Unification through Projectivity

Silvio Ghilardi*
Dipartimento di Matematica
Università degli Studi di Milano
Italy

May 24, 2002

Abstract

We introduce an algebraic approach to E-unification, through the notions of finitely presented and projective object. As applications and examples, we determine the unification type of varieties generated by a single finite quasi-primal algebra, of distributive lattices and of some other equational classes of algebras corresponding to fragments of intuitionistic logic.

1 Introduction

In this paper we present an algebraic approach to unification under equational conditions (see [3] for a survey of the subject), mainly in order to have a conceptual method for the *determination of the unification type*.

Usual algebraic or categorical approaches in the literature [1], [7], [15], [16] represent a unification problem as a pair of parallel morphisms between finitely generated free algebras. We shall follow a different idea here (see the appendix at the end of the paper for comparison and further motivations) and represent a unification problem as a finitely presented algebra (fp algebra, for short) A. A solution to A (or a unifier for A) will be a morphism $A \longrightarrow P$ with a fp projective algebra as a codomain. We shall formally prove in section 3 that this conceptualization does not alter the unification type.

The main feature of the above sketched approach is that unification depends only on the notion of finitely presented and projective object, hence it can be introduced in any abstract category and unification type is preserved under categorical equivalence. As an immediate consequence, unitarity of unification type in varieties generated by a primal algebra (see [14] for this result and the related unification algorithms) follows from unitarity of Boolean unification [13], given the equivalence of the corresponding categories. Unitarity of Boolean unification, in its turn, becomes a trivial consequence of the fact that finite non degenerate Boolean algebras are all projective (so that identity morphisms are 'algebraic' mgu's).

*The author wishes to thank one of the anonymous referees for information and helpful remarks.

Another advantage of the present approach is that for locally finite varieties (i.e. for varieties in which finitely generated algebras are finite), we can always replace in the definitions of section 3 'finitely presented' by 'finite', thus making the algebraic approach concretely operative. If, in addition, we have nice finite duality theorems, like in the case of distributive lattices and of Brouwverian semilattices, we can can shift all the relevant definitions (after reversing the direction of arrows) to the dual 'geometric' category in order to get the informations we look for.

The choice of the examples in sections 5, 6 below is mainly motivated by the author's interests and work projects in the field of algebraic logic; however, as projective algebras are widely investigated, there is concrete feeling that general results concerning them could be applied to unification theory.

2 The symbolic approach

We begin by an abstract approach in the style of e.g. [2]. Let $(P, \leq)$ be a preordered set ($\leq$ is supposed to be reflexive and transitive); recall that we can turn it into a poset $(P/\approx, \leq)$ by introducing the equivalence relation $p \approx q$ iff $(p \leq q \ \& \ q \leq p)$ and by ordering equivalence classes by $[p] \leq [q]$ iff $p \leq q$.

A μ-set for $(P, \leq)$ is a subset $M \subseteq P$ such that: i) every $p \in P$ is less or equal to some $m \in M$; ii) all elements of M are mutually $\leq$-incomparable. There might be no μ-set for $(P, \leq)$ (in this case we say that $(P, \leq)$ has *type* 0) or there might be many of them, due to the lack of antisymmetry. However all μ-sets for $(P, \leq)$, if any, must have the same cardinality. This is because the map associating each element with its own equivalence class restricts to a bijection from each μ-set M onto the set of all maximal elements of $(P/\approx, \leq)$.[1] We say that $(P, \leq)$ has *type* $1, \omega, \infty$ iff it has a μ-set of cardinality 1, of finite (greater than 1) cardinality or of infinite cardinality, respectively.

We say that two preordered sets $(P, \leq)$ and $(Q, \leq)$ are equivalent iff they are equivalent as categories. One way of saying this is the following [12]: $(P, \leq)$ is equivalent to $(Q, \leq)$ iff there exists a map $e : P \longrightarrow Q$ such that

(E1) for every $q \in Q$ there is $p \in P$ such that $e(p) \approx q$;

(E2) for every $p_1, p_2 \in P$, $p_1 \leq p_2$ iff $e(p_1) \leq e(p_2)$.

Notice that, by using choice axiom, it is possible to prove that this relation of equivalence is symmetric. Anyway, we are basically interested only in the following trivial fact:

Lemma 1 Two equivalent preordered sets have the same type.

Proof First notice that if $e : P \longrightarrow Q$ satisfies (E1)-(E2), then it maps each μ-set for $(P, \leq)$ onto a μ-set for $(Q, \leq)$. Thus if $(P, \leq)$ has type $1, \omega, \infty$ so does $(Q, \leq)$. In case $(P, \leq)$ has type 0, there cannot be any μ-set M for $(Q, \leq)$, otherwise one could get a μ-set for $(P, \leq)$ by choosing for every $m \in M$ exactly one $p \in P$ such that $e(p) \approx m$.

[1] Thus if the set of all maximal elements of $(P/\approx, \leq)$ satisfies (i) above (within $(P/\approx, \leq)$ itself), then there are μ-sets for $(P, \leq)$ and each of them is obtained by picking exactly one element from each maximal equivalence class, otherwise there are no μ-sets at all (this is essentially said in [2]).

Let us now introduce the standard background [3] for E-unification. We are given a signature $\mathcal{F} = (F, \alpha)$ in the usual sense (F is a finite set of function symbols and α an arity function). $T(\mathcal{F})$ is the set of terms built up from F with the help of a countable set Var of variables. A substitution is a map $\sigma : Var \longrightarrow T(\mathcal{F})$ which is constant on a cofinite subset of Var. Substitutions can be extended to $T(\mathcal{F})$ in the domain and do compose in the standard way.

An equation is a pair of terms which is usually written as $t_1 = t_2$. In this paper, sets of equations will be used to handle both equational theories and relations among generators (in the usual algebraic sense). So we introduce the following notation: given two sets of equations E and S, by

$$S \vdash_E t_1 = t_2$$

we mean that some formula of the kind

$$E_0^{\forall} \rightarrow (S_0 \rightarrow (t_1 = t_2))$$

is logically provable, where S_0 is a finite conjunction of members of S and $E_0^{\forall}$ is a finite conjunction of universal closures of members of E (this makes clear that only equations in E are seen as axioms of a theory). If, as it will happen in many cases, S is empty, we simply write

$$t_1 =_E t_2$$

instead of $\emptyset \vdash_E t_1 = t_2$.

Example 2 (to be used later on). Let E be the theory of Boolean algebras and let $S = \{\neg x_1 \wedge x_2 = 0\}$. Let t_0, t_1, t_2, t_3 be the terms $\neg x_1 \wedge x_2, x_1 \wedge x_2, x_1 \wedge \neg x_2, \neg x_1 \wedge \neg x_2$, respectively. For every term $t(x_1, x_2)$ containing at most the variables x_1, x_2 there exists exactly one subset $J \subseteq I$, where $I = \{t_1, t_2, t_3\}$, such that $S \vdash_E t = \bigvee_{t_i \in J} t_i$. In fact equations E can be used in order to reduce t into disjunctive normal form and assumption S can be used in order to remove t_0 (if needed).

For substitutions, given a theory E and a set of variables X, we say that σ and τ are E-equivalent under X, briefly $\sigma =_E^X \tau$ iff $\sigma(x) =_E \tau(x)$ holds for every variable $x \in X$. We also say that σ is more general than τ (with respect to E and X), in symbols $\tau \leq_E^X \sigma$ or simply $\tau \leq \sigma$, iff there is a substitution θ such that $\tau =_E^X \theta \circ \sigma$ (this means that, up to E-equivalence and as far as only variables in X are considered, τ is an instantiation of σ).

An E-unification problem is a finite set of pairs of terms

$$(a) \qquad (s_1, t_1), \ldots, (s_k, t_k)$$

and a solution to it (or a unifier for it) is a substitution σ such that

$$\sigma(s_1) =_E \sigma(t_1), \ldots, \sigma(s_k) =_E \sigma(t_k).$$

$U_E(a)$ is the set of unifiers for the unification problem (a); it is a preordered set with respect to the restriction of the preorder relation $\leq_E^X$, where X is the set of variables occurring in (a).

We are now ready for the main definition: we say that E has *unification type*:

- 1, iff for every solvable unification problem (a), $U_E(a)$ has type 1;

- ω, iff for every solvable unification problem (a), $U_E(a)$ has type 1 or ω - and there is a solvable unification problem (a) such that $U_E(a)$ has type ω;

- ∞, iff for every solvable unification problem (a), $U_E(a)$ has type 1 or ω or ∞ - and there is a solvable unification problem (a) such that $U_E(a)$ has type ∞;

- 0, iff there is a solvable unification problem (a) such that $U_E(a)$ has type 0.

