Untyping Typed Algebraic Structures

Damien Pous

Untyping Typed Algebraic Structures

Damien Pous*
CNRS

Laboratoire d'Informatique de Grenoble, UMR 5217, France

Abstract

Algebraic structures sometimes need to be typed. For example, matrices over a ring form a ring, but the product is a only a partial operation: dimensions have to agree. Therefore, an easy way to look at matrices algebraically is to consider "typed rings".

We prove some "untyping" theorems: in some algebras (semirings, Kleene algebras, residuated monoids), types can be reconstructed from valid untyped equalities. As a consequence, the corresponding untyped decision procedures can be extended to the typed setting.

Introduction

For any natural number n, $n \times n$-matrices over a semiring form a semiring. As a consequence, any theorem of semirings is true for square matrices. In this paper, we study the problem of generalising this strategy to rectangular matrices: from a valid semiring equality, like $x*(y+y')*z = x*y*z+x*y'*z$, we want to be able deduce that $M*(N+N')*P = M*N*P+M*N'*P$ holds whenever M is a $n \times m$-matrix, N and N' are $m \times p$-matrices, and P is a $p \times n'$-matrix. Similarly, we want to deduce from the former equality that $R(S \cup S')T = RST \cup RS'T$ holds whenever R, S, S', T are heterogeneous binary relations whose domains and co-domains make the equation meaningful. More generally, we want to reduce the problem of proving equalities in heterogeneous (typed) structures to that of proving equalities in the underlying homogeneous (standard) structures.

A motivation for this work comes from our Coq library ATBR [1], whose aim is to provide algebraic tools for working with binary relations in the Coq proof assistant [3]. Indeed, moving to an algebraic setting eases the formalisation of some diagrammatic proofs (Newman's lemma, abstract termination lemmas, up-to techniques for bisimulation), and it makes it possible to develop powerful tactics for automatically solving certain classes of goals (among which, theorems of decidable equational theories – semirings,

*Work partially funded by the French ANR projet blanc "Curry-Howard pour la Concurrence" CHOCO ANR-07-BLAN-0324

residuated lattices, Kleene algebras, ...). The results presented in this paper were actually implemented in this library, so as to extend our decision procedures to heterogeneous structures, for free.

Outline. We introduce our setting and make our notion of typed structure precise in Section 1. We study several algebraic structures in Section 2, and prove an "untyping" theorem for each of these. Section 3 is devoted to applications and future work; in particular, we explain how these theorems were used to extend decision procedures, and how the last one could be used to improve proof search in residuated lattices.

1 Typed Structures

All of our arguments being proof-theoretic, we shall work with syntactic models, by implicitly relying on initiality arguments to reach other models.

Let $\mathcal{X}$ be an arbitrary set of *variables*, ranged over using letters x, y. Given a signature Σ, we let u, v, w range over the set $T(\Sigma + \mathcal{X})$ of *terms with variables*. Given a set $\mathcal{T}$ of *types*, ranged over using letters n, m, p, and a type environment $\Gamma : \mathcal{X} \to \mathcal{T}^2$, we will define *typed terms* using type judgements of the form $\Gamma \vdash u : n \to m$: "in environment Γ, term u has type $n \to m$". Type judgements will always include the following rule:

$$\frac{\Gamma(x) = (n, m)}{\Gamma \vdash x : n \to m}\ \textsc{Tv}$$

Similarly, we will define *typed equalities* using judgements of the form $\Gamma \vdash u = v : n \to m$: "in environment Γ, terms u and v are equal at type $n \to m$". Equality judgements will always include the following rules:

$$\frac{\Gamma(x) = (n, m)}{\Gamma \vdash x = x : n \to m}\ \textsc{v} \qquad \frac{\Gamma \vdash u = v : n \to m \quad \Gamma \vdash v = w : n \to m}{\Gamma \vdash u = w : n \to m}\ \textsc{t} \qquad \frac{\Gamma \vdash u = v : n \to m}{\Gamma \vdash v = u : n \to m}\ \textsc{s}$$

By taking the singleton set $\{\emptyset\}$ for $\mathcal{T}$, we will recover standard, untyped structures: types become uninformative, and we will let $\vdash u = v$ denote the corresponding equality judgements, i.e., $\widehat{\emptyset} \vdash u = v : \emptyset \to \emptyset$, where $\widehat{\emptyset} : x \mapsto (\emptyset, \emptyset)$.

The question we study in this paper is the following: given a signature, a type judgement, and an equality judgement, does the following implication hold?

> *"For all u, v, n, m such that $\vdash u = v$, $\Gamma \vdash u, v : n \to m$, we have $\Gamma \vdash u = v : n \to m$".*

In other words, in order to prove a typed equality, is it safe to remove all type annotations, so as to work in the untyped underlying algebraic structure.

