# Lifting linear laws: On the preservation of linear equational laws under the pointwise lifting to sets

Andreas Abel

21 November 2018, 22 December 2018

**Abstract**

The pointwise lifting of an operation on elements to sets of elements is a common mathematical procedure. For instance, in the area of formal languages, concatenation of words is lifted pointwise to concatenation of languages, i.e., sets of words. Similar pointwise liftings occur in ring and number theory, e.g. when considering residue classes or ideals.

Certain equational laws routinely carry over from an operation to its pointwise lifting. For instance, word concatenation forms a monoid, and so does language concatenation. However, not all laws can be inherited; for instance, the pointwise inversion of a set of group elements is not an inverse to this set under pointwise multiplication (assuming this is the name of the binary operation of the group).

In this note, we demonstrate that linear equational laws, e.g., monoid laws and commutativity, always carry over to the pointwise lifting. Herein, an equational law is considered linear when both sides mention the same variables, and exactly once.

Our observation has been published before by Gautam in article *The validity of equations of complex algebras* [1].

## 1 Introduction

Given a magma $\mathsf{M} = (M, \oplus)$, i. e., a set $M$ and a binary operation $\oplus : M \times M \to M$, we define the pointwise lifting $\hat{\oplus} : \mathcal{P}(M) \times \mathcal{P}(M) \to \mathcal{P}(M)$ as usual by

$$\hat{a} \mathbin{\hat{\oplus}} \hat{b} = \{a \oplus b \mid a \in \hat{a} \text{ and } b \in \hat{b}\},$$

obtaining the lifted magma $\hat{\mathsf{M}} = (\hat{M}, \hat{\oplus})$, where $\hat{M} = \mathcal{P}(M)$. Now the following statements hold.

**Observation 1.**

1. *If* $\mathsf{M}$ *is a semigroup, so is* $\hat{\mathsf{M}}$.

2. *If* $\mathsf{M}$ *is commutative, so is* $\hat{\mathsf{M}}$.
3. *If* $\mathsf{M}$ *has a unit, so does* $\hat{\mathsf{M}}$.

In other words, associativity, commutativity, and unit laws are preserved under the pointwise lifting. The proofs are one-liners, e.g., consider commutativity:

*Proof.* Assume commutativity of $\mathsf{M}$, i.e., $a \oplus b = b \oplus a$ for all $a, b \in M$. Then $\hat{a} \hat{\oplus} \hat{b} = \hat{b} \hat{\oplus} \hat{a}$ follows for arbitrary $\hat{a}, \hat{b} \in \hat{M}$ by the following chain of equivalences:

$$\begin{array}{ll} & c \in (\hat{a} \hat{\oplus} \hat{b}) \\ \text{iff} & c = a \oplus b \text{ for some } a \in \hat{a} \text{ and } b \in \hat{b} \\ \text{iff} & c = b \oplus a \text{ for some } a \in \hat{a} \text{ and } b \in \hat{b} \\ \text{iff} & c \in (\hat{b} \hat{\oplus} \hat{a}) \end{array}$$

Besides commutativity of $\hat{M}$, we used only the definition of $\hat{\oplus}$. □

Yet many laws are *not* preserved, e.g., existence of inverses:

**Fallacy 1.** *If* $\mathsf{M}$ *is a group, so is* $\hat{\mathsf{M}}$.

**Counterexample 1.** $(\mathbb{Z}, +)$ is a group, but $\hat{\mathbb{Z}}$ is not, e.g., the set $\{1, 2\}$ does not have an inverse: There is no set $\hat{a}$ such that $\hat{a} \mathbin{\hat{+}} \{1, 2\} = \{0\}$.

What distiguishes laws that are preserved from those that may not be preserved? If we look at Table 1 we see that the preserved laws in the upper left area have a specific syntactic shape: They are *linear*, i.e., both sides of the equation use the same variables, and these *exactly once*.

| lifts pointwise | | may not lift | |
|---|---|---|---|
| $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ | associativity | $x^{-1} \cdot x = 1$ | left inverse |
| $x \cdot 1 = x$ | right unit | $x \cdot x = x$ | idempotency |
| $x \cdot y = y \cdot x$ | commutativity | | |
| | | $0 \cdot x = 0$ | left absorption |
| | | $x \cdot (y + z) = x \cdot y + x \cdot z$ | right distributivity |

Table 1: Lifting of equational laws.

In contrast, the laws in the upper right area are usually not preserved, and they are essentially non-linear, using $x$ twice.