Examples of each kind are supplied in [3], see also section 5 below for further examples.

Notice that the above definitions do not allow extra free constants (different from those explicitly considered in the signature) to occur in a unification problem (a) and in its solutions; see section 6 for this important extension.

3 The algebraic approach

In this section, we give another definition of unification type and in next section we shall prove that it is equivalent to the previous one.

Given an equational theory E, V_E is the variety of models of E, i.e. it is the category of algebras satisfying the equations in E with related morphisms. Among algebras in V_E, we are expecially interested in those which are finitely presented: we recall the related definition below.

A presentation is just a pair (X, S) consisting of a set X and of a set S of equations with variables among X. The presentation is said to be finite iff both X and S are finite. Given a presentation (X, S), we can build the algebra $\mathcal{F}(X, S) \in V_E$ as follows: take the set of all terms with variables among X and by divide it by the equivalence relation

$$t \sim s \quad \text{iff} \quad S \vdash_E t = s.$$

Operations are introduced by using representative elements of each equivalence class, i.e. for $f \in F$ with $\alpha(f) = n$, we have

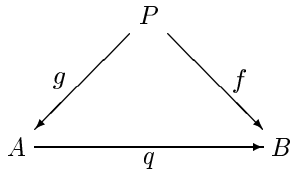
$$f([t_1], \ldots, [t_n]) = [f(t_1, \ldots, t_n)].$$

Example 3 Let E be the theory of Boolean algebras and let S, t_0, t_1, t_2, t_3, I be as in the example from the previous section. $\mathcal{F}(\{x_1, x_2\}, S)$ is (isomorphic to) the Boolean algebra $\mathcal{P}(I)$.

It can be shown that $\mathcal{F}(X, S)$ is uniquely determined, up to an isomorphism, by a suitable universal property; in case S is empty, we write $\mathcal{F}(X)$ instead of $\mathcal{F}(X, \emptyset)$ and call it the free algebra over X.

We say that A is *finitely presented* (fp for short) iff $A \simeq \mathcal{F}(X, S)$ for some finite presentation (X, S). The notion of finitely presented algebra is important because it is a purely categorical notion: in fact, it is well-known [8] that A is finitely presented iff the representable functor $V_E[A, -]$ preserves filtered colimits. So the notion of finitely presented object makes sense in any abstract category and does not need any symbolic apparatus in order to introduce it. For this reason, it is clearly preserved under equivalence of categories.

We need another kind of objects which are categorially characterizable, namely the projective objects. An object P in a category is said to be *projective* iff for every regular epic $q : A \longrightarrow B$ and for every arrow $f : P \longrightarrow B$, there is an arrow $g : P \longrightarrow A$ such that the triangle



commutes. We recall that a regular epi is an arrow which is the coequalizer of some pair of arrows. In categories like V_E, it is easily seen that regular epis are just surjective morphisms (the same is not true, however, for merely epic arrows). We shall make use of the following more or less standard Lemma:

Lemma 4 Let $P \in V_E$ be finitely presented. The following are equivalent:

(i) P is a projective object in V_E;

(ii) P is a projective object in V_E^{fp}, i.e. in the full subcategory of V_E determined by finitely presented algebras;

(iii) P is a retract of a free algebra $\mathcal{F}(X)$ for a finite X (i.e. there are morphisms $m : P \longrightarrow \mathcal{F}(X)$ and $q : \mathcal{F}(X) \longrightarrow P$ such that $q \circ m = 1_P$).

Proof (i)⇒(ii): this is immediate, because coequalizers in V_E^{fp} are coequalizers in V_E.[2]

(ii)⇒(iii): let P be $\mathcal{F}(X, S)$ for finite S, X. Consider the canonical quotient map $q : \mathcal{F}(X) \longrightarrow \mathcal{F}(X, S)$ and the identity map $\mathcal{F}(X, S) \longrightarrow \mathcal{F}(X, S)$. As q is a coequalizer in V_E^{fp},[3] it is sufficient to apply the definition of projective object.

(iii)⇒(i): consider a regular epi (i.e. a surjective morphism) $h : A \longrightarrow B$ and a morphism $f : P \longrightarrow B$. Let P be a retract of $\mathcal{F}(X)$, where $X = \{x_1, \ldots, x_n\}$ is finite, i.e. let $m : P \longrightarrow \mathcal{F}(X)$ and $q : \mathcal{F}(X) \longrightarrow P$ be such that $q \circ m = 1_P$. For every $x_i \in X$ pick $a_i \in A$ such that $h(a_i) = f(q([x_i]))$. The way $\mathcal{F}(X)$ is built (or, better, its universal property) shows that the map g defined as $g([t(x_1, \ldots, x_n)]) = t^A(a_1, \ldots, a_n)$ is well defined and is a morphism from $\mathcal{F}(X)$ into A (here t^A is of course the interpretation of the term t in A). Then we have $h \circ g = f \circ q$, because the $[x_i]$ generate $\mathcal{F}(X)$. Composing on the right with m, we get $h \circ (g \circ m) = f$, i.e. P is projective.

The above Lemma makes clear that the class of fp projective algebras is an extension of the class of finitely generated free algebras (the extension is indeed proper

[2]The coequalizer (both in V_E and in V_E^{fp}) of a couple of morphisms among fp algebras $f_1 : \mathcal{F}(Y, T) \longrightarrow \mathcal{F}(X, S)$ and $f_2 : \mathcal{F}(Y, T) \longrightarrow \mathcal{F}(X, S)$ is the obvious quotient map $\mathcal{F}(X, S) \longrightarrow \mathcal{F}(X, S \cup S')$, where S' is any set of pairs (t_1^y, t_2^y) (varying y in Y), in which terms t_1^y, t_2^y are chosen in such a way that $f_1([y]) = [t_1^y]$ and $f_2([y]) = [t_2^y]$.

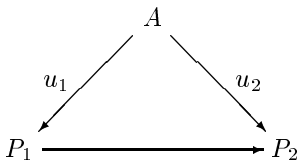
[3]See the previous footnote (consider the free algebra on a set having the same cardinality as S and the two morphisms into $\mathcal{F}(X)$ defined in the obvious way at the free generators, etc.).

and large, for instance all finite Boolean algebras are projective, whereas only those of cardinality 2^{2^n} are free).

We are now ready to introduce the relevant definition for E-unification from an algebraic point of view. In this context an E-unification problem is simply a finitely presented algebra A and a solution for it (also called a unifier for A) is a pair given by a projective fp algebra P and a morphism

$$u : A \longrightarrow P.$$

The set of unifiers for A is denoted by $U_E(A)$ (A is said to be unifiable or solvable iff $U_E(A)$ is not empty). Given two unifiers for A, say $u_1 : A \longrightarrow P_1$ and $u_2 : A \longrightarrow P_2$, we say that u_1 is more general than u_2 iff there exists a morphism making the triangle



commute. The definition of unification type is the expected one, namely we say that V_E has *unification type*:

- 1, iff for every solvable unification problem A, $U_E(A)$ has type 1;
- ω, iff for every solvable unification problem A, $U_E(A)$ has type 1 or ω - and there is a solvable unification problem A such that $U_E(A)$ has type ω;
- ∞, iff for every solvable unification problem A, $U_E(A)$ has type 1 or ω or ∞ - and there is a solvable unification problem A such that $U_E(A)$ has type ∞;
- 0, iff there is a solvable unification problem A such that $U_E(A)$ has type 0.

4 Equivalence of the two approaches

In this section, we shall premit the words 'symbolic' and 'algebraic', respectively, to any concept which has been introduced both in section 2 and in section 3. Thus, we shall provisionally speak of 'symbolic' and 'algebraic' unification types as distinct entities. Our aim is the proof of the following:

Theorem 5 For any equational theory E, the symbolic and the algebraic unification type coincide.

Proof Let a symbolic unification problem

$$(a) \qquad (s_1, t_1), \ldots, (s_k, t_k)$$

be given; suppose that $X = \{x_1, \ldots, x_n\}$ is the set of the variables occurring in the terms s_j, t_j $(j = 1, \ldots, k)$. We shall prove that the preordered set $U_E(a)$ is equivalent to the preordered set $U_E(A)$, where A is the fp algebra $\mathcal{F}(X, S)$, for $S = \{(s_1, t_1), \ldots, (s_k, t_k)\}$ (then Lemma 1 applies). We define an equivalence map

$$e : U_E(a) \longrightarrow U_E(A)$$

as follows. Let $\sigma \in U_E(a)$ and suppose that Y is the set of variables occurring in the terms $\sigma(x_1), \ldots, \sigma(x_n)$. Consider the free algebra $\mathcal{F}(Y)$, it is projective as all free algebras are. Define the algebraic unifier $e_\sigma : A \longrightarrow \mathcal{F}(Y)$ by

$$(u) \qquad e_\sigma([t]) \;=\; [\sigma(t)].$$

In order to see that the definition is correct, recall the construction of $A = \mathcal{F}(X, S)$ from section 3: if $t \sim t'$, then $S \vdash_E t = t'$, hence $\vdash_E \sigma(t) = \sigma(t')$, given that $\sigma \in U_E(a)$. We now have to prove conditions (E1)-(E2) from section 2.

