Nominal Algebra and the HSP Theorem

Murdoch J. Gabbay[1,2]

Abstract

Nominal algebra is a logic of equality developed to reason algebraically in the presence of binding. In previous work it has been shown how nominal algebra can be used to specify and reason algebraically about systems with binding, such as first-order logic, the lambda-calculus, or process calculi. Nominal algebra has a semantics in nominal sets (sets with a finitely-supported permutation action); previous work proved soundness and completeness.
The HSP theorem characterises the class of models of an algebraic theory as a class closed under homomorphic images, subalgebras, and products, and is a fundamental result of universal algebra.
It is not obvious that nominal algebra should satisfy the HSP theorem: nominal algebra axioms are subject to so-called *freshness conditions* which give them some flavour of implication; nominal sets have significantly richer structure than the sets semantics traditionally used in universal algebra. The usual method of proof for the HSP theorem does not obviously transfer to the nominal algebra setting.
In this paper we give the constructions which show that, after all, a 'nominal' version of the HSP theorem holds for nominal algebra; it corresponds to closure under homomorphic images, subalgebras, products, and an atoms-abstraction construction specific to nominal-style semantics.

Keywords: universal algebra, equational logic, nominal algebra, HSP or Birkhoff's theorem, nominal sets, nominal terms

1 Introduction

Algebra is the logic of equality. It has the virtue of simplicity; axioms assert equalities between terms, validity of equality is interpreted by identity in models, and two equal terms can be replaced in any context since they must denote the same element in all models. This simplicity also has benefits in the theory of models: every model of an algebraic theory can be exhibited as a homomorphic image of a subalgebra of a product of free algebras (for definitions see elsewhere [BS81] or Subsection 8). This result was first proved by Birkhoff [Bir35]. It is called *Birkhoff's theorem* [BS81, Theorem 11.12] — and also the **HSP** theorem (Homomorphism, Subalgebra, Product). We shall call it the HSP theorem, since Birkhoff's name is attached to several other results.

The HSP theorem is a useful source of negative results. To prove that a class of structures over a signature cannot be characterised in algebra it suffices to exhibit, for example, some structures in the class whose product is not in that class. For

[1] Homepage: `http://www.gabbay.org.uk`

[2] Thanks to Aad Mathijssen and to the anonymous referees. Supported by grant RYC-2006-002131 at the Polytechnic University of Madrid.

example we obtain a one-line proof that 'has precisely two elements' cannot be characterised in algebra since the product of a two-element set with itself has four elements. The HSP theorem also guarantees that we can factor out complexity, in much the same way that the fundamental theorem of arithmetic guarantees we can factor large numbers into products of primes. Specific instances include the Stone representation theorem for Boolean algebras, and the decomposition of groups into products of simple groups.

The HSP theorem can be useful for the study of logic and computation, as has been demonstrated for example by Salibra [MS06,Sal03] using combinators ($Sxyz = (xz)(yz)$ and $Kxy = x$).

Reasoning about systems with binding is somewhat resistent to algebraic treatments. Consider for example the following 'equalities' which arise naturally in informal practice:

λ-calculus:	$\lambda x.(tx) = t$	if $x \notin fv(t)$
First-order logic:	$\forall x.(\phi \Rightarrow \psi) = \phi \Rightarrow \forall x.\psi$	if $x \notin fv(\phi)$
π-calculus:	$\nu x.(P \mid Q) = P \mid \nu x.Q$	if $x \notin fv(P)$

Here $fv(t)$ denotes the free variables of t. It is easy to extend this list with more examples. Difficulties arise treating these 'equalities' algebraically. Firstly, there are *two* levels of variable:

- x and y are variables of the system being axiomatised, we call these *object-level* variables.
- t, u, ϕ, ψ, P, and Q range over terms of that system's syntax, we call them *meta-level* variables.

Equalities are subject to freshness side-conditions $x \notin fv(t)$. The two levels of variable, and the freshness conditions, make it impossible to translate informal 'equalities' like those above directly into universal algebra. Formalisation of such systems in the traditional algebraic framework can require a fair amount of emulation.

We recall De Bruijn's words [dB91]:

> "I think that in formalizing mathematics, and in particular in preparing mathematics for justification, it is usually elegant as well as efficient to do everything in the *natural* way."

Nominal Algebra [GM07a,Mat07] is a logic of equality which represents the two-level variable structure and freshness conditions noted above directly in its syntax. It uses a semantics in nominal sets [GP01]. Informal equalities can often be represented almost symbol-for-symbol. For example the equalities above are represented by the following axioms in nominal algebra:

λ-calculus:	$a\#X \vdash$	$\lambda[a](Xa) = X$
First-order logic:	$a\#X \vdash$	$\forall[a](X \Rightarrow Y) = X \Rightarrow \forall[a]Y$
π-calculus:	$a\#X \vdash$	$\nu[a](X \mid Y) = X \mid \nu[a]Y$

Here a and b are distinct *atoms* representing object-level variables; X and Y are distinct *unknowns* representing meta-level variables; $[a]t$ is an abstraction of an atom a in a term t. Each equality is equipped with a *freshness condition* of the form $a\#X$ that guarantees that X can only be instantiated to a term for which a is fresh.

Nominal algebra has been used to axiomatise substitution [GM08] and first-order logic [GM07b]. Also in other work [UPG04,FG07,CU03], nominal techniques have proved their ability to be 'ϵ away from informal practice', following de Bruijn's philosophy while remaining mathematically completely rigorous.

In this paper we fill an important gap in the foundational theory of nominal algebra; nominal algebra does indeed satisfy a version of the HSP theorem (Theorem 9.3). The HSP result is extended in an interesting way to include nominal abstractions; we give full details in the rest of the paper.

It is not obvious that the HSP result holds for nominal algebra: freshness side-conditions give nominal algebra axioms a flavour of implication (this undermines closure under homomorphic images), and nominal sets have structure which 'normal sets' do not. An attempt to directly transfer proofs of the HSP theorem to the nominal setting [BS81] fails. HSP is a fundamental result in universal algebra; nominal algebra should satisfy a version of it, to fully earn its name 'algebra'.

The constructions to prove the nominal HSP theorem are subtle and interesting. The fact that this holds gives a precise mathematical sense in which nominal algebra can be viewed as a continuation of the long mathematical tradition of universal algebra. We hope that HSP will be as useful to the algebraic study of logic and computation using nominal techniques, as it has been in universal algebra.

2 Nominal Algebra Syntax

Definition 2.1 Fix a countably infinite collection of **atoms** $a, b, c, \ldots$. We shall use a *permutative convention* that $a, b, c, \ldots$ range permutatively over atoms, so that for example a and b are always distinct. Fix a countably infinite collection of **unknowns** $X, Y, Z, \ldots$. Fix **term-formers** f to each of which is associated some unique **arity** n which is a nonnegative number. Assume these collections are disjoint. A **signature** Σ is some set of term-formers.

Definition 2.2 Let π range over **(finitely supported) permutations**. So π bijects atoms with themselves and there is a finite set of atoms S such that $\pi(a) = a$ for all atoms *not* in S. Write id for the identity permutation such that $id(a) = a$ always. Write $\pi \circ \pi'$ for functional composition and write π^{-1} for inverse. Write $\mathbb{P}$ for the set of all permutations.

It is easy to check that permutations with id and functional composition form a group.

Definition 2.3 Let **nominal terms** t, u, v in some signature Σ be:

$$t \quad ::= \quad a \;\mid\; [a]t \;\mid\; \pi \cdot X \;\mid\; \mathsf{f}(t_1, \ldots, t_n),$$

where $\mathsf{f} : n$ ranges over the elements of Σ.

We write $id \cdot X$ just as X, for brevity.

Definition 2.4 Write $t \equiv u$ for **syntactic identity** of terms. Let $a \in t$ be inductively defined by:

$$a \in a \qquad \frac{\pi(a) \neq a}{a \in \pi \cdot X} \qquad \frac{a \in t_i \quad (1 \leq i \leq n)}{a \in \mathsf{f}(t_1, \ldots, t_n)} \qquad \frac{a \in t}{a \in [b]t} \qquad a \in [a]t$$

If $a \in t$ then we say that 'a **occurs in** (the syntax of) t'. Let $X \in t$ be inductively defined by:

$$X \in \pi \cdot X \qquad \frac{X \in t_i \quad (1 \leq i \leq n)}{X \in \mathsf{f}(t_1, \ldots, t_n)} \qquad \frac{X \in t}{X \in [a]t}$$

If $X \in t$ then we say that 'X **occurs in** (the syntax of) t'. Similarly write $a \notin t$ and $X \notin t$ for 'does not occur in the syntax of t'.

Definition 2.5 A **freshness (assertion)** is a pair $a\#t$ of an atom a and a term t. An **equality (assertion)** is a pair $t = u$ where t and u are terms. Call a freshness of the form $a\#X$ (so $t \equiv X$) **primitive**. Write Δ for a finite set of *primitive* freshnesses and call it a **freshness context**. We drop set brackets in freshness contexts, e.g. writing $a\#X, b\#Y$ for $\{a\#X, b\#Y\}$.

Definition 2.6 Nominal algebra has two **judgement forms**, a pair $\Delta \vdash a\#t$ of a freshness context and a freshness assertion, and a pair $\Delta \vdash t = u$ of a freshness context and an equality assertion. We may write $\emptyset \vdash a\#t$ as $\vdash a\#t$ and $\emptyset \vdash t = u$ as $\vdash t = u$.

A **theory** $\mathsf{T} = (\Sigma, Ax)$ is a pair of a signature Σ and a possibly infinite set of *equality* judgement forms Ax in that signature; we call them the **axioms**.

A motivation of these definitions, with example theories, is elsewhere [GM07a].

3 A Derivation System

Now we need a notion of derivation which represents freshness assumptions on metavariables, and permits axioms involving abstraction and conditioned on freshness assumptions, just like we do in informal reasoning.

Definition 3.1 We define a **permutation action** $\pi \cdot t$ by:

$$\pi \cdot a \equiv \pi(a) \qquad \pi \cdot (\pi' \cdot X) \equiv (\pi \circ \pi') \cdot X \qquad \pi \cdot [a]t \equiv [\pi(a)]\pi \cdot t$$
$$\pi \cdot \mathsf{f}(t_1, \ldots, t_n) \equiv \mathsf{f}(\pi \cdot t_1, \ldots, \pi \cdot t_n)$$

Lemma 3.2 $\pi \cdot (\pi' \cdot t) \equiv (\pi \circ \pi') \cdot t$ *and* $id \cdot t \equiv t$.

Proof. By an easy induction on the structure of t. □

Definition 3.3 A **substitution** σ is a finitely supported function from unknowns to terms. Here, finite support means: for some finite set of unknowns $\sigma(X) \not\equiv X$, and for all other unknowns $\sigma(X) \equiv X$. Write $[t_1/X_1, \ldots, t_n/X_n]$ for the substitution σ such that $\sigma(X_i) \equiv t_i$ and $\sigma(Y) \equiv Y$, for all $Y \not\equiv X_i$ and all $1 \leq i \leq n$.

Definition 3.4 We define a **substitution action** $t\sigma$ on terms by:

$$a\sigma \equiv a \qquad (\pi \cdot X)\sigma \equiv \pi \cdot \sigma(X) \qquad ([a]t)\sigma \equiv [a]t\sigma$$
$$\mathsf{f}(t_1, \ldots, t_n)\sigma \equiv \mathsf{f}(t_1\sigma, \ldots, t_n\sigma)$$

We need this result for later:

Lemma 3.5 $\pi \cdot (t\sigma) \equiv (\pi \cdot t)\sigma$.

Proof. By a routine induction on syntax. We consider only the case of $t \equiv \pi' \cdot X$:

$$\begin{aligned} \pi \cdot ((\pi' \cdot X)\sigma) &\equiv \pi \cdot (\pi' \cdot \sigma(X)) && \text{Definition} \\ &\equiv (\pi \circ \pi') \cdot \sigma(X) && \text{Lemma 3.2} \end{aligned}$$

$$\begin{aligned} (\pi \cdot (\pi' \cdot X))\sigma &\equiv ((\pi \circ \pi') \cdot X)\sigma && \text{Definition} \\ &\equiv (\pi \circ \pi') \cdot \sigma(X) && \text{Definition.} \end{aligned}$$

For further details see elsewhere [UPG04,Mat07]. □

Definition 3.6 Let the **derivable** freshnesses by inductively defined by the rules in Figure 1. Here in accordance with our permutative convention a and b range over *distinct* atoms. We may abbreviate '$\Delta \vdash a\#t$ is derivable' to '$\Delta \vdash a\#t$'.

Definition 3.7 Let **derivations** be inductively defined by the rules in Figure 2.

Suppose that $\mathsf{T} = (\Sigma, Ax)$. We say that Π is a derivation **in** T when the following two conditions are satisfied:

- Π mentions only terms in the signature Σ.
- Π mentions only instances of $(ax_{\Delta' \vdash t=u})$ such that $(\Delta' \vdash t = u) \in Ax$ (if any).

We call $\Delta \vdash t = u$ **derivable in** T when a derivation Π exists in T concluding in $\Delta \vdash t = u$. (Note that in particular, if $\Delta \vdash t = u$ is derivable in T then t and u must be terms in the signature Σ.)

We may abbreviate '$\Delta \vdash t = u$ is derivable in T' to '$\Delta \vdash_{\mathsf{T}} t = u$'.

Definition 3.8 Fix a signature Σ. Call a term **ground** (in Σ) when it does not mention unknowns (and mentions only term-formers in Σ). We let variables named g and h range over ground terms; these are inductively characterised by

$$g, h, g', h' ::= a \mid [a]g \mid \mathsf{f}(g, \ldots, g)$$

Here f ranges over elements of Σ.

Call a derivation **ground** (in Σ) when:

- It does not mention any unknowns (so all terms in it are ground terms and it uses no instance of $(\#X)$ or (fr)).
- It mentions only term-formers in Σ.