2 Untyping Theorems

In this section, we study the previous question for four structures: monoids, semirings, Kleene algebras, and residuated monoids.

2.1 Monoids

Definition 1 (Typed monoid)**.** *Typed monoids* are defined by the signature $\{*_2, 1_0\}$, together with the following type and equality judgements (in addition to the rules from Section 1).

$$\frac{}{\Gamma \vdash 1 : n \to n}\ \textsc{To} \qquad \frac{\Gamma \vdash u : n \to m \qquad \Gamma \vdash v : m \to p}{\Gamma \vdash u * v : n \to p}\ \textsc{Td}$$

$$\frac{}{\Gamma \vdash 1 = 1 : n \to n}\ \textsc{o} \qquad \frac{\Gamma \vdash u = u' : n \to m \qquad \Gamma \vdash v = v' : m \to p}{\Gamma \vdash u * v = u' * v' : n \to p}\ \textsc{d}$$

$$\frac{\Gamma \vdash u : n \to m}{\Gamma \vdash u * 1 = u : n \to m}\ \textsc{do} \qquad \frac{\Gamma \vdash u : n \to m}{\Gamma \vdash 1 * u = u : n \to m}\ \textsc{od}$$

$$\frac{\Gamma \vdash u : n \to m \qquad \Gamma \vdash v : m \to p \qquad \Gamma \vdash w : p \to q}{\Gamma \vdash (u * v) * w = u * (v * w) : n \to q}\ \textsc{da}$$

(In other words, typed monoids are just categories.) The following intuitive properties are satisfied: equality is reflexive at each type and relate only correctly typed terms.

Lemma 2.

(i) For all u, n, m such that $\Gamma \vdash u : n \to m$, we have $\Gamma \vdash u = u : n \to m$.

(ii) For all u, v, n, m such that $\Gamma \vdash u = v : n \to m$, we have $\Gamma \vdash u : n \to m$ and $\Gamma \vdash v : n \to m$.

Moreover, in this setting, typability enjoys some form of injectivity (types are not uniquely determined due to the unit elements, which admit several types).

Lemma 3. *Let u, n, m, m' such that $\Gamma \vdash u : n \to m$ and $\Gamma \vdash u : n \to m'$; then $m = m'$.*

We need another lemma to obtain the untyping theorem: all terms related by the untyped equality admit the same types.

Lemma 4. *Let u, v such that $\vdash u = v$; for all n, m, we have $\Gamma \vdash u : n \to m$ iff $\Gamma \vdash v : n \to m$.*

Proof. By induction on the derivation $\vdash u = v$, the interesting case is when the rule for the compatibility of $*$ (D) is used last: if $\Gamma \vdash u * v : n \to m$, then there must be some p such that $\Gamma \vdash u : n \to p$ and $\Gamma \vdash v : p \to m$. By induction hypothesis, we deduce $\Gamma \vdash u' : n \to p$ and $\Gamma \vdash v' : p \to m$, so that we can conclude with rule (TD). ■

Theorem 5. *Let u, v such that $\vdash u = v$; for all n, m such that $\Gamma \vdash u, v : n \to m$, we have $\Gamma \vdash u = v : n \to m$.*

Proof. We reason by induction over the derivation $\vdash u = v$; the interesting cases are the following ones:

- the last rule used is the transitivity rule (T): we have $\vdash u = v, \vdash v = w$, $\Gamma \vdash u : n \to m$, and $\Gamma \vdash w : n \to m$, and we need to show that $\Gamma \vdash u = w : n \to m$. By Lemma 4, we have $\Gamma \vdash v : n \to m$, so that, by the induction hypotheses, we get $\Gamma \vdash u = v : n \to m$ and $\Gamma \vdash v = w : n \to m$, which allow us to apply rule (T) in the typed setting.
- the last rule used is the compatibility of $*$ (D): we have $\vdash u = u'$, $\vdash v = v'$, $\Gamma \vdash u * v : n \to m$, and $\Gamma \vdash u' * v' : n \to m$, and we need to show that $\Gamma \vdash u * v = u' * v' : n \to m$. By case analysis on the typing judgements, we deduce that $\Gamma \vdash u : n \to p$, $\Gamma \vdash v : p \to m$, $\Gamma \vdash u' : n \to q$, $\Gamma \vdash v' : q \to m$, for some p, q. Thanks to Lemma 3, we have $p = q$, so that we can conclude using the induction hypotheses ($\Gamma \vdash u = u' : n \to p$ and $\Gamma \vdash v = v' : p \to m$), and rule (D). ■

Note that the converse of Theorem 5 ($\Gamma \vdash u = v : n \to m$ entails $\vdash u = v$) is straightforward, so that we actually have an equivalence.