Proof of (E1): let $u : A \longrightarrow P$ be an algebraic unifier for A. By Lemma 4, P is a rectract of a finitely generated free algebra, hence there exist some finite Y' and some morphisms

$$P \xrightarrow{m} \mathcal{F}(Y') \xrightarrow{q} P,$$

such that $q \circ m = 1_P$. Let us consider the morphism $m \circ u : A \longrightarrow \mathcal{F}(Y')$; define the substitution σ by taking $\sigma(x_i)$ (for $i = 1, \ldots n$, the other variables are left unchanged) to be any term t_i such that $m(u([x_i])) = [t_i]$. Otherwise said, by definition, we have for all $x_i \in X$

$$m(u([x_i])) = [\sigma(x_i)].$$

By an easy induction, we can get also that

$$m(u([t])) = [\sigma(t)]$$

for every term t containing at most the variables X. In particular, for every $j = 1, \ldots, k$, we have that $(m \circ u)[s_j] = [\sigma(s_j)]$ and that $(m \circ u)[t_j] = [\sigma(t_j)]$. But $[s_j] = [t_j]$ (by the construction of $A = \mathcal{F}(X, S)$), hence $[\sigma(s_j)] = [\sigma(t_j)]$, which means $\sigma(s_j) =_E \sigma(t_j)$ (by the construction of free algebras). This shows that $\sigma \in U_E(a)$. Now let $Y \subseteq Y'$ be the set of variables of Y' occurring in the terms $\sigma(x_1), \ldots, \sigma(x_n)$. We have to show that $u \leq e_\sigma$ and that $e_\sigma \leq u$, where e_σ is defined by (u) above.

Let $\iota : \mathcal{F}(Y) \longrightarrow \mathcal{F}(Y')$ be the map associating the equivalence class of any t in $\mathcal{F}(Y)$ with the equivalence class of the same t in $\mathcal{F}(Y')$; as $\mathcal{F}(Y)$ cannot be empty,[4] we can define $r : \mathcal{F}(Y') \longrightarrow \mathcal{F}(Y)$ by putting $r([t]) = [\theta(t)]$, for a substitution θ mapping the variables in Y into themselves and the variables in $Y' \backslash Y$ into some arbitrarily fixed term. We trivially have that $r \circ \iota$ is the identity map.

We also have that the square

$$\begin{array}{ccc} A & \xrightarrow{\;u\;} & P \\ {\scriptstyle e_\sigma}\downarrow & & \downarrow{\scriptstyle m} \\ \mathcal{F}(Y) & \xrightarrow[\;\iota\;]{} & \mathcal{F}(Y') \end{array}$$

commutes, as for every term t, $m(u([t]))$ and $\iota(e_\sigma[t]))$ are both equal to $[\sigma(t)]$. Now we have that

$$r \circ m \circ u \;=\; r \circ \iota \circ e_\sigma \;=\; e_\sigma,$$

[4] This cannot happen, even in the case that the signature does not contain constant symbols, for the following reason: $\mathcal{F}(Y)$ must contain $[\sigma(x_i)]$ for all $x_i \in X$, so if it is empty, X is empty too. But then, if also the signature does not contain constants, the unification problem (a) and the algebra A are both empty, so there is nothing to prove at all.

thus $e_\sigma \leq u$ holds; on the other hand,

$$q \circ \iota \circ e_\sigma \;=\; q \circ m \circ u \;=\; u,$$

thus $u \leq e_\sigma$ holds too.

Proof of left-to-right side of (E2): suppose that for $\sigma, \tau \in U_E(a)$, we have that $\tau \leq_E^X \sigma$; this means that there exists a substitution θ such that $\theta \circ \sigma =_E^X \tau$. Let Y, Z be the variables occurring in the $\sigma(x_i), \tau(x_i)$, respectively; we can freely suppose that $\theta(y)$ (for $y \in Y$) contains at most the variables in Z.[5] Let $g : \mathcal{F}(Y) \longrightarrow \mathcal{F}(Z)$ be the morphism so defined

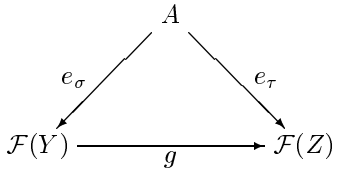
$$g([v]) \;=\; [\theta(v)]$$

for every $[v] \in \mathcal{F}(Y)$. For every $[t] \in A$, we have that

$$g(e_\sigma([t])) = g([\sigma(t)]) = [\theta \circ \sigma(t)] = [\tau(t)] = e_\tau([t]),$$

that is $e_\tau \leq e_\sigma$.

Proof of right-to-left side of (E2): let σ, τ be such that $e_\tau \leq e_\sigma$; in other words, we have a commutative triangle



Consider any substitution θ satisfying the condition $g([y]) = [\theta(y)]$ for all $y \in Y$. By induction, we get $g([t]) = [\theta(t)]$, for all $[t] \in \mathcal{F}(Y)$, hence for $x_i \in X$ we get

$$[\tau(x_i)] = e_\tau([x_i]) = g(e_\sigma([x_i])) = g([\sigma(x_i)]) = [\theta \circ \sigma(x_i)].$$

This means that $\tau(x_i) =_E \theta \circ \sigma(x_i)$, i.e. that $\tau \leq_E^X \sigma$.

In the case of Boolean algebras to be unifiable and to be projective do coincide for fp algebras: this is because to be unifiable here means to be non degenerate and because all fp (=finite) non degenerate Boolean algebras are projective [9]. So any solvable unification problem A does trivially have a most general unifier (in the algebraic sense) which is the identity map $1_A : A \longrightarrow A$. We shall see how to extract from this argument explicit formulas for symbolic mgu's in the next section. Now we only give an example showing how the proof of the above Theorem works in concrete cases.

Example 6 Let E be the theory of Boolean algebras and let t_0, t_1, t_2, t_3, I be as in the example from section 2. Let (a) be the unification problem $t_0 = 0$. We saw in section 3 that A is (isomorphic to) $\mathcal{P}(I)$, which is projective. This means that $1_A : A \longrightarrow A$ is an algebraic unifier. To get a symbolic mgu for (a) from the algebraic unifier 1_A, let us follow the argument of the above '*Proof of* $(E1)$' and so let us first

[5] If there are extra variables, they can be instantiated by some term in Z, thus passing to a substitution θ' still satisfying the condition $\theta' \circ \sigma =_E^X \tau$. Notice that $\mathcal{F}(Z)$ cannot be empty, for the same reason as above.

look for a free algebra $\mathcal{F}(Y')$ and for morphisms $m : A \longrightarrow \mathcal{F}(Y')$, $q : \mathcal{F}(Y') \longrightarrow A$ such that $q \circ m = 1_A$. We take $Y' = \{x_1, x_2\}$ (notice that $\mathcal{F}(Y')$ is nothing but $\mathcal{P}(I \cup \{t_0\})$); q is just intersection with I and a suitable m is defined by $m(U) = U$ (if $t_1 \notin U$), $m(U) = U \cup \{t_0\}$ (if $t_1 \in U$). Now to find an mgu we must look at what the equivalence class of x_i $(i = 1, 2)$ is in A and at what its image under m is in $\mathcal{F}(Y')$. Clearly $[x_1]$ in A is $\{t_1, t_2\}$, because these are the two clauses containing x_1; on the other hand

$$m([x_1]) = \{t_0, t_1, t_2\} = [(\neg x_1 \wedge x_2) \vee (x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2)]$$

which can be simplified to $[x_1 \vee x_2]$. Analogously, we get $[x_2] = \{t_1\}$ and $m([x_2]) = [x_2]$.[6] So our mgu is given by

$$x_1 \mapsto x_1 \vee x_2 \qquad x_2 \mapsto x_2.$$

We give also an example showing the inverse passage, i.e. from a symbolic unifier to an algebraic one (this passage is less important in the applications). Let us consider the unifier σ (which is not maximal) mapping x_1 into $\top$ and x_2 into x_1. Here we must take the free algebra $\mathcal{F}(\{x_1\})$ (which is conveniently represented as $\mathcal{P}(\{x_1, \neg x_1\})$) and we must find a morphism $u : A \longrightarrow \mathcal{P}(\{x_1, \neg x_1\})$ mapping the equivalence class of x_1 into the quivalence class of $\top$ and the equivalence class of x_2 into the equivalence class of x_1. The existence of such a morphism (which must be unique because $[x_1], [x_2]$ generate A) is guaranteed precisely by the fact that σ is a solution to (a): the required u is the inverse image along the set-theoretic function $\{x_1, \neg x_1\} \longrightarrow I$ mapping x_1 to t_1 and $\neg x_1$ to t_2.