We conclude this section with Theorems 3.11 and 3.13. These are two basic results about derivations and derivability which will be useful later.

$$\frac{}{\Delta \vdash a\#b}\,(\#ab) \qquad \frac{(\pi^{-1}(a)\#X \in \Delta)}{\Delta \vdash a\#\pi \cdot X}\,(\#X) \qquad \frac{\Delta \vdash a\#t_1 \;\cdots\; \Delta \vdash a\#t_n}{\Delta \vdash a\#\mathsf{f}(t_1,\ldots,t_n)}\,(\#\mathsf{f})$$

$$\frac{}{\Delta \vdash a\#[a]t}\,(\#[]a) \qquad \frac{\Delta \vdash a\#t}{\Delta \vdash a\#[b]t}\,(\#[]b)$$

Fig. 1. Derivation rules for freshness

$$\frac{}{\Delta \vdash t = t}\,(\mathit{refl}) \qquad \frac{\Delta \vdash t = u}{\Delta \vdash u = t}\,(\mathit{symm}) \qquad \frac{\Delta \vdash t = u \quad \Delta \vdash u = v}{\Delta \vdash t = v}\,(\mathit{tran})$$

$$\frac{\Delta \vdash \pi(a)\#\pi \cdot \sigma(X) \quad \text{for every } a\#X \in \Delta'}{\Delta \vdash \pi \cdot t\sigma = \pi \cdot u\sigma}\,(ax_{\Delta' \vdash t=u})$$

$$\frac{\Delta \vdash t = u}{\Delta \vdash [a]t = [a]u}\,(\mathit{cong}[]) \qquad \frac{\Delta \vdash t = u}{\Delta \vdash \mathsf{f}(\ldots,t,\ldots) = \mathsf{f}(\ldots,u,\ldots)}\,(\mathit{cong}\mathsf{f})$$

$$\frac{\Delta, a\#X \vdash t = u \quad (a \notin t,u)}{\Delta \vdash t = u}\,(\mathit{fr}) \qquad \frac{\Delta \vdash a\#t \quad \Delta \vdash b\#t}{\Delta \vdash (a\ b)\cdot t = t}\,(\mathit{perm})$$

Fig. 2. Derivation rules for equality

Definition 3.9 Let $\mathcal{X}$ be a finite set of unknowns. Take c to be any atom. Let σ be the substitution such that $\sigma(X) = c$ for every $X \in \mathcal{X}$ and $\sigma(Y) = Y$ for all other Y.

We inductively define a translation 'Π translates to $\Pi\sigma$' on derivations Π that do not mention c, and that mention only unknowns in $\mathcal{X}$, as follows:

- The rule $(\#X)$. Suppose that $\pi^{-1}(a)\#X \in \Delta$. Then

$$\Pi \;=\; \frac{(\pi^{-1}(a)\#X \in \Delta)}{\Delta \vdash a\#\pi \cdot X}\,(\#X) \qquad \text{translates to} \qquad \Pi\sigma \;=\; \frac{}{\vdash a\#c}\,(\#ab).$$

- The rule (fr).

$$\Pi \;=\; \frac{\begin{array}{c}\vdots\,\Pi'\\ \Delta, a\#X \vdash t = u\end{array}}{\Delta \vdash t = u}\,(\mathit{fr}) \qquad \text{translates to} \qquad \Pi\sigma \;=\; \frac{\begin{array}{c}\vdots\,\Pi'\sigma\\ \vdash t\sigma = u\sigma\end{array}}{}$$

- The rule (perm).

$$\Pi \;=\; \frac{\begin{array}{cc}\vdots\,\Pi' & \vdots\,\Pi''\\ \Delta \vdash a\#t & \Delta \vdash b\#t\end{array}}{\Delta \vdash (a\ b)\cdot t = t}\,(\mathit{perm}) \text{ translates to } \Pi\sigma \;=\; \frac{\begin{array}{cc}\vdots\,\Pi'\sigma & \vdots\,\Pi''\sigma\\ \vdash a\#t\sigma & \vdash b\#t\sigma\end{array}}{\vdash (a\ b)\cdot t\sigma = t\sigma}\,(\mathit{perm})$$

(Recall that by Lemma 3.5 $((a\ b)\cdot t)\sigma \equiv (a\ b)\cdot(t\sigma)$.)

- Other cases are routine.

Lemma 3.10 *Suppose that* $\mathsf{T} = (\Sigma, Ax)$. *Let* Π *be a derivation of* $\vdash g = h$ *in* T. *Let* $\mathcal{X}$ *be the (finite) set of unknowns mentioned in* Π. *Let* c *be an atom not mentioned in* Π. *Let* σ *be the substitution such that* $\sigma(X) = c$ *for every* $X \in \mathcal{X}$ *and* $\sigma(Y) = Y$ *for all other* Y.

Then $\Pi\sigma$ *(Definition 3.9) is a derivation of* $\vdash t\sigma = u\sigma$. *Furthermore,* $\Pi\sigma$ *mentions only ground terms (it does not mention any unknowns).*

Proof. Definition 3.9 is designed to make this true. The proof is by a routine induction on Π. □

Theorem 3.11 *Suppose that* $\mathsf{T} = (\Sigma, Ax)$. *If* $\vdash_{\mathsf{T}} g = h$, *and if* g *and* h *are ground terms, then a ground derivation exists for* $\vdash g = h$ *in* T.

Proof. Let Π be any derivation of $\vdash_{\mathsf{T}} g = h$. Let $\mathcal{X}$ be the unknowns mentioned in Π. Let c be any atom not mentioned in Π. Let σ be the substitution such that $\sigma(X) = c$ for every $X \in \mathcal{X}$ and $\sigma(Y) = Y$ for all other Y. It follows by Lemma 3.10 that $\Pi\sigma$ is a ground derivation of $\vdash g\sigma = h\sigma$. Since g and h are ground, $g\sigma \equiv g$ and $h\sigma \equiv h$. The result follows. □

Definition 3.12 Let π and π' be two permutations. Write

$$\mathrm{ds}(\pi, \pi') \quad \text{for the set} \quad \{a \mid \pi(a) \neq \pi'(a)\},$$

the **difference set** of π and π'. We write $\Delta \vdash \mathrm{ds}(\pi, \pi')\#t$ for a set of proof-obligations $\Delta \vdash a\#t$, one for each $a \in \mathrm{ds}(\pi, \pi')$.

Theorem 3.13 *If* $\Delta \vdash \mathrm{ds}(\pi, \pi')\#t$ *then* $\Delta \vdash_{\mathsf{T}} \pi \cdot t = \pi' \cdot t$.

Proof. By induction on the number of elements in $\mathrm{ds}(\pi, \pi')$; the base case follows by (*refl*). □

4 Nominal Sets

A model of a nominal algebra theory T is a nominal set which interprets the term-formers so as to make the axioms valid. We use *nominal* sets [GP01] because they permit a direct semantic interpretation of freshness judgements $a\#x$ and permutations $\pi \cdot x$, an interpretation which is not conveniently definable on 'ordinary' sets.

4.1 Basic definitions

Definition 4.1 A **nominal set** $\mathbb{X}$ is a pair $(|\mathbb{X}|, \cdot)$ of a(n ordinary) set $|\mathbb{X}|$ with a $\mathbb{P}$-group action such that each $x \in \mathbb{X}$ has **finite support**, where:

- A $\mathbb{P}$-group action $\cdot$ is a function $\mathbb{P} \times |\mathbb{X}| \to |\mathbb{X}|$ such that for all $x \in |\mathbb{X}|$ and all permutations π and π',

$$id \cdot x = x \quad \text{and} \quad \pi \cdot (\pi' \cdot x) = (\pi \circ \pi') \cdot x.$$

- 'Finite support' means there is some finite set of atoms $\mathcal{A}$ such that

$$\text{if } \pi \in \mathbb{P} \text{ and } \pi(a) = a \text{ for every } a \in \mathcal{A}, \text{ then } \pi \cdot x = x.$$

We write $x \in \mathbb{X}$ as shorthand for $x \in |\mathbb{X}|$ and call x an **element** of $\mathbb{X}$.

In [GP01, Proposition 3.4] it is shown that if an element $x \in \mathbb{X}$ has finite support, then there is a unique least finite set of atoms that supports x.

Definition 4.2 When $x \in \mathbb{X}$ has a finite supporting set, call the least set of atoms supporting x the **support** of x, and write it as $supp(x)$.

We write $a\#x$ (read 'a fresh for x') when $a \notin supp(x)$.

Example 4.3 The set $\mathbb{A}$ of all atoms with action $\pi \cdot a = \pi(a)$ is a nominal set; the support of $a \in \mathbb{A}$ is $\{a\}$. Note that for $x, y \in \mathbb{A}$, $x\#y$ when $x \neq y$.

4.2 Equivariant functions

Definition 4.4 Suppose that $\mathbb{X}_1, \ldots, \mathbb{X}_n, \mathbb{Y}$ are nominal sets. Call a function $f \in (|\mathbb{X}_1| \times \ldots \times |\mathbb{X}_n|) \to |\mathbb{Y}|$ **equivariant** when

$$\pi \cdot f(x_1, \ldots, x_n) = f(\pi \cdot x_1, \ldots, \pi \cdot x_n)$$

for all $x_1 \in |\mathbb{X}_1|, \ldots, x_n \in |\mathbb{X}_n|$.

Lemma 4.5 *Suppose $\mathbb{X}_1, \ldots, \mathbb{X}_n, \mathbb{Y}$ are nominal sets and $f \in (|\mathbb{X}_1| \times \ldots \times |\mathbb{X}_n|) \to |\mathbb{Y}|$ is equivariant. Then*

$$supp(f(x_1, \ldots, x_n)) \subseteq (supp(x_1) \cup \ldots \cup supp(x_n)).$$

As a corollary, $a\#x_i$ for $1 \leq i \leq n$ implies $a\#f(x_1, \ldots, x_n)$.

Proof. By Definition 4.4 $\pi \cdot f(x_1, \ldots, x_n) = f(\pi \cdot x_1, \ldots, \pi \cdot x_n)$, so if $\pi \cdot x_i = x_i$ for $1 \leq i \leq n$ then $\pi \cdot f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$. The result follows.

The corollary is immediate. □

4.3 Products

Lemma 4.6 *Basic results of nominal sets are:*

(i) $supp(x) = \{a \in \mathbb{A} \mid \{b \in \mathbb{A} \mid (a\ b) \cdot x \neq x\}$ *is not finite*$\}$.

(ii) *If $a\#x$ for every $a \in \mathrm{ds}(\pi, \pi')$ (Definition 3.12) then $\pi \cdot x = \pi' \cdot x$.*

(iii) *If $a\#x$ then $\pi(a)\#\pi \cdot x$.*

Proof. Elsewhere [GP01, Proposition 3.4] and by easy calculations. □

Definition 4.7 Let I be a countably infinite indexing set and $(\mathbb{X}_i)_{i \in I}$ an I-indexed collection of nominal sets. Write $\Pi_{i \in I}\mathbb{X}_i$ for the nominal set with underlying set those I-tuples $(x_i)_{i \in I} \in \Pi_{i \in I}|\mathbb{X}_i|$ such that there exists some finite set of atoms A such that $supp(x_i) \subseteq A$ for all $i \in I$.

We give this the component-wise permutation action, so $\pi \cdot (x_i)_{i\in I} = (\pi \cdot x_i)_{i\in I}$; it is not hard to prove that all $(x_i)_{i\in I} \in \Pi_{i\in I}\mathbb{X}_i$ have finite support.

We write $\mathbb{X}^n$ for $\Pi_{i\in\{1,\ldots,n\}}\mathbb{X}_i$ where $\mathbb{X}_i = \mathbb{X}$ for $1 \leq i \leq n$.

($\Pi_{i\in I}\mathbb{X}_i$ is the product object in the category of nominal sets [GP01].)

Lemma 4.8 *$a\#(x_i)_{i\in I}$ if and only if $a\#x_i$ for every $i \in I$.*

Proof. By an easy calculation using part i of Lemma 4.6 (see [GP01]). □

4.4 Sets

Subsets of (the underlying set of) a nominal set will be important later when we build free algebras.

Definition 4.9 $\mathcal{X} \subseteq |\mathbb{X}|$ inherits a **pointwise** permutation action

$$\pi \cdot \mathcal{X} = \{\pi \cdot x \mid x \in \mathcal{X}\}.$$

We will always use the pointwise action on $\mathcal{X} \subseteq |\mathbb{X}|$.

$a\#\mathcal{X}$ does *not* imply that $a\#x$ for every $x \in \mathcal{X}$. For example $\mathbb{A} \subseteq \mathbb{A}$ and it is a fact that $a\#\mathbb{A}$ — but $a \in \mathbb{A}$ and not $a\#a$. Furthermore $\mathcal{X} \subseteq |\mathbb{X}|$ does *not* imply that $\mathcal{X}$ is finitely supported. For example if we order $\mathbb{A}$ as $\{a_1, a_2, a_3, \ldots\}$ then it is a fact that $\{a_1, a_3, a_5, \ldots\}$ is not finitely supported. However, the finitely-supported subsets of $|\mathbb{X}|$ form a nominal set — they have a permutation action, and by construction they are finitely supported.

Lemma 4.10 *Suppose $\mathbb{X}$ is a nominal set and $\mathcal{X} \subseteq |\mathbb{X}|$ is finitely-supported. Suppose that $a_1\#\mathcal{X}, \ldots, a_n\#\mathcal{X}$. There exists some $x \in \mathcal{X}$ such that $a_1\#x, \ldots, a_n\#x$.*

Proof. Choose any $x \in \mathcal{X}$. Let $b_1, \ldots, b_n$ be fresh (so $b_i\#\mathcal{X}$ and $b_i\#x$ for $1 \leq i \leq n$). By part ii of Lemma 4.6 $(b_1\ a_1) \cdots (b_n\ a_n) \cdot \mathcal{X} = \mathcal{X}$. Write $y = (b_1\ a_1) \cdots (b_n\ a_n) \cdot x$. By Definition 4.9 $y \in \mathcal{X}$ and we conclude $a_i\#y$ for $1 \leq i \leq n$ by part iii of Lemma 4.6 and the assumption $b_i\#x$. □

Further discussion of nominal sets is elsewhere [GP01].