2.2 Non commutative semirings

Definition 6 (Typed semirings)**.** *(Non commutative) typed semirings* are defined by the signature $\{*_2, +_2, 1_0, 0_0\}$, together with the following type and equality judgements (in addition to the rules from Definition 1 and Section 1).

$$\frac{}{\Gamma \vdash 0 : n \to m}\ \text{TZ} \qquad \frac{\Gamma \vdash u : n \to m \qquad \Gamma \vdash v : n \to m}{\Gamma \vdash u + v : n \to m}\ \text{TP}$$

$$\frac{}{\Gamma \vdash 0 = 0 : n \to m}\ \text{Z} \qquad \frac{\Gamma \vdash u = u' : n \to m \qquad \Gamma \vdash v = v' : n \to m}{\Gamma \vdash u + v = u' + v' : n \to m}\ \text{P}$$

$$\frac{\Gamma \vdash u : n \to m}{\Gamma \vdash u + 0 = u : n \to m}\ \text{PZ} \qquad \frac{\Gamma \vdash u, v : n \to m}{\Gamma \vdash u + v = v + u : n \to m}\ \text{PC}$$

$$\frac{\Gamma \vdash u, v, w : n \to m}{\Gamma \vdash (u + v) + w = u + (v + w) : n \to m}\ \text{PA}$$

$$\frac{\Gamma \vdash u : n \to m \qquad \Gamma \vdash v, w : m \to p}{\Gamma \vdash u * (v + w) = u * v + u * w : n \to p}\ \text{DP} \qquad \frac{\Gamma \vdash u : n \to m}{\Gamma \vdash u * 0 = 0 : n \to p}\ \text{DZ}$$

$$\frac{\Gamma \vdash u : n \to m \qquad \Gamma \vdash v, w : p \to n}{\Gamma \vdash (v + w) * u = v * u + w * u : p \to m}\ \text{PD} \qquad \frac{\Gamma \vdash u : n \to m}{\Gamma \vdash 0 * u = 0 : p \to m}\ \text{ZD}$$

(In other words, typed semiring are categories whose homsets are equipped with a commutative monoid structure, and where composition distributes over theses monoid structures.)

Lemma 2 is also valid in this setting; however, due to the presence of an annihilator element (0), Lemmas 3 and 4 no longer hold: we have $\Gamma \vdash 0 : 0 \to 1$ and $\Gamma \vdash 0 : 0 \to 2$, while $1 \neq 2$, and we have $\vdash x * 0 * x = 0$, where 0 can have any type while $x * 0 * x$ only admits $\Gamma(x)$ as a valid type.

We therefore have to adopt another strategy: we reduce the problem to the annihilator-free structure, by showing that equality proofs can be factorised so as to use rules (PZ), (DZ), and (ZD) as oriented rewriting rules.

Definition 7. Let u be a term; we denote by u^+ the normal form of u, obtained using the following convergent rewriting system:

$$u + 0 \to u \qquad 0 + u \to u \qquad 0 * u \to 0 \qquad u * 0 \to 0$$

We call *strict* the elements whose normal form is not zero: u is strict if $u^+ \neq 0$. We let $\_ \vdash^+ \_ = \_ : \_ \to \_$ denote the equality judgement obtained by removing rules (DZ) and (ZD), and replacing rules (DP) and (PD) with the following variants, where the factor has to be *strict*.

$$\frac{\Gamma \vdash u : n \to m \qquad u^+ \neq 0 \qquad \Gamma \vdash v, w : m \to p}{\Gamma \vdash^+ u * (v + w) = u * v + u * w : n \to p}\ \text{DP}^+$$

$$\frac{\Gamma \vdash u : n \to m \qquad u^+ \neq 0 \qquad \Gamma \vdash v, w : p \to n}{\Gamma \vdash^+ (v + w) * u = v * u + w * u : p \to m}\ \text{PD}^+$$

Type derivations about strict terms enjoy the kind of injectivity we had for monoids:

Lemma 8. *For all strict u such that $\Gamma \vdash u : n \to m$ and $\Gamma \vdash u : n' \to m'$, we have $n = n'$ iff $m = m'$.*

Then, using the same methodology as previously, one easily obtain the untyping theorem for our modified equality judgement:

Proposition 9. *Let u, v such that $\vdash^+ u = v$; for all n, m such that $\Gamma \vdash u, v : n \to m$, we have $\Gamma \vdash^+ u = v : n \to m$.*

Note that the patched rules for distributivity, (DP$^+$) and (PD$^+$) are required in order to obtain the counterpart of Lemma 4: if u was not required to be strict, then we would have $\vdash^+ 0 * (x + y) = 0 * x + 0 * y$, and the right-hand side can be typed in environment $\Gamma = \{x \mapsto (n, p),\ y \mapsto (m, q)\}$ while the left-hand side cannot.