5 Applications and Examples

In this section, we shall exclusively use the algebraic approach of section 3 in order to determine unification types.

We saw above that in the case of Boolean algebras (and in the equivalent case of varieties generated by a primal algebra) to be unifiable and to be projective do coincide for fp algebras. This situation (coincidence of 'unifiable' and 'projective') is indeed a larger phenomenon.

A finite algebra A is said to be *quasi-primal* iff there exists a ternary term $t(x, y, z)$ such that for every $a, b, c \in A$, we have that $t(a, b, c) = a$ if $a \neq b$ and $t(a, b, c) = c$ if $a = b$. Equivalently (see [5]), A is quasi-primal iff all subalgebras of A are simple and the variety $V(A)$ generated by A is arithmetical (that is, congruence-permutable and congruence-distributive). Being A finite, $V(A)$ is locally finite, so that fp algebras are just finite algebras. We shall make use of the following characterization Theorem for finite projective algebras in $V(A)$:

Theorem 7 [17] Let A be a finite quasi-primal algebra; a finite algebra in $V(A)$ is projective iff it admits every non-trivial minimal subalgebra of A as a direct factor.

Theorem 8 If A is a finite quasi-primal algebra, then the variety $V(A)$ has unitary unification type.

[6] Notice that we do not use subscripts for square brackets, because the context makes clear where equivalence classes are taken.

Proof We shall show that each finite unifiable algebra $B \in V(A)$ is projective. As B is unifiable, there is a morphism $u : B \longrightarrow P$, where P is finite and projective. If $A_1, \ldots, A_n$ are the non-trivial minimal subalgebras of A, it follows from Theorem 7 that for each $i = 1, \ldots, n$ there exists at least one morphism $f_i : B \longrightarrow A_i$ (compose u with the appropriate projection). Now consider the algebra $B \times A_1 \times \cdots \times A_n$ (which is projective again by Theorem 7) and the morphism

$$\langle 1_B, f_1, \ldots, f_n \rangle : B \longrightarrow B \times A_1 \times \cdots \times A_n,$$

associating $\langle b, f_1(b), \ldots, f_n(b) \rangle$ with $b \in B$. If p_B is the projection onto B, we have that

$$p_B \circ \langle 1_B, f_1, \ldots, f_n \rangle \;=\; 1_B,$$

so B is projective being the retract of a projective algebra (see Lemma 4(iii)).

We give a further example in which 'unifiable' and 'projective' coincide for fp algebras. A *Brouwerian semilattice* B is a semilattice with unit (i.e. a commutative idempotent monoid, or equivalently a poset with finite infs) endowed with a further binary operation $\rightarrow$ satisfying the condition:

$$b_1 \wedge b_2 \leq b_3 \;\text{ iff }\; b_1 \leq b_2 \rightarrow b_3$$

for every $b_1, b_2, b_3 \in B$. It can be shown that Brouwerian semilattices are a variety, indeed a locally finite variety (for this and other basic properties see [10]).

We need some easy background about adjoints among posets. Suppose that $f : (P, \leq) \longrightarrow (Q, \leq)$ is an order-preserving map between posets; suppose also that $(P, \leq)$ is complete and that f preserves meets. Then there exists another order-preserving map $f^* : (Q, \leq) \longrightarrow (P, \leq)$ satisfying the condition:

$$(A) \qquad f^*(q) \leq p \;\text{ iff }\; q \leq f(p)$$

for every $p \in P, q \in Q$ ($f^*(q)$ turns out to be the infimum of the set of all r such that $q \leq f(r)$). If f is surjective, we have that

$$(S) \qquad f \circ f^* \;=\; 1_Q,$$

because $f \circ f^* \circ f = f$ follows from (A). If $(P, \leq)$ and $(Q, \leq)$ are Brouwerian semilattices and f preserves implication, we have also that the so-called Frobenius condition

$$(F) \qquad p \wedge f^*(q) \;=\; f^*(f(p) \wedge q)$$

holds for every $p \in P, q \in Q$.

Theorem 9 The variety of Brouwerian semilattices has unitary unification type.

Proof Notice that all finite (=fp)[7] algebras are unifiable, as the one element algebra is projective, being the free algebra on zero generators. We show that all finite algebras are projective: for this, it is sufficient to show that every surjective morphism

[7] Any finite algebra is finitely presented if the signature contains only finitely many function symbols (take the multiplication tables as a presentation). The converse is true for locally finite varieties (i.e. for varieties in which finitely generated free algebras are finite).

$q : A \longrightarrow B$ between finite Brouwverian semilattices has a section, i.e. that there is a morphism $s : B \longrightarrow A$ such that $q \circ s = 1_B$ (see Lemma 4(ii) and the definition of projective). Indeed, we leave the reader to check (by using $(A), (S), (F)$ above) that we can put $s(b) = q^*(1) \to q^*(b)$ in order to get an appropriate s.[8]

The case of Brouwerian semilattices is quite instructive for the problem of extracting symbolic unifiers from algebraic proofs. In fact from *the mere statement* that all finite algebras are projective and from an effective description of finitely generated free algebras (see e.g. [10]), it is in principle possible to get a unification algorithm (the procedure is the same as in the example of section 4 for Boolean algebras). However, the extremely fast-growing size of free algebras makes this proposal unfeasible even for very small values of the cardinality of the set of variables involved in the unification problem.[9] On the other hand, *the proof* of Theorem 9 contains a quite simple formula for most general unifiers. First notice that any unification problem $s_i = t_i$ $(i = 1, \ldots, n)$ can be reduced to the matching problem $t = 1$, where $t = \bigwedge_{i=1}^{n}(s_i \leftrightarrow t_i)$; secondly, the left adjoint q^* to a canonical quotient map $q : \mathcal{F}(X) \longrightarrow \mathcal{F}(X, \{t = 1\})$ maps $[v]$ onto $[t \wedge v]$. Consequently, the morphism s described in the proof of Theorem 9, maps $[x]$ into $[1 \wedge t] \to [t \wedge x]$, which can be simplified to $[t \to x]$. This means that the unification problem $t = 1$ has mgu given by $x \mapsto (t \to x)$, for every variable x occurring in t (keep in mind again the '*Proof of* $(E1)$' within Theorem 5).

Similar formulas (coincident with the 'Löwenheim formulas' of [13]) can be given for the Boolean case too. In fact, one can prove that finite unifiable (i.e. non degenerate) Boolean algebras are projective just by a slight modification of the proof of Theorem 9. The modification is the following: if $\mathcal{F}(X, \{t = 1\})$ is non degenerate, then there exists a morphism $\alpha : \mathcal{F}(X, \{t = 1\}) \longrightarrow \mathbf{2}$, where $\mathbf{2}$ is the two element Boolean algebra (α is induced by a two-valued assignment satisfying t). Build a section s of the quotient map $q : \mathcal{F}(X) \longrightarrow \mathcal{F}(X, \{t = 1\})$ by putting $s([v]) = q^*([v])$ (if $\alpha([v]) = 0$) and $s([v]) = q^*([1]) \to q^*([v])$ (if $\alpha([v]) = 1$).[10] We consequently get an mgu for the solvable unification problem $t = 1$ by fixing an assignment satisfying t and by mapping each variable x into $t \wedge x$ or into $t \to x$ depending on the fact that x is sent to either 0 or 1 by that assignment. So, once again, we obtained explicit formulas for an mgu, although in the present case a satisfiability problem must be solved first.

Anther way of applying the results of section 4 is through *duality theorems* for fp algebras:[11] we give here a couple of examples, both for locally finite varieties.

Theorem 10 The category of finite distributive lattices[12] is dual to the category of finite posets and order-preserving maps. A finite distributive lattice is projective iff its dual poset is a semilattice with unit.

[8] An alternative proof of this Theorem can be easily obtained through Köhler duality [10] (see section 6).

[9] The free Brouwerian semilattice on three generators has more than 10^{14} elements!