5 Semantics

We use nominal sets to give a semantics to nominal algebra signatures and theories:

Definition 5.1 A **Σ-algebra** $\mathbb{X}$ consists of the following data:

- An **underlying nominal set** $\mathbb{X} = (|\mathbb{X}|, \cdot)$.
- An equivariant map $\text{-}_{\mathbb{X}} \in \mathbb{A} \to |\mathbb{X}|$ to interpret atoms; we write $a_{\mathbb{X}} \in \mathbb{X}$.
- An equivariant map $abs_{\mathbb{X}} \in \mathbb{A} \times \mathbb{X} \to \mathbb{X}$ such that $a\#abs_{\mathbb{X}}(a, x)$ always, to interpret abstraction.
- An equivariant map $\mathsf{f}_{\mathbb{X}} \in |\mathbb{X}^n| \to |\mathbb{X}|$ for each term-former $\mathsf{f} : n \in \Sigma$ to interpret term-formers.

We tend to write $\mathbb{X}$ and $\mathbb{Y}$ for Σ-algebras.

Definition 5.2 Consider a Σ-algebra $\mathbb{X}$. A **valuation** ς in $\mathbb{X}$ maps unknowns X to elements $\varsigma(X) \in |\mathbb{X}|$. Suppose that t is a term in Σ. The **interpretation** $[\![t]\!]^{\mathbb{X}}_{\varsigma}$, or just $[\![t]\!]_{\varsigma}$ if $\mathbb{X}$ is understood, is defined inductively by:

$$[\![a]\!]_{\varsigma} = a_{\mathbb{X}} \qquad [\![\pi \cdot X]\!]_{\varsigma} = \pi \cdot \varsigma(X) \qquad [\![[a]t]\!]_{\varsigma} = abs_{\mathbb{X}}(a,[\![t]\!]_{\varsigma})$$
$$[\![\mathsf{f}(t_1,\ldots,t_n)]\!]_{\varsigma} = \mathsf{f}_{\mathbb{X}}([\![t_1]\!]_{\varsigma},\ldots,[\![t_n]\!]_{\varsigma})$$

Interpretations are equivariant:

Lemma 5.3 *Suppose that $\mathbb{X}$ is a Σ-algebra and ς is a valuation to $|\mathbb{X}|$. Then $\pi \cdot [\![t]\!]_{\varsigma} = [\![\pi \cdot t]\!]_{\varsigma}$ for any π.*

Proof. By induction on the structure of t, using Lemma 4.5 for the cases of a, $[a]t$ and $\mathsf{f}(t_1,\ldots,t_n)$. □

Definition 5.4 Suppose that $\mathbb{X}$ is a Σ-algebra. Define a notion of **validity** by:

$$[\![\Delta]\!]_{\varsigma} \text{ (\textbf{is valid}) when } a\#\varsigma(X) \text{ for each } a\#X \in \Delta$$
$$[\![\Delta \vdash a\#t]\!]_{\varsigma} \text{ when } [\![\Delta]\!]_{\varsigma} \text{ implies } a\#[\![t]\!]_{\varsigma}$$
$$[\![\Delta \vdash t = u]\!]_{\varsigma} \text{ when } [\![\Delta]\!]_{\varsigma} \text{ implies } [\![t]\!]_{\varsigma} = [\![u]\!]_{\varsigma}$$

Definition 5.5 Suppose that $\mathsf{T} = (\Sigma, Ax)$. A **model of** T is a Σ-algebra $\mathbb{X}$ such that $[\![\Delta \vdash t = u]\!]_{\varsigma}$ for every axiom $\Delta \vdash t = u$ in Ax and every valuation ς.

The nominal sets semantics for nominal algebra is **sound** ([GM07a,Mat07]):

Theorem 5.6 (Soundness) *Suppose $\mathsf{T} = (\Sigma, Ax)$ is a theory, $\mathbb{X}$ is a Σ-algebra which is a model of T, and ς is a valuation to $|\mathbb{X}|$. Then:*

- *If $\Delta \vdash a\#t$ then $[\![\Delta \vdash a\#t]\!]_{\varsigma}$ is valid.*
- *If $\Delta \vdash_{\mathsf{T}} t = u$ then $[\![\Delta \vdash t = u]\!]_{\varsigma}$ is valid.*

Proof. We work by induction on the length of derivations (Figures 1 and 2):

- $(\#ab)$. We must show $a\#b_{\mathbb{X}}$. By Lemma 4.5 this follows from $a\#b$, which is a standard property of freshness (see Example 4.3).
- $(\#X)$. By inductive hypothesis we know $\pi^{-1}(a)\#\varsigma(X)$. By part iii of Lemma 4.6 we conclude $a\#\pi \cdot \varsigma(X)$.
- $(\#[]a)$. $a\#abs(a,[\![t]\!]_{\varsigma})$ holds by assumption.
- $(\#[]b)$. By Lemmas 4.5 and 4.8 and by the fact that $a\#b$, we have that $a\#[\![t]\!]_{\varsigma}$ implies $a\#abs(b,[\![t]\!]_{\varsigma})$.
- $(\#\mathsf{f})$. If $a\#[\![t_1]\!]_{\varsigma}$, …, $a\#[\![t_n]\!]_{\varsigma}$ then by Lemma 4.5 $a\#([\![t_1]\!]_{\varsigma},\ldots,[\![t_n]\!]_{\varsigma})$ and we conclude $a\#\mathsf{f}_{\mathbb{X}}([\![t_1]\!]_{\varsigma},\ldots,[\![t_n]\!]_{\varsigma})$ using Lemma 4.8.
- $(refl)$, $(symm)$, $(tran)$, $(cong[])$, $(cong\mathsf{f})$. By properties of equality.
- $(perm)$. By part ii of Lemma 4.6, $a\#[\![t]\!]_{\varsigma}$ and $b\#[\![t]\!]_{\varsigma}$ imply $(a\ b) \cdot [\![t]\!]_{\varsigma} = [\![t]\!]_{\varsigma}$. We conclude $[\![(a\ b) \cdot t]\!]_{\varsigma} = [\![t]\!]_{\varsigma}$ by Lemma 5.3.
- $(ax_{\Delta' \vdash t=u})$. It suffices to show that if $\pi(a)\#[\![\pi \cdot \sigma(X)]\!]_{\varsigma}$ for every $a\#X \in \Delta'$ then $[\![\pi \cdot t\sigma]\!]_{\varsigma} = [\![\pi \cdot u\sigma]\!]_{\varsigma}$.

So suppose $\pi(a)\#[\![\pi \cdot \sigma(X)]\!]_\varsigma$ for every $a\#X \in \Delta'$. By Lemma 5.3 and part iii of Lemma 4.6 also $a\#[\![\sigma(X)]\!]_\varsigma$ for all $a\#X \in \Delta'$. Define ς' by $\varsigma'(X) = [\![\sigma(X)]\!]_\varsigma$ for all X. Then $a\#\varsigma'(X)$ for all $a\#X \in \Delta'$, that is, $[\![\Delta']\!]_{\varsigma'}$ holds. $\Delta' \vdash t = u$ is an axiom of T so $[\![t]\!]_{\varsigma'} = [\![u]\!]_{\varsigma'}$ holds. Using Lemma 5.3 we deduce that $[\![\pi \cdot t]\!]_{\varsigma'} = [\![\pi \cdot u]\!]_{\varsigma'}$. By a straightforward induction on syntax we can verify that $[\![\pi \cdot t]\!]_{\varsigma'} = [\![\pi \cdot t\sigma]\!]_\varsigma$ and $[\![\pi \cdot u]\!]_{\varsigma'} = [\![\pi \cdot u\sigma]\!]_\varsigma$, and we conclude $[\![\pi \cdot t\sigma]\!]_\varsigma = [\![\pi \cdot u\sigma]\!]_\varsigma$.

- The case of (fr). Suppose that $[\![\Delta]\!]_\varsigma$ is valid and Π is a derivation of $a\#X, \Delta \vdash_{\mathsf{T}} t = u$.

  If $a\#\varsigma(X)$ then $[\![a\#X, \Delta]\!]_\varsigma$ is valid and by hypothesis $[\![t = u]\!]_\varsigma$ is valid and we are done.

  Suppose $a \in \mathit{supp}(\varsigma(X))$. Choose some a' such that $a'\#\varsigma(X)$ and also $a'\#\varsigma(Y)$ for every $a\#Y \in \Delta$. Write Δ' for Δ with every $a\#Y \in \Delta$ replaced by $a'\#Y$. Then $\Delta' \vdash_{\mathsf{T}} t = u$; we obtain a derivation by replacing every a in Π by a', to obtain a derivation Π'. Now $[\![a'\#X, \Delta]\!]_\varsigma$ is valid and Π' is no longer than Π. Therefore $[\![t = u]\!]_\varsigma$ is valid as required.

□

The nominal sets semantics for nominal algebra is **complete**:

Theorem 5.7 *Fix a theory $\mathsf{T} = (\Sigma, Ax)$ and an equality-in-context $\Delta \vdash t = u$ where t and u are nominal terms in the signature Σ.*

Suppose that for all models $\mathbb{V}$ of T and all valuations ς to $|\mathbb{V}|$, if $[\![\Delta]\!]_\varsigma$ is valid then $[\![t]\!]^{\mathbb{V}}_\varsigma = [\![u]\!]^{\mathbb{V}}_\varsigma$. Then $\Delta \vdash_{\mathsf{T}} t = u$.

Proof. See [GM07a] or (for full details) see [Mat07]. □

6 Free algebras

The usual technique to obtain models for a theory is to add constant symbols to the language and to quotient the set of terms by provable equality — the extra constant symbols ensures there are 'enough elements' in the model. In nominal algebra constants have empty support; if d has arity 0 then $\vdash a\#\mathsf{d}$ is derivable for any a. Adding extra constant symbols only ensures a supply of elements with empty support. Therefore, we add extra term-formers which may have arity greater than 0. This is consistent with methods employed in previous work, see for example [Gab07, Theorem 9.3] and [GM07a, Section 5].

6.1 Ground terms

Fix a signature Σ and $\mathcal{D}$ a possibly infinite set of term-formers disjoint from Σ (the 'extra term-formers' mentioned above).

Definition 6.1 Let **ground terms** $\mathbb{F}(\Sigma, \mathcal{D})$ be inductively generated by

$$g \quad ::= \quad a \mid [a]g \mid \mathsf{f}(g_1, \ldots, g_n) \mid \mathsf{d}(a_1, \ldots, a_m).$$

Here $\mathsf{f} : n$ ranges over elements of Σ, and $\mathsf{d} : m$ ranges over elements of $\mathcal{D}$. Give this

a permutation action $\pi \cdot g$ as in Definition 3.1; in full:

$$\pi \cdot a \equiv \pi(a) \qquad \pi \cdot \mathsf{f}(g_1, \ldots, g_n) \equiv \mathsf{f}(\pi \cdot g_1, \ldots, \pi \cdot g_n)$$
$$\pi \cdot [a]g \equiv [\pi(a)]\pi \cdot g \qquad \pi \cdot \mathsf{d}(a_1, \ldots, a_n) \equiv \mathsf{d}(\pi(a_1), \ldots, \pi(a_m)).$$

Lemma 6.2 *If $g \in \mathbb{F}(\Sigma, \mathcal{D})$ then $supp(g) = \{a \in \mathbb{A} \mid a \in g\}$. As a corollary, $a \notin g$ if and only if $a\#g$.*

$\mathbb{F}(\Sigma, \mathcal{D})$ with its permutation action, as defined in Definition 6.1, is a nominal set.

Proof. Elements of $\mathbb{F}(\Sigma, \mathcal{D})$ are labelled trees. Structurally, $[a]g'$ is a tree with a root note labelled '[]' and two daughters, one is a, the other is g'; the ability of abstraction to actually abstract comes later when we take equivalence classes in $\mathbb{F}(\mathsf{T}, \mathcal{D})$. $supp(g) = \{a \in \mathbb{A} \mid a \notin g\}$ follows by an easy induction on the tree structure of g using Lemma 4.8. It follows that $\mathbb{F}(\Sigma, \mathcal{D})$ is a nominal set. □

We need a technical lemma:

Lemma 6.3 *If $g \in \mathbb{F}(\Sigma, \mathcal{D})$ then $a \notin g$ implies $\vdash a\#g$.*

Proof. By an easy induction on syntax using the rules in Figure 1. □

Definition 6.4 Call a derivation Π an $\mathbb{F}(\mathsf{T}, \mathcal{D})$-derivation when:

- Π does not use $(cong\mathsf{d})$ for any $\mathsf{d} \in \mathcal{D}$.
  We discuss this condition in Remark 6.6 below.
- Π only mentions term-formers in $\Sigma \cup \mathcal{D}$.
  That is, we should only mention terms in the signature we are working in.
- Π does not use (fr).
  This can be 'guaranteed' in the sense given by Theorem 3.11.
- Π does not mention unknowns and in particular does not mention $(\#X)$.
  This can be also 'guaranteed' in the sense given by Theorem 3.11.

Write $\Pi(\mathsf{T}, \mathcal{D})$ for the set of $\mathbb{F}(\mathsf{T}, \mathcal{D})$-derivations.

Definition 6.5 If $g \in \mathbb{F}(\Sigma, \mathcal{D})$ write $[g]_{\mathsf{T}}$ for the set of $g' \in \mathbb{F}(\Sigma, \mathcal{D})$ such that some $\Pi \in \Pi(\mathsf{T}, \mathcal{D})$ exists of $\vdash_{\mathsf{T}} g = g'$. Write $\mathbb{F}(\mathsf{T}, \mathcal{D})$ for the nominal set such that

- $|\mathbb{F}(\mathsf{T}, \mathcal{D})| = \{[g]_{\mathsf{T}} \mid g \in \mathbb{F}(\Sigma, \mathcal{D})\}$.
- $\pi \cdot [g]_{\mathsf{T}} = [\pi \cdot g]_{\mathsf{T}}$.

Remark 6.6 We exclude $(cong\mathsf{d})$ to avoid the following pathological situation: if we allow $(cong\mathsf{d})$ and T contains the axiom $\vdash a = b$ then the reader can easily verify that $supp[\mathsf{d}(a_1, \ldots, a_n)]_{\mathsf{T}} = \emptyset$. This is unwanted behaviour: the intended rôle of $\mathsf{d}(a_1, \ldots, a_n)$ is to be an 'unknown element with support $\{a_1, \ldots, a_n\}$' in a model we are building, and this should hold independently of the axioms in T.

This is also why our syntax of ground terms does not allow terms of the form $\mathsf{d}(g_1, \ldots, g_n)$ for general $g_1, \ldots, g_n$. Note that in related work [GM06,GM08] we do allow such terms; we use them to build a model with a substitution action.