We now have to show that than any equality proof can be normalised, so as to obtain a strict equality proof relating the normal forms:

Proposition 10. *For all u, v such that $\vdash u = v$, we have $\vdash^+ u^+ = v^+$.*

Proof. We first show by induction that whenever $\vdash u = v$, u is strict iff v is strict (†). Then we proceed by induction on the derivation $\vdash u = v$, we detail only some cases:

- (D) we have $\vdash^+ u^+ = u'^+$ and $\vdash^+ v^+ = v'^+$ by induction; we need to show that $\vdash^+ (u * v)^+ = (u' * v')^+$. If one of u, u', v, v' is not strict, then $(u * v)^+ = (u' * v')^+ = 0$, thanks to (†), so that we are done; otherwise, $(u * v)^+ = u^+ * v^+$, and $(u' * v')^+ = u'^+ * v'^+$, so that we can apply rule (D).
- (DZ) trivial, since $(u * 0)^+ = 0$.
- (DP) we need to show $\vdash^+ (u * (v + w))^+ = (u * v + u * w)^+$; if one of u, v, w is not strict, both sides reduce to the same term, so that we can apply Lemma 2(i) (which holds in this setting); otherwise we have $(u * (v + w))^+ = u^+ * (v^+ + w^+)$ and $(u * v + u * w)^+ = u^+ * v^+ + u^+ * w^+$, so that we can apply rule (DP$^+$) (u^+ is obviously strict). ■

Since the normalisation procedure preserves types and equalities, we finally obtain the desired untyping theorem.

Lemma 11. *For all u, n, m such that $\Gamma \vdash u : n \to m$, we have $\Gamma \vdash u^+ : n \to m$ and $\Gamma \vdash u = u^+ : n \to m$.*

Theorem 12. *Let u, v such that $\vdash u = v$; for all n, m such that $\Gamma \vdash u, v : n \to m$, we have $\Gamma \vdash u = v : n \to m$.*

Proof. By Lemma 11, using the transitivity and symmetry rules, it suffices to show $\Gamma \vdash u^+ = v^+ : n \to m$. This is clearly the case whenever $\Gamma \vdash^+ u^+ = v^+ : n \to m$, which follows from Props. 10 and 9. ■

2.3 Kleene Algebras

Kleene algebras are idempotent semirings equipped with a Kleene star operation [6]; they admit several important models, among which *regular languages* which is initial, and binary relations. Like previously, this structure can be typed in a rather natural way:

Definition 13 (Typed Kleene algebras)**.** *Typed Kleene algebras* are defined by the signature $\{*_2, +_2, \star_1, 1_0, 0_0\}$, together with the following type and equality judgements (in addition to the rules from Definitions 1 and 6, and Section 1), where $\Gamma \vdash u \leq v : n \to m$ is an abbreviation for $\Gamma \vdash u + v = v : n \to m$.

$$\frac{\Gamma \vdash u : n \to n}{\Gamma \vdash u^\star : n \to n}\ \textsc{Ts}$$

$$\frac{\Gamma \vdash u : n \to m}{\Gamma \vdash u + u = u : n \to m}\ \textsc{pi} \qquad \frac{\Gamma \vdash u : n \to n}{\Gamma \vdash 1 + u * u^\star = u^\star : n \to n}\ \textsc{sp}$$

$$\frac{\Gamma \vdash u * v \leq v : n \to m}{\Gamma \vdash u^\star * v \leq v : n \to m}\ \textsc{sl} \qquad \frac{\Gamma \vdash v * u \leq v : n \to m}{\Gamma \vdash v * u^\star \leq v : n \to m}\ \textsc{sr}$$

Lemma 14. *The following rules are admissible.*

$$\frac{}{\Gamma \vdash 0^\star = 1 : n \to n}\ \textsc{sz} \qquad \frac{\Gamma \vdash u = v : n \to n}{\Gamma \vdash u^\star = v^\star : n \to n}\ \textsc{s}$$

One can extend the proofs from the previous section, by adding the rule $0^\star \to 1$ to the rewriting system used for normalising terms, and by requiring v to be strict in the strict versions of rules (SL) and (SR). We do not detail the proofs here: they are available as Coq proof scripts [10].