[10] We leave the reader to check that s so defined is a Boolean morphism, by using the fact that q^* preserves $\wedge$, as a consequence of (F) and (S) above (notice however that q^* does not preserve $\top$, so it could not be directly used instead of s).

[11] According to the standard terminology, we say that a category $\mathbf{C}$ is dual to another category $\mathbf{D}$ iff $\mathbf{D}$ is equivalent to the opposite category of $\mathbf{C}$.

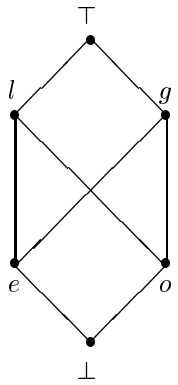
[12] We consider part of the definition of being a lattice the presence of zero and one elements.

Proof The proof of this Theorem can be essentially found in textbooks, such as [4], [9]. We merely sketch it. The dual of a finite poset is the distributive lattice of its downward closed subsets and the dual of an order-preserving map is the inverse image morphism. The dual of a finite distributive lattice is the poset of its join-irreducible elements (i.e. the non-zero elements which are less or equal to a or to b in case they are less or equal to $a \vee b$); the dual of a morphism is easily found just by observing that its left adjoint maps join-irreducible elements into join-irreducible elements.

In order to determine *injective* objects (i.e. dual of projective objects) in the category of finite posets and order-preserving maps (so that Lemma 4(ii) applies), first observe that an order-preserving map is regular monic iff it is injective and also reflects the partial order relation. Given that, it is easy to check that semilattices with unit are injective; vice versa, if $(P, \leq)$ is injective, then the embedding into its downward closed subsets is regular monic, hence it must have a retract and it is not difficult to see that this retract must map a downward closed subset into its sup.

We are now ready to determine the unification type of distributive lattices. We shall work in the dual category of finite posets and order-preserving maps, hence all the definitions of section 3 must be dualized (i.e. direction of arrows must be reversed): a unification problem now is a finite poset, a unifier for it a map with domain a semilattice with unit, a unifier u_1 is more general than a unifier u_2 iff there exists an order-preserving map f such that $u_1 \circ f = u_2$, etc.

Let us introduce the six element poset $P = \{\bot, e, o, l, g, \top\}$, whose partial order relation $\leq$ is given by the following diagram



Lemma 11 For every natural number n, there is a unifier $u_n : (P_n, \leq) \longrightarrow (P, \leq)$ such that any unifier for $(P, \leq)$ which is more general than u_n has as a domain a poset having at least n elements.

Proof Let $(P_n, \leq)$ be $(\mathcal{P}(\underline{n}), \subseteq)$, where $\underline{n}$ is the set $\{1, \ldots, n\}$. Notice that $(\mathcal{P}(\underline{n}), \subseteq)$ is a semilattice with unit. Define $u_n(S)$ to be:

- $\bot$, if S is empty;

- $\top$, if S has at least 3 elements or if it has two elements which are both odd or even;

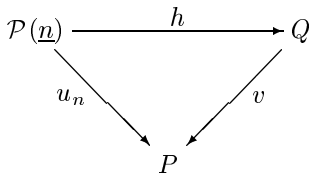
- g, if S has two elements, say i and j, such that i is odd, j is even and $i > j$;

- l, if S has two elements, say i and j, such that i is odd, j is even and $i < j$;

- e, if S contains only one element, which is even;

- o, if S contains only one element, which is odd.

It is not difficult to see that u_n is order-preserving, i.e. a unifier. Now suppose that $v : (Q, \leq) \longrightarrow (P, \leq)$ is more general than u_n, i.e. that we have an order-preserving map h such that the triangle



commutes. We prove that we cannot have $h(\{i\}) = h(\{j\})$ for $i < j$. Suppose the contrary, then i, j must be for instance both even (they cannot be one odd and the other one even, as h cannot collapse elements with different u_n-values). Take an odd k such that $i < k < j$ and let s be the sup of $h(\{i\})$ and $h(\{k\})$: it exists, as $(Q, \leq)$ is a finite semilattice. We have that s is greater or equal to $h(\{k\})$ and to $h(\{i\}) = h(\{j\})$. Furthermore, $h(\{i, k\}) \geq s$, by the fact that $\{i\}$ and $\{k\}$ are both included in $\{i, k\}$, by the fact that h is order-preserving and by the definition of sup. Similarly, $h(\{j, k\}) \geq s$. As v preserves the partial order relation and the triangle commutes, we get

$$v(s) \geq e, \quad v(s) \geq o, \quad l \geq v(s), \quad g \geq v(s),$$

which is impossible, given the above diagram for $(P, \leq)$.

Lemma 12 If a finite poset $(Q, \leq)$ has both a minimum and a maximum element, then the preordered set of its unifiers is filtered.

Proof We have to show that, given two unifiers $u_1 : (Q_1, \leq) \longrightarrow (Q, \leq)$ and $u_2 : (Q_2, \leq) \longrightarrow (Q, \leq)$ for $(Q, \leq)$, there is a unifiers which is more general than both of them. Let $(R, \leq)$ be obtained by adding a new top element $\top$ and a new bottom element $\bot$ to the disjoint union of $(Q_1, \leq)$ and $(Q_2, \leq)$. Clearly $(R, \leq)$ is again a semilattice with unit and the canonical injection ι_i of $(Q_i, \leq)$ $(i = 1, 2)$ into it is order-preserving. Now define a new unifier $u : (R, \leq) \longrightarrow (Q, \leq)$ by mapping r into $u_i(r)$, if r comes from Q_i, and by mapping it into the top or the bottom element of Q if it is equal to $\top$ or $\bot$, respectively. As we have that $u \circ \iota_1 = u_1$ and $u \circ \iota_2 = u_2$, u is more general than u_1, u_2.

Theorem 13 The variety of distributive lattices has unification type 0.

Proof Take the finite poset $(P, \leq)$ of Lemma 11; by Lemma 12, the preordered set of its unifiers is filtered and a filtered preordered set can have only type 0 or 1. The latter is impossible, by Lemma 11, as we are not allowed to introduce infinite posets in building unifiers.

A *pseudocomplemented distributive lattice* is a distributive lattice D endowed with a further unary operation $\neg$ satisfying the condition

$$a \wedge b \leq 0 \text{ iff } a \leq \neg b,$$

for every $a, b \in D$. Pseudocomplemented distributive lattices are a locally finite variety (finitely generated free algebras are described in [18]). The following Theorem can be proved by complicating the arguments used in the proof of Theorem 10 (see in any case [19]):

Theorem 14 The category of finite pseudocomplemented distributive lattices is dual to the category of finite posets and order-preserving maps $f : (P, \leq) \longrightarrow (Q, \leq)$ satisfying the following further requirement (let $m(P), m(Q)$ be the sets of minimal elements of $(P, \leq)$ and $(Q, \leq)$, respectively):

(1) $\quad \forall \mu \in m(Q)\, \forall p \in P \;\; (\mu \leq f(p) \;\Rightarrow\; \exists \nu \in m(P)\; (\nu \leq p \;\&\; f(\nu) = \mu)).$

A finite pseudocomplemented distributive lattice is projective iff its dual poset P is not empty, has sups of pairs of elements and satisfies the further requirement:

(2) $\quad \forall \mu \in m(P)\, \forall p_1, p_2 \in P \;\; (\mu \leq p_1 \vee p_2 \;\Rightarrow\; \mu \leq p_1 \text{ or } \mu \leq p_2).$

Theorem 15 The variety of pseudocomplemented distributive lattices has unification type 0.

Proof Notice that Lemma 11 can be proved in the same way as in the case of distributive lattices (with trivial observations like that $\mathcal{P}(\underline{n})$ satisfies (2) and u_n satisfies (1)). Lemma 12 also holds, with slight modifications in the proof: $(R, \leq)$ is now obtained by adding only a new top element $\top$ to the disjoint union of $(Q_1, \leq)$ and $(Q_2, \leq)$. The new unifier $u : (R, \leq) \longrightarrow (Q, \leq)$ is again defined by mapping r into $u_i(r)$, if r comes from Q_i, and by mapping it into the top element of Q if it is equal to $\top$. The fact that $(Q, \leq)$ has a bottom element (i.e. a unique minimal element) is used in order to show that u satisfies (1). The remaining facts to check (namely that $(R, \leq)$ satisfies (2) and that ι_1, ι_2 satisfy (1)) are trivial. Given that Lemmas 11, 12 hold, Theorem 15 follows by the same argument we used in the proof of Theorem 13.

