Unique embeddability property

Marco Abbadini. *University of Salerno, Italy*

Work in progress with Clint Van Alten

University of Witwatersrand, March 30, 2023

Abelian groups and commutative monoids

Monoid: $(xy)z = x(yz)$, $x1 = 1x = x$. Commutativity: $xy = yx$.

Cancellation property:

$$xz = yz \Rightarrow x = y; \qquad zx = zy \Rightarrow x = y.$$

Fact

Every cancellative commutative monoid M can be embedded (as a monoid) in an Abelian group G.

Example: the additive monoid $\mathbb{N}$ can be embedded in the additive group $\mathbb{Z}$.

Construction: $(M \times M)/\sim \ldots$

Abelian groups and commutative monoids

Is this the only possible embedding?

- $\mathbb{N} \hookrightarrow \mathbb{Z}$,
- $\mathbb{N} \hookrightarrow \mathbb{Q}$,
- $\mathbb{N} \hookrightarrow \mathbb{R}$,

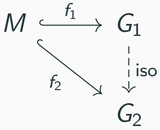
In all these cases, the subgroup generated by the image of the embedding is isomorphic to $\mathbb{Z}$.

Abelian groups and commutative monoids

Fact

For each cancellative commutative monoid M, there is a **unique** (up to isomorphism) embedding $f\colon M \hookrightarrow G$ of M into an Abelian group G whose image generates G (as a group).

Uniqueness up to isomorphism means:



For which other algebraic structures do we have this uniqueness? Is there a general technique to prove uniqueness?

Groups and monoids

For arbitrary (i.e. non-necessarily commutative) monoids/groups, we do **not** have this uniqueness of embeddings.

For example, the monoid $\{a, b, c\}^*$ of words on three letters has at least two non-isomorphic embeddings into groups whose images generate the groups.

- into the free group $\mathrm{Free}(\{a, b, c\})$ on three elements ($a \mapsto a$, $b \mapsto b$, $c \mapsto c$) and
- into the free group $\mathrm{Free}(\{a, b\})$ on two elements ($a \mapsto a$, $b \mapsto b$, $c \mapsto ab^{-1}a$).

Rational vector spaces and Abelian groups

Fact

Every torsion-free Abelian group G can be embedded (as a group) into a rational vector space V.

(Example: $\mathbb{Z} \hookrightarrow \mathbb{Q}$.)

I have seen proofs using localization, tensor product, free abelian groups...

Are all these constructions the same? Yes.

Fact

For each torsion-free Abelian group G, there is (up to isomorphism) a **unique** embedding (of Abelian groups) $f \colon G \hookrightarrow V$ into a rational vector space whose image generates V (as a rational vector space).

Complex and real vector spaces

Fact

Any real vector space can be embedded into a complex vector space.

However, this embedding is **not** unique: For example: $\mathbb{R} \times \mathbb{R}$ can be embedded (as a real vector space) into $\mathbb{C} \times \mathbb{C}$ or into $\mathbb{C}$ in non-isomorphic ways.

What makes the uniqueness?

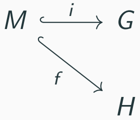
What makes the uniqueness?

What makes the uniqueness?

Recall

For each cancellative commutative monoid M, there is (up to isomorphism) a **unique** embedding $f\colon M \hookrightarrow G$ of M into an Abelian group G whose image generates (as a group) G.

Sketch of proof of uniqueness. Suppose you have two injective monoid homomorphisms with generating images.



For ease of notation, we assume i to be the inclusion of a submonoid M of G (M should then generate the group G).

To be found: isomorphism $\psi\colon G \to H$ that extends f.

What makes the uniqueness?

It is not difficult to prove that every $z \in G$ is a difference $z = x - y$ of elements of M. Then, set $\psi(z) \coloneqq f(x) - f(y) \in H$.

Is this a well-defined function?

Suppose $x - y = x' - y'$ and let us prove $f(x) - f(y) = f(x') - f(y')$.

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

Further, one proves that ψ is a group isomorphism that extends f.

What makes the uniqueness?

Key fact used

For every Abelian group G and all $x, y, x', y' \in G$,

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

Fact

Any equation between two terms in the language of Abelian groups is equivalent to an equation in the language of monoids.

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

What makes the uniqueness?

Fact

Every equation in the language of $\mathbb{Q}$-vector spaces is equivalent to an equation in the language of Abelian groups.

Example

$$\frac{1}{2}x + y = \frac{2}{3}z$$

is equivalent to

$$3x + 6y = 4z.$$

Claim: this is related to the **uniqueness** of the embedding of Abelian groups into $\mathbb{Q}$-vector spaces.

What makes the uniqueness?

The analogous statement for arbitrary groups (not necessarily Abelian) is **false**.

Example: $x = yz^{-1}y$ cannot be expressed via an equation in the language of monoids.

Claim: this is related to the **non**-uniqueness of the embedding of monoids into groups.

What makes the uniqueness?

The equation $x = iy$ (in the language of complex vector spaces) is **not** equivalent to an equation in the language of real vector spaces.

Claim: this is related to the **non**-uniqueness of the embedding of real vector spaces into complex vector spaces.

Main result

Very informal statement of main result:

Unique embeddability of A into $B \iff$ every equation in B can be expressed in A.

Definition

An algebraic language $\mathcal{L}$ consists of a set (whose elements are called function symbols), and, for each function symbol τ, of a natural number (called the arity of τ).