Lemma 6.7 *Suppose that $x \in \mathbb{F}(\mathsf{T}, \mathcal{D})$. Then:*

- $id \cdot x = x$.
- $\pi' \cdot (\pi \cdot x) = (\pi' \circ \pi) \cdot x$.
- *x is supported by $\{a \in \mathbb{A} \mid \nvdash a\#g\}$ for any $g \in x$.*

As a corollary $\mathbb{F}(\mathsf{T}, \mathcal{D})$ defined in Definition 6.5 above is *a nominal set, and furthermore if $\vdash a\#g$ then $a\#[g]_{\mathsf{T}}$.*

Proof. Suppose that $x \in \mathbb{F}(\mathsf{T}, \mathcal{D})$. By construction $x = [g]_{\mathsf{T}}$ for some $g \in \mathbb{F}(\Sigma, \mathcal{D})$. $id \cdot [g]_{\mathsf{T}} = [g]_{\mathsf{T}}$ and $\pi' \cdot (\pi \cdot [g]_{\mathsf{T}}) = (\pi' \circ \pi) \cdot [g]_{\mathsf{T}}$ follow by Lemma 3.2.

Write $A = \{a \mid \nvdash a\#g\}$. This is finite by Lemma 6.3. It suffices to show that A supports $[g]_{\mathsf{T}}$. Let π be a permutation such that $\pi(a) = a$ for all $a \in A$. We must show $\pi \cdot [g]_{\mathsf{T}} = [g]_{\mathsf{T}}$. By definition it suffices to show $[\pi \cdot g]_{\mathsf{T}} = [g]_{\mathsf{T}}$, that is, $\vdash_{\mathsf{T}} \pi \cdot g = g$. By Theorem 3.13 this follows from $\vdash \mathrm{ds}(\pi, id)\#g$. But this follows since $\mathrm{ds}(\pi, id)$ and A are disjoint.

The corollary follows from Definition 4.2. □

The following technical lemma will be useful later:

Lemma 6.8 *Suppose that $x \in \mathbb{F}(\mathsf{T}, \mathcal{D})$. Then $a_1\#x, \ldots, a_n\#x$ if and only if there exists some $g \in x$ such that $\vdash a_1\#g, \ldots, \vdash a_n\#g$ are all derivable.*

Proof. For the left-right implication we use Lemma 4.10 to pick some $g \in x$ such that $a_1\#g, \ldots, a_n\#g$. By Lemma 6.2 this is equivalent to $a_1 \notin g, \ldots, a_n \notin g$. We conclude $\vdash a_1\#g, \ldots, \vdash a_n\#g$ by 6.3.

The right-to-left implication is by Lemma 6.7. □

The following example shows why Lemma 6.8 is non-trivial:

Example 6.9 Consider a theory ATOM with one axiom $\vdash a = b$. $[a]_{\mathsf{T}} = \mathbb{A}$ and therefore $a\#[a]_{\mathsf{T}}$. Also $\vdash_{\mathsf{ATOM}} a = b$ and $\vdash a\#b$ *are* derivable. For further discussion see elsewhere [Mat07, 3.4.3].

Definition 6.10 is analogous to the standard construction of an algebra out of terms-quotiented-by-derivable-equality [BS81, Definition 10.4]. We investigate its initiality properties in Subsection 9.1.

Definition 6.10 Suppose $\mathsf{T} = (\Sigma, Ax)$ and suppose $\mathcal{D}$ is a set of term-formers disjoint from Σ. The **free algebra** of T over $\mathcal{D}$, we overload notation from Definition 6.5 and write it $\mathbb{F}(\mathsf{T}, \mathcal{D})$, is the Σ-algebra with:

- Underlying nominal set $\mathbb{F}(\mathsf{T}, \mathcal{D})$ as defined in Definition 6.5.
- Interpretation of atoms $a_{\mathbb{F}(\mathsf{T},\mathcal{D})} = [a]_{\mathsf{T}}$.
- Interpretation of abstraction $abs_{\mathbb{F}(\mathsf{T},\mathcal{D})}(a, x) = [[a]g]_{\mathsf{T}}$ for some $g \in x$.
- $\mathsf{f}_{\mathbb{F}(\mathsf{T},\mathcal{D})}(x_1, \ldots, x_n) = [\mathsf{f}(g_1, \ldots, g_n)]_{\mathsf{T}}$ for some $g_1 \in x_1, \ldots, g_n \in x_n$, for each term-former $\mathsf{f} : n$ in Σ.

We overload $\mathbb{F}(\mathsf{T}, \mathcal{D})$ to stand both for the Σ-algebra and its underlying nominal set.

Lemma 6.11 $\mathbb{F}(\mathsf{T}, \mathcal{D})$ is *a Σ-algebra.*

Proof. The underlying set $\mathbb{F}(\mathsf{T},\mathcal{D})$ is a nominal set by Lemma 6.7. For the interpretation functions we must show that they are well-defined — that is, we must show that for [-]- and $\mathsf{f}_{\mathbb{F}(\mathsf{T},\mathcal{D})}$ the choices of $g \in x$ and $g_1 \in x_1, \ldots, g_n \in x_n$ do not matter — and that they are equivariant. This is easy using the definitions of $[\text{-}]_{\mathsf{T}}$ and the permutation action.

The only slightly non-trivial part is to show that $a\#abs_{\mathbb{F}(\mathsf{T},\mathcal{D})}(a,x)$ holds, that is, that $a\#[[a]g]_{\mathsf{T}}$. Choose b fresh (so $b \notin g$ and $b\#[[a]g]_{\mathsf{T}}$). Since $b\#[[a]g]_{\mathsf{T}}$, also $a\#(b\ a)\cdot[[a]g]_{\mathsf{T}}$ by part iii of Lemma 4.6. By definition of the permutation action also $a\#[[b](b\ a)\cdot g]_{\mathsf{T}}$. Since $\vdash a\#[b](b\ a)\cdot g$ and $\vdash b\#[b](b\ a)\cdot g$ by Lemma 6.3 and the derivation rules of Figure 1, we know $\vdash_{\mathsf{T}} [b](b\ a)\cdot g = [a]g$ by (*perm*). Then $[[b](b\ a)\cdot g]_{\mathsf{T}} = [[a]g]_{\mathsf{T}}$ and we obtain $a\#[[a]g]_{\mathsf{T}}$ as required. □

Lemma 6.12 *Suppose Σ is a signature and $\mathcal{D}$ is a set of fresh term-formers (so $\mathcal{D}\cap\Sigma=\emptyset$). Suppose that t is a term in $\Sigma\cup\mathcal{D}$. Suppose that $\sigma(X)\in\mathbb{F}(\Sigma,\mathcal{D})$ for every $X\in t$. Suppose that ς is a valuation to $|\mathbb{F}(\mathsf{T},\mathcal{D})|$ such that $\sigma(X)\in\varsigma(X)$ for every $X\in t$.*

Then $[t\sigma]_{\mathsf{T}} = [\![t]\!]_{\varsigma}$.

Proof. By an easy induction on the structure of t:

- The case a. Note that from the definitions $a\sigma \equiv a$ and $[\![a]\!]_{\varsigma} = [a]_{\mathsf{T}}$. It follows that $[a\sigma]_{\mathsf{T}} = [\![a\sigma]\!]_{\varsigma}$.
- The case of $\pi\cdot X$.

$$[(\pi\cdot X)\sigma]_{\mathsf{T}} = \pi\cdot[\sigma(X)]_{\mathsf{T}} = \pi\cdot\varsigma(X) = [\![\pi\cdot X]\!]_{\varsigma}.$$

- The case $[a]t$. We use the inductive hypothesis:

$$\begin{aligned}[([a]t)\sigma]_{\mathsf{T}} = [[a](t\sigma)]_{\mathsf{T}} = abs_{\mathbb{F}(\mathsf{T},\mathcal{D})}(a,[t\sigma]_{\mathsf{T}})\\ = abs_{\mathbb{F}(\mathsf{T},\mathcal{D})}(a,[\![t]\!]_{\varsigma}) = [\![[a](t\sigma)]\!]_{\varsigma} = [\![([a]t)\sigma]\!]_{\varsigma}.\end{aligned}$$

- The cases of $\mathsf{f}(t_1,\ldots,t_n)$ for $\mathsf{f}\in\Sigma$ and $\mathsf{d}(a_1,\ldots,a_n)$ are similar, but simpler.

□

Theorem 6.13 *$\mathbb{F}(\mathsf{T},\mathcal{D})$ is a model of T.*

Proof. Suppose $\Delta\vdash t=u$ is an axiom of T. Suppose that ς is a valuation to $|\mathbb{F}(\mathsf{T},\mathcal{D})|$ and suppose that $a\#\varsigma(X)$ for every $a\#X\in\Delta$. We must show that $[\![t]\!]_{\varsigma} = [\![u]\!]_{\varsigma}$.

Let $\mathcal{X}$ be the set of all unknowns mentioned in Δ, t, or u. By Lemma 6.8, for every $X\in\mathcal{X}$ there is an element $g_X\in\varsigma(X)$ such that $\vdash a\#g_X$ for every $a\#X\in\Delta$. Let σ be the substitution such that $\sigma(X)\equiv g_X$ when $X\in\mathcal{X}$ and $\sigma(X)\equiv X$ when $X\notin\mathcal{X}$. By construction $\vdash a\#\sigma(X)$ for every $a\#X\in\Delta$, so $\vdash_{\mathsf{T}} t\sigma = u\sigma$ by $(ax_{\Delta\vdash t=u})$. This derivation is clearly in $\Pi(\mathsf{T},\mathcal{D})$ (Definition 6.4) so $[t\sigma]_{\mathsf{T}} = [u\sigma]_{\mathsf{T}}$. Therefore $[t\sigma]_{\mathsf{T}} = [\![t]\!]_{\varsigma}$ and $[u\sigma]_{\mathsf{T}} = [\![u]\!]_{\varsigma}$ by Lemma 6.12 and the result follows. □

7 The inverse mapping

Fix a signature Σ and a finite set of fresh term-formers $\mathcal{D} = \{\mathsf{d}_1, \ldots, \mathsf{d}_n\}$ (so $\Sigma \cap \mathcal{D} = \emptyset$). Let M be the greatest arity of the elements of $\mathcal{D}$.

Definition 7.1 For each finite $\mathcal{A} \subseteq \mathbb{A}$ with cardinality at least M, make a fixed but arbitrary choice of the following data:

- For each i such that $1 \leq i \leq n$ some choice of unknown X_i; our choice is injective in the sense that $X_i = X_j$ implies $i = j$ for $1 \leq i, j \leq n$. Write $\mathcal{X} = \{X_1, \ldots, X_n\}$. We call X_i the 'unknown corresponding to d_i'.
- A choice $\mathcal{B}$ of a set of atoms with the same cardinality as $\mathcal{A}$, but disjoint from it (so $\mathcal{B} \cap \mathcal{A} = \emptyset$).
- For each i with $1 \leq i \leq n$ let
  · $a_{i1}, \ldots, a_{im}$ be some choice of m distinct elements of $\mathcal{A}$ in some arbitrary order, and
  · $b_{i1}, \ldots, b_{im}$ be some choice of m distinct elements of $\mathcal{B}$ in some arbitrary order, where m is the arity of d_i. We call $a_{i1}, \ldots, a_{im}$, and $b_{i1}, \ldots, b_{im}$ the 'choices of atoms in order corresponding to d_i'.

Definition 7.2 Suppose that $\mathcal{A} \subseteq \mathbb{A}$ has cardinality at least M. Write $\mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})$ for the set of $g \in \mathbb{F}(\Sigma, \mathcal{D})$ such that $\{a \mid a \in g\} \subseteq \mathcal{A}$.

If $g \in \mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})$ then let $\mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})^{\text{-}1}(g)$ be the tuple $(\Delta \vdash g^{\text{-}1}, \sigma, \mathcal{B}, \mathcal{X})$ where:

- $\Delta = \{b\#X \mid X \in \mathcal{X},\ b \in \mathcal{B}\} \cup$
  $\{a\#X_i \mid a \in \mathcal{A},\ X_i \in \mathcal{X},\ \vdash a\#\mathsf{d}(a_{i1}, \ldots, a_{im})\}$.
  (Note that $a\#\mathsf{d}(a_{i1}, \ldots, a_{im})$ if and only if $a \notin \{a_{i1}, \ldots, a_{im}\}$.)
- $\sigma(X_i) = \mathsf{d}_i(a_{i1}, \ldots, a_{im})$.
- $\sigma(Y) = id \cdot Y$ for all $Y \notin \mathcal{X}$.
- $g^{\text{-}1}$ is defined inductively by:

$$a^{\text{-}1} \equiv a \qquad ([a]g)^{\text{-}1} \equiv [a]g^{\text{-}1} \qquad \mathsf{f}(g_1, \ldots, g_n)^{\text{-}1} \equiv \mathsf{f}(g_1^{\text{-}1}, \ldots, g_n^{\text{-}1})$$
$$\mathsf{d}(a'_1, \ldots, a'_n)^{\text{-}1} \equiv (a'_1\ b_1) \cdots (a'_n\ b_n)(b_1\ a_1) \cdots (b_n\ a_n) \cdot X$$

We call this construction the **inverse mapping**.

The following technical lemma will be useful later:

Lemma 7.3 $\mathsf{d}_i(a_{i1}, \ldots, a_{in})^{\text{-}1} \equiv X_i$.

Proof. We unpack definitions and observe that $(a_1\ b_1) \cdots (a_n\ b_n)(b_1\ a_1) \cdots (b_n\ a_n) = id$. □

We may use Lemma 7.4 without comment:

Lemma 7.4 *Suppose that $g, h \in \mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})$. Suppose that*

$$(\Delta \vdash t, \sigma, \mathcal{B}, \mathcal{X}) = \mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})^{\text{-}1}(g) \quad \textit{and} \quad (\Delta' \vdash u, \sigma', \mathcal{B}', \mathcal{X}') = \mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})^{\text{-}1}(h).$$

then $\Delta = \Delta'$, $\sigma = \sigma'$, $\mathcal{B}' = \mathcal{B}$, and $\mathcal{X}' = \mathcal{X}$.

