Free extension for universal algebras

Algebra Seminar, NMSU, USA

Marco Abbadini

March 14, 2022

University of Salerno, Italy

Abelian group = set G with a binary operation $+$ (the group operation), a constant element 0 (the neutral element) and a unary operation $-$ (additive inverse) such that

(associativity)	$\forall x, y, z$	$(x+y)+z = x+(y+z)$;
(commutativity)	$\forall x, y$	$x+y = y+x$;
(0 is neutral)	$\forall x$	$x+0 = x$;
($-$ is the inverse)	$\forall x$	$x+(-x) = 0$.

Let G be an Abelian group, and let S a subset of G that generates G. For every group H and every function $f\colon S \to H$, there is at most one group homomorphism $\overline{f}\colon G \to H$ that extends f.

$$\begin{tikzcd} S \arrow[r, hook] \arrow[dr, "f"'] & G \arrow[d, dashed, "!\overline{f}"] \\ & H. \end{tikzcd}$$

In general, this extension may fail to exist.

E.g.: take $S = G$ and f a function that is not a group homomorphism.

Proposition

Let G be an Abelian group and let $M \subseteq G$ be such that

1. M is closed under $+$ and 0, and
2. M generates the Abelian group G.

For every Abelian group H and every function $f\colon M \to H$ such that

1. $f(x+y) = f(x) + f(y)$, and
2. $f(0) = 0$.

there exists a unique group homomorphism $\overline{f}\colon G \to H$ that extends f.

$$\begin{tikzcd} M \arrow[r, hook] \arrow[dr, "f"'] & G \arrow[d, dashed, "\exists!\overline{f}"] \\ & H. \end{tikzcd}$$

Example

$$\begin{tikzcd} \mathbb{N} \arrow[r, hook] \arrow[dr, "f"'] & \mathbb{Z} \arrow[d, dashed, "\exists! \overline{f}"] \\ & H. \end{tikzcd}$$

Define $\overline{f}(n) := nf(1)$.

We refer to the previous proposition as 'Abelian groups have the free extension property over the sublanguage $\{+, 0\}$'.

The analogous statement for groups that are not necessarily abelian is false.

Let $\mathrm{Free}(u, v)$ be the free group on $\{u, v\}$.

Let $M \subseteq \mathrm{Free}(u, v)$ be the submonoid of $\mathrm{Free}(u, v)$ generated by $\{u, v, uv^{-1}u\}$. Example of an element of M:

$$uvvuv^{-1}uuv^{-1}uu.$$

M generates the group $\mathrm{Free}(u, v)$.

Consider the additive group $\mathbb{Z}$ and the map $f\colon M \to \mathbb{Z}$ that maps $w \in M$ to the number of occurrences of v^{-1} in w.

We have $f(w \cdot z) = f(w) + f(z)$, and $f(1) = 0$.

The map f cannot be extended to a group homomorphism, because $f(uv^{-1}u) = 1$, but $f(u) - f(v) + f(u) = 0$.

Recall (free extension property of Abelian groups over $\{+, 0\}$)

G group, M generating submonoid, H group and $f\colon M \to H$ monoid homomorphism. There is a group hom. $\overline{f}\colon G \to H$ that extends f.

Lemma

Let G be an Abelian group and M a generating subset closed under $+$ and 0. For every $x \in G$ there are $u, v \in M$ such that $x = u - v$.

Proof of the free extension property.

Set $\overline{f}(u - v) \coloneqq f(u) - f(v)$. It is well-defined: for $u, v, u', v' \in M$:

$$\begin{aligned} u - v = u' - v' &\iff u + v' = u' + v \\ &\implies f(u + v') = f(u' + v) \\ &\iff f(u) + f(v') = f(u') + f(v) \\ &\iff f(u) - f(v) = f(u') - f(v'). \end{aligned}$$

Further, one proves that $\overline{f}$ is a group homomorphism. □

Key fact used

For every Abelian group G and all $u, v, u', v' \in G$,

$$u - v = u' - v' \iff u + v' = u' + v.$$

Any equation in the language of Abelian groups is equivalent to an equation in the language $\{+, 0\}$.

Example

For every abelian group G and all $x, y, z \in G$,

$$x - y + z = y \iff x + z = y + y.$$

The analogous statement for groups that are not necessarily abelian is false.

For example,

$$x = uv^{-1}u$$

cannot be expressed via an equation in the language $\{\cdot, 1\}$.

Otherwise, we would have a contradiction with the fact that the map f from $\{u, v, uv^{-1}u\}^*$ to the additive monoid $\mathbb{Z}$ that maps w to the number of occurrences of v^{-1} in w is a monoid homomorphism.

