Part II

General power constructions

This part contains the *algebraic theory of power domain constructions*. Power constructions are defined by axioms concerning existence and properties of some basic operations. One might worry about the actual choice of these axioms, but we think that our choice is quite natural. This opinion is strengthened by the fact that our definition covers the known power constructions, and allows to characterize them algebraically.

The basic operations and their axioms are presented in chapter 9. The subsequent chapters contain consequences of these axioms i.e. facts that hold for *all* power domain constructions. In chapter 10, a host of derived operations is defined by means of the basic operations, and their algebraic properties are studied. Among those, there is a multiplication that makes the power domain $\mathcal{P}\mathbf{1}$ over the one-point domain into a semiring, and the remaining power domains into $\mathcal{P}\mathbf{1}$-modules. The relations between some classifying properties of power constructions and of the semiring $\mathcal{P}\mathbf{1}$ are studied in chapter 11.

As power constructions are algebraic structures on a higher level, it is possible and useful to define homomorphisms between power constructions. These *power homomorphisms* are introduced in chapter 12. They allow to define *initial* and *final* constructions for a given semiring $\mathcal{P}\mathbf{1}$. The discussion of the initial construction is prepared by considering R-$\mathbf{X}$-modules in chapter 13. In chapters 14 and 15, we then prove that initial and final constructions exist for every semiring, and we derive their basic properties.

Since the concept of a semiring is very general, we thus obtain a host of power domain constructions. Their number is further increased by various methods to obtain new constructions from given ones.

The *core* of a power domain is the smallest sub-domain that still admits the power operations including multiplication. Taking the cores of all power domains of a power construction is shown to be a power construction again with the same characteristic semiring. Power constructions whose power domains equal their core, i.e. are minimal, are called *reduced*. Reduced power constructions enjoy many pleasant properties. The core and the notion of being reduced are studied in chapter 14.

A family of given power constructions may be combined to form a product power construction. In chapter 16, we present the definition of the product and its main properties. This chapter also deals with the question of factorization of power constructions.

Chapter 9

Specification of power constructions

In this chapter, we present the algebraic specification of power domain constructions. Power constructions are algebraic structures on a higher level: they have not just one carrier set with some operations, but instead map every domain $\mathbf{X}$ to a power domain $\mathcal{P}\mathbf{X}$ (see section 9.1). The power domains are equipped with special elements playing the role of an empty set and a binary operation representing set union (section 9.2). These operations together make the power domains into monoid domains (section 9.3). In addition, there has to be a singleton map for every ground domain that maps ground domain members into power domain elements representing formal singletons (section 9.4).

The most complex family of operations connected with a power construction is function extension. For every two domains $\mathbf{X}$ and $\mathbf{Y}$, there has to be a second order function *ext* that maps functions from $\mathbf{X}$ to $\mathcal{P}\mathbf{Y}$ into functions from $\mathcal{P}\mathbf{X}$ to $\mathcal{P}\mathbf{Y}$. The extension functional *ext* has to satisfy 7 axioms enumerated in section 9.5.

Section 9.6 shows that the well known powerset construction is a partial power domain construction that is defined for discretely ordered domains, i.e. sets, only. The final section 9.7 summarizes the specification of power domain constructions.

9.1 Constructions

A power construction is something like a function which applied to a domain $\mathbf{X}$ yields a new domain, the power domain over $\mathbf{X}$. It is not really a function since there is no *set* of all domains. There may be total constructions that are applicable to all domains, as well as partial constructions applicable to a special class of domains only.

Definition 9.1.1 A *(domain) construction* $\mathcal{F} : \mathbf{X} \mapsto \mathcal{F}\mathbf{X}$ attaches a domain $\mathcal{F}\mathbf{X}$ to every domain $\mathbf{X}$ belonging to a distinguished class *def* $\mathcal{F}$. $\mathcal{F}$ is a *total* construction if *def* $\mathcal{F}$ is the class of all domains, otherwise a *partial* one.

A *power (domain) construction* $\mathcal{P}$ is a domain construction satisfying the axioms presented in the next paragraphs. $\mathcal{P}\mathbf{X}$ is called the *power domain* over the *ground domain* $\mathbf{X}$. The elements of (the carrier of) $\mathcal{P}\mathbf{X}$ are called *formal sets*.

If a power construction $\mathcal{P}$ is defined for a class $C = \mathit{def}\ \mathcal{P}$, then the power domains $\mathcal{P}\mathbf{X}$ are not required to be in C again.

Often, a power domain cannot be realized concretely as a set of subsets of the ground domain. Hence the notion of formal sets in contrast to actual sets, i.e. the ordinary subsets of the ground domain. Formal set operations will be notationally distinguished from actual set operations by means of additional bars, e.g. $\uplus$ vs. $\cup$.

In the following, the symbol $\mathcal{P}$ denotes a generic partial power construction defined for a class $\mathrm{D} = \mathit{def}\ \mathcal{P}$ of domains. We immediately require the class D to contain the one-point-domain $\mathbf{1}$ because the power domain $\mathcal{P}\mathbf{1}$ plays an important algebraic role.

9.2 Empty set and finite union

As a first requirement, we want the power domain $\mathcal{P}\mathbf{X}$ to contain a formal empty set and to provide formal set union. Both the existence of an empty set and the axioms for union may be subject to discussions.

None of the original power domain constructions contained the empty set. However, they were sometimes extended by the empty set in later developments. The power constructions without empty set are briefly considered in section 17.7. For our work, the empty set is important and cannot be dispensed with.

Mathematical set theory suggests that union be commutative, associative, and idempotent. The last requirement turns out to be the least important one. For the sake of generality, we omit it as far as possible. Thus, the following results apply for 'multi-power' domain constructions as well.

For a (generalized) power construction $\mathcal{P}$, all power domains $\mathcal{P}\mathbf{X}$ have to be equipped with a commutative and associative operation $\uplus : [\mathcal{P}\mathbf{X} \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}]$. In addition, there has to be a point θ in $\mathcal{P}\mathbf{X}$ which is the neutral element of union '$\uplus$'. If union is idempotent, it is a real power construction, and otherwise a multi-power construction.

9.3 Monoid domains

To have generally applicable notions, we define the algebra of domains with empty set and union in a more abstract setting.

Definition 9.3.1 (Monoid domains and additive maps)

A *monoid domain* (or simply monoid) $(M, +, 0)$ is a domain M together with an associative operation $+ : [M \times M \to M]$ and an element 0 of (the carrier of) M which is the neutral element of '+'.

The monoid is *commutative* iff '+' is.

A map $f : [X \to Y]$ between two monoids is *additive* iff it is a *monoid homomorphism*, i.e. $f(0_X) = 0_Y$ and $f(a + b) = fa + fb$ hold.

Many authors, including myself in previous papers, call the additive maps linear. However, the term 'linear' is more appropriate for the module homomorphisms introduced in section 11.1. In many common cases, including the usual power constructions, additivity and linearity coincide as indicated in section 11.12.

9.4 Singleton sets

Returning to the power construction, we next require a morphism which maps elements into singleton sets. We denote it by $\iota = \{\!|.|\!\} : [\mathbf{X} \to \mathcal{P}\mathbf{X}]$, $x \mapsto \{\!|x|\!\}$.

