An algebraic version of Herbrand's theorem

Marco Abbadini

School of Computer Science, University of Birmingham, UK

Salerno, Italia
24 April 2025

Based on joint works with Francesca Guffanti:

- Quantifier-free formulas and quantifier alternation depth in doctrines. *Journal of Pure and Applied Algebra*. Accepted. Preprint on arXiv.
- Freely adding one layer of quantifiers to a Boolean doctrine. Submitted. Preprint on arXiv.

Algebraic logic

Message

First-order logic can be done algebraically.

I.e.: the toolkit of the algebraic logician can be used also in the first-order setting.

In this talk we will see an example: an algebraic version of Herbrand's theorem.

Theorem (Herbrand's theorem, 1930 – for existential statements)

A universal theory $\mathcal{T}$ proves a sentence $\exists x\, \alpha(x)$ with α quantifier-free if and only if there are finitely many terms $c_1, \ldots, c_n$ such that $\mathcal{T}$ proves $\alpha(c_1) \vee \cdots \vee \alpha(c_n)$.

Example.

Language: a relation symbol $\leq$, and two constant symbols max and min.

Theory: $\leq$ is a partial order, max is maximum, min is minimum.

- $\exists x\, (\max \leq x)$.
- There is an element strictly between min and max:
  $\exists x\, (\min \leq x \leq \max,\ x \neq \min, x \neq \max)$

Herbrand's theorem is often formulated in this version for existential statements, but Herbrand's results cover all first-order formulas.

I will present an algebraic version of Herbrand's theorem for existential statements.

How we got it: we wanted to know how to freely add one layer of quantifier alternation depth to a Boolean doctrine...

What are the algebras of classical first-order logic?

[First-order Boolean doctrines, going back to the work of Lawvere in the '60s]

Boolean algebras are precisely the Lindenbaum-Tarski algebras of propositional theories; up to iso, Boolean algebras are precisely the algebras of the form

$$\mathcal{L}\text{-Form}/{\equiv_\Sigma},$$

where $\mathcal{L}$ is a propositional language ($=$ a set of propositional variables), and Σ is a propositional theory (a set of $\mathcal{L}$-formulas).

We do the same for classical first-order logic.

How do we view propositional logic inside first-order logic? A "propositional variable" becomes a nullary relation symbol.

In the first-order setting, the language $\mathcal{L}$ of propositional variables is replaced by a set $\mathcal{L}$ of relation symbols (with their associated arity).

For simplicity, we consider the case where we do not have function symbols.

Roughly speaking: first-order Boolean doctrines are precisely the algebras of the form

$$\mathcal{L}\text{-Form}/\equiv_{\Sigma}$$

for $\mathcal{L}$ ranging among all sets of relation symbols, and Σ among all sets of $\mathcal{L}$-sentences.

But what algebraic structure are we considering here?

Fix an infinite set of variables Var.

A first-order Boolean doctrine (modelling $\mathcal{L}\text{-}\mathrm{Form}/{\equiv_\Sigma}$) is a many-sorted algebras with the following data:

1. A family of Boolean algebras, one for each finite subset X of Var (the Boolean algebra of formulas whose free variables belong to X), linked by
2. substitutions and
3. quantifiers.

(We avoid equality, for simplicity.)

Definition

A first-order Boolean doctrine **P** (over an empty functional language) consists of

1. [Family of Boolean algebras] For $X \subseteq_{\text{fin}} \mathrm{Var}$, we have a Boolean algebra $\mathbf{P}(X)$.

to be continued...

2. [Substitutions] For $X, Y \subseteq_{\mathrm{fin}} \mathrm{Var}$ and $\sigma \colon X \to Y$, we have a Boolean homomorphism $\mathbf{P}_\sigma \colon \mathbf{P}(X) \to \mathbf{P}(Y)$...
   (We denote $\mathbf{P}_\sigma(\alpha)$ also by $\alpha\left[\left({}^{\sigma(x)}/_{x}\right)_{x \in X}\right]$)
   ... such that
   - (Functoriality: identity) For all $X \subseteq_{\mathrm{fin}} \mathrm{Var}$,

     $$\mathbf{P}_{\mathrm{id}_X} = \mathrm{id}_{\mathbf{P}(X)}, \quad \text{i.e.} \quad \alpha\left[\left({}^{x}/_{x}\right)_{x \in X}\right] = \alpha.$$