The laws in the lower right area have a linear left hand side, and this suffices for partial preservation. For instance, from right distributivity we have the inclusion

$$\hat{a} \mathbin{\hat{\cdot}} (\hat{b} \mathbin{\hat{+}} \hat{c}) \subseteq (\hat{a} \mathbin{\hat{\cdot}} \hat{b}) \mathbin{\hat{+}} (\hat{a} \mathbin{\hat{\cdot}} \hat{c}).$$

It is instructive to see why a generic proof of the reverse inclusion fails.

**Fallacy 2.** $(\hat{a} \mathbin{\hat{\cdot}} \hat{b}) \mathbin{\hat{+}} (\hat{a} \mathbin{\hat{\cdot}} \hat{c}) \subseteq \hat{a} \mathbin{\hat{\cdot}} (\hat{b} \mathbin{\hat{+}} \hat{c})$.

Attempting a proof, starting with $d \in (\hat{a} \mathbin{\hat{\cdot}} \hat{b}) \mathbin{\hat{+}} (\hat{a} \mathbin{\hat{\cdot}} \hat{c})$, we only obtain that $d = a \cdot b + a' \cdot c$ for some $a, a' \in \hat{a}$ and $b \in \hat{b}$ and $c \in \hat{c}$. The lack of linearity stiffles this proof attempt, as we end up with potentially different $a, a' \in \hat{a}$.

**Counterexample 2.** $(\mathbb{N} \mathbin{\hat{\cdot}} \{1\}) \mathbin{\hat{+}} (\mathbb{N} \mathbin{\hat{\cdot}} \{1\}) \not\subseteq \mathbb{N} \mathbin{\hat{\cdot}} (\{1\} \mathbin{\hat{+}} \{1\})$, as the left hand side is $\mathbb{N}$ but the right hand side is $2\mathbb{N}$, the set of even numbers.

In case of the absorption law, we get the inclusion $\hat{0} \mathbin{\hat{\cdot}} \hat{a} \subseteq \hat{0}$ from linearity of the left hand side, yet the converse inclusion $\hat{0} \subseteq \hat{0} \mathbin{\hat{\cdot}} \hat{a}$ fails for empty $\hat{a}$.

In the remainder of this note, we shall demonstrate that:

**Theorem 1.** *Linear equational laws are preserved by the pointwise lifting to sets.*

# 2 Linear Equational Laws

We formalize the concept of linear equations using the framework of multi-sorted algebras.

Assume a set $S$ of sort symbols and a signature $\Sigma$ of function symbols. $\Sigma$ maps function symbols $f$ to their type consisting of a list $\vec{s} = s_{1..n}$ of domain sorts and a codomain sort $s$. We express this as $(f : s_1 \times \cdots \times s_n \to s) \in \Sigma$ or $(f : \vec{s} \to s) \in \Sigma$. We may refer to the pair $(S, \Sigma)$ or just $\Sigma$ (with $S$ given implicitly) as *algebra*.

We assume a countably infinite set $X$ of variables $x$. A context $\Gamma$ is a finite map from variables $x$ to sorts $s$. Contexts $\Gamma$ and $\Gamma'$ are said to be disjoint if their domains do not intersect, $\mathsf{dom}(\Gamma) \cup \mathsf{dom}(\Gamma') = \emptyset$. We write $\Gamma \uplus \Gamma'$ for the disjoint union of contexts. We write $x{:}s$ for the singleton context.

We inductively define the indexed set $\mathsf{Tm}(\Gamma; s)$ containing the linear (first-order) terms $t$ of sort $s$ in context $\Gamma$ by the following rules.

$$\frac{}{x \in \mathsf{Tm}(x{:}s; s)} \qquad \frac{(t_i \in \mathsf{Tm}(\Gamma_i; s_i))_{i=1..n}}{f(t_{1..n}) \in \mathsf{Tm}(\biguplus_{i=1..n} \Gamma_i; s)}\ f : s_1 \times \cdots \times s_n \to s \in \Sigma$$

As customary, we write $\Gamma \vdash t : s$ for $t \in \mathsf{Tm}(\Gamma; s)$.

An *interpretation* $I$ of algebra $(S, \Sigma)$ assigns to each sort $s \in S$ a set $I(s)$ and to each function symbol $f : s_{1..n} \to s \in \Sigma$ a function $I(f) : I(s_1) \times \cdots \times I(s_n) \to I(s)$. The interpretation $I(\Gamma)$ of a context $\Gamma$ contains all finite maps $\rho$ with domain $\mathsf{dom}(\Gamma)$ that assign variables $x$ to elements of $I(\Gamma(x))$. The interpretation $I(t)\rho$ of a linear term $\Gamma \vdash t : s$ is defined by induction on $t$, given $\rho \in I(\Gamma)$:

$$\begin{array}{rcl} I(x)(x \mapsto a) & = & a \\ I(f(t_1, \ldots, t_n))\rho & = & I(f)(I(t_1)\rho_1, \ldots, I(t_n)\rho_n) \\ \text{where } \rho & = & \biguplus_{i=1..n} \rho_i \end{array}$$

The partitioning of $\rho$ into the $\rho_i$ shall follow the partitioning of $\Gamma$ into the $\Gamma_i$ as given by the introduction rule for $f(\vec{t})$.

