

# Constructive Algebra

---

Daniel Wessel, Università di Verona, Dip.to di Informatica

Autumn School *Proof & Computation*

Fischbachau, September 16–22, 2018

[github.com/danielwessel/pc18](https://github.com/danielwessel/pc18)

## Entailment relations

# Entailment relations

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

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

$$\frac{U \not\sim V}{U \vdash V} \text{ (R)} \quad \frac{U \vdash V}{U, U' \vdash V, V'} \text{ (M)} \quad \frac{U \vdash V, a \quad U, a \vdash V}{U \vdash V} \text{ (T)}$$

# Entailment relations

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

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

$$\frac{U \not\leq V}{U \vdash V} \text{ (R)} \quad \frac{U \vdash V}{U, U' \vdash V, V'} \text{ (M)} \quad \frac{U \vdash V, a \quad U, a \vdash V}{U \vdash V} \text{ (T)}$$

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

$$\frac{\alpha \supseteq U \quad U \vdash V}{\alpha \not\leq V}$$

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

## **Completeness theorem\* (Scott)**

The following are equivalent.

1.  $U \vdash V$
2.  $\forall \alpha \in \text{Spec}(\vdash) (U \subseteq \alpha \rightarrow \alpha \not\subseteq V)$

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  $i : S \rightarrow L_S$  such that

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

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

$$\begin{array}{ccc} (S, \vdash) & \xrightarrow{i} & L_S \\ & \searrow \forall f & \downarrow \exists! g \\ & & L \end{array}$$

## Example: support of a ring

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

$$\vdash 0$$

$$a \vdash ab$$

$$a, b \vdash a + b$$

$$ab \vdash a, b$$

$$1 \vdash$$

## Example: support of a ring

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

$$\vdash 0$$

$$a \vdash ab$$

$$a, b \vdash a + b$$

$$ab \vdash a, b$$

$$1 \vdash$$

$$D(0) = 1$$

$$D(a) \leq D(ab)$$

$$D(a) \wedge D(b) \leq D(a + b)$$

$$D(ab) \leq D(a) \vee D(b)$$

$$D(1) = 0$$



## Example: support of a ring

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

$\vdash 0$	$D(0) = 1$
$a \vdash ab$	$D(a) \leq D(ab)$
$a, b \vdash a + b$	$D(a) \wedge D(b) \leq D(a + b)$
$ab \vdash a, b$	$D(ab) \leq D(a) \vee D(b)$
$1 \vdash$	$D(1) = 0$

We get Joyal's lattice ("a notion of zero").

The dual of  $\vdash$  yields the **universal support** on **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)

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

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

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

Artin gave an affirmative answer.

*"[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  $\leq$  of a ring  $\mathbf{R}$  is **compatible** if, for all  $a, b, c \in \mathbf{R}$ ,

$$a \leq b \rightarrow a + c \leq b + c$$

$$0 \leq a \wedge 0 \leq b \rightarrow 0 \leq ab$$

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

$$P \cap -P = 0$$

$$P \cdot P \subseteq P$$

$$P + P \subseteq P$$

$$P \cup -P = \mathbf{R}$$

# Orders as ideal objects

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

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

Let  $\vdash$  be generated by all instances of

$$a, -a \vdash$$

$$a, b \vdash ab$$

$$a, b \vdash a + b$$

$$\vdash a, -a \quad \text{for } a \neq 0$$



## Proposition

Let  $U \in \text{Fin}(\mathbf{R})$ . 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  $U$ .

# Orders as ideal objects

## Proof strategy.

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

Show that

- (i)  $\text{Inc}(U)$  implies  $U \vdash$
- (ii)  $\text{Inc}$  is monotone
- (iii)  $\text{Inc}$  obeys

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

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



## 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. □

- 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  $\vdash \subseteq \text{Fin}(S) \times \text{Pow}(S)$ .

$\vdash$  is a **generalized entailment relation** if it is reflexive and transitive:

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

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.

- [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.