By means of the operations θ and $\uplus$, we may extend $\{\!|.|\!\}$ to finite sequences of ground domain points:

$$\{\!|x_1, \ldots, x_n|\!\} = \begin{cases} \{\!|x_1|\!\} \uplus \cdots \uplus \{\!|x_n|\!\} & \text{if } n > 0 \\ \theta & \text{if } n = 0 \end{cases}$$

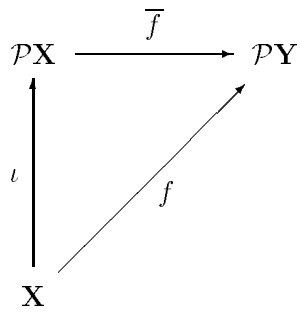
Because of commutativity and associativity, one is free to permute the n arguments of $\{\!|x_1, \ldots, x_n|\!\}$. If union is idempotent, one additionally might delete and add multiple occurrences of elements. Thus $\{\!|.|\!\}$ becomes a mapping from finite actual sets to formal sets in this case.

9.5 Function extension

So far, we required the existence of singletons, empty set, and binary union. Singleton and union are not yet interrelated by axioms, and there are no axioms yet relating power domains over different ground domains. Both relationships are established by the extension functional. It takes a set-valued function defined on points of a ground domain and extends it to formal sets.

Definition 9.5.1 Let $\mathbf{X}$ be a domain in D and $\mathbf{Z}$ an arbitrary domain. A function $F : [\mathcal{P}\mathbf{X} \to \mathbf{Z}]$ is an *extension* of a function $f : [\mathbf{X} \to \mathbf{Z}]$ iff $F\{\!|x|\!\} = fx$ holds for all x in X, or equivalently iff $F \circ \iota = f$.

For every two domains $\mathbf{X}$ and $\mathbf{Y}$ in D, *ext* is a morphism mapping morphisms from $\mathbf{X}$ to $\mathcal{P}\mathbf{Y}$ into morphisms from $\mathcal{P}\mathbf{X}$ to $\mathcal{P}\mathbf{Y}$. For every $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$, the extended function $\overline{f} = extf$ should be an additive extension of f. These axioms imply $\overline{f}\,\{\!|x_1, \ldots, x_n|\!\} = fx_1 \uplus \cdots \uplus fx_n$ for $n > 0$.



We call the *ext* axioms indicated above primary axioms because their relevance is immediate. In addition, we require some 'secondary axioms' which will be stated below as (Si). (S1) and (S2) specify additivity in the functional argument. In the next section, power constructions are shown to be functors by means of (S3) and (S4).

- For all domains $\mathbf{X}$, $\mathbf{Y}$ in D, there is a morphism $ext = \overline{\ } : [[\mathbf{X} \to \mathcal{P}\mathbf{Y}] \to [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]]$ with

(P1) $\overline{f}\,\theta = \theta$

(P2) $\overline{f}\,(A \uplus B) = (\overline{f}\,A) \uplus (\overline{f}\,B)$

(P3) $\overline{f}\,\{\!|x|\!\} = fx$ or: $\overline{f} \circ \iota = f$

Together, (P1) through (P3) mean $\overline{f}$ is an additive extension of f.

(S1) $ext\,(\lambda x.\,\theta)\,A = \theta$ or shortly $ext\,\underline{\theta} = \underline{\theta}$ where $\underline{\theta}$ denotes the constant function $\lambda x.\,\theta$.

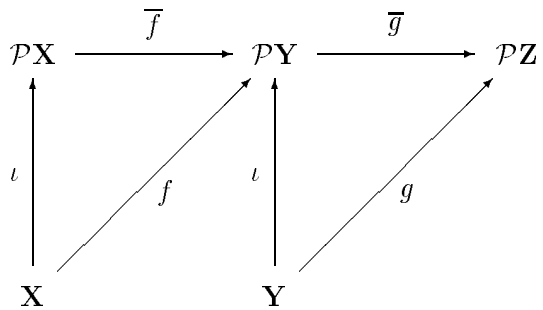
(S2) $ext\,(\lambda x.\,fx \uplus gx)\,A = (ext\,f\,A) \uplus (ext\,g\,A)$.
Raising '$\uplus$' to functions, one may shortly write $\overline{f \uplus g} = \overline{f} \uplus \overline{g}$.

(S3) $ext\,(\lambda x.\,\{\!|x|\!\})\,A = A$ or: $\overline{\iota} = id$

(S4) For every two morphisms $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ and $g : [\mathbf{Y} \to \mathcal{P}\mathbf{Z}]$,

$$ext\,g\,(ext\,f\,A) = ext\,(\lambda a.\,ext\,g\,(fa))\,A$$

holds for all A in $\mathcal{P}\mathbf{X}$, or: $\overline{g} \circ \overline{f} = \overline{\overline{g} \circ f}$



Note that we do not require $\overline{f}$ to be the only morphism satisfying (P1) through (P3) for given f. However, an important class of power constructions will have this property. For these constructions, (S1) through (S4) become provable (see section 14.5). That is why we call them secondary axioms.

9.6 Examples

Sets may be conceived as discrete domains, and all functions between discrete domains are continuous. Hence, ordinary is a partial power domain construction defined for discrete domains.

- $\mathcal{P}_{set}\,\mathbf{X} = \mathcal{P}\mathbf{X} = \{A \mid A \subseteq \mathbf{X}\}$ ordered discretely for discrete domains $\mathbf{X}$,
- $\theta = \emptyset$,
- $A \uplus B = A \cup B$,
- $\{\!|x|\!\} = \{x\}$,
- $ext\, f\, A = \bigcup_{a \in A} fa$.

Union is obviously commutative, associative, and the empty set is its neutral element. The axioms for extension read as follows:

(P1) $\bigcup_{a \in \emptyset} fa = \emptyset$ (P2) $\bigcup_{c \in A \cup B} fc = \bigcup_{a \in A} fa \cup \bigcup_{b \in B} fb$

(P3) $\bigcup_{x \in \{a\}} fx = fa$

(S1) $\bigcup_{a \in A} \emptyset = \emptyset$ (S2) $\bigcup_{a \in A}(fa \cup ga) = \bigcup_{a \in A} fa \cup \bigcup_{a \in A} ga$

(S3) $\bigcup_{a \in A}\{a\} = A$ (S4) $\bigcup\{gb \mid b \in \bigcup_{a \in A} fa\} = \bigcup_{a \in A}\bigcup_{b \in fa} gb$

All these equations hold, i.e. $\mathcal{P}_{set}$ is a power construction.

$ext\, f$ is not the only additive extension of f if $\mathbf{X}$ is infinite. Another additive extension of $f : \mathbf{X} \to \mathcal{P}_{set}\mathbf{Y}$ is $FA = \begin{cases} \bigcup_{a \in A} fa & \text{if } A \text{ is finite} \\ \mathbf{Y} & \text{otherwise} \end{cases}$
An extension functional defined in this manner would however violate axiom (S3).

The empty set and all singletons are finite, and finite unions of finite sets are finite. Hence, there is another power construction for sets:

$$\mathcal{P}_{fin}\,\mathbf{X} = \{A \subseteq \mathbf{X} \mid A \text{ is finite}\}$$

whose operations are the restrictions of the operations above. In this construction, every function $f : \mathbf{X} \to \mathcal{P}_{fin}\,\mathbf{Y}$ has a unique additive extension.

The two partial constructions introduced in this section are considered to some more extent in section 23.5.

9.7 Summary

A power construction is a tuple $(\mathrm{D}, \mathcal{P}, \theta, \uplus, \iota, \overline{\ })$ where

- D is a class of domains;
- $\mathcal{P}$ maps domains belonging to class D into domains;
- $\theta = (\theta_X)_{X\in\mathrm{D}}$ with $\theta_X : \mathcal{P}X$
- $\uplus = (\uplus_X)_{X\in\mathrm{D}}$ with $\uplus_X : [\mathcal{P}X \times \mathcal{P}X \to \mathcal{P}X]$
- $\iota = (\iota_X)_{X\in\mathrm{D}}$ with $\iota_X : [X \to \mathcal{P}X]$
- $\overline{\ } = (ext_{XY})_{X,Y\in\mathrm{D}}$ with $ext_{XY} : [[X \to \mathcal{P}Y] \to [\mathcal{P}X \to \mathcal{P}Y]]$

satisfying the axioms (domain indices are dropped!)