Proposition

Let B be a Boolean algebra, and let $L \subseteq B$ be such that

1. L is closed under $\vee$, $\wedge$, 0 and 1, and
2. L generates the Boolean algebra B.

For every Boolean algebra C and every function $f\colon L \to C$ that preserves $\vee$, $\wedge$, 0 and 1, there exists a unique Boolean homomorphism $\overline{f}\colon B \to C$ that extends f.

$$
\begin{tikzcd}
A \arrow[r, hook] \arrow[dr, "f"'] & B \arrow[d, dashed, "\exists!\overline{f}"] \\
& C.
\end{tikzcd}
$$

'Boolean algebras have the free extension property over the sublanguage $\{\vee, \wedge, 0, 1\}$'.

A proof of this is analogous to the proof of the free extension property of Abelian groups over $\{+, 0\}$'.

The proof consists of rewriting certain equations in the language of Boolean algebras into an equivalent system of equations in the language $\{\vee, \wedge, 0, 1\}$.

Example

$$x \wedge \neg y = z \iff \begin{cases} y \wedge z = 0; \\ x \vee y = z \vee y. \end{cases}$$

Main result

An algebraic language consists of a set (with elements called function symbols), and, for each function symbol, a natural number (called arity).

E.g.: $\{+, 0, -\}$; arity of $+$ is 2, arity of 0 is 0, arity of $-$ is 1.

An algebra for an algebraic language $\mathcal{L}$ consists of a set A and, for every function symbol $\tau \in \mathcal{L}$, a function $A^n \to A$, where n is the arity of τ.

E.g.: an Abelian group is an algebra for the language $\{+, 0, -\}$.

A class of algebras for a fixed language is called a variety or equational class if it is axiomatized by identities ($=$ universally quantified equations).

Example

The class of Abelian groups is an equational class of algebras.

$$\begin{array}{ll} \forall x, y, z & (x + y) + z = x + (y + z); \\ \forall x, y & x + y = y + x; \\ \forall x & x + 0 = x; \\ \forall x & x + (-x) = 0. \end{array}$$

Non-example

Cancellative commutative monoids.

$$\forall x, y, z \quad x + z = y + z \Rightarrow x = y.$$

Other examples of equational classes

Groups, monoids, commutative monoids, semigroups.

Rings, commutative rings, rngs, commutative rngs, $\mathbb{R}$-vector spaces, $\mathbb{K}$-vector spaces (for a fixed field $\mathbb{K}$), R-modules (for a fixed ring R), algebras over a fixed field $\mathbb{K}$.

Boolean algebras, lattices, distributive lattices, bounded distributive lattices, Heyting algebras, semilattices.

Sets.

Other non-examples

Fields, integral domains.

Let $\mathcal{V}$ be an equational class of algebras, and let Σ be a sublanguage of the language of $\mathcal{V}$.

E.g.:

1. $\mathcal{V} = \{\text{Abelian groups}\}$, $\Sigma = \{+, 0\}$, or
2. $\mathcal{V} = \{\text{Boolean algebras}\}$, $\Sigma = \{\vee, \wedge, 0, 1\}$, or
3. $\mathcal{V} = \{\text{groups}\}$, $\Sigma = \{\cdot, 1\}$.

Definition

We say that $\mathcal{V}$ has the free extension property over Σ if, for every $B \in \mathcal{V}$, every generating $A \subseteq B$ closed under every $\tau \in \Sigma$, every $C \in \mathcal{V}$ and every function $f\colon A \to C$ that preserves every $\tau \in \Sigma$, there is a unique homomorphism $\overline{f}\colon B \to C$ that extends f.

$$
\begin{tikzcd}
A \arrow[r, hook] \arrow[dr, "f"'] & B \arrow[d, dashed, "\exists!\overline{f}"] \\
& C.
\end{tikzcd}
$$

The class of Abelian groups has the free extension property over $\{+, 0\}$.

The class of groups does not have the free extension property over $\{\cdot, 1\}$.

The class of Boolean algebras has the free extension property over $\{\vee, \wedge, 0, 1\}$.

Definition

We say that equations in $\mathcal{V}$ are expressible in Σ (or that $\mathcal{V}$ has the expressibility property over Σ) if, for each pair $(\sigma(x_1, \ldots, x_n), \rho(x_1, \ldots, x_n))$ of terms in the language of $\mathcal{V}$, there is a finite set of pairs $(\alpha_i(x_1, \ldots, x_n), \beta_i(x_1, \ldots, x_n))$ $(i \in \{1, \ldots, m\})$ in the language Σ such that, for every $A \in \mathcal{V}$ and all $x_1, \ldots, x_n \in A$,

$$\begin{gathered} \sigma(x_1, \ldots, x_n) = \rho(x_1, \ldots, x_n) \\ \Updownarrow \\ \forall i \in \{1, \ldots, m\} \;\; \alpha_i(x_1, \ldots, x_n) = \beta_i(x_1, \ldots, x_n). \end{gathered}$$

Equations in the class of Abelian groups are expressible in $\{+, 0\}$.