Proof. The construction of Δ and Δ' does not depend on g and h. Similarly for σ and σ', $\mathcal{B}'$ and $\mathcal{B}$, and $\mathcal{X}'$ and $\mathcal{X}$. □

Lemma 7.5 *Suppose that* $g \in \mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})$ *and* $(\Delta \vdash g^{-1}, \sigma, \mathcal{B}, \mathcal{X}) = \mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})^{-1}(g)$. *Then for any* $\mathsf{T} = (\Sigma, Ax)$ *there is an* $\mathbb{F}(\Sigma, \mathcal{D})$*-derivation of* $\vdash_{\mathsf{T}} g^{-1}\sigma = g$.

Proof. We work by induction on g. All cases are routine, we consider only the case $g \equiv \mathsf{d}_i(a'_1, \ldots, a'_n)$ for $\mathsf{d}_i \in \mathcal{D}$ where n is the arity of d_i. Then

$$g^{-1} \equiv (a'_1\ b_{i1}) \cdots (a'_n\ b_{in})(b_{i1}\ a_{i1}) \cdots (b_{in}\ a_{in}) \cdot X_i$$

and $\sigma(X_i) \equiv \mathsf{d}_i(a_{i1}, \ldots, a_{in})$. The result follows by an easy calculation using the definition of the permutation action. □

Corollary 7.6 *Suppose that* $g, h \in \mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})$. *Suppose that*

$$\mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})^{-1}(g) = (\Delta \vdash g^{-1}, \sigma, \mathcal{B}, \mathcal{X}) \quad \textit{and} \quad \mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})^{-1}(h) = (\Delta \vdash h^{-1}, \sigma, \mathcal{B}, \mathcal{X}).$$

Then $\Delta \vdash_{\mathsf{T}} g^{-1} = h^{-1}$ *implies* $\vdash_{\mathsf{T}} g = h$.

Proof. By Lemma 7.5 $\Delta \vdash g^{-1}\sigma = g$ and $\Delta \vdash h^{-1}\sigma = h$. The result follows using (*tran*). □

Lemma 7.7 *Suppose that* $\mathsf{d}(a'_1, \ldots, a'_m) \in \mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})$ *and suppose* $a \in \mathcal{A}$. *Then* $\Delta \vdash a\#\mathsf{d}(a'_1, \ldots, a'_m)^{-1}$ *if and only if* $a \notin \{a'_1, \ldots, a'_m\}$.

Proof. Recall our choices of $a_1, \ldots, a_m$ and $b_1, \ldots, b_m$ from $\mathcal{A}$ and $\mathcal{B}$ respectively. By construction $\mathsf{d}(a'_1, \ldots, a'_m)^{-1} \equiv \pi' \cdot X$ for some $X \in \mathcal{X}$, were

$$\pi' \ = \ (a'_1\ b_1) \cdots (a'_m\ b_m)(b_1\ a_1) \cdots (b_m\ a_m).$$

By the syntax-directed structure of the rules in Figure 1, $\Delta \vdash a\#\pi' \cdot X$ if and only if $\Delta \vdash \pi'^{-1}(a)\#X$. The result follows by the construction of Δ. □

Lemma 7.8 *Suppose that* $\pi(c) = c$ *for all* $c \in \mathbb{A} \setminus \mathcal{A}$. *Suppose that* $g \in \mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})$ *and suppose that* $\mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})^{-1}(g) = (\Delta \vdash g^{-1}, \sigma, \mathcal{B}, \mathcal{X})$. *Then:*

- $\Delta \vdash a\#(\pi \cdot g)^{-1}$ *if and only if* $\Delta \vdash a\#\pi \cdot (g^{-1})$.
- *For any* $\mathsf{T} = (\Sigma, Ax)$ *there is an* $\mathbb{F}(\Sigma, \mathcal{D})$*-derivation of* $\Delta \vdash_{\mathsf{T}} (\pi \cdot g)^{-1} = \pi \cdot g^{-1}$, *providing that* $\pi(c) = c$ *for all* $c \in \mathbb{A} \setminus \mathcal{A}$.

Proof.

- We work by induction on g. The only non-trivial case is when $g \equiv \mathsf{d}(a'_1, \ldots, a'_m)$ where m is the arity of d. It suffices to show that $\Delta \vdash a\#\pi' \cdot X$ if and only if $\Delta \vdash a\#\pi'' \cdot X$ where $X \in \mathcal{X}$ is our choice of unknown in $\mathcal{X}$ to correspond to $\mathsf{d} \in \mathcal{D}$ and
$$\pi' \ = \ (\pi(a'_1)\ b_1) \cdots (\pi(a'_m)\ b_m)(b_1\ a_1) \cdots (b_m\ a_m)$$
and
$$\pi'' \ = \ \pi \circ (a'_1\ b_1) \cdots (a'_m\ b_m)(b_1\ a_1) \cdots (b_m\ a_m).$$
This follows by easy calculations using the construction of Δ and the assumption that $\pi(b_i) = b_i$ for $1 \leq i \leq m$.

- We work by induction on g. The only non-trivial case is again when $g \equiv \mathsf{d}(a'_1, \ldots, a'_m)$ where m is the arity of d. It suffices to derive

$$\Delta \vdash \pi' \cdot X = \pi'' \cdot X$$

for X, π', and π'' as in the first part of this result. By Theorem 3.13 it suffices to show $\Delta \vdash \mathrm{ds}(\pi', \pi'')\#X$. This follows by easy calculations as in the first part. □

If Π is a nominal algebra derivation, write $a \in \Pi$ when a occurs in the syntax of Π (that is, when there exists some term t in the syntax of Π such that $a \in t$). Theorem 7.9 is an important technical result (compare with Lemma 6.18 from [GM08] and Lemma 3.4.23 from [Mat07]):

Theorem 7.9 *Suppose that* $g, h \in \mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})$. *Suppose that*

$$\mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})^{-1}(g) = (\Delta \vdash g^{-1}, \sigma, \mathcal{B}, \mathcal{X}) \quad \textit{and} \quad \mathbb{F}(\Sigma, \mathcal{D}, \mathcal{A})^{-1}(h) = (\Delta \vdash h^{-1}, \sigma, \mathcal{B}, \mathcal{X}).$$

Then:

- *If* $\vdash a\#g$ *then* $\Delta \vdash a\#g^{-1}$.
- *If a derivation* $\Pi \in \Pi(\mathsf{T}, \mathcal{D})$ *exists of* $\vdash_{\mathsf{T}} g = h$ *and* $\{a \mid a \in \Pi\} \subseteq \mathcal{A}$ *then* $\Delta \vdash_{\mathsf{T}} g^{-1} = h^{-1}$.

Proof. We inductively transform Π into a derivation of $\Delta \vdash_{\mathsf{T}} t = u$.

- The cases of $(\#ab)$, $(\#[]a)$, $(\#[]b)$, $(cong[])$, $(refl)$, $(symm)$ and $(tran)$ are easy.
- The case $(\#\mathsf{f})$. There are two possibilities:
  - Suppose $\vdash a\#\mathsf{f}(g_1, \ldots, g_n)$ for $\mathsf{f} \in \Sigma$.
    By assumption $\vdash a\#g_i$ for $1 \leq i \leq n$ so $\Delta \vdash a\#g_i^{-1}$ by inductive hypothesis. By construction $\mathsf{f}(g_1, \ldots, g_n)^{-1} \equiv \mathsf{f}(g_1^{-1}, \ldots, g_n^{-1})$ and the result follows.
  - Suppose $\vdash a\#\mathsf{d}_i(a'_1, \ldots, a'_m)$ for $\mathsf{d}_i \in \mathcal{D}$ and m the arity of d_i.
    By assumption $\vdash a\#a'_i$ for $1 \leq i \leq m$. It follows that $a \notin \{a'_1, \ldots, a'_m\}$. The result follows by Lemma 7.7.
- $(cong\mathsf{f})$. There are two cases:
  - The case of $\mathsf{f} \in \Sigma$ easily follows using the inductive hypothesis.
  - The case of $\mathsf{d} \in \mathcal{D}$ is impossible, since we assumed that Π does not mention $(cong\mathsf{d})$.
- $(perm)$. By inductive hypothesis $\Delta \vdash a\#g^{-1}$ and $\Delta \vdash b\#g^{-1}$. Then $\Delta \vdash_{\mathsf{T}} (a\ b) \cdot g^{-1} = g^{-1}$ by $(perm)$. By Lemma 7.8 $\Delta \vdash_{\mathsf{T}} ((a\ b) \cdot g)^{-1} = (a\ b) \cdot g^{-1}$. The result follows.
- $(ax_{\Delta' \vdash v=w})$. Then $\vdash \pi \cdot \Delta'\tau$ and $\vdash_{\mathsf{T}} \pi \cdot v\tau = \pi \cdot w\tau$ for some permutation π and substitution τ.
  We must show $\Delta \vdash_{\mathsf{T}} (\pi \cdot v\tau)^{-1} = (\pi \cdot w\tau)^{-1}$ and by inductive hypothesis we may assume $\Delta \vdash_{\mathsf{T}} (\pi \cdot \Delta\tau)^{-1}$.
  By Lemma 7.8 it suffices to show

$$\Delta \vdash_{\mathsf{T}} \pi \cdot (v\tau)^{-1} = \pi \cdot (w\tau)^{-1}$$

given

$$\Delta \vdash_{\mathsf{T}} \pi \cdot (\Delta\tau)^{-1}.$$

Define τ' by:

$$\tau'(X) \equiv \tau(X)^{-1} \qquad (\tau(X) \not\equiv X)$$

$$\tau'(Y) \equiv id \cdot Y \qquad (\tau(Y) \equiv id \cdot Y)$$

Then $(v\tau)^{-1} \equiv v\tau'$, $(w\tau)^{-1} \equiv w\tau'$ and $(\Delta'\tau)^{-1} \equiv \Delta'\tau'$, so it suffices to show

$$\Delta \vdash_{\mathsf{T}} \pi \cdot v\tau' = \pi \cdot w\tau'.$$

By $(ax_{\Delta' \vdash v=w})$ this follows from $\Delta \vdash \pi \cdot \Delta'\tau'$.

□

8 Homomorphisms, Subalgebras and Product Algebras

We now establish some basic definitions required for stating the nominal HSP theorem.

8.1 Algebra homomorphisms

Definition 8.1 For Σ-algebras $\mathbb{X}$ and $\mathbb{Y}$, a **Σ-algebra homomorphism** from $\mathbb{X}$ to $\mathbb{Y}$ is an equivariant function $\theta : |\mathbb{X}| \to |\mathbb{Y}|$ such that:

- $\theta a_{\mathbb{X}} = a_{\mathbb{Y}}$ for every atom.
- $\theta abs_{\mathbb{X}}(a, x) = abs_{\mathbb{X}}(a, \theta x)$.
- $\theta \mathsf{f}_{\mathbb{X}}(x_1, \ldots, x_n) = \mathsf{f}_{\mathbb{Y}}(\theta x_1, \ldots, \theta x_n)$ for every f in Σ.

Suppose $\mathbb{X}$ and $\mathbb{Y}$ are Σ-algebras. Call $\mathbb{Y}$ a **homomorphic image** of $\mathbb{X}$ when there is a Σ-algebra homomorphism θ from $\mathbb{X}$ to $\mathbb{Y}$ such that $\theta \in |\mathbb{X}| \to |\mathbb{Y}|$ is a surjection onto $|\mathbb{Y}|$.

Lemma 8.2 *Suppose Σ is a signature and suppose that $\mathbb{X}$ and $\mathbb{Y}$ are Σ-algebras. Suppose θ is a Σ-algebra homomorphism from $\mathbb{X}$ to $\mathbb{Y}$.*

Suppose that ς' is a valuation to $\mathbb{X}$ and ς is a valuation to $\mathbb{Y}$. Finally suppose that $\theta(\varsigma'(X)) = \theta(\varsigma(X))$ for all unknowns X.

Then $\theta([\![t]\!]_{\varsigma'}) = [\![t]\!]_{\varsigma}$.

Proof. By an easy induction on t. □

Lemma 8.3 *Suppose Σ is a signature and $\mathsf{T} = (\Sigma, Ax)$ is a theory. Suppose that $\mathbb{X}$ and $\mathbb{Y}$ are Σ-algebras and suppose $\mathbb{Y}$ is a homomorphic image of $\mathbb{X}$.*

Then if $\mathbb{X}$ is a model of T, then so is $\mathbb{Y}$.

Proof. Write θ for the Σ-algebra homomorphism from $|\mathbb{X}|$ to $|\mathbb{Y}|$. Recall that by assumption θ is surjective.

Choose any $(\Delta \vdash t = u) \in Ax$ and a valuation ς to $\mathbb{Y}$. It suffices to show that $[\![\Delta \vdash t = u]\!]^{\mathbb{Y}}_{\varsigma}$ is valid.

Suppose $[\![\Delta]\!]^{\mathbb{Y}}_{\varsigma}$ is valid; unpacking definitions this means that $a\#\varsigma(X)$ for every $a\#X \in \Delta$.

For each unknown X let $\mathcal{X} = \{x \in \mathbb{X} \mid \theta(x) = \varsigma(X)\}$. We can verify that for any permutation π, $\pi \cdot \mathcal{X} = \{x \in \mathbb{X} \mid \theta(x) = \pi \cdot \varsigma(X)\}$. Therefore if $\pi \cdot \varsigma(X) = \varsigma(X)$ then $\pi \cdot \mathcal{X} = \mathcal{X}$ and it follows that $supp(\mathcal{X}) \subseteq supp(\varsigma(X))$. We construct a valuation ς' to $\mathbb{X}$ by for each unknown X setting $\varsigma'(X) = x$ for some choice of $x \in \mathcal{X}$ such that $a\#x$ for every $a\#X \in \Delta$. Such a choice exists by Lemma 4.10.