(C) $A \uplus B = B \uplus A$

(A) $A \uplus (B \uplus C) = (A \uplus B) \uplus C$

(N) $\theta \uplus A = A \uplus \theta = A$

(P1) $\overline{f}\,\theta = \theta$

(P2) $\overline{f}\,(A \uplus B) = (\overline{f}\,A) \uplus (\overline{f}\,B)$

(P3) $\overline{f} \circ \iota = f$

(S1) $\overline{\lambda x.\,\theta} = \lambda X.\,\theta$

(S2) $\overline{f \uplus g} = \overline{f} \uplus \overline{g}$ with '$\uplus$' raised to functions

(S3) $\overline{\iota} = id$

(S4) $\overline{g} \circ \overline{f} = \overline{\overline{g} \circ f}$

Chapter 10

Derived operations in a power construction

The operations as specified in the previous chapter allow to derive many other operations with useful algebraic properties. We first consider some set operations including function mapping (10.1), big union (10.2), and Cartesian product (10.3). Function mapping turns the power construction into a locally continuous functor.

In section 10.4, we concentrate on the power domain $\mathcal{P}\mathbf{1}$ over the one-point-domain $\mathbf{1}$ and show that it incorporates the inherent logic of the power construction in its operations. In section 10.5, existential quantification $\mathcal{E}$ is introduced. Given a formal set and a predicate, $\mathcal{E}$ intuitively tells whether some member of the set satisfies the predicate. In chapter 15, $\mathcal{E}$ will be used to define power domain constructions in terms of second order predicates. In section 10.6, other set predicates are derived from $\mathcal{E}$.

Elements of a power domain $\mathcal{P}\mathbf{X}$ may be multiplied by logical values, i.e. members of $\mathcal{P}\mathbf{1}$ (see section 10.7). Intuitively, multiplication of A by the logical value b results in the conditional *if* b *then* A *else* $\emptyset$. In case $\mathbf{X} = \mathbf{1}$, this operation induces a binary operation within $\mathcal{P}\mathbf{1}$. This operation may be interpreted as conjunction (section 10.8). The algebraic properties of these products make $\mathcal{P}\mathbf{1}$ into a semiring with union as addition, whereas the power domains become left semiring modules (cf. section 11.1).

Further derived operations are filtering of formal sets through predicates (section 10.9) and multiplication by logical values from the right (section 10.10). This alternative product has dual properties to the left product of section 10.7. It makes the power domains into right semiring modules.

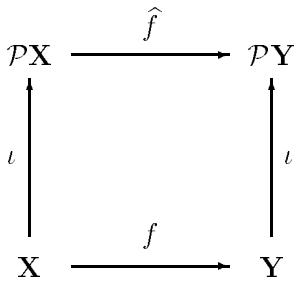
10.1 Mapping of functions over sets

Given a morphism $f : [\mathbf{X} \to \mathbf{Y}]$, it can be composed with the singleton operation to obtain $\iota \circ f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$. The resulting set-valued function can be extended to set arguments. Thus, we obtain

$$map = \widehat{\ } : \ [[\mathbf{X} \to \mathbf{Y}] \to [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]] \qquad \widehat{f} = \overline{\iota \circ f}.$$

The primary and some secondary axioms of extension may be translated into corresponding properties of *map*.

(P1)' $\widehat{f}\,\theta = \theta$
(P2)' $\widehat{f}\,(A \uplus B) = (\widehat{f}\,A) \uplus (\widehat{f}\,B)$
(P3)' $\widehat{f} \circ \iota = \iota \circ f$ or: $\widehat{f}\,\{\!|x|\!\} = \{\!|fx|\!\}$
(S3)' $\widehat{id} = id$
(S4)' $\widehat{g} \circ \widehat{f} = \widehat{g \circ f}$



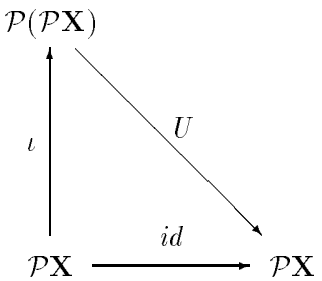
Proof:
(P1)' $\widehat{f}\,\theta = \overline{\iota \circ f}\,(\theta) = \theta$ by (P1)
(P2)' immediately by (P2)
(P3)' $\widehat{f} \circ \iota = \overline{\iota \circ f} \circ \iota = \iota \circ f$ by (P3)
(S3)' $\widehat{id} = \overline{\iota \circ id} = \overline{\iota} = id$ by (S3)
(S4)' $\widehat{g} \circ \widehat{f} = \overline{\iota \circ g} \circ \overline{\iota \circ f} \overset{(S4)}{=} \overline{\overline{\iota \circ g} \circ \iota \circ f} \overset{(P3)}{=} \overline{\iota \circ g \circ f} = \widehat{g \circ f}$ □

The properties (P1)' through (P3)' imply $\widehat{f}\,\{\!|x_1, \ldots, x_n|\!\} = \{\!|fx_1, \ldots, fx_n|\!\}$. The last two properties show that $\mathcal{P}$ becomes a functor by means of *map*. Since *map* is continuous when considered a second order function, this functor is locally continuous. Thus, theorems 7.4.4 and 7.5.6 apply, i.e.

- If $\mathcal{P}$ preserves FIN, then it also preserves F-ALG and F-CONT.
- If $\mathcal{P}$ preserves ALG, then it also preserves CONT.

10.2 Big union

If $\mathbf{X}$ is in D such that $\mathcal{P}\mathbf{X}$ is back in D again, the identity $id : [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}]$ may be extended to a morphism $U = \overline{id} : [\mathcal{P}(\mathcal{P}\mathbf{X}) \to \mathcal{P}\mathbf{X}]$. The axioms (P1) through (P3) of extension imply
(1) $U\,\theta = \theta$
(2) $U\,(A \uplus B) = UA \uplus UB$
(3) $U\,\{\!|S|\!\} = S$
whence $U\,\{\!|S_1, \ldots, S_n|\!\} = S_1 \uplus \cdots \uplus S_n$. Thus, U is a formal big union of formal sets of formal sets.



10.3 Double extension

Let $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$ be three domains in D, and let $\star : [\mathbf{X} \times \mathbf{Y} \to \mathcal{P}\mathbf{Z}]$ be a binary operation written in infix notation. By double extension, one obtains

$$A \overset{\rightarrow}{\star} B = ext\,(\lambda a.\, ext\,(\lambda b.\, a \star b)\,B)\,A \quad \text{and} \quad A \overset{\leftarrow}{\star} B = ext\,(\lambda b.\, ext\,(\lambda a.\, a \star b)\,A)\,B$$

The results are two morphisms $\overrightarrow{\star}$, $\overleftarrow{\star} : [\mathcal{P}\mathbf{X} \times \mathcal{P}\mathbf{Y} \to \mathcal{P}\mathbf{Z}]$.

A power construction is *symmetric* iff $A \overrightarrow{\star} B = A \overleftarrow{\star} B$ holds for all $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$ in D, A in $\mathcal{P}\mathbf{X}$, B in $\mathcal{P}\mathbf{Y}$, and $\star : [\mathbf{X} \times \mathbf{Y} \to \mathcal{P}\mathbf{Z}]$. Power constructions are not automatically symmetric. Later, we shall meet examples for this.