Theorems 9, 13, 15 shows the behaviour of E-unification in relevant fragments of intuitionistic logic, for the whole intuitionistic logic (i.e. for Heyting algebras) the unification type is ω, as shown in [6].

6 Unification with extra constants

As remarked in section 2, we have not considered unification problems and related solutions containing an additional finite set of constants C not appearing in the signature. These constants might be subjected to a further finite set of equations S_0

(if S_0 is empty, then they are free).[13] This extension of the approach of section 2 corresponds to consider unification problems in the theory $E(C, S_0)$ obtained from E by adding the constants C to the signature and the equations S_0 to the axioms. So we may define the *stable unification type* of E as the 'worst' unification type of $E(C, S_0)$, varying the pair (C, S_0) (i.e. E has unitary stable unification type iff $E(C, S_0)$ has unitary unification type for all finite pairs (C, S_0), E has ω as stable unification type iff all $E(C, S_0)$ have unification type 1 or ω - and there is a finite pair (C, S_0) such that $E(C, S_0)$ has unification type ω, etc.).

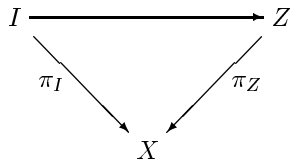
In order to deal with stable unification types, the key point, from an algebraic point of view, is given by the following Proposition:

Proposition 16 Given a finite pair (C, S_0) as above, we have that the category $V_{E(C,S_0)}$ is isomorphic to the comma category A/V_E,[14] where A is the fp algebra $\mathcal{F}(C, S_0)$; moreover, $V^{fp}_{E(C,S_0)}$ is isomorphic to $A/(V^{fp}_E)$.

Proof Suppose that $C = \{c_1, \ldots, c_n\}$; algebras in $V_{E(C,S_0)}$ are the algebras $B \in V_E$ endowed with further specified elements (to be preserved by morphisms in $V_{E(C,S_0)}$) $c_1^B, \ldots, c_n^B$ such that $B \models t_1^B(c_1^B, \ldots, c_n^B) = t_2^B(c_1^B, \ldots, c_n^B)$ holds for every $(t_1, t_2) \in S_0$. The isomorphism functor $V_{E(C,S_0)} \longrightarrow A/V_E$ acts 'identically' on morphisms and associates with the algebra $(B, c_1^B, \ldots, c_n^B)$ the morphism $\beta : A \longrightarrow B$ defined by $\beta([t(c_1, \ldots, c_n)]) = t^B(c_1^B, \ldots, c_n^B)$. The inverse functor $A/V_E \longrightarrow V_{E(C,S_0)}$ still acts identically on morphisms and associates with the object $\beta : A \longrightarrow B$ the algebra $(B, \beta([c_1]), \ldots, \beta([c_n]))$.

For the second part of the Proposition, given the above description of the isomorphism functor, it is sufficient to show that $(B, c_1^B, \ldots, c_n^B)$ is finitely presented in $V_{E(C,S_0)}$ iff B is finitely presented in V_E. In fact, if (X, S) is a presentation for $(B, c_1^B, \ldots, c_n^B)$ in $V_{E(C,S_0)}$, then $(X \cup \{c_1, \ldots, c_n\}, S \cup S_0)$ is a presentation for B in V_E. Vice versa, if (X, S) is a presentation for B in V_E, then pick terms $t_1, \ldots, t_n$ such that $c_1^B = [t_1], \ldots, c_n^B = [t_n]$: it turns out that $(X, S \cup \{c_1 = t_1, \ldots, c_n = t_n\})$ is a presentation for $(B, c_1^B, \ldots, c_n^B)$ in $V_{E(C,S_0)}$.

In order to see a first simple example of the application of the above Proposition, let us consider the case in which V_E is the category $\mathbf{B}$ of Boolean algebras. The category of finite Boolean algebras $\mathbf{B}^{fp}$ is dual to the category of finite sets $\mathbf{Set}_{fin}$. Thus, recalling the definitions of comma category under and over a given object, for every finite Boolean algebra A, the category $A/(\mathbf{B}^{fp})$ is dual to the category $\mathbf{Set}_{fin}/X$, where X is the finite set which is dual to A. It is easily seen that in $\mathbf{Set}_{fin}/X$, an object $\pi_Z : Z \longrightarrow X$ is injective iff π_Z is a surjective map and it is (co)-unifiable iff there exists a commutative triangle



[13] Usually S_0 is taken to be empty in the literature. The reason why we prefer not to do so is because we would not like free algebras (which, unlike fp algebras, are not categorially characterizable) to appear in statements like Proposition 16 below.

[14] We recall that this category has morphisms with domain A as objects and the obvious commutative triangles as arrows (see [12]).

where (I, π_I) is an injective object, i.e. where π_I is surjective. But this implies that π_Z is surjective too, hence once again to be unifiable and to be projective do coincide in $A/(\mathbf{B}^{fp})$, thus showing the unitarity of stable unification type for Boolean algebras. The same result applies also to varieties generated by a primal algebra because 'to have stable unitary unification type' is a categorical property (it depends only on the unification types of the comma categories under finitely presented objects). More generally, it is possible to show that *varieties $V(A)$ generated by a single finite quasi-primal algebra A have unitary stable unification type*: in fact, the essential point in the proof of Theorem 7 depends only on some few categorical properties which are inherited from $V(A)^{fp}$ by the comma categories we are interested in.[15]

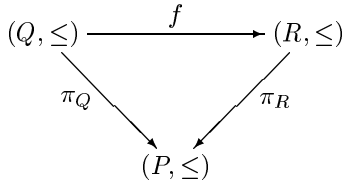
Let us concentrate now on the case of Brouwerian semilattices which is more intersting. The key point for our investigations is the following duality Theorem (see [10]):

Theorem 17 The category of finite Brouwerian semilattices is dual to the category $\mathbf{K}$ of finite posets and strict open partial maps.

A partial map $f : (P, \leq) \longrightarrow (Q, \leq)$ between finite posets is said to be strict open iff the following two conditions are satisfied:

- for all $p, q \in dom(f)$, if $p < q$ then $f(p) < f(q)$;
- for all $p \in dom(f)$, for all $q \in Q$, if $q < f(p)$ then there exists $p' \in dom(f)$ such that $p' < p$ and $f(p') = q$.

In order to deal with the stable unification type of Brouwverian semilattices, we shall consequently work with (duals of) unification problems in the category $\mathbf{K}/(P, \leq)$, where $(P, \leq)$ is an arbitrary fixed finite poset. Objects in $\mathbf{K}/(P, \leq)$ are just triples $(Q, \leq, \pi_Q)$, where $(Q, \leq)$ is a finite poset and $\pi_Q : Q \longrightarrow P$ is a strict open partial map; an arrow in $\mathbf{K}/(P, \leq)$ of domain $(Q, \leq, \pi_Q)$ and codomain $(R, \leq, \pi_R)$ is a strict open partial map $f : Q \longrightarrow R$ such that the triangle



commutes. Notice that the commutativity of the triangle means that the composition of f and π_R (as relations) is equal to π_Q: in particular, for every $q \in Q$, q is in the domain of π_Q iff both (q is in the domain of f and $f(q)$ is in the domain of π_R).

[15] We give some further details for the interested reader. Let us consider only the case in which the signature contains at least one costant symbol (there is no loss of generality in that for signatures augmented with extra constants): this implies that (i) projections are regular epi (i.e. they are surjective). Moreover standard arguments from universal algebra (essentially Corollaries 6.10 and 10.2 of [5]) can be used in order to prove that in $V(A)^{fp}$ (ii) every regular epi is isomorphic to a projection. Now it is easy to show that in any regular category with an initial object and satisfying (i) and (ii), projective objects are just those containing the initial object as a direct factor. As (ii) can be transferred from $V(A)^{fp}$ to our comma categories by a general argument, at this point it is possible to repeat word by word the proof of Theorem 8.

Lemma 18 An arrow $f : (Q, \leq, \pi_Q) \longrightarrow (R, \leq, \pi_R)$ is regular monic in $\mathbf{K}/(P, \leq)$ iff it is injective and totally defined.

Proof Given a pair of parallel arrows $f_1 : (S, \leq, \pi_S) \longrightarrow (T, \leq, \pi_T)$ and $f_2 : (S, \leq, \pi_S) \longrightarrow (T, \leq, \pi_T)$, their equalizer in $\mathbf{K}/(P, \leq)$ is just the subset of S given by $\{s \in S \mid \forall s' \leq s$ either $(s' \in dom(f_1) \cap dom(f_2)$ and $f_1(s') = f_2(s'))$ or $(s' \notin dom(f_1)$ and $s' \notin dom(f_2))\}$, endowed with the restriction of $\leq$ and of π_Q. Hence regular monics are injective totally defined functions.