By construction $[\![\Delta]\!]^{\mathbb{X}}_{\varsigma'}$ is valid, and so by assumption $[\![t]\!]^{\mathbb{X}}_{\varsigma'} = [\![u]\!]^{\mathbb{X}}_{\varsigma'}$. We apply θ to both sides of the equality and use Lemma 8.2 to conclude that $[\![t]\!]^{\mathbb{Y}}_{\varsigma} = [\![u]\!]^{\mathbb{Y}}_{\varsigma}$ as required. □

8.2 Subalgebras

Definition 8.4 For Σ-algebras $\mathbb{X}$ and $\mathbb{Y}$, call $\mathbb{X}$ a **subalgebra** of $\mathbb{Y}$ when the following conditions are satisfied:

- $|\mathbb{X}| \subseteq |\mathbb{Y}|$.
- $a_{\mathbb{X}} = a_{\mathbb{Y}}$ for all atoms a.
- $abs_{\mathbb{X}}(a, x) = abs_{\mathbb{Y}}(a, x)$ for all atoms a and $x \in |\mathbb{X}|$.
- For every term-former f in signature Σ, if f has arity n and $x_1, \ldots, x_n \in |\mathbb{X}|$ then $\mathsf{f}_{\mathbb{X}}(x_1, \ldots, x_n) = \mathsf{f}_{\mathbb{Y}}(x_1, \ldots, x_n)$.

In other words, $\mathbb{X}$ is closed under the interpretation of the term-formers which it inherits from $\mathbb{Y}$.

Lemma 8.5 *For Σ-algebras $\mathbb{X}$, $\mathbb{Y}$ and a theory $\mathsf{T} = (\Sigma, Ax)$, if $\mathbb{Y}$ is a model of T and $\mathbb{X}$ is a subalgebra of $\mathbb{Y}$ then $\mathbb{X}$ is a model of T.*

Proof. Suppose $(\Delta \vdash t = u) \in Ax$ and suppose ς is a valuation to $|\mathbb{X}|$ such that $a\#\varsigma(X)$ for every $a\#X \in \Delta$. Since ς is also a valuation to $|\mathbb{Y}|$, it follows that $[\![t]\!]_{\varsigma} = [\![u]\!]_{\varsigma}$. Therefore $\mathbb{X}$ satisfies all the axioms of T. □

8.3 Products

Definition 8.6 Let I be a (possibly countably infinite) indexing set and $(\mathbb{X}_i)_{i \in I}$ be an I-indexed collection of Σ-algebras. The **product algebra** $\Pi_{i \in I}\mathbb{X}_i$ is the Σ-algebra with:

- Underlying nominal set $\Pi_{i \in I}\mathbb{X}_i$ as defined in Definition 4.7, considering each $\mathbb{X}_i$ as a nominal set.

  Recall that this has the component-wise permutation action; $\pi \cdot (x_i)_{i \in I} = (\pi \cdot x_i)_{i \in I}$.
- $a_{\Pi_{i \in I}\mathbb{X}_i} = (a_{\mathbb{X}_i})_{i \in I}$.
- $abs_{\Pi_{i \in I}\mathbb{X}_i}(a, (x_i)_{i \in I}) = \Pi_{i \in I}\, abs_{\mathbb{X}_i}(a, x_i)$.
- For each term-former f of arity n the component-wise interpretation function

$$\mathsf{f}_{\Pi_{i \in I}\mathbb{X}_i}((x_i^1)_{i \in I}, \ldots, (x_i^n)_{i \in I}) = (\mathsf{f}_{\mathbb{X}_i}(x_i^1, \ldots, x_i^n))_{i \in I}.$$

It is easy to check that $\Pi_{i \in I}\mathbb{X}_i$ *is* a Σ-algebra:

Lemma 8.7 *For any I-indexed collection of Σ-algebras $(\mathbb{X}_i)_{i\in I}$, if $\mathbb{X}_i$ is a model of $\mathsf{T} = (\Sigma, Ax)$ for every $i \in I$ then so is $\Pi_{i\in I}\mathbb{X}_i$.*

Proof. Suppose that ς is a valuation to $|\Pi_{i\in I}\mathbb{X}_i|$. Suppose that $(\Delta \vdash t = u) \in Ax$ and suppose that $a\#\varsigma(X)$ for every $a\#X \in \Delta$. We must show that $[\![t]\!]_\varsigma = [\![u]\!]_\varsigma$.

For each $i \in I$ we obtain a valuation ς_i to $|\mathbb{X}_i|$ projecting to the ith component of $\varsigma(X)$. By Lemma 4.8 we know that $a\#\varsigma_i X$ for every $a\#X \in \Delta$. It follows that the ith projection of $[\![t]\!]_\varsigma$ is equal to the ith projection of $[\![u]\!]_\varsigma$, and thus that $[\![t]\!]_\varsigma = [\![u]\!]_\varsigma$.□

8.4 Atoms-abstraction

Suppose $\mathbb{X}$ is a nominal set and suppose $x \in \mathbb{X}$ and $a \in \mathbb{A}$.

Definition 8.8 Define **atoms-abstraction** by

$$[a]x = \{(b, (b\ a)\cdot x) \mid b\#x\} \cup \{(a, x)\}.$$

Write $[\mathbb{A}]\mathbb{X}$ for the nominal set such that:

- $|[\mathbb{A}]\mathbb{X}| = \{[a]x \mid a \in \mathbb{A},\ x \in \mathbb{X}\}$.
- $\pi \cdot [a]x = [\pi(a)]\pi \cdot x$.

(Note that by our permutative convention b ranges over atoms not equal to a.) It is not hard to prove that $[\mathbb{A}]\mathbb{X}$ *is* a nominal set. This definition is known [GP01] and has been extensively used and studied. We mention those of its properties that we need, with references to proofs.

Lemma 8.9 *If $x'_1, \ldots, x'_n \in [\mathbb{A}]\mathbb{V}$ then for any fresh c (so $c\#x'_1, \ldots, x'_n$) there exist $x_1, \ldots, x_n \in \mathbb{V}$ such that $x'_i = [c]x_i$ for $1 \le i \le n$.*

Proof. By [GP01, Proposition 5.5]. □

Lemma 8.10 *If $[c]x = [c]x'$ then $x = x'$.*

Proof. By [GP01, Proposition 5.5]. □

Lemma 8.11 *$[c]x = [d]y$ if and only if $y = (c\ d)\cdot x$ and $c\#y$.*

Proof. By [GP01, Proposition 5.5]. □

Lemma 8.12 *$supp([c]x) = supp(x) \setminus \{c\}$.*

Proof. By [GP01, Proposition 5.2]. □

Lemma 8.13 *If $c\#x$ and $c'\#x$ then $[c]x = [c']x$.*

Proof. By definition $(c'\ c)\cdot[c]x = [c'](c'\ c)\cdot x$. By Lemma 8.12 $c'\#[c]x$ and $c\#[c]x$. By assumption $c'\#x$ and $c\#x$. The result follows by part ii of Lemma 4.6. □

Definition 8.14 Suppose that $\mathbb{V}$ is a Σ-algebra. Define $[\mathbb{A}]\mathbb{V}$ by:

- $|[\mathbb{A}]\mathbb{V}| = [\mathbb{A}]|\mathbb{V}|$.
- $a_{[\mathbb{A}]\mathbb{V}} = [c]a_{\mathbb{V}}$ (for any $c \neq a$).
- $abs_{[\mathbb{A}]\mathbb{V}}(a, [c]x) = [c]\,abs_{\mathbb{V}}(a, x)$ (for any $c \neq a$).

- $\mathsf{f}_{[\mathbb{A}]\mathbb{V}}([c]x_1,\ldots,[c]x_n) = [c]\mathsf{f}_{\mathbb{V}}(x_1,\ldots,x_n)$.

Lemma 8.15 *$[\mathbb{A}]\mathbb{V}$ is a Σ-algebra.*

Proof. There are several things to check:

- $a_{[\mathbb{A}]\mathbb{V}}$ is well-defined. Suppose $c, c' \neq a$. By Lemma 4.5 $c\#a_{\mathbb{V}}$ and $c'\#a_{\mathbb{V}}$. By Lemma 8.13 $[c]a_{\mathbb{V}} = [c']a_{\mathbb{V}}$.
- $abs_{[\mathbb{A}]\mathbb{V}}$ is well-defined. Suppose that $[c]x = [d]y$. By Lemma 8.11 $y = (c\ d)\cdot x$ and $c\#y$. We reason as follows:

$$\begin{array}{lll} abs_{[\mathbb{A}]\mathbb{V}}(a,[d]y) & = [d]abs_{\mathbb{V}}(a,(c\ d)\cdot x) & \text{Definition 8.14} \\ & = [d](c\ d)\cdot abs_{\mathbb{V}}(a,x) & abs_{\mathbb{V}} \text{ equivariant} \\ & = [c]abs_{\mathbb{V}}(a,x) & \text{Lemmas 4.5 and 8.11} \\ & = abs_{[\mathbb{A}]\mathbb{V}}(a,[c]x) & \text{Definition 8.14} \end{array}$$

- $abs_{[\mathbb{A}]\mathbb{V}}$ is equivariant. This follows easily from the definitions:

$$\begin{array}{lll} \pi\cdot abs_{[\mathbb{A}]\mathbb{V}}([c]x) & = \pi\cdot[c]abs_{\mathbb{V}}(x) & \text{Definition 8.14} \\ & = [\pi(c)]abs_{\mathbb{V}}(\pi\cdot x) & \text{Definition 8.8, } abs_{\mathbb{V}} \text{ equivariant} \\ & = abs_{[\mathbb{A}]\mathbb{V}}([\pi(c)]\pi\cdot x) & \text{Definition 8.14} \\ & = abs_{[\mathbb{A}]\mathbb{V}}(\pi\cdot[c]x). & \text{Definition 8.8} \end{array}$$

- $\mathsf{f}_{[\mathbb{A}]\mathbb{V}}$ is well-defined. Suppose $x'_1,\ldots,x'_n \in |[\mathbb{A}]\mathbb{V}|$. Suppose that $x'_i = [c]x_i$ for $1\leq i\leq n$ and also $x'_i = [d]y_i$ for $1\leq i\leq n$. By Lemma 8.11 $y_i = (c\ d)\cdot x_i$ and $c\#y_i$ for $1\leq i\leq n$. We reason as follows:

$$\begin{array}{lll} [d]\mathsf{f}_{\mathbb{V}}(y_1,\ldots,y_n) & = [d]\mathsf{f}_{\mathbb{V}}((c\ d)\cdot x_1,\ldots,(c\ d)\cdot x_n) & \\ & = [d](c\ d)\cdot\mathsf{f}_{\mathbb{V}}(x_1,\ldots,x_n) & \mathsf{f}_{\mathbb{V}} \text{ equivariant} \\ & = [c]\mathsf{f}_{\mathbb{V}}(x_1,\ldots,x_n) & \text{Lemmas 4.5 and 8.11} \end{array}$$

- $\mathsf{f}_{[\mathbb{A}]\mathbb{V}}$ is total. Suppose $x'_1,\ldots,x'_n \in |[\mathbb{A}]\mathbb{V}|$. Choose fresh c (so $c\#x'_1,\ldots,x'_n$). By Lemma 8.9 there exist $x_i \in |\mathbb{V}|$ such that $x'_i = [c]x_i$ for $1\leq i\leq n$. The result follows.
- $\mathsf{f}_{[\mathbb{A}]\mathbb{V}}$ is equivariant. This follows exactly as for $abs_{[\mathbb{A}\mathbb{V}}$.

□

Definition 8.16 If $\mathbb{V}$ is a Σ-algebra and ς is a valuation to $|\mathbb{V}|$, then write $[c]\varsigma$ for the valuation to $|[\mathbb{A}]\mathbb{V}|$ such that X maps to $[c]\varsigma(X)$.

Lemma 8.17 *Suppose that $\mathbb{V}$ is a Σ-algebra and ς is a valuation to $|\mathbb{V}|$. Then if $c\notin t$ then*

$$[\![t]\!]^{[\mathbb{A}]\mathbb{V}}_{[c]\varsigma} = [c]([\![t]\!]^{\mathbb{V}}_{\varsigma}).$$

Proof. By induction on t:

- The case $t\equiv a$. $[\![a]\!]^{[\mathbb{A}]\mathbb{V}}_{[c]\varsigma} = a_{[\mathbb{A}]\mathbb{V}} = [c]a_{\mathbb{V}} = [c]([\![a]\!]^{\mathbb{V}}_{\varsigma})$.
- The case $t\equiv c$. Here there is nothing to prove, since we assumed that $c\notin t$.

- The case $t \equiv \mathsf{f}(t_1, \ldots, t_n)$.

$$\begin{array}{lll}
[\![\mathsf{f}(t_1,\ldots,t_n)]\!]^{[\mathbb{A}]\mathbb{V}}_{[c]\varsigma} & = \mathsf{f}_{[\mathbb{A}]\mathbb{V}}([\![t_1]\!]^{[\mathbb{A}]\mathbb{V}}_{[c]\varsigma},\ldots,[\![t_n]\!]^{[\mathbb{A}]\mathbb{V}}_{[c]\varsigma}) & \\
& = \mathsf{f}_{[\mathbb{A}]\mathbb{V}}([c][\![t_1]\!]^{\mathbb{V}}_{\varsigma},\ldots,[c][\![t_n]\!]^{\mathbb{V}}_{\varsigma}) & \text{Inductive hypothesis} \\
& = [c]\mathsf{f}_{\mathbb{V}}([\![t_1]\!]^{\mathbb{V}}_{\varsigma},\ldots,[\![t_n]\!]^{\mathbb{V}}_{\varsigma}) & \text{Definition 8.14} \\
& = [c][\![\mathsf{f}(t_1,\ldots,t_n)]\!]^{\mathbb{V}}_{\varsigma} &
\end{array}$$

□

Corollary 8.18 *Suppose that $c \notin t$ and $c \notin u$. Then $[\![t]\!]^{\mathbb{V}}_{\varsigma} = [\![u]\!]^{\mathbb{V}}_{\varsigma}$ if and only if $[\![t]\!]^{[\mathbb{A}]\mathbb{V}}_{[c]\varsigma} = [\![u]\!]^{[\mathbb{A}]\mathbb{V}}_{[c]\varsigma}$.*

Proof. Suppose $c \notin t$ and $c \notin u$.

If $[\![t]\!]^{\mathbb{V}}_{\varsigma} = [\![u]\!]^{\mathbb{V}}_{\varsigma}$ then $[c][\![t]\!]^{\mathbb{V}}_{\varsigma} = [c][\![u]\!]^{\mathbb{V}}_{\varsigma}$ and the result follows by Lemma 8.17.