Our two sample power constructions for discrete domains — set of arbitrary subsets and set of finite subsets — are both symmetric because of

$$\bigcup_{a \in A} \bigcup_{b \in B} a \star b = \bigcup_{b \in B} \bigcup_{a \in A} a \star b$$

For two singletons, $\{\!|a|\!\} \overrightarrow{\star} \{\!|b|\!\} = \{\!|a|\!\} \overleftarrow{\star} \{\!|b|\!\} = a \star b$ may be shown using (P3) twice. Because of (P1) and (P2), '$\overrightarrow{\star}$' is obviously additive in its first argument:

$$\theta \overrightarrow{\star} B = \theta \qquad (A_1 \uplus A_2) \overrightarrow{\star} B = (A_1 \overrightarrow{\star} B) \uplus (A_2 \overrightarrow{\star} B)$$

For additivity in the second argument, (S1) and (S2) have to be employed in addition because B appears in the functional argument of the outer occurrence of *ext*. Thus, we get

$$A \overrightarrow{\star} \theta = \theta \qquad A \overrightarrow{\star} (B_1 \uplus B_2) = (A \overrightarrow{\star} B_1) \uplus (A \overrightarrow{\star} B_2)$$

'$\overleftarrow{\star}$' has the same properties; the proofs are however exchanged.

For formal finite sets, one then obtains

$$\{\!|x_1, \ldots, x_n|\!\} \overrightarrow{\star} \{\!|y_1, \ldots, y_m|\!\} = \{\!|x_1, \ldots, x_n|\!\} \overleftarrow{\star} \{\!|y_1, \ldots, y_m|\!\} = (x_1 \star y_1) \uplus (x_1 \star y_2) \uplus \cdots \uplus (x_1 \star y_m) \uplus (x_2 \star y_1) \uplus \cdots \uplus (x_n \star y_m)$$

Cartesian product of formal sets is a special instance of double extension. If $\mathbf{X}$ and $\mathbf{Y}$ are in D such that $\mathbf{X} \times \mathbf{Y}$ is also in D, then

$$A \overrightarrow{\times} B = ext\,(\lambda a.\, ext\,(\lambda b.\, \{\!|(a,b)|\!\})\, B)\, A \quad \text{and}$$
$$A \overleftarrow{\times} B = ext\,(\lambda b.\, ext\,(\lambda a.\, \{\!|(a,b)|\!\})\, A)\, B$$

are formal Cartesian products.

If the class D where the power construction is defined is closed w.r.t. Cartesian product, then symmetry may be defined in terms of formal Cartesian products because of the following proposition:

Proposition 10.3.1 Let $\mathbf{X}$ and $\mathbf{Y}$ be in D such that $\mathbf{X} \times \mathbf{Y}$ also is in D. Then for all $\mathbf{Z}$ in D and $\star : [\mathbf{X} \times \mathbf{Y} \to \mathcal{P}\mathbf{Z}]$, $A \overrightarrow{\star} B = ext\,(\star)\,(A \overrightarrow{\times} B)$ and $A \overleftarrow{\star} B = ext\,(\star)\,(A \overleftarrow{\times} B)$ hold.

Proof:

$$\begin{aligned} ext\,(\star)\,(A \overrightarrow{\times} B) &= ext\,(\star)\,(ext\,(\lambda a.\, ext\,(\lambda b.\, \{\!|(a,b)|\!\})\, B)\, A) \\ &\overset{(S4)}{=} ext\,(\lambda a.\, ext\,(\star)\,(ext\,(\lambda b.\, \{\!|(a,b)|\!\})\, B))\, A \\ &\overset{(S4)}{=} ext\,(\lambda a.\, ext\,(\lambda b.\, ext\,(\star)\,\{\!|(a,b)|\!\})\, B)\, A \\ &\overset{(P3)}{=} ext\,(\lambda a.\, ext\,(\lambda b.\, a \star b)\, B)\, A \end{aligned}$$

The statement about '$\overleftarrow{\star}$' and '$\overleftarrow{\times}$' is proved analogously. □

Corollary 10.3.2 Let $\mathcal{P}$ be a power construction such that D = *def* $\mathcal{P}$ is closed w.r.t. product, i.e. $\mathbf{X}$, $\mathbf{Y}$ in D implies $\mathbf{X} \times \mathbf{Y}$ in D. Then $\mathcal{P}$ is symmetric iff for all $\mathbf{X}$, $\mathbf{Y}$ in D, A in $\mathcal{P}\mathbf{X}$, and B in $\mathcal{P}\mathbf{Y}$, $A \overrightarrow{\times} B = A \overleftarrow{\times} B$ holds.

10.4 The logic of power constructions

Each power construction is equipped with an inherent logic. In this section, we present the domain of logical values together with disjunction and existential quantification. The corresponding conjunction is defined in section 10.8.

The domain of logical values is obtained by interpreting the power domain $\mathcal{P}\mathbf{1}$ where $\mathbf{1} = \{\diamond\}$. It has at least two elements: θ and $\{|\diamond|\}$, and is equipped with the binary operation '$\uplus$'. We interpret θ as F, $\{|\diamond|\}$ as T, and '$\uplus$' as formal disjunction '$\curlyvee$'. From the power axioms, one gets the following properties:

- '$\curlyvee$' is commutative and associative.
- $\mathsf{F} \curlyvee a = a \curlyvee \mathsf{F} = a$ for all a in $\mathcal{P}\mathbf{1}$.
- In case of a real power construction, one additionally has $a \curlyvee a = a$ for all a in $\mathcal{P}\mathbf{1}$.

Table of values for a generalized power construction:

$\curlyvee$	F	T
F	F	T
T	T	?

for a real power construction:

$\curlyvee$	F	T
F	F	T
T	T	T

Further statements about $\mathcal{P}\mathbf{1}$ beyond the ones above are not possible for generic power constructions. In particular, one does not know whether there are further logical values besides T and F, and $a \curlyvee \mathsf{T} = \mathsf{T}$ does not generally hold, even for real power constructions. There is no information about the relative order of F and T; F might be below T, above T, or incomparable to T.

The two power set constructions — set of arbitrary subsets and set of finite subsets — both have the same logic: $\mathcal{P}\mathbf{1}$ is $\{\emptyset, \{\diamond\}\}$ or $\{\mathsf{F}, \mathsf{T}\}$ with ordinary disjunction.

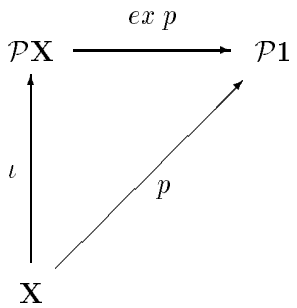
10.5 Existential quantification

Extension $ext : [[\mathbf{X} \to \mathcal{P}\mathbf{Y}] \to [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]]$ is polymorphic over the domains $\mathbf{X}$ and $\mathbf{Y}$. In this section, we consider the special case $\mathbf{Y} = \mathbf{1}$; section 10.7 is concerned with $\mathbf{X} = \mathbf{1}$.

Extension to the one-point domain $ex : [[\mathbf{X} \to \mathcal{P}\mathbf{1}] \to [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{1}]]$ [1] may be logically interpreted along the lines of the previous section. It has the following properties:

[1] This morphism is called *ex* to distinguish it from the fully polymorphic *ext*.