   - (Functoriality: composition) For all $X, Y, Z \subseteq_{\mathrm{fin}} \mathrm{Var}$, for all $f \colon X \to Y$ and $g \colon Y \to Z$, we have

     $$\mathbf{P}_{g \circ f} = \mathbf{P}_g \circ \mathbf{P}_f,$$

     $$\text{i.e.} \quad \alpha\left[\left({}^{f(x)}/_{x}\right)_{x \in X}\right]\left[\left({}^{g(y)}/_{y}\right)_{y \in Y}\right] = \alpha\left[\left({}^{gf(x)}/_{x}\right)_{x \in X}\right].$$

to be continued...

In general, one would fix a priori a functional language $\mathbb{F}$, and then the substitutions are defined for each $\sigma \colon X \to \mathrm{Term}(Y)$

3. For all $X \subseteq_{\text{fin}} \mathrm{Var}$, $y \in \mathrm{Var} \setminus X$, $\alpha \in \mathbf{P}(X \cup \{y\})$,
   - there is a (necessarily unique) element $\forall y\, \alpha \in \mathbf{P}(X)$ s.t., for all $\beta \in \mathbf{P}(X)$,

$$\beta \leq \forall y\, \alpha \ \text{ in } \mathbf{P}(X) \iff \underbrace{\mathbf{P}_{X \hookrightarrow X \cup \{y\}}(\beta)}_{\beta[(x/x)_{x \in X}]} \leq \alpha \ \text{ in } \mathbf{P}(X \cup \{y\});$$

   - there is a (necessarily unique) element $\exists y\, \alpha \in \mathbf{P}(X)$ s.t., for all $\beta \in \mathbf{P}(X)$,

$$\exists y\, \alpha \leq \beta \iff \alpha \leq \mathbf{P}_{X \hookrightarrow X \cup \{y\}}(\beta);$$

and, moreover,...

...for all $X, X' \subseteq_{\mathrm{fin}} \mathrm{Var}$, for all $\sigma \colon X \to X'$, for all $y \in \mathrm{Var} \setminus (X \cup X')$, for all $\alpha \in \mathbf{P}(X \cup \{y\})$,

- $$\mathbf{P}_\sigma(\forall y\, \alpha) = \forall y\, \mathbf{P}_{\sigma \cup \mathrm{id}_{\{y\}} \colon X \cup \{y\} \to X' \cup \{y\}}(\alpha).$$

  i.e.

  $$(\forall y\, \alpha)\left[({}^{\sigma(x)}/_{x})_{x \in X}\right] = \forall y\, \left(\alpha\left[({}^{\sigma(x)}/_{x})_{x \in X}\right]\right).$$
- and analogously for $\exists$.

Folklore: first-order Boolean doctrines are the algebras of classical first-order logic.

Disclaimer: the "classical first-order logic" meant here is the one whose semantics allows the usage of empty structures.

If one doesn't want the empty structures, they can impose on the first-order Boolean doctrine "$\exists x \top = \top$".

Outside this talk, first order Boolean doctrines are defined as certain contravariant functors

$$\mathsf{C}^{\mathrm{op}} \to \mathsf{BA}$$

from a category C with finite products to the category of Boolean algebras.

What for us is "a finite set of variables" (a "context") becomes an object in a category C.

1. This smoothly covers also the <u>many-sorted</u> first-order logic.
2. There is no way to count the number of variables in a context.

For this talk we will stick to the presentation in the previous slides:

- we have an infinite set Var of variables,
- we have a family of Boolean algebras indexed by the finite sets of Var
- linked by substitutions and quantifiers.

First-order Boolean algebras (over a fixed functional language $\mathbb{F}$) form a **variety** of many-sorted algebras!

(One sort for each $X \subseteq_{\text{fin}} \mathrm{Var}$.)

Therefore, for example, we have free algebras!

This allows us to frame Herbrand's theorem algebraically.

Theorem (Herbrand's theorem, 1930 – for existential statements)

A universal theory $\mathcal{T}$ proves a sentence $\exists x\, \alpha(x)$ with α quantifier-free if and only if there are finitely many terms $c_1, \dots, c_n$ such that $\mathcal{T}$ proves $\alpha(c_1) \vee \cdots \vee \alpha(c_n)$.