Vice versa, if $f : (Q, \leq, \pi_Q) \longrightarrow (R, \leq, \pi_R)$ is injective and totally defined, then it is an equalizer: to see it, take its cokernel, that is take the object $(R', \leq, \pi_{R'})$ obtained from $(R, \leq, \pi_R)$ by duplicating points not in the image of f. We have two injections (which are both arrows in $\mathbf{K}/(P, \leq)$) from $(R, \leq, \pi_R)$ into $(R', \leq, \pi_{R'})$, of which f is an equalizer.

Next step is the characterization of injective objects in $\mathbf{K}/(P, \leq)$. We need some previous definitions. A sieve of a poset $(Q, \leq)$ is just a downward closed subset. An element $q \in Q$ is said to dominate a sieve S iff $S = \{q' \mid q' < q\}$ (notice that nothing prevents S from being empty). An arrow $f : (Q, \leq) \longrightarrow (R, \leq)$ in $\mathbf{K}$ always preserves domination, in the sense that if q dominates S and if $q \in dom(f)$, then $f(q)$ dominates $f(S)$. We say that f reflects domination (is *d-reflective* for short) iff for every sieve S of Q, for every $r \in R$, if r dominates $f(S)$ then there exists $q \in Q$ such that q dominates S, $q \in dom(f)$ and $f(q) = r$.

Lemma 19 An object $(I, \leq, \pi_I)$ is injective in $\mathbf{K}/(P, \leq)$ iff π_I is d-reflective.

Proof Suppose that $(I, \leq, \pi_I)$ is injective in $\mathbf{K}/(P, \leq)$, that S is a sieve of $(I, \leq)$ and that p dominates $\pi_I(S)$. Build $(I', \leq, \pi_{I'})$ just by adding a new point $*$ above S and by mapping it into p (the resulting $\pi_{I'}$ is a strict open partial map because p dominates $\pi_I(S)$). As the inclusion ι of $(I, \leq, \pi_I)$ into $(I', \leq, \pi_{I'})$ is regular monic by the previous Lemma, it must have a retract. This retract $r : (I', \leq, \pi_{I'}) \longrightarrow (I, \leq, \pi_I)$ must be a strict open partial map such that $r \circ \iota = 1_I$ (because r is a retract of ι) and such that $\pi_I \circ r = \pi_{I'}$ (because r is an arrow of $\mathbf{K}/(P, \leq)$). The first condition implies that $r(*)$ dominates S (recall that $*$ dominates S and that strict open partial maps preserve domination), whereas the second condition implies that π_I maps $r(*)$ onto p (as $\pi_{I'}(*) = p$).

Vice versa, suppose that π_I is d-reflective. Consider a regular monic $i : (Q_0, \leq, \pi_{Q_0}) \longrightarrow (Q, \leq, \pi_Q)$ and a morphism $f : (Q_0, \leq, \pi_{Q_0}) \longrightarrow (I, \leq, \pi_I)$ in $\mathbf{K}/(P, \leq)$. If we apply Lemma 20 below to $f_0 = f \circ i^{op}$, we get $\bar{f} : (Q, \leq) \longrightarrow (I, \leq)$ such that $f_0 \subseteq \bar{f}$, $\pi_I \circ \bar{f} = \pi_Q$ and $dom(\bar{f}) \subseteq dom(f_0) \cup dom(\pi_Q)$. Thus in particular $\bar{f} : (Q, \leq, \pi_Q) \longrightarrow (I, \leq, \pi_I)$ is a morphism of $\mathbf{K}/(P, \leq)$. We need only to prove that $\bar{f} \circ i = f$. As $f = f \circ i^{op} \circ i$ and as $f \circ i^{op} \subseteq \bar{f}$, we trivially have that $f \subseteq \bar{f} \circ i$. For the other inclusion, it is sufficient to prove that $dom(\bar{f} \circ i) \subseteq dom(f)$ (we are dealing with partial functions, not with arbitrary relations). If $q \in dom(\bar{f} \circ i)$, then $i(q) \in dom(\bar{f})$, i.e. either $i(q) \in dom(f \circ i^{op})$ or $i(q) \in dom(\pi_Q)$. In the former case, $q \in dom(f)$, in the latter case $q \in dom(\pi_{Q_0})$ (because $\pi_Q \circ i = \pi_{Q_0}$) and again $q \in dom(f)$, as $dom(\pi_{Q_0}) = dom(\pi_I \circ f) \subseteq dom(f)$.

Lemma 20 Let $(Q, \leq, \pi_Q)$ and $(I, \leq, \pi_I)$ be objects of $\mathbf{K}/(P, \leq)$ and let $f_0 : (Q, \leq) \longrightarrow (I, \leq)$ be a strict open partial map; suppose also that the above data satisfy the following conditions:

(i) π_I is d-reflective;

(ii) $\pi_I \circ f_0 \subseteq \pi_Q$;

(iii) for all $q \in Q$, if $q \in dom(\pi_Q) \cap dom(f_0)$, then $f_0(q) \in dom(\pi_I)$;

(iv) for all $q, q' \in Q$, if $q \in dom(f_0)$, $q' < q$ and $q' \in dom(\pi_Q)$, then $q' \in dom(f_0)$.

Then there exists a strict open partial map $\bar{f} : Q \longrightarrow I$ such that $f_0 \subseteq \bar{f}$, $\pi_I \circ \bar{f} = \pi_Q$ and $dom(\bar{f}) \subseteq dom(f_0) \cup dom(\pi_Q)$.

Proof We build an increasing sequence of strict open partial maps

$$f_0 \subset f_1 \subset \cdots \subset f_i \subset \cdots$$

satisfying (ii)-(iii)-(iv) and satisfying also the condition $dom(f_i) \subseteq dom(f_0) \cup dom(\pi_Q)$. We shall stop only when $dom(\pi_Q) \subseteq dom(f_i)$ (for this i, we shall get $\pi_I \circ f_i = \pi_Q$ from (ii)-(iii)). The process ends because our posets are finite.

Suppose, by induction, that f_i is given and that $dom(\pi_Q) \not\subseteq dom(f_i)$. Pick $q \in dom(\pi_Q)$ such that $q \notin dom(f_i)$ and such that all $q' < q$ which are in the domain of π_Q are also in the domain of f_i. Now $\pi_Q(q)$ dominates the sieve $\{\pi_Q(q') \,|\, q' < q \;\&\; q' \in dom(\pi_Q)\}$ which is equal to the sieve $\{\pi_I(f_i(q')) \,|\, q' < q \;\&\; q' \in dom(\pi_I \circ f_i)\}$, by (ii)-(iii) and the choice of q. As $\{f_i(q') \,|\, q' < q \;\&\; q' \in dom(f_i)\}$ is a sieve of I and as π_I is d-reflective, there is $x \in I$ dominating it, belonging to the domain of π_I and such that $\pi_I(x) = \pi_Q(q)$. Now build f_{i+1} by adding to f_i the pair (q, x). f_{i+1} still satisfies (ii)-(iii)-(iv) and is strict open by (iv) and the fact that $q \in dom(\pi_Q) \backslash dom(f_i)$.

Lemma 21 Suppose that $(I, \leq, \pi_I)$ is an injective object in $\mathbf{K}/(P, \leq)$ and suppose that the morphism of $\mathbf{K}/(P, \leq)$

$$h : (I, \leq, \pi_I) \longrightarrow (J, \leq, \pi_J)$$

is a surjective (though not necessarily total) map. Then $(J, \leq, \pi_J)$ is injective as well.

Proof We apply Lemma 19. Let S be a sieve of J and let p dominate $\pi_J(S)$; consider the sieve of I given by $S' = \{x \in I \,|\, \exists y \geq x \; (y \in dom(h) \;\&\; h(y) \in S)\}$. We first check that $\pi_I(S') = \pi_J(S)$. In fact $q \in \pi_I(S')$ iff

$$\exists y' \in dom(\pi_I) \; (q = \pi_I(y') \;\&\; \exists y \geq y' \; (y \in dom(h) \;\&\; h(y) \in S))$$

iff (by the fact that $dom(\pi_I) \subseteq dom(h)$, which is a consequence of $\pi_I = \pi_J \circ h$)

$$\exists y \in dom(\pi_I) \; (\pi_I(y) = q \;\&\; h(y) \in S)$$

iff (by surjectivity of h and the fact that $\pi_I = \pi_J \circ h$)

$$\exists z \in dom(\pi_J) \; (z \in S \;\&\; \pi_J(z) = q)$$

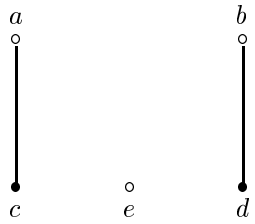
iff $q \in \pi_J(S)$, as claimed. As $(I, \leq, \pi_I)$ is injective, there exists $z \in dom(\pi_I)$ such that $\pi_I(z) = p$ and z dominates S'. It follows that $z \in dom(h)$ and that $h(z)$ dominates $h(S')$ because morphisms in $\mathbf{K}$ preserve domination. It remains to check that $h(S') = S$. In fact, $x \in h(S')$ iff

$$\exists y' \in dom(h) \; (h(y') = x \;\&\; \exists y \geq y' \; (y \in dom(h) \;\&\; h(y) \in S))$$

iff $x \in S$, by surjectivity of h.