(P1) $ex\ p\ \theta = \mathsf{F}$
(P2) $ex\ p\ (A \uplus B) = (ex\ p\ A) \curlyvee (ex\ p\ B)$
(P3) $ex\ p\ \{\!|x|\!\} = p\ x$
(S1) $ex\ (\lambda x.\, \mathsf{F})\ A = \mathsf{F}$
(S2) $ex\ (\lambda x.\, p\ x \curlyvee q\ x)\ A = (ex\ p\ A) \curlyvee (ex\ q\ A)$
(S4) $ex\ p\ (ext\ f\ A) = ex\ (\lambda a.\, ex\ p\ (f a))\ A$



whence $ex\ f\ \{\!|x_1, \ldots, x_n|\!\} = f x_1 \curlyvee \cdots \curlyvee f x_n$. Thus, ex means existential quantification. It takes a predicate $p : [\mathbf{X} \to \mathcal{P}\mathbf{1}]$ and a formal set A and tells whether some member of A satisfies p. (S4) then informally reads: There is x in $\bigcup_{a \in A} f a$ satisfying p iff there is a in A such that there is x in $f a$ satisfying p.

Existential quantification may also be used to translate formal sets into second order predicates. For this end, we exchange the order of arguments of ex by uncurrying, twisting, and then currying again. The outcome is a morphism $\mathcal{E} : [\mathcal{P}\mathbf{X} \to [[\mathbf{X} \to \mathcal{P}\mathbf{1}] \to \mathcal{P}\mathbf{1}]]$ mapping formal sets into second order predicates. The properties of ex presented above translate easily into properties of $\mathcal{E}$:

(P1) $\mathcal{E}\ \theta = \lambda p.\, \mathsf{F}$
(P2) $\mathcal{E}\ (A \uplus B) = \lambda p.\, (\mathcal{E}\ A\ p) \curlyvee (\mathcal{E}\ B\ p)$
(P3) $\mathcal{E}\ \{\!|x|\!\} = \lambda p.\, p\ x$
(S4) $\mathcal{E}\ (ext\ f\ A) = \lambda p.\, \mathcal{E}\ A\ (\lambda a.\, \mathcal{E}\ (f a)\ p)$

These results suggest to define a power construction for given domain $\mathcal{P}\mathbf{1}$ by (a slight variant of) $\mathcal{P}\mathbf{X} = [[\mathbf{X} \to \mathcal{P}\mathbf{1}] \to \mathcal{P}\mathbf{1}]$. This method to obtain power constructions will be presented and explored in chapter 15.

By (S1), $ex\ (\lambda x.\, \mathsf{F})\ A = \mathsf{F}$ holds for all formal sets A. And what about $ex\ (\lambda x.\, \mathsf{T})$? It maps the empty set to F by (P1), and singletons to T by (P3). Hence, it is a predicate checking for non-emptiness — at least in the case of real power constructions with idempotent union. In case of multi-power constructions, it is better interpreted as cardinality.

- $ne = ex\ (\lambda x.\, \mathsf{T}) : [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{1}]$

(P1) $ne\ \theta = \mathsf{F}$
(P2) $ne\ (A \uplus B) = (ne\ A) \curlyvee (ne\ B)$
(P3) $ne\ \{\!|x|\!\} = \mathsf{T}$
(S4) $ne\ (ext\ f\ A) = ext\ (ne \circ f)\ A$

- For all B in $\mathcal{P}\mathbf{1}$, $ne\ B = B$.

Proof: Properties (P1) through (P3) are immediate. For (S4), note $ne \circ ext\ f = ext\ \underline{\mathsf{T}} \circ ext\ f = ext\ (ext\ \underline{\mathsf{T}} \circ f) = ext\ (ne \circ f)$ holds by (S4) where $\underline{\mathsf{T}}$ abbreviates $\lambda x.\, \mathsf{T}$.

The function $\lambda x.\, \mathsf{T} = \lambda x.\, \{\diamond\}$ on domain $\mathbf{1}$ coincides with the singleton map ι since the only possible argument is $\diamond$. Thus, $ne = ext\ \iota = id$ on $\mathcal{P}\mathbf{1}$ because of (S3). □

For a real power construction, $\mathsf{T} \curlyvee \mathsf{T} = \mathsf{T}$ holds. Then by (P1) through (P3), $ne\ \{\!|x_1, \ldots, x_n|\!\}$ is T if $n > 0$, and F if $n = 0$.

10.6 Other set predicates

Assume $\mathcal{P}$ is a real power construction i.e. $A \uplus A = A$, and assume $\mathcal{P}\mathbf{1}$ provides a negation $\neg : [\mathcal{P}\mathbf{1} \to \mathcal{P}\mathbf{1}]$ such that $\neg\mathsf{F} = \mathsf{T}$ and $\neg\mathsf{T} = \mathsf{F}$. (There are real power constructions that do not admit such a negation.) Then one may define a conjunction by $a \curlywedge b = \neg(\neg a \curlyvee \neg b)$. (In section 10.8, we define a conjunction for every power construction without using negation.)

With these assumptions, one may derive further predicates on formal sets.

- $\mathit{forall} : [[\mathbf{X} \to \mathcal{P}\mathbf{1}] \to [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{1}]]$ defined by $\mathit{forall}\ p\ S = \neg(\mathit{ex}\ (\lambda x.\, \neg(p\, x))\ S)$
  This implies $\mathit{forall}\ p\ \{\!|x_1, \ldots, x_n|\!\} = p\, x_1 \curlywedge \cdots \curlywedge p\, x_n$ for $n > 0$.
- $\mathit{empty} : [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{1}]$ defined by $\mathit{empty}\ S = \neg(\mathit{ex}\ (\lambda x.\, \mathsf{T})\ S) = \mathit{forall}\ (\lambda x.\, \mathsf{F})\ S$
  Hence, we obtain $\mathit{empty}\ \{\!|x_1, \ldots, x_n|\!\} = \begin{cases} \mathsf{T} & \text{if } n = 0 \\ \mathsf{F} & \text{if } n > 0 \end{cases}$

For the tests of containment, inclusion, and set equality, we need an equality morphism $==: [\mathbf{X} \times \mathbf{X} \to \mathcal{P}\mathbf{1}]$ given on the ground domain.

- $_\ \mathit{in}\ _ : \quad [\mathbf{X} \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{1}] \quad x\ \mathit{in}\ B \quad = \quad \mathit{ex}\ (\lambda b.\, x == b)\ B$
- $_\ \overline{\subseteq}\ _ : \quad [\mathcal{P}\mathbf{X} \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{1}] \quad A\ \overline{\subseteq}\ B \quad = \quad \mathit{forall}\ (\lambda a.\, a\ \mathit{in}\ B)\ A$
- $_ == _ : \quad [\mathcal{P}\mathbf{X} \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{1}] \quad (A == B) \quad = \quad (A\ \overline{\subseteq}\ B) \curlywedge (B\ \overline{\subseteq}\ A)$

10.7 Multiplication by a logical value

In this section, we consider extension of a morphism with domain $\mathbf{1}$, i.e. the instance $\mathit{ext} : [[\mathbf{1} \to \mathcal{P}\mathbf{X}] \to [\mathcal{P}\mathbf{1} \to \mathcal{P}\mathbf{X}]]$. The function space $[\mathbf{1} \to \mathcal{P}\mathbf{X}]$ is isomorphic to $\mathcal{P}\mathbf{X}$. Thus, we get a morphism $[\mathcal{P}\mathbf{X} \to [\mathcal{P}\mathbf{1} \to \mathcal{P}\mathbf{X}]]$. Uncurrying and exchanging arguments leads to the 'product' $\cdot : [\mathcal{P}\mathbf{1} \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}]$. The definition is $b \cdot S = \mathit{ext}\,(\lambda\diamond.\, S)\,b$. We call this product external since its left operand is not a member of $\mathcal{P}\mathbf{X}$. The axioms of ext imply the characteristic properties of the product.