Equations in the class of groups are not expressible in $\{\cdot, 1\}$ (see $x = uv^{-1}u$).

Equations in the class of Boolean algebras are expressible over $\{\vee, \wedge, 0, 1\}$.

Free extension property

Given $B \in \mathcal{V}$, a generating Σ-subalgebra A, $C \in \mathcal{V}$ and a Σ-homomorphism $f\colon A \to C$, there is a unique homomorphism $\overline{f}\colon B \to C$ extending f.

Expressibility property

Every equation in the language of $\mathcal{V}$ is equivalent (in $\mathcal{V}$) to a finite set of equations in the language Σ.

Main theorem

$$\begin{gathered}\mathcal{V} \text{ has the free extension property over } \Sigma \\ \Updownarrow \\ \text{equations in } \mathcal{V} \text{ are expressible in } \Sigma.\end{gathered}$$

Usage in practice: one proves that equations in $\mathcal{V}$ are expressible in Σ, and concludes that $\mathcal{V}$ has the free extension property over Σ.

Recall

Let G be an Abelian group and M a generating submonoid. For every $x \in G$ there are $u, v \in M$ such that $x = u - v$.

Definition

A class $\mathfrak{K}$ of terms in the language of $\mathcal{V}$ <u>complements</u> Σ if, given $A \in \mathcal{V}$ and a Σ-subalgebra S, the set $\{\tau(x_1, \ldots, x_n) \mid \tau \in \mathfrak{K}, x_1, \ldots, x_n \in S\}$ contains S and is closed under every symbol in the language of $\mathcal{V}$.

Examples

- For $\mathcal{V} = \{\text{Abelian groups}\}$, $\{x - y\}$ complements $\{+, 0\}$.
- For $\mathcal{V} = \{\text{Boolean algebras}\}$, $\Sigma = \{0, 1, \vee, \wedge\}$,

$$\{(u_1 \vee \neg v_1) \wedge \cdots \wedge (u_n \vee \neg v_n) \mid n \in \mathbb{N}\}$$

  complements Σ.
- For $\mathcal{V} = \{\text{Abelian groups}\}$, a class that complements $\{+\}$?

Proposition

Suppose that $\mathfrak{K}$ complements Σ. Equations in $\mathcal{V}$ are expressible in Σ iff, for every pair $\sigma(x_1, \ldots, x_n)$ and $\rho(y_1, \ldots, y_m)$ with $\sigma, \rho \in \mathfrak{K}$, the equation

$$\sigma(x_1, \ldots, x_n) = \rho(y_1, \ldots, y_m)$$

is equivalent to a finite system of equations in the language Σ in variables x_1, ..., x_n, y_1, ..., y_m.

Free extension property

Given $B \in \mathcal{V}$, a generating Σ-subalgebra A, $C \in \mathcal{V}$ and a Σ-homomorphism $f : A \to C$, there is a unique homomorphism $\overline{f} : B \to C$ extending f.

Expressibility property

Every equation in the language of $\mathcal{V}$ is equivalent (in $\mathcal{V}$) to a finite set of equations in the language Σ.

Examples

1. $\mathcal{V} = \{\text{Abelian groups}\}$, $\Sigma = \{+, 0\}$. YES.
2. $\mathcal{V} = \{\text{groups}\}$, $\Sigma = \{*, 1\}$. NO.
3. $\mathcal{V} = \{\text{Boolean algebras}\}$, $\Sigma = \{\vee, \wedge, 0, 1\}$. YES.
4. $\mathcal{V} = \{\text{Abelian groups}\}$, $\Sigma = \{+\}$. YES.
5. $\mathcal{V} = \{\text{Abelian groups}\}$, $\Sigma = \emptyset$. NO.
6. $\mathcal{V} = \{\text{commutative monoids}\}$, $\Sigma = \{+\}$. NO.

To sum up

$$\mathcal{V} \text{ has the free extension property over } \Sigma$$
$$\Updownarrow$$
$$\text{equations in } \mathcal{V} \text{ are expressible in } \Sigma.$$

'Complementation' gives a manageable way to check that equations in $\mathcal{V}$ are expressible in Σ.

This equivalence generalizes to varieties of possibly infinitary algebras (possibly without rank, but with free algebras), i.e. algebras for a varietal theory (Linton), or equivalently algebras for a monad over Set.

The implication 'expressibility $\Rightarrow$ free extension' is almost straightforward. The converse implication makes use of free algebras.

The result that I presented for finitary algebras (where the expressibility property consists of rewriting every equation into a <u>finite</u> set of equations) is then a consequence of the compactness theorem.