Theorem 22 The variety of Brouwerian semilattices has stable unification type equal to ω.

Proof Every arrow in $\mathbf{K}$ factors through a partial surjection followed by the (total) inclusion of a sieve, so every unifier of a unification problem $(Q, \leq, \pi_Q)$ is less general, by Lemma 21, than the inclusion into Q of an injective sieve of Q (we say that a sieve of Q is injective iff it is an injective object in $\mathbf{K}/(P, \leq)$, with respect to the restrictions of $\leq$ and π_Q). As Q is finite, it clearly follows that the preordered set of its unifiers admits a finite μ-set. It remains to show that the stable unification type cannot be 1; for this, it is sufficient to produce $(Q, \leq, \pi_Q)$ having at least one injective sieve (this guarantees that it is unifiable), but no maximum injective sieve (notice that unifiers which are inclusions are comparable by inclusion only). An example of such a $(Q, \leq, \pi_Q)$ is given in the following diagram (we take as $(P, \leq)$ the singleton poset and use a white instead of a black point in order to mark elements which are in the domain of π_Q):



Here there are two maximal injective sieves given by the elements $\{a, c, e\}$ and $\{b, d, e\}$, respectively; their union is the total sieve which is not injective, because $\{c, d\}$ is not dominated by any element in the domain of π_Q, although its image (which is empty) is dominated by the unique element of P.

Notice that, as the singleton poset is the dual of the free Brouwerian semilattice on one generator, the proof of Theorem 22 shows that it is sufficient to add one free constant for the unification type to change from 1 to ω.

7 Appendix: related work

In this appendix we make some comparison with other standard algebraic approaches to unification theory and give further motivations for the origin of the ideas explained in section 3.

In current literature [1], [7], [15], [16] in order to deal with unification theory, the full subcategory V_E^f of V_E consisting of finitely generated free algebras is first taken into consideration. A unification problem is seen as a pair of parallel morphisms in V_E^f:

$$(*) \qquad f_1 : \mathcal{F}(Y) \longrightarrow \mathcal{F}(X), \qquad f_2 : \mathcal{F}(Y) \longrightarrow \mathcal{F}(X).$$

A solution (i.e. a unifier) for $(*)$ is any morphism u in V_E^f with domain $\mathcal{F}(X)$ such that $g \circ f_1 = g \circ f_2$. Different unifiers are compared through commutativity of the obvious

triangles. In this context, mgus becomes weak coequalizers (defined like equalizers, but without the uniqueness condition in the formulation of the universal property).

One of the main aims of a conceptual approach to symbolic problems is to get *invariance* with respect to different presentations (see [11]). From this point of view the above mentioned algebraic approach to unification represents in the same way e.g. the unification problems $t = u$ and $t' = u'$ in case we have $t =_E t'$ and $u =_E u'$. Still, however, unification problems like

$$t = u, \quad u = v$$

and

$$t = v, \quad u = v$$

which look quite the same have different representations (less trivial examples could be obtained e.g. by adding linearly dependent equations to a linear system). In fact, a pair of parallel arrows like $(*)$ simply plays the role of being *a presentation for their coequalizer*. This coequalizer in general does not belong to V_E^f because it may not be a free algebra anymore, but it is a finitely presented algebra. This suggests to consider as a unification problem *directly a fp algebra* A. Next step is to identify unifiers; as a first attempt, one could consider as a unifier any morphism $u : A \longrightarrow \mathcal{F}(Z)$ with a finitely generated free algebra as a codomain. In fact, if A is presented as the coequalizer of $(*)$, then any solution to $(*)$ must factor through A (by the definition of coequalizer) and conversely. There is still an objection to this: free algebras are characterizable through reference to the forgetful functor, whereas for fp algebras there is a neat internal categorical characterization (preservation of filtered colimits by the representable functor). Avoiding reference to free algebras would make unification type a categorical invariant and would eliminate any indirect hidden reference to some kind of presentations. The idea is that of replacing morphisms taking values into free algebras by morphisms taking values into fp *projective* algebras. This choice (which was suggested to the author by the prominent role played in intuitionistic unification by fp projective Heyting algebras [6]) does not alter the unification type because projective algebras are retract of free algebras (full details have been given in section 4). Moreover, practical experience shows that it is convenient: for instance, the examples of section 5 show that in many particular cases it is much easier to build unifiers and operate on them if we are allowed to work on projective algebras instead of on free algebras only. For instance, proof of Lemma 12 would not work if we could use free algebras only, proof of Lemma 11 would not work either in the case of pseudocomplemented distributive lattices. Even in the case of Theorems 8 and 9 some additional work would be required. In fact, this additional work is always the same in all the cases, it is simply the work needed in order to build a free algebra of which some given projective algebra is a retract. Given that, it is of course much better and clearer to directly enlarge the set of unifiers, as proposed in section 3.

References

[1] Baader, F. *Unification in Commutative Theories*, J. Symbolic Computation 8, pp. 479-497 (1989);

[2] Baader, F. *Characterizations of Unification Type Zero*, Proceeedings RTA'89, Springer LNCS 355, pp. 2-14 (1989);

[3] Baader, F., Siekmann J. H. *Unification Theory*, in Gabbay, D. M., Hogger, C. J., Robinson, J. A. (eds.) "Handbook of Logic in Artificial Intelligence and Logic Programming", Oxford University Press. pp. 41-125 (1993);

[4] Balbes R., Dwinger P. *Distributive lattices*, University of Missouri Press (1974);

[5] Burris S., Sankappanavar H.P. *A Course in Universal Algebra*, Springer-Verlag (1981);

[6] Ghilardi S. *Unification and projectivity in propositional logic*, Quaderno n.58/96, Dipartimento di Matematica, Università degli Studi di Milano (1996);

[7] Goguen J. *What is unification?*, in Aït-Kaci, H., Nivat M. (eds.) "Resolution of Equations in Algebraic Structures", vol.1, Academic Press, pp. 217-262 (1989);

[8] Gabriel P., Ulmer F. *Lokal präsentierbare Kategorien*, Springer LNM 221 (1971);

[9] Grätzer G. *Lattice Theory: first concepts and Distributive Lattices*, W.H. Freeman Co. (1971);

[10] Köhler P. *Brouwerian Semilattices*, Trans. Amer. Math. Soc., 268, pp.103-126 (1981);

[11] Lawvere, F. W. *Introduction to Part I*, in 'Model Theory and Topoi', Springer LNM 445, pp.3-14 (1975);

[12] Mac Lane, S. *Categories for the Working Mathematician*, Springer-Verlag (1971):

[13] Martin U., Nipkow T. *Boolean Unification - the story so far*, J. of Symbolic Computation 7, pp.275-293 (1989);

[14] Nipkow T. *Unification in primal algebras, their powers and their varieties*, J. Assoc. Comput. Mach. 37, pp.742-776 (1990);

[15] Nutt, W. *Unification in Monoidal Theories*, Proceedings CADE'90, Springer LNCS 449, pp. 618-632 (1990);

[16] Rydeheard, D.E., Burstall R.M. *A Categorical Unification Algorithm*, Proceedings of the Workshop on Category Theory and Computer Programming, Springer LNCS 240, pp. 493-505 (1985);

[17] Quackenbush R.W. *Demi-semi-primal algebras and Mal'cev-type conditions*, Math. Z., 122, pp.166-176 (1971);

[18] Urquhart A. *Free distributive pseudocomplemented lattices*, Algebra Universalis, 3, pp.13-15 (1973);

[19] Urquhart A. *Projective distributive p-algebras*, Bull. Austral. Math. Soc., 24, pp.269-275 (1981).

Author's address:
Silvio Ghilardi
Dipartimento di Matematica, Università degli Studi di Milano
via C. Saldini 50, 20133 Milano, Italy
e-mail: ghilardi@vmimat.mat.unimi.it