Conversely suppose $[\![t]\!]^{[\mathbb{A}]\mathbb{V}}_{[c]\varsigma} = [\![u]\!]^{[\mathbb{A}]\mathbb{V}}_{[c]\varsigma}$. By Lemma 8.17 $[c][\![t]\!]^{\mathbb{V}}_{\varsigma} = [c][\![u]\!]^{\mathbb{V}}_{\varsigma}$. The result follows by Lemma 8.10. □

Lemma 8.19 *If $\mathbb{X}$ is a model of $\mathsf{T} = (\Sigma, Ax)$ then so is $[\mathbb{A}]\mathbb{X}$.*

Proof. Suppose that ς is a valuation to $|[\mathbb{A}]\mathbb{X}|$. Suppose that $(\Delta \vdash t = u) \in Ax$ and suppose that $a\#\varsigma(X)$ for every $a\#X \in \Delta$. We must show that $[\![t]\!]^{[\mathbb{A}]\mathbb{X}}_{\varsigma} = [\![u]\!]^{[\mathbb{A}]\mathbb{X}}_{\varsigma}$.

Choose some c not mentioned in Δ, t, u, and such that $c\#\varsigma(X)$ for every X mentioned in Δ, t, u. Using Lemma 8.9 we can construct a valuation ς' to $|\mathbb{X}|$ such that $\varsigma(X) = ([c]\varsigma')(X)$ for every X mentioned in Δ, t, u, and therefore such that

$$[\![t]\!]^{[\mathbb{A}]\mathbb{X}}_{\varsigma} = [\![t]\!]^{[\mathbb{A}]\mathbb{X}}_{[c]\varsigma'} \qquad \text{and} \qquad [\![u]\!]^{[\mathbb{A}]\mathbb{X}}_{\varsigma} = [\![u]\!]^{[\mathbb{A}]\mathbb{X}}_{[c]\varsigma'}.$$

By Corollary 8.18

$$[\![t]\!]^{[\mathbb{A}]\mathbb{X}}_{[c]\varsigma'} = [c][\![t]\!]^{\mathbb{X}}_{\varsigma'} \qquad \text{and} \qquad [\![u]\!]^{[\mathbb{A}]\mathbb{X}}_{[c]\varsigma'} = [c][\![u]\!]^{\mathbb{X}}_{\varsigma'}.$$

By Lemma 8.12 $a\#\varsigma'(X)$ for every $a\#X \in \Delta$. We assumed that $\mathbb{X}$ is a model of T, so $[\![t]\!]^{\mathbb{X}}_{\varsigma'} = [\![u]\!]^{\mathbb{X}}_{\varsigma'}$ and therefore $[c][\![t]\!]^{\mathbb{X}}_{\varsigma'} = [c][\![u]\!]^{\mathbb{X}}_{\varsigma'}$. The result follows. □

9 Varieties and Equational Classes of Algebras

Definition 9.1 A **(nominal algebra) variety** $\mathcal{V}$ for a signature Σ is a collection of Σ-algebras closed under

- homomorphic images (Subsection 8.1),
- subalgebras (Subsection 8.2),
- countable products (Subsection 8.3),[3] and
- atoms-abstraction (Subsection 8.4).

That is:

- If $\mathbb{V} \in \mathcal{V}$ and $\mathbb{V}'$ is a homomorphic image of $\mathbb{V}$, then $\mathbb{V}' \in \mathcal{V}$.
- If $\mathbb{V} \in \mathcal{V}$ and $\mathbb{V}'$ is a subalgebra of $\mathbb{V}$ then $\mathbb{V}' \in \mathcal{V}$.

[3] It is not hard to generalise to closure under uncountable or larger products.

- If I is any countable indexing set and $\mathbb{V}_i \in \mathcal{V}$ for all $i \in I$ then $\Pi_{i\in I}\mathbb{V}_i \in \mathcal{V}$.
- If $\mathbb{V} \in \mathcal{V}$ then $[\mathbb{A}]\mathbb{V} \in \mathcal{V}$.

The notion of nominal algebra variety is standard [BS81] — except that we insist on closure under atoms-abstraction. Atoms-abstraction leaves 'ordinary sets' unaffected and in that sense Definition 9.1 specialises to the usual notion of variety.

Definition 9.2 Call a collection $\mathcal{V}$ of Σ-algebras **(nominal algebra) equational** when there is some theory $\mathsf{T} = (\Sigma, Ax)$ in nominal algebra such that $\mathcal{V}$ is the collection of *all* models of T.

From now on unless stated otherwise 'variety' means 'nominal algebra variety' and 'equational' means 'nominal algebra equational'.

Our main result is a version of the HSP theorem [BS81] for nominal algebra:

Theorem 9.3 *A collection of Σ-algebras $\mathcal{V}$ is equational (the collection of all models of some theory) if and only if it is a variety (closed under homomorphic images, subalgebras, countable products, and atoms-abstraction).*

The proof is the rest of this section, up to and including Subsection 9.3.

9.1 Surjections out of free algebras

Fix a signature Σ and a collection of Σ-algebras $\mathcal{V}$. In practice we care about the case that $\mathcal{V}$ is a variety, but nothing in this subsection depends on that.

Lemma 9.4 *Suppose $\mathbb{Y}$ is a model of theory $\mathsf{T} = (\Sigma, Ax)$. Suppose $\mathcal{D}$ is a set of fresh term-formers (so $\mathcal{D} \cap \Sigma = \emptyset$). Then the following data determines a Σ-algebra homomorphism from $\mathbb{F}(\mathsf{T}, \mathcal{D})$ to $\mathbb{Y}$: for each n-ary term-former $\mathsf{d} \in \mathcal{D}$*

- *a choice of n atoms $a_1, \ldots, a_n$ and*
- *a choice of element $\theta\mathsf{d}(a_1, \ldots, a_n) \in |\mathbb{Y}|$ such that*

$$supp(\theta\mathsf{d}(a_1, \ldots, a_n)) \subseteq \{a_1, \ldots, a_n\}.$$

This is an initiality property [Mac71] adapted to our particular situation of nominal sets.

Proof. We define a function, by abuse of notation write it θ, from $\mathbb{F}(\Sigma, \mathcal{D})$ to $|\mathbb{Y}|$ by:

- $\theta\mathsf{d}(\pi(a_1), \ldots, \pi(a_n)) = \pi \cdot \theta\mathsf{d}(a_1, \ldots, a_n)$.
- $\theta a = a_{\mathbb{Y}}$.
- $\theta[a]g = abs_{\mathbb{Y}}(a, g)$.
- $\theta\mathsf{f}(g_1, \ldots, g_n) = \mathsf{f}_{\mathbb{Y}}(\theta g_1, \ldots, \theta g_n)$.

Suppose we could prove that if $[g]_{\mathsf{T}} = [h]_{\mathsf{T}}$ then $\theta g = \theta h$. Then we can view θ as a function $\theta_{\mathbb{F}(\mathsf{T},\mathcal{D})}$ from $|\mathbb{F}(\mathsf{T}, \mathcal{D})|$ to $|\mathbb{Y}|$.

Also:

- It is easy to prove by induction on g that $\pi \cdot \theta g = \theta(\pi \cdot g)$, and it follows that

$$\pi \cdot (\theta_{\mathbb{F}(\mathsf{T},\mathcal{D})}[g]_{\mathsf{T}}) = \pi \cdot \theta g = \theta(\pi \cdot g) = \theta_{\mathbb{F}(\mathsf{T},\mathcal{D})}[g]_{\mathsf{T}}.$$

- $\theta_{\mathbb{F}(\mathsf{T},\mathcal{D})} a_{\mathbb{F}(\mathsf{T},\mathcal{D})} = \theta a = a_{\mathbb{Y}}$.
- $\theta_{\mathbb{F}(\mathsf{T},\mathcal{D})} abs_{\mathbb{F}(\mathsf{T},\mathcal{D})}(a, g) = \theta[a]g = abs(a, \theta g) = abs(a, \theta_{\mathbb{F}(\mathsf{T},\mathcal{D})}[g]_{\mathsf{T}})$.
- $\theta_{\mathbb{F}(\mathsf{T},\mathcal{D})} \mathsf{f}_{\mathbb{F}(\mathsf{T},\mathcal{D})}([g_1]_{\mathsf{T}}, \ldots, [g_n]_{\mathsf{T}}) = \theta \mathsf{f}(g_1, \ldots, g_n)$
$= \mathsf{f}_{\mathbb{Y}}(\theta g_1, \ldots, \theta g_n)$
$= \mathsf{f}_{\mathbb{Y}}(\theta_{\mathbb{F}(\mathsf{T},\mathcal{D})}[g_1]_{\mathsf{T}}, \ldots, \theta_{\mathbb{F}(\mathsf{T},\mathcal{D})}[g_n]_{\mathsf{T}})$.

It follows that θ viewed as a function from $|\mathbb{F}(\mathsf{T}, \mathcal{D})|$ to $|\mathbb{Y}|$ is also a Σ-algebra homomorphism and we are done.

It remains to prove that $[g]_{\mathsf{T}} = [h]_{\mathsf{T}}$ implies $\theta g = \theta h$. Suppose $\Pi \in \Pi(\mathsf{T}, \mathcal{D})$ (Definition 6.4) is a derivation of $\vdash_{\mathsf{T}} g = h$. Let $\mathcal{A} = \{a \mid a \in \Pi\}$ and let $\mathcal{D}'$ be the term-formers mentioned in Π. Let

$$(\Delta \vdash g^{-1}, \sigma, \mathcal{B}, \mathcal{X}) = \mathbb{F}(\Sigma, \mathcal{D}', \mathcal{A})^{-1}(g) \quad \text{and} \quad (\Delta \vdash h^{-1}, \sigma, \mathcal{B}, \mathcal{X}) = \mathbb{F}(\Sigma, \mathcal{D}', \mathcal{A})^{-1}(h).$$

Let $\varsigma(X) = \theta(\sigma(X))$. By an easy inductive argument we deduce that $\theta g = [\![g^{-1}]\!]^{\mathbb{Y}}_{\varsigma}$ and $\theta h = [\![h^{-1}]\!]^{\mathbb{Y}}_{\varsigma}$. By Theorem 7.9 $\Delta \vdash_{\mathsf{T}} g^{-1} = h^{-1}$. The result follows by Soundness (Theorem 5.6). □

We need some notation for the proof of Theorem 9.8:

Definition 9.5 Suppose that $\mathsf{T} = (\Sigma, Ax)$. Suppose that Σ-algebras $\mathbb{X}$ and $\mathbb{Y}_i$ for $i \in I$ are models of T. Suppose $\theta_i \in \mathbb{X} \Rightarrow \mathbb{Y}_i$ is a family of homomorphisms. Then write $\Pi_{i \in I} \theta_i$ for the natural map from $\mathbb{X}$ to $\Pi_{i \in I} \mathbb{Y}_i$, mapping $x \in |\mathbb{X}|$ to $(\theta_i x)_{i \in I} \in |\Pi_{i \in I} \mathbb{Y}_i|$.

It is easy to verify that $\Pi_{i \in I} \theta_i$ above is a homomorphism.

Theorem 9.6 *If $\mathbb{V} \in \mathcal{V}$ then there exists some (sufficiently large) set of fresh term-formers $\mathcal{D}$ such that there exists a Σ-algebra homomorphism θ from $\mathbb{F}(\mathsf{T}, \mathcal{D})$ to $\mathbb{V}$, such that θ is a surjection on underlying sets.*

That is: every element of $\mathcal{V}$ is a homomorphic image of some sufficiently large free algebra.

Proof. Write $\mathsf{car}(\mathbb{V})$ for the cardinality of $|\mathbb{V}|$. Suppose that $\mathcal{D}$ is a set of fresh term-formers with at least $\mathsf{car}(\mathbb{V})$ term-formers of every arity $n > 0$, and with no term-formers of arity 0. We shall exhibit a suitable θ from $\mathbb{F}(\mathsf{T}, \mathcal{D})$ to $\mathbb{V}$.

For each permutation equivalence class $\{\pi v \mid \pi \in \mathbb{P}\} \subseteq |\mathbb{V}|$ choose a representative $v \in |\mathbb{V}|$. For each v,

- order $supp(v)$ as $a_1, \ldots, a_n$, pick a unique n-ary term-former $\mathsf{d} \in \mathcal{D}$ (which has not been assigned to any other v'), and
- assign $\theta \mathsf{d}(a_1, \ldots, a_n) = v$.

For each remaining unassigned $\mathsf{d}(a,\ldots)$ assign $\theta\mathsf{d}(a,\ldots) = a_{\mathbb{V}}$.[4] By Lemma 9.4 this assignment extends to a homomorphism from $\mathbb{F}(\mathsf{T},\mathcal{D})$ to $\mathbb{V}$.

It remains to show that this is a surjection, but this is easy: Consider any $v' \in |\mathbb{V}|$. By construction there exists some representative v such that $v' \in \{\pi v \mid \pi \in \mathbb{P}\}$. So write $v' = \pi v$. By construction $v = \theta\mathsf{d}(a_1,\ldots,a_n)$ for some $\mathsf{d}(a_1,\ldots,a_n)$ and so $v' = \theta\mathsf{d}(\pi a_1,\ldots,\pi a_n)$. □

9.2 Injections out of free algebras

Fix a signature Σ and a set of Σ-algebras $\mathcal{V}$. As in Subsection 9.1 we care most about the case that $\mathcal{V}$ is a variety, but nothing in this subsection depends on assuming that.

Definition 9.7 Let $\mathsf{T} = (\Sigma, Ax)$ where Ax is the collection of judgements valid in all $\mathbb{V} \in \mathcal{V}$ for all valuations. Call T the theory **generated by** $\mathcal{V}$.

That is, $(\Delta \vdash t = u) \in Ax$ when for every $\mathbb{V} \in \mathcal{V}$ and every valuation ς to $|\mathbb{V}|$, it is the case that if $a\#\varsigma(X)$ for every $a\#X \in \Delta$ then $[\![t]\!]^{\mathbb{V}}_{\varsigma} = [\![u]\!]^{\mathbb{V}}_{\varsigma}$.