2.4 Residuated Monoids

A residuated monoid is a tuple $(X, \leq, *, 1, /, \backslash)$, such that $(X, \leq)$ is a partial order, $(X, *, 1)$ is a monoid whose product is monotonic ($u \leq u'$ and $v \leq v'$ entail $u * v \leq u' * v'$), and $/, \backslash$ are two binary operations, respectively called *left* and *right division*, characterised by the following equivalences:

$$u * w \leq v \Leftrightarrow w \leq u \backslash v$$
$$w * u \leq v \Leftrightarrow w \leq v / u$$

Such a structure can be typed in a natural way, by using the following rules:

$$\frac{\Gamma \vdash u : n \to m \qquad \Gamma \vdash v : n \to p}{\Gamma \vdash v \backslash u : p \to m}\ \textsc{tl} \qquad \frac{\Gamma \vdash u : n \to m \qquad \Gamma \vdash v : p \to m}{\Gamma \vdash u / v : n \to p}\ \textsc{tr}$$

$$\frac{}{x \vdash x}\ \textsc{v} \qquad \frac{}{\epsilon \vdash 1}\ \textsc{Io} \qquad \frac{l, l' \vdash u}{l, 1, l' \vdash u}\ \textsc{Eo} \qquad \frac{l \vdash u \qquad l' \vdash u'}{l, l' \vdash u * u'}\ \textsc{Id} \qquad \frac{l, v, w, l' \vdash u}{l, v * w, l' \vdash u}\ \textsc{Ed}$$

$$\frac{l, v \vdash u}{l \vdash u/v}\ \textsc{Ir} \qquad \frac{k \vdash v \qquad l, w, l' \vdash u}{l, w/v, k, l' \vdash u}\ \textsc{Er} \qquad \frac{v, l \vdash u}{l \vdash v \backslash u}\ \textsc{Il} \qquad \frac{k \vdash v \qquad l, w, l' \vdash u}{l, k, v \backslash w, l' \vdash u}\ \textsc{El}$$

Figure 1: Gentzen Proof System for Residuated Monoids.

Although we can easily define inference rules to capture provability in typed residuated monoids – as we did in the previous sections, we need to resort to a characterisation due to Ono and Komori [9] to obtain the corresponding untyping theorem. Let letters l, k range over lists of terms, let l, k denote the concatenation of lists l and k, and let ϵ be the empty list; we will use the Gentzen proof system presented on Fig. 1, relating lists of terms to terms. Its presentation is quite standard: there is an axiom rule (v), and, for each operator, and introduction and an elimination rule. The system is cut-free, it admits cut-elimination, and it is correct and complete:

Proposition 15.

(i) For all u, we have $u \vdash u$.

(ii) For all l, l', l'', u, v such that $l \vdash u$ and $l', u, l'' \vdash v$, we have $l', l, l'' \vdash v$.

(iii) For all u, v, we have $u \vdash v$ iff $u \leq v$ holds in all residuated monoids.

Proof. The first point is easy; see [9] for cut admissibility and completeness. ■

Notably, since the proof system has the sub-formula property, this leads to the decidability of the equational theory of residuated monoids.

We extend this Gentzen system to the typed setting in Fig. 2, where the typing judgement has been extended to lists of terms, using the following rules:

$$\frac{}{\Gamma \vdash \epsilon : n \to n}\ \textsc{Te} \qquad \frac{\Gamma \vdash u : n \to m \qquad \Gamma \vdash l : m \to p}{\Gamma \vdash u, l : n \to p}\ \textsc{Tc}$$

Like previously, the untyped proof system can be recovered by considering trivial types and environments. Note that there are several ways to add type decorations to the proof system; we chose to add a minimal set of decorations, in such a way that the following sanity requirement is satisfied:

Lemma 16. *For all l, u, n, m, if $\Gamma; l \vdash u : n \to m$ holds, then we have $\Gamma \vdash l : n \to m$ and $\Gamma \vdash u : n \to m$.*

$$\frac{\Gamma(x) = (n, m)}{\Gamma; x \vdash x : n \to m}\ \textsc{v} \qquad \frac{}{\Gamma; \epsilon \vdash 1 : n \to n}\ \textsc{Io} \qquad \frac{\Gamma; l, l' \vdash u : n \to m}{\Gamma; l, 1, l' \vdash u : n \to m}\ \textsc{Eo}$$

$$\frac{\Gamma; l \vdash u : n \to m \qquad \Gamma; l' \vdash u' : m \to p}{\Gamma; l, l' \vdash u * u' : n \to p}\ \textsc{Id} \qquad \frac{\Gamma; l, v, w, l' \vdash u : n \to m}{\Gamma; l, v * w, l' \vdash u : n \to m}\ \textsc{Ed}$$

$$\frac{\Gamma \vdash v : m \to p \qquad \Gamma; l, v \vdash u : n \to p}{\Gamma; l \vdash u/v : n \to m}\ \textsc{Ir}$$

$$\frac{\Gamma \vdash l' : m \to q \qquad \Gamma; k \vdash v : n \to m \qquad \Gamma; l, w, l' \vdash u : p \to q}{\Gamma; l, w/v, k, l' \vdash u : p \to q}\ \textsc{Er}$$

$$\frac{\Gamma \vdash v : p \to m \qquad \Gamma; v, l \vdash u : p \to n}{\Gamma; l \vdash v\backslash u : m \to n}\ \textsc{Il}$$

$$\frac{\Gamma \vdash l : p \to m \qquad \Gamma; k \vdash v : m \to n \qquad \Gamma; l, w, l' \vdash u : p \to q}{\Gamma; l, k, v\backslash w, l' \vdash u : p \to q}\ \textsc{El}$$