*Remark* 1. The interpretation of terms is actually oblivious to linearity. One could first define well-sorted terms and their interpretation, and then introduce the linearity restriction. However, our *procedere*, introducing linear terms directly, is most suitable for our purposes.

A *linear equation* is a pair of linear terms $t, t' \in \mathsf{Tm}(\Gamma; s)$ of the same sort $s$ in the same context $\Gamma$. We write such an equation as $\Gamma \vdash t = t' : s$. The equation is *valid* in interpretation $I$ if $I(t)\rho = I(t')\rho$ for all $\rho \in I(\Gamma)$.

# 3 An Invertible Fundamental Theorem

For a $\Sigma$-algebra, fix an interpretation written $(\!|\_|\!)$, i.e., we use the notations $(\!|s|\!)$, $(\!|f|\!)$, $(\!|\Gamma|\!)$ and $(\!|t|\!)$. This interpretation serves to interpret terms as "elements". A second interpretation of terms as "sets" or predicates is given by:

$$\begin{array}{lll} [\![s]\!] & = \mathcal{P}(\!|s|\!) & \\ [\![f]\!] & : [\![s_1]\!] \times \cdots \times [\![s_n]\!] \to [\![s]\!] & \text{for } f : \vec{s} \to s \in \Sigma \\ [\![f]\!](\hat{a}_1, \ldots, \hat{a}_n) & = \{(\!|f|\!)(a_1, \ldots, a_n) \mid a_1 \in \hat{a}_1, \ldots, a_n \in \hat{a}_n\} & \end{array}$$

The induced interpretation of terms $\Gamma \vdash t : s$ is written $[\![t]\!] : [\![\Gamma]\!] \to [\![s]\!]$. For $\hat{\rho} \in [\![\Gamma]\!]$ and $\rho \in (\!|\Gamma|\!)$ we write $\rho \in \hat{\rho}$ if $\rho(x) \in \hat{\rho}(x)$ for all $x \in \mathsf{dom}(\Gamma)$.

**Theorem 2** (Fundamental theorem and inversion)**.** *Let* $\Gamma \vdash t : s$ *and* $\hat{\rho} \in [\![\Gamma]\!]$. *Then*

$$[\![t]\!]\hat{\rho} = \{(\!|t|\!)\rho \mid \rho \in \hat{\rho}\}$$

Direction $\supseteq$ is a soundness property resembling the fundamental theorem of logical relations and holds regardless of linearity. Direction $\subseteq$ is "new" and holds thanks to linearity.

*Proof.* For $\supseteq$, we assume $\rho \in \hat{\rho}$ and show $(\!|t|\!)\rho \in [\![t]\!]\hat{\rho}$ by induction on $\Gamma \vdash t : s$.

*Case*

$$\frac{}{x{:}s \vdash x : s}$$

Assumption $\rho \in \hat{\rho}$ proves $(\!|x|\!)\rho = \rho(x) \in \hat{\rho}(x) = [\![x]\!]\hat{\rho}$ immediately.

*Case*

$$\frac{(\Gamma_i \vdash t_i : s_i)_{i=1..n}}{\Gamma \vdash f(t_{1..n}) : s}\ \Gamma = \biguplus_{i=1..n} \Gamma_i$$

We have the partitionings $\rho = \biguplus_i \rho_i$ and $\hat{\rho} = \biguplus_i \hat{\rho}_i$, according to the partitioning of $\Gamma$, such that $\rho_i \in \hat{\rho}_i$ for $i = 1..n$. By induction hypothesis, $(\!|t_i|\!)_{\rho_i} \in [\![t_i]\!]_{\hat{\rho}_i}$ for $i = 1..n$. Thus, by definition of $[\![f]\!]$, we conclude $(\!|f|\!)((\!|t_i|\!)_{\rho_i})_{i=1..n} \in [\![f]\!]([\![t_i]\!]_{\hat{\rho}_i})_{i=1..n}$ which is $(\!|f(\vec{t})|\!)\rho \in [\![f(\vec{t})]\!]_{\hat{\rho}}$ by definition of term interpretation.

Direction $\subseteq$, stating that $b \in [\![t]\!]\hat{\rho}$ implies $b = (\!|t|\!)\rho$ for some $\rho \in \hat{\rho}$, is proven by induction on $\Gamma \vdash t : s$ as well.