Proposition 10.7.1

(P1·) $\mathsf{F} \cdot S = \theta$
(P2·) $(a \curlyvee b) \cdot S = (a \cdot S) \uplus (b \cdot S)$
(P3·) $\mathsf{T} \cdot S = S$
(S1·) $b \cdot \theta = \theta$
(S2·) $b \cdot (S_1 \uplus S_2) = (b \cdot S_1) \uplus (b \cdot S_2)$
(S4·) $\mathit{ext}\, f\, (b \cdot S) = b \cdot (\mathit{ext}\, f\, S)$
(S4a·) $(a \cdot b) \cdot S = a \cdot (b \cdot S)$
(SY·) If $\mathcal{P}$ is symmetric, then $\mathit{ext}\,(\lambda x.\, b \cdot fx)\, S = b \cdot (\mathit{ext}\, f\, S)$

Algebraists will notice that these properties essentially are the axioms of left modules. This topic will be further explored in section 11.1.

Proof:

$$
\begin{array}{lll}
(\mathrm{P1}\cdot) & \mathsf{F}\cdot S = ext\,(\lambda\diamond.\,S)\,\theta = \theta & \\
(\mathrm{P2}\cdot) & (a \curlyvee b)\cdot S = ext\,(\lambda\diamond.\,S)\,(a \uplus b) \text{ etc.} & \\
(\mathrm{P3}\cdot) & \mathsf{T}\cdot S = ext\,(\lambda\diamond.\,S)\,\{\!|\diamond|\!\} = (\lambda\diamond.\,S)\,\diamond = S & \\
(\mathrm{S1}\cdot) & b\cdot\theta = ext\,(\lambda\diamond.\,\theta)\,b = \theta & \\
(\mathrm{S2}\cdot) & b\cdot(S_1 \uplus S_2) = ext\,(\lambda\diamond.\,S_1 \uplus S_2)\,b \text{ etc.} & \\
(\mathrm{S4}\cdot) & ext\,f\,(b\cdot S) = ext\,f\,(ext\,(\lambda\diamond.\,S)\,b) & \\
 & (\mathrm{S4}): \quad = ext\,(\lambda\diamond.\,ext\,f\,((\lambda\diamond.\,S)\,\diamond))\,b & \\
 & \quad = ext\,(\lambda\diamond.\,ext\,f\,S)\,b & \\
 & \quad = b\cdot(ext\,f\,S) & \\
(\mathrm{S4a}\cdot) & (a\cdot b)\cdot S = ext\,(\lambda\diamond.\,S)\,(a\cdot b) & \\
 & (\mathrm{S4}\cdot): \quad = a\cdot(ext\,(\lambda\diamond.\,S)\,b) & \\
 & \quad = a\cdot(b\cdot S) & \\
(\mathrm{SY}\cdot) & ext\,(\lambda x.\,b\cdot fx)\,S = ext\,(\lambda x.\,ext\,(\lambda\diamond.\,fx)\,b)\,S & \\
 & \text{by symmetry:} \quad = ext\,(\lambda\diamond.\,ext\,(\lambda x.\,fx)\,S)\,b & \\
 & \quad = b\cdot(ext\,f\,S) & \square
\end{array}
$$

Interpreted logically, the product $b\cdot S$ resembles the conditional 'if b then S else θ'. At least for the cases $b = \mathsf{T}$ and $b = \mathsf{F}$, product and conditional coincide because of $\mathsf{T}\cdot S = S$ and $\mathsf{F}\cdot S = \theta$.

10.8 Conjunction

Up to now, the logical domain $\mathcal{P}\mathbf{1}$ was only equipped with constants F and T and a disjunction '$\curlyvee$'. We now interpret the external product on $\mathcal{P}\mathbf{1}$ as conjunction since $a\cdot b$ resembles 'if a then b else θ'.

$$\curlywedge : [\mathcal{P}\mathbf{1}\times\mathcal{P}\mathbf{1}\to\mathcal{P}\mathbf{1}],\ a \curlywedge b = a\cdot b$$

The algebraic properties of conjunction are given by the next proposition:

Proposition 10.8.1

- $\mathsf{F} \curlywedge b = b \curlywedge \mathsf{F} = \mathsf{F}$
- Distributivities: $(a_1 \curlyvee a_2) \curlywedge b = (a_1 \curlywedge b) \curlyvee (a_2 \curlywedge b)$
  $a \curlywedge (b_1 \curlyvee b_2) = (a \curlywedge b_1) \curlyvee (a \curlywedge b_2)$
- Neutral element: $\mathsf{T} \curlywedge b = b \curlywedge \mathsf{T} = b$
- Associativity: $(a \curlywedge b) \curlywedge c = a \curlywedge (b \curlywedge c)$
- If the construction $\mathcal{P}$ is symmetric, then '$\curlywedge$' is commutative.

Proof:

- F: immediate by (P1·) and (S1·)
- Distributivities: (P2·) and (S2·)

- T: $\mathsf{T} \barwedge b = b$ holds by (P3·). $b \barwedge \mathsf{T} = \mathit{ext}\,(\lambda\diamond.\,\{\!|\diamond|\!\})\,b = b$ holds by (S3).
- Associativity is just (S4a·).
- Commutativity: $a \barwedge b = \mathit{ext}\,(\lambda\diamond.\,b)\,a = \mathit{ext}\,(\lambda\diamond.\,b \cdot \mathsf{T})\,a =$ using (SY·) $b \cdot \mathit{ext}\,(\lambda\diamond.\,\mathsf{T})\,a = b \barwedge (a \barwedge \mathsf{T}) = b \barwedge a$ □

The axioms of generic power constructions do not allow to derive more algebraic properties for conjunction. In particular, idempotence of conjunction, the opposite distributivities, and the laws of absorption do not generally hold. On the other hand, the existing laws are powerful enough to obtain the following table of values:

$\barwedge$	F	T
F	F	F
T	F	T

10.9 Filtering a set through a predicate

We also want to provide an operation that filters a set through a given predicate w.r.t. the $\mathcal{P}\mathbf{1}$-logic. The operation $\mathit{filter} : [[\mathbf{X} \to \mathcal{P}\mathbf{1}] \to [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}]]$ should be additive in its set argument as well as in its predicate argument and operate on singletons as one expects i.e.

$$\mathit{filter}\,p\,\{\!|x|\!\} \;=\; \text{if } p\,x \text{ then } \{\!|x|\!\} \text{ else } \theta \;=\; p\,x \cdot \{\!|x|\!\}$$

This suggests to define $\mathit{filter}\,p\,S = \mathit{ext}\,(\lambda x.\,p\,x \cdot \{\!|x|\!\})\,S$
Employing the axioms of extension, one immediately gets

(P1f) $\mathit{filter}\,p\,\theta = \theta$

(P2f) $\mathit{filter}\,p\,(A \uplus B) = (\mathit{filter}\,p\,A) \uplus (\mathit{filter}\,p\,B)$

(P3f) $\mathit{filter}\,p\,\{\!|x|\!\} = p\,x \cdot \{\!|x|\!\}$

(S1f) $\mathit{filter}\,(\lambda x.\,\mathsf{F})\,S = \theta$

(S2f) $\mathit{filter}\,(p \barvee q)\,A = (\mathit{filter}\,p\,A) \uplus (\mathit{filter}\,q\,A)$

(S3f) $\mathit{filter}\,(\lambda x.\,\mathsf{T})\,S = S$

(S4f) $\mathit{filter}\,p\,(b \cdot S) = b \cdot (\mathit{filter}\,p\,S)$ by (S4·).