Figure 2: Typed Gentzen Proof System for Residuated Monoids.

Proof. We first prove that the typing judgements enjoy the following property: (†) If $\Gamma \vdash u : n \to m$ and $\Gamma \vdash u : n' \to m'$, then either $n = n'$ and $m = m'$, or $n = m$ and $n' = m'$. (The alternative comes from the presence of unit elements.) We then proceed by induction on the derivation of $\Gamma; l \vdash u : n \to m$. The interesting cases are the following ones:

(Ir) we assume by induction that $\Gamma \vdash l, v : n \to p$ and $\Gamma \vdash u : n \to p$; we have to show $\Gamma \vdash l : n \to m$ and $\Gamma \vdash u/v : n \to m$. Necessarily, $\Gamma \vdash l : n \to q$ and $\Gamma \vdash v : q \to p$ for some q. Thanks to (†) and the first premise of rule (Ir) ($\Gamma \vdash v : m \to p$), we have $m = q$ (and possibly $m = q = p$); we conclude with the typing rule (Tr).

(Er) we assume by induction that $\Gamma \vdash k : n \to m$, $\Gamma \vdash v : n \to m$, $\Gamma \vdash l, w, l' : p \to q$ and $\Gamma \vdash u : p \to q$; we have to prove $\Gamma \vdash l, w/v, k, l' : p \to q$ and $\Gamma \vdash u : p \to q$. The latter derivation comes straight from the induction hypotheses, for the former, we necessarily have $\Gamma \vdash l : p \to n'$, $\Gamma \vdash w : n' \to m'$, and $\Gamma \vdash l' : m' \to q$ for some n', m'. Thanks to (†) and the first premise of rule (Er) ($\Gamma \vdash l' : m \to q$), we have $m = m'$. We deduce $\Gamma \vdash w/v : n' \to n$ by rule (Tr), so that we can conclude. ■

As we shall explain below, we did not manage to obtain the untyping theo-

rem in all of its generality: we do not know how to handle the unit element. Therefore, in the sequel, we focus on the unit-free structures, obtained by forgetting rules (To), (Io), and (Eo). Moreover, since left and right division play a symmetrical role with respect to the product operation, we shall also remove the rules about left division, to focus on right division – our results easily extend to the case where both divisions are assumed, see the Coq proof scripts for complete proofs [10].

We now embark in the proof of the untyping theorem. First of all, since we removed unit elements, typing derivations are uniquely determined:

Lemma 17. *For all u, n, m, n', m', if $\Gamma \vdash u : n \to m$ and $\Gamma \vdash u : n' \to m'$, then $n = n'$ and $m = m'$.*

Then, the key lemma is the following one:

Lemma 18. *For all l, u, n, m such that $l \vdash u$ and $\Gamma \vdash u : n \to m$, if all elements of l can be assigned a type, then $\Gamma; l \vdash u : n \to m$.*

Proof. By induction on the derivation $l \vdash u$, and case analysis on the last used rule:

(v) this case is immediate.

(Id) if $\Gamma \vdash u * u' : n \to p$ then we have some m such that $\Gamma \vdash u : n \to m$ and $\Gamma \vdash u' : m \to p$. The elements of l, l' being typable, so are those of l and l', so that we deduce by induction that $\Gamma; l \vdash u : n \to m$ and $\Gamma; l' \vdash u' : m \to p$, which allow us to conclude.

(Ed) if the elements of $l, v * w, l'$ are typable, so are $v * w$, and then, v and w. This allows one to conclude by induction and the typed version of rule (Ed).

(Ir) if $\Gamma \vdash u/v : n \to m$ then $\Gamma \vdash u : n \to p$ and $\Gamma \vdash v : m \to p$ for some p. By induction hypothesis, $\Gamma; l, v \vdash u : n \to p$, from which we deduce $\Gamma; l \vdash u/v : n \to p$ by the typed version of rule (Ir).