Universal theory $\leftrightsquigarrow$ Boolean doctrine: family of Boolean algebras linked by substitutions satisfying functoriality (no quantifiers).

Universal sentences in the theory $\leftrightsquigarrow$ element in the Boolean doctrine.

$\forall \underline{x}\, \alpha(\underline{x}) = \top$ in $\mathbf{P}(\varnothing)$ e' equivalente a $\alpha(\underline{x}) = \top$ in $\mathbf{P}(\underline{x})$.

What is $\exists x\, \alpha(x)$ then?

Short answer: a certain element in the free first-order Boolean doctrine over the Boolean doctrine corresponding to $\mathcal{T}$.

The forgetful functor from first-order Boolean doctrines over $\mathbb{F}$ to Boolean doctrines over $\mathbb{F}$ has a left adjoint.

It maps a Boolean doctrine $\mathbf{P}$ to the first-order Boolean doctrine denoted $\mathbf{P}^{\forall\exists}$.

$\mathbf{P}^{\forall\exists}$ is obtained by freely adding all quantifiers modulo the axioms of first-order Boolean doctrines and modulo all equations in the language of Boolean doctrines holding in $\mathbf{P}$.

Theorem (Herbrand's theorem for $\exists$-statements)

A universal theory $\mathcal{T}$ proves $\exists x\, \alpha(x)$ with α q.f. if and only if there are finitely many terms $c_1, \ldots, c_n$ such that $\mathcal{T}$ proves $\alpha(c_1) \vee \cdots \vee \alpha(c_n)$.

Theorem (Algebraic version, A., Guffanti, 2024)

Let $\mathbf{P}$ be a Boolean doctrine over a functional language $\mathbb{F}$. For every variable x, and every $\alpha \in \mathbf{P}(\{x\})$, we have

$$\exists x\, \alpha = \top \quad \textit{in } \mathbf{P}^{\forall\exists}(\varnothing)$$

if and only if there are finitely many constants $c_1, \ldots, c_n \in \mathbb{F}$ such that

$$\alpha[{}^{c_1}/_{x}] \vee \cdots \vee \alpha[{}^{c_n}/_{x}] = \top \quad \textit{in } \mathbf{P}(\varnothing).$$

($\mathcal{T}$ cannot be an arbitrary theory $\rightsquigarrow$ we need freeness of $\mathbf{P}^{\forall\exists}$ over $\mathbf{P}$)

(Herbrand's theorem holds for inclusive logic. terms $\rightsquigarrow$ constants)

We actually proved in the setting of first-order Boolean doctrines as certain functors $\mathsf{C}^{\mathrm{op}} \to \mathsf{BA}$.

Thus, it covers also many-sorted logic.

Sketch of the proof

The difficult implication is: suppose

$$\exists x\, \alpha = \top;$$

prove that there are finitely many constants $c_1, \dots, c_n \in \mathbb{F}$ such that

$$\alpha[c_1/x] \vee \cdots \vee \alpha[c_n/x] = \top.$$

We prove the contrapositive: Suppose that for all constants $c_1, \dots, c_n \in \mathbb{F}$ we have

$$\alpha[{}^{c_1}/_x] \vee \cdots \vee \alpha[{}^{c_n}/_x] \neq \top.$$

We prove that

$$\exists x\, \alpha \neq \top;$$

We build a model of the Boolean doctrine **P** in which $\exists x\, \alpha$ does not hold.

Sketch:

1. The hypothesis means that the "existential ideal" generated by α is proper. Or, equivalently, that the "universal filter" generated by $\neg\alpha$ is proper.
2. Then we construct a model in a way similar to Henkin's proof of Gödel's completeness theorem (which, in one of its equivalent formulations, says that a consistent theory has a model). This will produce a model in which $\forall x\, \neg\alpha$ is valid, i.e. in which $\exists x\, \alpha$ fails.