Property (P3f) implies $\mathit{filter}\,(\lambda x.\,b)\,\{\!|x|\!\} = b \cdot \{\!|x|\!\}$. One might believe that this equation may be generalized from singletons to arbitrary sets. However, this is only valid for symmetric constructions.

(SYf) If $\mathcal{P}$ is symmetric then (SYf) $\mathit{filter}\,(\lambda x.\,b)\,S = b \cdot S$.

Proof: $\mathit{filter}\,(\lambda x.\,b)\,S = \mathit{ext}\,(\lambda x.\,b \cdot \{\!|x|\!\})\,S = b \cdot (\mathit{ext}\,(\lambda x.\,\{\!|x|\!\})\,S) = b \cdot S$ using (SY·) and then (S3). (SY·) was shown for symmetric constructions only. □

Filtering by a predicate p first and then by a predicate q is intuitively equivalent to filtering by $p \barwedge q$.

Proposition 10.9.1 (Composition of filter operations)
$\mathit{filter}\,q \circ \mathit{filter}\,p \;=\; \mathit{filter}\,(p \barwedge q)$

Proof:

$$\begin{array}{lcl}
\mathit{filter}\, q \circ \mathit{filter}\, p & = & \mathit{ext}\,(\lambda x.\, q\, x \cdot \{\!|x|\!\}) \circ \mathit{ext}\,(\lambda y.\, p\, y \cdot \{\!|y|\!\}) \\
(\mathrm{S4}): & = & \mathit{ext}\,(\lambda y.\, \mathit{ext}\,(\lambda x.\, q\, x \cdot \{\!|x|\!\})\,(p\, y \cdot \{\!|y|\!\})) \\
(\mathrm{S4f}): & = & \mathit{ext}\,(\lambda y.\, p\, y \cdot (\mathit{ext}\,(\lambda x.\, q\, x \cdot \{\!|x|\!\})\,\{\!|y|\!\})) \\
(\mathrm{P3}): & = & \mathit{ext}\,(\lambda y.\, p\, y \cdot (q\, y \cdot \{\!|y|\!\})) \\
(\mathrm{Associativity}): & = & \mathit{ext}\,(\lambda y.\, (p\, y \mathbin{\dot{\wedge}} q\, y) \cdot \{\!|y|\!\}) \\
 & = & \mathit{filter}\,(p \mathbin{\dot{\wedge}} q) \qquad \square
\end{array}$$

10.10 Multiplication by a logical value from the right

In section 10.7, we defined a left external product, i.e. multiplication by a logical value from the left:

$$\cdot_L = \cdot : [\mathcal{P}\mathbf{1} \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}],\ b \cdot S = \mathit{ext}\,(\lambda\diamond.\, S)\, b$$

In the previous section, we saw that $\mathit{filter}\,(\lambda x.\, b)\, S$ does not generally coincide with $b \cdot S$ except in the symmetric case. The idea is now to write filtering by a constant predicate as a right product.

$$\cdot_R = \cdot : [\mathcal{P}\mathbf{X} \times \mathcal{P}\mathbf{1} \to \mathcal{P}\mathbf{X}],\ S \cdot b = \mathit{filter}\,(\lambda x.\, b)\, S$$

We want to use the same operation symbol '$\cdot$' for left and right product. The following proposition assures that this may be safely done even in the case $\mathbf{X} = \mathbf{1}$.

Proposition 10.10.1 For all a, b in $\mathcal{P}\mathbf{1}$, $a \cdot_L b = a \cdot_R b$ holds.

Proof:

$$\begin{array}{lcl}
a \cdot_R b & = & \mathit{filter}\,(\lambda x.\, b)\, a \;=\; \mathit{filter}\,(\lambda x.\, b)\,(a \cdot_L \mathsf{T}) \\
(\mathrm{S4f}): & = & a \cdot_L \mathit{filter}\,(\lambda x.\, b)\, \mathsf{T} \\
\mathsf{T} = \{\diamond\},\ (\mathrm{P3f}): & = & a \cdot_L (b \cdot_L \mathsf{T}) \;=\; a \cdot_L b
\end{array}$$

$\square$

The algebraic properties of the right product are analogous to that of the left product. In the following, capital letters range over $\mathcal{P}\mathbf{X}$ and small letters over $\mathcal{P}\mathbf{1}$.

Proposition 10.10.2

(1) $S \cdot \mathsf{F} = \theta$

(2) $S \cdot (a \mathbin{\dot{\vee}} b) = (S \cdot a) \uplus (S \cdot b)$

(3) $S \cdot \mathsf{T} = S$

(4) $\theta \cdot b = \theta$

(5) $(S_1 \uplus S_2) \cdot b = (S_1 \cdot b) \uplus (S_2 \cdot b)$

(6) $\mathit{ext}\,(\lambda x.\, f x \cdot b)\, S = (\mathit{ext}\, f\, S) \cdot b$

(7) $S \cdot (a \cdot b) = (S \cdot a) \cdot b$

(8) $(a \cdot S) \cdot b = a \cdot (S \cdot b)$

(9) $a \cdot \{\!|x|\!\} = \{\!|x|\!\} \cdot a$

(10) If $\mathcal{P}$ is symmetric, then $a \cdot S = S \cdot a$

Proof: For a constant b in $\mathcal{P}\mathbf{1}$, we abbreviate $\lambda x.\, b$ by $\underline{b}$.

(1) $S \cdot \mathsf{F} \;=\; \mathit{filter}\, \underline{\mathsf{F}}\, S \;=\; \theta$ by (S1f)

(2) $S \cdot (a \uplus b) \;=\; \mathit{filter}\, (\lambda x.\, a \uplus b)\, S$ Use (S2f)

(3) $S \cdot \mathsf{T} \;=\; \mathit{filter}\, \underline{\mathsf{T}}\, S \;=\; S$ by (S3f)

(4) $\theta \cdot b \;=\; \mathit{filter}\, \underline{b}\, \theta \;=\; \theta$ by (P1f)

(5) $(S_1 \uplus S_2) \cdot b \;=\; \mathit{filter}\, \underline{b}\, (S_1 \uplus S_2)$ Use (P2f)

(6)
$$\begin{aligned} (\mathit{ext}\, f\, S) \cdot b \;&=\; \mathit{ext}\, (\lambda x.\, b \cdot \{\!|x|\!\})\, (\mathit{ext}\, f\, S) \\ (\mathrm{S4}): \;&=\; \mathit{ext}\, (\lambda y.\, \mathit{ext}\, (\lambda x.\, b \cdot \{\!|x|\!\})\, (f y))\, S \\ &=\; \mathit{ext}\, (\lambda y.\, \mathit{filter}\, \underline{b}\, (f y))\, S \;=\; \mathit{ext}\, (\lambda y.\, (f y) \cdot b)\, S \end{aligned}$$

(7)
$$\begin{aligned} S \cdot (a \cdot b) \;&=\; \mathit{filter}\, (\underline{a} \barwedge \underline{b})\, S \qquad \text{using Prop. 10.9.1} \\ &=\; \mathit{filter}\, \underline{b}\, (\mathit{filter}\, \underline{a}\, S) \;=\; (S \cdot a) \cdot b \end{aligned}$$

(8)
$$\begin{aligned} (a \cdot S) \cdot b \;&=\; (\mathit{ext}\, (\lambda \diamond.\, S)\, a) \cdot b \\ (6): \;&=\; \mathit{ext}\, (\lambda \diamond.\, S \cdot b)\, a \;=\; a \cdot (S \cdot b) \end{aligned}$$

(9) $\{\!|x|\!\} \cdot a \;=\; \mathit{filter}\, \underline{a}\, \{\!|x|\!\} \;=\; a \cdot \{\!|x|\!\}$ by (P3f)

(10) $a \cdot S = S \cdot a$ is just a re-formulation of (SYf) which holds for symmetric constructions. □

In the general non-symmetric case, left factors may be drawn off the set argument of *ext* by (S4·), and right factors may be drawn off the functional argument by part (6) of the proposition above. Unless $a \cdot S = S \cdot a$ holds, it is impossible to draw right factors off the set argument and left factors off the functional argument.