(Er) (interesting case) assume $\Gamma \vdash u : p \to q$; the elements of $l, w/v, k, l'$ being typable, we have $\Gamma \vdash w/v : m' \to n$ for some m', n, whence $\Gamma \vdash w : m' \to m$ and $\Gamma \vdash v : n \to m$ for some m. Then, by induction, we have $\Gamma; k \vdash v : n \to m$ and $\Gamma; l, w, l' \vdash u : p \to q$. Finally, in order to obtain $\Gamma; l, w/v, k, l' \vdash u : p \to q$ by the typed version of rule (Er), we need to check that $\Gamma \vdash l' : m \to q$. This comes from Lemmas 16 and 17: since $\Gamma; l, w, l' \vdash u : p \to q$, we obtain $\Gamma \vdash l, w, l' : p \to q$, and since $\Gamma \vdash w : m' \to m$, we necessarily have $\Gamma \vdash l' : m \to p$. (This step is not valid with units: if $w = 1$, then $\Gamma \vdash l, 1, l' : p \to q$ could be obtained from $\Gamma \vdash l' : m'' \to q$, with m'' possibly different from m.) ■

Theorem 19. *For all l, u such that $l \vdash u$, for all n, m such that $\Gamma \vdash l : n \to m$ and $\Gamma \vdash u : n \to m$, we have $\Gamma; l \vdash u : n \to m$.*

Proof. Immediate consequence of Lemma 18: all elements of l are typable, since we assumed $\Gamma \vdash l : n \to m$. ■

Note that Lemma 18 does not hold in presence of units: the untyped derivation below is valid, however, in environment $\Gamma \triangleq \{x \mapsto (a, a);\ y \mapsto (b, b)\}$, we have $\Gamma \vdash y * y : b \to b$, and all elements of the list $y, 1/x, x, y$ are typable, but the list cannot be typed as a whole, so that $\Gamma; y, 1/x, x, y \vdash y * y : b \to b$ cannot hold, by Lemma 16.

$$\dfrac{\dfrac{}{x \vdash x}\,\text{V} \qquad \dfrac{\dfrac{\dfrac{}{y \vdash y}\,\text{V} \quad \dfrac{}{y \vdash y}\,\text{V}}{y, y \vdash y * y}\,\text{ID}}{y, 1, y \vdash y * y}\,\text{EO}}{y, 1/x, x, y \vdash y * y}\,\text{ER}$$

We do not know whether this counter-example can be further extended to refute Theorem 19 when units are allowed.

3 Conclusions and Future Work

We defined various typed structures, corresponding standard, untyped structures, and we proved several theorems, allowing to recover a typed equality from an untyped one. All proofs have been formalised in the Coq proof assistant [10]. We conclude by discussing applications and directions for future work.

3.1 Applications

Decision of typed Kleene algebras in Coq. The fact that the untyping theorem holds for typed Kleene algebras is quite important in our ATBR Coq library [2]: it allows us to extend a decision procedure for (untyped) Kleene algebras to the typed setting. The decision procedure being quite involved – it goes through finite automata constructions, we can hardly imagine to prove its soundness in the typed setting; even writing a type-preserving version of the algorithm seems challenging.

At another level we used the untyping theorem for semirings in order to formalise Kozen's completeness proof [6] for Kleene algebras (the fact that regular languages are the initial model of Kleene algebras, which we had to formalise in order our tactic to work in any model). Indeed, this proof heavily relies on matrix constructions, so that having adequate lemmas and tactics for working with possibly rectangular matrices was a big plus: this

allowed us to avoid the ad-hoc constructions Kozen used to inject rectangular matrices into square ones.

Kozen also studied the idea of typed Kleene algebras, in order to avoid these constructions [7]. He provided a different answer, however: using model-theoretic arguments, he proved an untyping theorem for the Horn theory of "1-free Kleene algebras" – Kleene algebras without neutral elements. The restriction to 1-free expressions is required, as shown by the following counter-example: $\vdash 0 = 1 \Rightarrow u = v$ is a theorem of Kleene algebras (actually, of semirings), although there are non trivial typed semirings, e.g., matrices, where $0 = 1$ holds for empty matrices, while $u = v$ is not universally true at other types.

Improving proof search for residuated monoids. The Gentzen proof system for residuated monoids has the sub-formula property, so that it can be used to decide the equational theory of residuated monoids, using a simple proof search algorithm [8, 4]. Our untyping theorem could be used to cut off useless branches during this search. Indeed, recall the typed rules (Id) and (Er):

$$\frac{\Gamma; l \vdash u : n \to m \qquad \Gamma; l' \vdash u' : m \to p}{\Gamma; l, l' \vdash u * u' : n \to p}\ \textsc{Id}$$

$$\frac{\Gamma \vdash l' : m \to q \qquad \Gamma; k \vdash v : n \to m \qquad \Gamma; l, w, l' \vdash u : p \to q}{\Gamma; l, w/v, k, l' \vdash u : p \to q}\ \textsc{Er}$$

When using these rules during proof search, one has to choose where to split the left-hand side of the sequent (where to put the coma between l, l' and k, l', respectively). While all possibilities have to be tried in the untyped setting, this is not the case in the typed setting: the cutting point has to respect types.

