and distributive lattices". In: *Logic Colloquium '98. Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic, Prague, Czech Republic, August 9–15, 1998*. Ed. by Samuel R. Buss, Petr Hájek, and Pavel Pudlák. Vol. 13. Lect. Notes Logic. Natick, MA: A. K. Peters, 2000, pp. 127–139.

[Fuc11] László Fuchs. *Partially Ordered Algebraic Systems*. Mineola, New York: Dover Publications, 2011.

References II

[Joy75] André Joyal. “Les théorèmes de Chevalley-Tarski”. In: *Cahiers de topologie et géométrie différentielle catégoriques* 16.3 (1975), pp. 256–258.

[Sch12] Konrad Schmüdgen. “Around Hilbert’s 17th problem”. In: *Documenta Mathematica. Extra Volume: Optimization Stories* (2012), pp. 433–438.

[Sco74] Dana Scott. “Completeness and axiomatizability in many-valued logic”. In: *Proceedings of the Tarski Symposium (Proc. Sympos. Pure Math., Vol. XXV, Univ. California, Berkeley, Calif., 1971)*. Ed. by Leon Henkin et al. Providence, RI: Amer. Math. Soc., 1974, pp. 411–435.