Definition

A <u>model</u> of a first-order Boolean doctrine $\mathbf{P}$ (no funct. symb.) consists of

1. a set M,
2. for each $X \subseteq_\omega \mathrm{Var}$ and $\alpha \in \mathbf{P}(X)$, an element $[\![\alpha]\!] \in \mathscr{P}(M^X)$

such that

- $[\![\alpha \vee_X \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$, and similarly for $\wedge_X$, $\neg_X$, $\top_X$ and $\bot_X$;
- for every $\sigma \colon X \to Y$ and $\alpha \in \mathbf{P}(X)$,

$$[\![\mathbf{P}_\sigma(\alpha)]\!] = \{b \in M^Y \mid b \circ \sigma \in [\![\alpha]\!]\};$$

- for every $X \subseteq_\omega \mathrm{Var}$, $y \in \mathrm{Var} \setminus X$ and $\alpha \in \mathbf{P}(X \cup \{y\})$,

$$[\![\forall y\, \alpha]\!] = \{a \in M^X \mid \text{for all } b \in M \text{ we have "} a \cup (y \mapsto b)\text{"} \in [\![\alpha]\!]\},$$

$$[\![\exists y\, \alpha]\!] = \{a \in M^X \mid \text{there is } b \in M \text{ s.t. "} a \cup (y \mapsto b)\text{"} \in [\![\alpha]\!]\},$$

with $a \cup (y \mapsto b) \in M^{X \cup \{y\}}$ the map that on X is a, and in y is b.

Definition

A model of a ~~first-order~~ Boolean doctrine $\mathbf{P}$ (no funct. symb.) consists of

1. a set M,
2. for each $X \subseteq_\omega \mathrm{Var}$ and $\alpha \in \mathbf{P}(X)$, an element $[\![\alpha]\!] \in \mathscr{P}(M^X)$

such that

- $[\![\alpha \vee_X \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$, and similarly for $\wedge_X$, $\neg_X$, $\top_X$ and $\bot_X$;
- for every $\sigma \colon X \to Y$ and $\alpha \in \mathbf{P}(X)$,

$$[\![\mathbf{P}_\sigma(\alpha)]\!] = \{b \in M^Y \mid b \circ \sigma \in [\![\alpha]\!]\};$$

Suppose that for all constants $c_1, \ldots, c_n \in \mathbb{F}$ we have

$$\alpha[{}^{c_1}/_{x}] \vee \cdots \vee \alpha[{}^{c_n}/_{x}] \neq \top.$$

We prove that

$$\exists x\, \alpha \neq \top;$$

We build a model of the Boolean doctrine **P** in which $\exists x\, \alpha$ does not hold.

Sketch: We produce a model of the Boolean doctrine **P** where $\exists x\, \alpha$ fails, i.e. $[\![\alpha]\!] = \varnothing$.

The set M identifies a first-order Boolean doctrine, in which the Boolean algebra associated to $X \subseteq_{\text{fin}}$ is $\mathcal{P}(M^X)$. Recall that, for every X, we have a function

$$[\![-]\!]_X \colon \mathbf{P}(X) \to \mathcal{P}(M^X).$$

The fact that M is a model says precisely that this gives a homomorphism of Boolean doctrines

$$\mathbf{P} \to \mathcal{P}(M^-).$$

Then one uses the universal property

$$\begin{tikzcd} \mathbf{P} \arrow[r] \arrow[dr] & \mathbf{P}^{\forall\exists} \arrow[d, dashed, "\exists!"] \\ & \mathcal{P}(M^-) \end{tikzcd}$$

and from the fact that $[\![\alpha]\!] = \varnothing$, one deduces that $\exists x\, \alpha = \bot$ in $\mathbf{P}^{\forall\exists}$.

[End of sketch of proof]

Herbrand's theorem: "**only little can be proved**". Proof theory is very good for this: e.g. with cut elimination.

What tools do we have in the algebraic setting?

We use **models** (= counterexamples), and to produce them, we used a proof similar to the proof of Gödel completeness theorem.

- With models we use the **axiom of choice** (in the Henkin-style proof).
  Instead, Herbrand's original proof was **constructive**.
  Is there a **doctrinal "choice-free"** proof?
  (Maybe using canonical extensions? / Boolean valued models)
  Maybe the proof then will be easier.

- We are working on “the Stone dual” of Herbrand’s theorem for existential statements.
  Our current approach: to deduce it from the algebraic version. Will it be possible to derive it directly? Will it be easier?

Thank you!