Theorem 9.8 *Suppose that $\mathcal{V}$ is a collection of Σ-algebras. Let T be the theory generated by $\mathcal{V}$. Suppose $\mathcal{D}$ is any set of fresh term-formers (so $\mathcal{D} \cap \Sigma = \emptyset$).*

Then there exists some indexing set I and algebras $\mathbb{V}_i \in \mathcal{V}$ for $i \in I$ such that there exists a Σ-algebra homomorphism θ from $\mathbb{F}(\mathsf{T},\mathcal{D})$ to $\Pi_{i\in I}\mathbb{V}_i$ such that θ is an injection on underlying sets.

Proof. Let I be the set of pairs (g,h) of ground terms in the signature $\Sigma \cup \mathcal{D}$ such that $[g]_{\mathsf{T}} \neq [h]_{\mathsf{T}}$.

Choose some $i = (g,h) \in I$.

Let $\mathcal{A} = \{a \mid a \in g\} \cup \{a \mid a \in h\}$. Let $\mathcal{D}'$ be the set of term-formers in $\mathcal{D}$ occurring in g and h. Recalling Lemma 7.4, suppose that

$$\mathbb{F}(\Sigma,\mathcal{D}',\mathcal{A})^{\text{-}1}(g) = (\Delta \vdash t,\ \sigma,\mathcal{B},\mathcal{X}) \quad \text{and} \quad \mathbb{F}(\Sigma,\mathcal{D}',\mathcal{A})^{\text{-}1}(h) = (\Delta \vdash u,\ \sigma,\mathcal{B},\mathcal{X}).$$

We assumed that $\not\vdash_{\mathsf{T}} g = h$ so by Corollary 7.6 $\Delta \not\vdash_{\mathsf{T}} t = u$. By our assumption that T is generated by $\mathcal{V}$, there exists some model $\mathbb{V}_i$ in $\mathcal{V}$ and valuation ς such that $[\![\Delta]\!]^{\mathbb{V}_i}_{\varsigma}$ is valid and $[\![t]\!]^{\mathbb{V}_i}_{\varsigma} \neq [\![u]\!]^{\mathbb{V}_i}_{\varsigma}$. Let

$$\{c_1,\ldots,c_p\} \quad \text{be} \quad \Big(\bigcup_{X\in\mathcal{X}} supp(\varsigma X)\Big) \setminus \mathcal{A}$$

in some order. Write $\mathbb{V}'_i$ for $[\mathbb{A}]^p\mathbb{V}_i$ and write ς' for $[c_1]\ldots[c_p]\varsigma$.

$\mathcal{V}$ is closed under atoms-abstraction so $\mathbb{V}'_i \in \mathcal{V}$. By Corollary 8.18

$$[\![t]\!]^{\mathbb{V}'_i}_{\varsigma'} \neq [\![u]\!]^{\mathbb{V}'_i}_{\varsigma'}.$$

We construct a partial assignment θ by

$$\theta\mathsf{d}(a_1,\ldots,a_n) = \varsigma' X$$

[4] This is why we insist that the fresh term-formers d have arity at least 1, and so are applied to at least one atom; this makes it easy to pick a default value to which to map them in $\mathbb{V}$.

for each $\mathsf{d} \in \mathcal{D}'$, where $X \in \mathcal{X}$ is the unknown corresponding to d, and $a_1, \ldots, a_n$ is the choice of atoms in order corresponding to d, in the sense given in Definition 7.1.

We want to use Lemma 9.4 to obtain a homomorphism θ from $\mathbb{F}(\mathsf{T}, \mathcal{D})$ to $\mathbb{V}'_i$ but in order to do so we must verify that $supp(\varsigma' X) \subseteq \{a_1, \ldots, a_n\}$.

Suppose that $a \notin \{a_1, \ldots, a_n\}$. By the rules in Figure 1 $\vdash a\#\mathsf{d}(a_1, \ldots, a_n)$. By Theorem 7.9 $\Delta \vdash a\#\mathsf{d}(a_1, \ldots, a_n)^{-1}$. By assumption $[\![\Delta]\!]^{\mathbb{V}'_i}_{\varsigma'}$ so by Soundness (Theorem 5.6) $a\#[\![\mathsf{d}(a_1, \ldots, a_n)^{-1}]\!]^{\mathbb{V}'_i}_{\varsigma'}$. Using Lemma 7.3 we deduce that $a\#\varsigma' X$. It follows that $supp(\varsigma' X) \subseteq \{a_1, \ldots, a_n\}$ as required.

Note that by construction $\theta([g]_{\mathsf{T}}) \neq \theta([h]_{\mathsf{T}})$.

It follows by the choice of $\mathbb{V}_i$ that $\Pi_{i \in I}\theta$ from $\mathbb{F}(\mathsf{T}, \mathcal{D})$ to $\Pi_{i \in I}\mathbb{V}'_i$ is injective as a map on underlying sets. □

Remark 9.9 The reader might ask why we bother with $[\mathbb{A}]\mathbb{V}$ when we can build this as the subalgebra of $\mathbb{V}$ in the image of $abs_{\mathbb{V}}$. The answer is that we cannot: $abs_{\mathbb{V}}$ is not necessarily injective in the sense given by Lemma 8.10. Without this property Corollary 8.18 is not possible and the proof of Theorem 9.8 fails. In a sorted version of nominal algebra with abstraction sorts we can insist that $abs_{\mathbb{V}}$ coincide with 'real' nominal sets abstraction — but in fact, this just pushes technicalities elsewhere; into the notions of algebra, subalgebra, product, and homomorphic image, and ultimately into the fact that to map out of an abstraction sort a term-former, write it abs, is required. This is an $abs_{\mathbb{V}}$ by another name.

Lemma 9.10 *Suppose that $\mathcal{V}$ is a variety and suppose T is the theory generated by $\mathcal{V}$. Then $\mathbb{F}(\mathsf{T}, \mathcal{D}) \in \mathcal{V}$ for every set of fresh term-formers $\mathcal{D}$.*

Proof. By Theorem 9.8 there is some indexing set I, set of Σ-algebras $\mathbb{V}_i \in \mathcal{V}$ for $i \in I$, and Σ-algebra homomorphism θ from $\mathbb{F}(\mathsf{T}, \mathcal{D})$ to $\Pi_{i \in I}\mathbb{V}_i$ that is an injection on underlying sets. $\mathcal{V}$ is closed under products so $\Pi_{i \in I}\mathbb{V}_i \in \mathcal{V}$. The image of $|\mathbb{F}(\mathsf{T}, \mathcal{D})|$ is a subalgebra of $\Pi_{i \in I}\mathbb{V}_i$, and $\mathbb{F}(\mathsf{T}, \mathcal{D})$ is a homomorphic image (by inverting θ) of that subalgebra. $\mathcal{V}$ is closed under subalgebras and homomorphic images, and the result follows. □

9.3 Proof of the nominal HSP theorem

Proof. [Proof of Theorem 9.3] Suppose that $\mathcal{V}$ is equational. By Lemma 8.7 $\mathcal{V}$ is closed under products. By Lemma 8.3 $\mathcal{V}$ is closed under homomorphic images. By Lemma 8.5 $\mathcal{V}$ is closed under subalgebras. By Lemma 8.19 $\mathcal{V}$ is closed under atoms-abstraction. Therefore $\mathcal{V}$ is a variety.

Conversely, suppose $\mathcal{V}$ is a variety. Let T be the theory on Σ generated by $\mathcal{V}$ as described in Definition 9.7. Let $\mathbb{V}$ be any model of T. By Theorem 9.6 there exists some $\mathcal{D}$ such that $\mathbb{V}$ is a homomorphic image of $\mathbb{F}(\mathsf{T}, \mathcal{D})$. By Lemma 9.10 $\mathbb{F}(\mathsf{T}, \mathcal{D}) \in \mathcal{V}$. Since $\mathcal{V}$ is closed under homomorphisms, $\mathbb{V} \in \mathcal{V}$ as required. Therefore $\mathcal{V}$ is equational. □

10 Conclusions

The form and intended use of nominal algebra fit squarely into the mathematical tradition of using the logic of equalities for specification and reasoning; nominal algebra is a flavour of universal algebra [BS81].

As discussed in the Introduction, universal algebra enjoys the HSP theorem [BS81, Theorem 11.12]. The technical contribution of this paper is to establish that nominal algebra satisfies a similar property. We must assume closure not only under homomorphisms, subalgebras, and product algebras (the 'H', 'S', and 'P' in 'HSP' respectively), but also under atoms-abstraction algebras whose (rather elegant) construction is introduced in this paper in Subsection 8.4. One might imagine that atoms-abstraction might be built out of homomorphisms, subalgebras, and product algebras. This may be possible, but the obvious constructions seem to fail. It remains an open problem whether closure under abstractions does or does not follow from the other closure properties considered in this paper.

The term-language of nominal algebra is *nominal terms* [UPG04]. Nominal terms extend first-order terms (the language of universal algebra) with object-level variables (atoms), and with constructs to support binding (nominal abstraction), α-equivalence (permutations), and capture-avoidance (freshness conditions). Nominal algebra was developed with Mathijssen [GM07a,Mat07]. A sound and complete semantics in nominal sets [GP01] has been explored (for full details see [Mat07, Section 3]).

The technical constructions used in this paper are similar to those used in the proofs of completeness for nominal algebra [Mat07, Subsection 3.4] but they are not a special case of them. Informally speaking, in the completeness proof we start with open terms and create ground terms (the σ from [Mat07, Subsection 3.4]); in this paper we start from ground terms and create open terms, a typical example is in the last paragraph of Lemma 9.4. Therefore, a different set of technical lemmas is required and they seem to 'point in the other direction' from the lemmas required to prove completeness. It would be interesting to place the two sets of proofs in a single development and draw out their common core. This is future work.

Another 'nominal' logic is nominal logic [Pit03]. This does not directly use nominal terms and nominal algebra is not the equality fragment of nominal logic; the two logics have different treatments of freshness [Mat07, Subsection 3.4.3] — nominal equational logic by Pitts and Clouston [CP07] is closer to being the equality fragment of nominal logic. To our knowledge an HSP result has not (yet) been obtained for nominal equational logic.

Sun has developed 'binding algebras' [Sun99]. Like nominal algebra, binding algebras are an algebraic framework enriched with constructs to support binding. Binding algebras are based on a functional semantics (that is, binding is modelled by a form of functional abstraction in syntax, and by restricted function-spaces in the semantics). Nominal techniques are not functional; binding is modelled by the Gabbay-Pitts model of abstraction in nominal sets [GP01]. Functional and nominal approaches seem to tend to achieve the same things in different ways; consider for example nominal rewriting [FG07] and combinatory reduction systems [KvOvR93] or higher-order rewrite systems [MN98]. Therefore it is not a surprise

to find a 'functional' algebraic framework for binding in the literature. The precise connection with nominal algebra is not well-understood. Concerning an HSP result for binding algebras, this is noted as an open problem [Sun99, Discussion 9.1] and to our knowledge it has not yet been solved.

References

[Bir35] Garrett Birkhoff. On the structure of abstract algebras. *Proceedings of the Cambridge Philosophical Society*, 31:433–454, 1935.

[BS81] S. Burris and H. Sankappanavar. *A Course in Universal Algebra*. Graduate texts in mathematics. Springer, 1981.

[CP07] Ranald A. Clouston and Andrew M. Pitts. Nominal equational logic. *ENTCS*, 172:223–257, 2007.

[CU03] J. Cheney and C. Urban. System description: Alpha-Prolog, a fresh approach to logic programming modulo alpha-equivalence. In *UNIF'03*, pages 15–19. Universidad Politecnica de Valencia, 2003.

[dB91] N.G. de Bruijn. Checking mathematics with computer assistance. *Notices of the American Mathematical Society (AMS)*, 38(1):8–15, 1991.

[FG07] Maribel Fernández and Murdoch J. Gabbay. Nominal rewriting (journal version). *Information and Computation*, 205(6):917–965, 2007.

[Gab07] Murdoch J. Gabbay. Fresh Logic. *Journal of Applied Logic*, 5(2):356–387, June 2007.

[GM06] Murdoch J. Gabbay and Aad Mathijssen. Capture-avoiding Substitution as a Nominal Algebra. In *ICTAC*, volume 4281 of *Lecture Notes in Computer Science*, pages 198–212, 2006.

[GM07a] Murdoch J. Gabbay and Aad Mathijssen. A formal calculus for informal equality with binding. In *WoLLIC'07: 14th Workshop on Logic, Language, Information and Computation*, volume 4576 of *Lecture Notes in Computer Science*, pages 162–176, 2007.

[GM07b] Murdoch J. Gabbay and Aad Mathijssen. One-and-a-halfth-order Logic (journal version). *Journal of Logic and Computation*, 18(4):521–562, November 2007.

[GM08] Murdoch Gabbay and Aad Mathijssen. Capture-Avoiding Substitution as a Nominal Algebra. *Formal Aspects of Computing*, 20(4-5):451–479, January 2008.

[GP01] Murdoch J. Gabbay and A. M. Pitts. A New Approach to Abstract Syntax with Variable Binding (journal version). *Formal Aspects of Computing*, 13(3–5):341–363, 2001.

[KvOvR93] J.-W. Klop, V. van Oostrom, and F. van Raamsdonk. Combinatory reduction systems. *Theoretical Computer Science*, 121:279–308, 1993.

[Mac71] S. Mac Lane. *Categories for the Working Mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer, 1971.

[Mat07] Aad Mathijssen. *Logical Calculi for Reasoning with Binding*. PhD thesis, Technische Universiteit Eindhoven, 2007.

[MN98] Richard Mayr and Tobias Nipkow. Higher-order rewrite systems and their confluence. *Theoretical Computer Science*, 192:3–29, 1998.

[MS06] G. Manzonetto and A. Salibra. Boolean algebras for lambda calculus. In *21th IEEE Symposium on Logic in Computer Science (LICS 2006)*, pages 317–326. IEEE Computer Society, 2006.

[Pit03] A. M. Pitts. Nominal logic, a first order theory of names and binding. *Information and Computation*, 186(2):165–193, 2003.

[Sal03] Antonino Salibra. Topological incompleteness and order incompleteness of the lambda calculus. *ACM Trans. Comput. Logic*, 4(3):379–401, 2003.

[Sun99] Yong Sun. An algebraic generalization of frege structures - binding algebras. *Theoretical Computer Science*, 211:189–232, 1999.

[UPG04] Christian Urban, Andrew M. Pitts, and Murdoch J. Gabbay. Nominal Unification. *Theoretical Computer Science*, 323(1–3):473–497, 2004.