E.g.: $\mathcal{L} = \{\cdot, (-)^{-1}, 1\}$; arity of $\cdot$ is 2, arity of $(-)^{-1}$ is 1, arity of 1 is 0.

Definition

An algebra for an algebraic language $\mathcal{L}$ consists of a set A and, for each function symbol $\tau \in \mathcal{L}$, of a function $[\![\tau]\!]^A \colon A^n \to A$ (called interpretation in A of τ), where n is the arity of τ.

E.g.: any group is an algebra for the language $\{\cdot, (-)^{-1}, 1\}$.
$\cdot \colon A^2 \to A$.
$(-)^{-1} \colon A \to A$.
$1 \colon \{*\} \to A$.

Definition

An SP-class is a class $\mathcal{V}$ of algebras for a common algebraic language $\mathcal{L}$ that is closed under **s**ubalgebras and **p**roducts, i.e.:

1. (**S**ubalgebras) For every $A \in \mathcal{V}$, every subalgebra of A (i.e. a subset of A closed under all interpretations in A of the function symbols), $B \in \mathcal{V}$.
2. (**P**roducts) For every family $(A_i)_{i \in I}$ of algebras in $\mathcal{V}$, the product algebra $\prod_{i \in I} A_i$ (i.e. the cartesian product $\prod_{i \in I} A_i$ equipped with the component-wise interpretation of the function symbols) belongs to $\mathcal{V}$.

Example

The class of groups, wrt the language $\{\cdot, (-)^{-1}, 1\}$, is an SP-class. Indeed, for any group, any subset that is closed under multiplication, inverse and contains the identity element is also a group; moreover, product of groups is a group.

Examples of SP-classes

Groups, Abelian groups, monoids, commutative monoids, cancellative commutative monoids, semigroups, torsion-free Abelian groups, torsion-free groups.

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 $\mathbb{K}$, Lie-algebras.

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

Sets.

Non-examples

Fields (the product of two fields is not a field), integral domains (the product of two integral domains is not an integral domain).

Setting

- An algebraic language $\mathcal{L}_+$ and a sublanguage $\mathcal{L}_- \subseteq \mathcal{L}_+$.
- Two SP-classes $\mathcal{V}_+$ and $\mathcal{V}_-$ for $\mathcal{L}_+$ and $\mathcal{L}_-$, respectively.

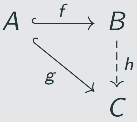
We assume "$\mathcal{V}_+ \subseteq \mathcal{V}_-$" i.e.: taking $A \in \mathcal{V}_+$ and forgetting the interpretation of the operations in $\mathcal{L}_+ \setminus \mathcal{L}_-$, we obtain an algebra in $\mathcal{V}_-$.

For example:

1. $\mathcal{V}_+ = \{\text{Abelian groups}\}$, $\mathcal{V}_- = \{\text{cancellative commutative monoids}\}$.
2. $\mathcal{V}_+ = \{\text{Abelian groups}\}$, $\mathcal{V}_- = \{\text{commutative monoids}\}$.
3. $\mathcal{V}_+ = \{\text{groups}\}$, $\mathcal{V}_- = \{\text{monoids}\}$.

Definition

Unique embeddability property :=
Given $A \in \mathcal{V}_-$, $B, C \in \mathcal{V}_+$, and injective $\mathcal{V}_-$-homomorpisms $f\colon A \hookrightarrow B$ and $g\colon A \hookrightarrow C$ whose images $\mathcal{V}_+$-generate B and C respectively, there is a $\mathcal{V}_+$-isomorphism $h\colon B \to C$ making the following diagram commute.



We have the unique embeddability property for $\mathcal{V}_+ = \{\text{Abelian groups}\}$ and $\mathcal{V}_- = \{\text{commutative monoids}\}$.

We do not have the unique embeddability property for $\mathcal{V}_+ = \{\text{groups}\}$ and $\mathcal{V}_- = \{\text{monoids}\}$.

Definition

Expressibility property :=
every equation

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

in $\mathcal{L}_+$ is equivalent to a system of equations in $\mathcal{L}_-$.

I.e.: for each pair $(\sigma(x_1, \ldots, x_n), \rho(x_1, \ldots, x_n))$ of terms in $\mathcal{L}_+$, there is a finite set of pairs $(\alpha_i(x_1, \ldots, x_n), \beta_i(x_1, \ldots, x_n))_i$ of terms in $\mathcal{L}_-$ s.t., for all $A \in \mathcal{V}_+$ and $x_1, \ldots, x_n \in A$,

$$\sigma(x_1, \ldots, x_n) = \rho(x_1, \ldots, x_n) \;\Leftrightarrow\; \forall i \;\; \alpha_i(x_1, \ldots, x_n) = \beta_i(x_1, \ldots, x_n).$$

For Abelian groups and commutative monoids we have the expressibility property

For groups and monoids we do not have the expressibility property.

Main theorem

Unique embeddability property $\iff$ expressibility property.

How to use it:

1. Prove that equations in the richer language can be expressed in the poorer language (e.g.: $x - y = x' - y'$ iff $x + y' = y + x'$). Deduce the unique embeddability property.
2. If one suspects that a given equation (such as $x = yz^{-1}y$ or $x = iy$) in the richer language cannot be expressed in the poorer language, the equation can guide to two non-isomorphic embeddings that disprove the unique embeddability property. In turn, these two non-isomorphic embeddings can be used to prove that the given equation is in fact not expressible in the poorer language.

Thank you!