*Case*

$$\frac{}{x{:}s \vdash x : s}$$

$\hat{\rho} = (x \mapsto \hat{b})$ for some $\hat{b} \subseteq (\!|s|\!)$, thus, assumption $b \in [\![x]\!]\hat{\rho}$ simplifies to $b \in \hat{b}$. Hence, $\rho := (x \mapsto b)$ fulfills $\rho \in \hat{\rho}$ and $b = (\!|x|\!)\rho$.

*Case*

$$\frac{(\Gamma_i \vdash t_i : s_i)_{i=1..n}}{\Gamma \vdash f(t_{1..n}) : s}\ \Gamma = \biguplus_{i=1..n} \Gamma_i$$

Mimicking the partitioning of $\Gamma$, we partition $\hat{\rho} = \biguplus_{i=1..n} \hat{\rho}_i$. Assumption $b \in [\![f(\vec{t})]\!]\hat{\rho}$ entails $b = (\!|f|\!)(a_{1..n})$ for some $(a_i \in [\![t_i]\!]\hat{\rho}_i)_{i=1..n}$. By induction hypothesis there are $\rho_i \in \hat{\rho}_i$ such that $a_i = (\!|t_i|\!)\rho_i$. The $\rho_i$ are disjoint (thanks to linearity!), thus $\rho = \biguplus_i \rho_i$ is well-defined, and futher, $\rho \in \hat{\rho}$. This implies $b = (\!|f(\vec{t})|\!)\rho$. □

The proof of direction $\subseteq$ would fail if $t$ were not linear.

# 4 Lifting of linear laws

We now have the tools to prove Theorem 1 which states that *linear equational laws are preserved by the pointwise lifting to sets*. In the terminology developed in the previous sections, we have to show that linear equations that are valid under interpretation $(\!|\_|\!)$ are also valid under $[\![\_]\!]$.

*Proof of Theorem 1.* Assume $(\!|\_|\!)$ models a linear equation $\Gamma \vdash t = t' : s$. We show that it is also valid under interpretation $[\![\_]\!]$. To this end, assume $b \in [\![t]\!]\hat{\rho}$. By Theorem 2 direction "$\subseteq$", there is $\rho \in \hat{\rho}$ such that $b = (\!|t|\!)\rho$. Since the equation is valid for interpretation $(\!|\_|\!)$, we have $b = (\!|t'|\!)\rho$. Thus, by Theorem 2 direction "$\supseteq$", $b \in [\![t']\!]\hat{\rho}$. Our line of reasoning is symmetric, thus, $[\![t']\!]\hat{\rho} \subseteq [\![t]\!]\hat{\rho}$ as well, and together, $[\![t]\!]\hat{\rho} = [\![t']\!]\hat{\rho}$. □

Observe that direction $[\![t]\!]\hat{\rho} \subseteq [\![t']\!]\hat{\rho}$ only requires the linearity of $t$, not of $t'$. Thus, laws like $\hat{0} \hat{\cdot} \hat{a} \subseteq \hat{0}$ as mentioned in the introduction can also be established following our blueprint.

# 5 Discussion

Could the theorems in this note be obtained by parametricity-like theorem for linearity? Even further, could they be obtained by internal parametricity in a linear dependent type theory?

## 6 Related Work

The observation that linear laws lift to sets was already made by Gautam [1]. He uses the terminology *complex algebra* for the algebra lifted to subsets (complexes); his paper is nicely written and easily accessible for the reader with general mathematical literacy.

Grätzer and Whitney [2] generalize the observation to arbitrary relations (beyond equality), even infinitary ones.

Shafaat [3] shows that if an algebra lifts to a power algebra (another word for complex algebra), then it can be defined by linear equations.

Related concepts are further *varieties* and *power structures*.

**Acknowledgments** Thanks to an attentive audience in the presentation of this note in the *Programming Logic* seminar at Chalmers University on 21th November 2018. Thanks to David Sands and Lutz Schröder for pointing to related work. Special thanks to Alexander Kurz who referred me to the work of Gautham [1], Shafaat [3] and Grätzer and Whitney [2].

## References

[1] N.D. Gautam. The validity of equations of complex algebras. *Archiv für mathematische Logik und Grundlagenforschung*, 3:117–124, 1957.

[2] G. Grätzer and S. Whitney. Infinitary varieties of structures closed under the formation of complex structures. *Colloquium Mathematicae*, 48(1):1–5, 1984.

[3] A. Shafaat. On varieties closed under the construction of power algebras. *Bulletin of the Australian Mathematical Society*, 11(2):213–218, 1974.