Now, starting from an untyped list of terms l and an untyped term u, one can easily compute an abstract 'most general type and environment' (n, m, Γ), such that $\Gamma \vdash l : n \to m$ and $\Gamma \vdash v : n \to m$ hold (taking $\mathbb{N}$ as the set of types, for example). Thanks to the untyping theorem, if $l \vdash u$ holds, then we also have $\Gamma; l \vdash u : n \to m$, so that we have at least one proof that respects the most general type, and we can restrict proof search to the corresponding well-behaved branches. Moreover, this trick could be refined during proof search, by generalising the most general type whenever possible: moving to a premise may release some typing constraints (e.g., in rule (Id), since half of the terms are thrown in both premises).

We plan to implement these ideas in the ATBR library.

3.2 Future work

Handling other structures. The Gentzen proof system we presented [9] for residuated monoids was actually designed for residuated (semi-)lattices, obtained by further requiring the partial order to be a (semi-)lattice. Our results can be extended to such residuated structures, as long as we do not introduce annihilator elements (bottom (0) and top ($\top$) elements): with division, it is no longer clear how to normalise terms, and how to factorise proofs so as to reduce to the annihilator-free case. (We have $x/0 = \top$ and $\top/x = \top$, but expressions like $0/x$ and $x/\top$ cannot be simplified.)

Action algebras [11, 5] (also called residuated Kleene algebras – they combine the ingredients from residuated semi-lattices and Kleene algebras) are closely related structures, in which divisions make it possible to obtain a variety rather than a quasi-variety: inference rules (SL) and (SR), about the star operation, can be replaced by the following axioms:

$$\frac{}{\vdash (u\backslash u)^\star = u\backslash u}\ \text{SL'} \qquad\qquad \frac{}{\vdash (u/u)^\star = u/u}\ \text{SR'}$$

We do not know whether an untyping theorem can be obtained for this structure; we can think of two strategies to attack this problem: 1) find a cut-free extension of the Gentzen proof system for residuated semi-lattice (this is leaved as an open question in [5] – it would entail decidability of the equational theory of action algebras), and adapt the current proof for residuated monoids. 2) find a 'direct' proof of the untyping theorem for residuated monoids, without going through the Gentzen proof system, so that the methodology used to obtain the untyping theorem for Kleene algebras can be extended.

A generic theory? The typed structures we focused on can be described in terms of categories equipped with additional structure on their homsets: objects of the category play the role of our types. Moreover, the untyping theorems can be rephrased as asserting the existence of a faithful functor to a one-object category.

It would therefore be interesting to find out whether our typed structures can be given a generic definition in category theory, and whether one can give a reasonable characterisation of the class of structures for which the untyping theorem holds.

Acknowledgements. The author is grateful to Tom Hirschowitz and Thomas Braibant for the highly stimulating discussions we had about this work.

References

[1] T. Braibant and D. Pous. Coq development: Algebraic tools for working with binary relations. Available from `http://sardes.inrialpes.fr/~braibant/atbr/`, May 2009.

[2] T. Braibant and D. Pous. A reflexive tactic for deciding Kleene algebras. In *Proc. 1st Coq Workshop*. Technische Universität München, August 2009.

[3] T. Coquand and G. Huet. The Coq proof assistant, 1984. `http://coq.inria.fr/`.

[4] P. Jipsen. The residuated lattice inequations quiz, 2000. `http://www1.chapman.edu/~jipsen/reslat/reslatquiz.htm/`.

[5] P. Jipsen. From semirings to residuated Kleene lattices. *Studia Logica*, 76(2):291–303, 2004.

[6] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, 1994.

[7] D. Kozen. Typed Kleene algebra. Technical Report TR98-1669, Computer Science Department, Cornell University, March 1998.

[8] M. Okada and K. Terui. The finite model property for various fragments of intuitionistic linear logic. *Journal of Symbolic Logic*, 64(2):790–802, 1999.

[9] H. Ono and Y. Komori. Logics without the contraction rule. *Journal of Symbolic Logic*, 50(1):169–201, 1985.

[10] D. Pous. Web appendix and Coq proof script of this paper, 2009. `http://sardes.inrialpes.fr/~pous/utas/`.

[11] V. R. Pratt. Action logic and pure induction. In *JELIA*, volume 478 of *Lecture Notes in Computer Science*, pages 97–120. Springer Verlag, 1990.