Chapter 11

The characteristic semiring

In the previous chapter, we saw that the power domain $\mathcal{P}\mathbf{1}$ becomes a semiring with addition being union, 0 the empty set, 1 a singleton, and multiplication derived from extension. We call this semiring the *characteristic semiring* of the power domain construction $\mathcal{P}$. In this chapter, we study the relation between a power construction and its semiring. We introduce certain classifications of power constructions and investigate to what extent these classifications are determined by properties of the characteristic semiring.

Section 11.1 contains the definitions of the algebraic concepts of semirings, left and right modules, and linearity of functions. In section 11.2, we present examples of power constructions and their semirings. In particular, the semirings of the known power constructions are presented. The notion of characteristic semiring is generalized in section 11.3. The characteristic semiring of $\mathcal{P}$ need no longer be identical to $\mathcal{P}\mathbf{1}$, but may also be isomorphic to $\mathcal{P}\mathbf{1}$ if the isomorphism is assumed to be fixed. In section 11.4, we then consider the effect of the power operations to finite linear combinations in the $\mathcal{P}\mathbf{1}$-modules $\mathcal{P}\mathbf{X}$.

In section 11.5, power domain constructions are called real iff union is idempotent in all power domains. This property is equivalent to $1 + 1 = 1$ in the characteristic semiring. The next section 11.6 compares symmetric constructions where two extensions commute, commutative constructions where the product by a logical value commutes, and constructions with commutative characteristic semiring. In section 11.7, constructions are studied where linear maps on the power domains are uniquely determined by their values on singletons.

In section 11.8, all power constructions are classified into four principal classes according to whether the singletons are incomparable to the empty set, strictly below the empty set, strictly above the empty set, or equal to the empty set. These classes correspond to semiring classes where 0 and 1 are incomparable, $1 < 0$, $1 > 0$, or $1 = 0$ respectively holds.

In section 11.9, criteria are found for the singleton map being an embedding of the ground domain into the power domain. Section 11.10 shows that even if the ground domain and its image under the singleton map are not isomorphic, this image may be taken as an alternative ground domain.

All modules belonging to proper rings are shown to be discrete in section 11.11. Thus power constructions $\mathcal{P}$ with $\mathcal{P}\mathbf{1}$ being a ring are degenerated from the point of view of domain

theory. The final section 11.12 investigates *additive semirings* characterized by the fact that all additive functions between their modules are linear.

11.1 Semirings and modules

The host of algebraic properties of power constructions may be described in terms of well-known algebraic structures.

Definition 11.1.1 (Semiring)

A *semiring domain* or shortly *semiring* $(R, +, 0, \cdot, 1)$ is a domain R with elements 0 and 1, and continuous operations $+, \cdot : [R \times R \to R]$ such that $(R, +, 0)$ is a commutative monoid, $(R, \cdot, 1)$ is a monoid, and multiplication '$\cdot$' is additive in both arguments, i.e.

$$a \cdot 0 = 0 \cdot a = 0 \qquad a \cdot (b_1 + b_2) = (a \cdot b_1) + (a \cdot b_2) \qquad (a_1 + a_2) \cdot b = (a_1 \cdot b) + (a_2 \cdot b)$$

The semiring is *commutative* iff its multiplication is, and it is *idempotent* iff its addition is, i.e. $a + a = a$ holds.

A *semiring homomorphism* $h : [R \to R']$ between two semirings is a continuous mapping that preserves the semiring operations:

$$h\,(a + b) = h\,a + h\,b \qquad h\,(0) = 0' \qquad h\,(a \cdot b) = h\,a \cdot h\,b \qquad h\,(1) = 1'$$

The power domain $\mathcal{P}\mathbf{1}$ is such a semiring with $0 = \mathsf{F} = \theta$, $a + b = a \veebar b = a \uplus b$, $1 = \mathsf{T} = \{\!|\diamond|\!\}$, and $a \cdot b = a \barwedge b = ext\,(\lambda\diamond.\, b)\,a$ as shown in the previous sections.

Semirings are generalizations of both rings and distributive lattices. These in turn are generalizations of fields and Boolean algebras. Hence, both the notations $(R, +, 0, \cdot, 1)$ of the definition above and $(R, \veebar, \mathsf{F}, \barwedge, \mathsf{T})$ as used in the previous sections seem to be adequate.

When semiring domains are considered which are lattices, there is a high risk to confuse the order '$\leq$' of the domain and the lattice order '$\sqsubseteq$' defined by $a + b = b$. Generally, there is no relation between these two orders. In special cases only, they are equal or just opposite.

Definition 11.1.2 (Modules)

Let $R = (R, +, 0, \cdot, 1)$ be a semiring domain and $M = (M, +, 0)$ be a commutative monoid domain. $(R, M, \cdot)$ is a *(left) module* iff

$$\cdot : [R \times M \to M]$$

$$a \cdot 0_M = 0_M \qquad a \cdot (B_1 + B_2) = (a \cdot B_1) + (a \cdot B_2)$$
$$0_R \cdot A = 0_M \qquad (a_1 + a_2) \cdot B = (a_1 \cdot B) + (a_2 \cdot B)$$
$$1_R \cdot A = A \qquad a \cdot (b \cdot C) = (a \cdot b) \cdot C$$

We also say 'M is a (left) R-module'.

Let M_1 and M_2 be two (left) R-modules. A morphism $f : [M_1 \to M_2]$ is *(left) linear* iff

$$f\,(A + B) = f\,A + f\,B \quad \text{and} \quad f\,(r \cdot A) = r \cdot f\,A$$

$(R, M, \cdot)$ is a *right module* iff

$$\cdot : [M \times R \to M]$$

$$0_M \cdot b = 0_M \qquad (A_1 + A_2) \cdot b = (A_1 \cdot b) + (A_2 \cdot b)$$
$$A \cdot 0_R = 0_M \qquad A \cdot (b_1 + b_2) = (A \cdot b_1) + (A \cdot b_2)$$
$$A \cdot 1_R = A \qquad (A \cdot b) \cdot c = A \cdot (b \cdot c)$$

We also say 'M is a right R-module'.

Let M_1 and M_2 be two right R-modules. A morphism $f : [M_1 \to M_2]$ is *right linear* iff

$$f\,(A + B) = fA + fB \quad \text{and} \quad f\,(A \cdot r) = fA \cdot r$$

We assume left modules as the standard; thus, the word 'left' may be omitted. Right modules do not become left modules by simply twisting the arguments. The very last equation of right modules becomes $c \cdot (b \cdot A) = (b \cdot c) \cdot A$ by twisting. Thus, a right R-module is a left R^t-module where R^t is R with multiplication twisted. For commutative semirings however, the notions of left and right module coincide.

Particularly prominent modules are those over a field; they are called vector spaces. The notion of linearity is drawn from there.

The most important results of the previous sections may be summarized to

Theorem 11.1.3 Let $\mathcal{P}$ be a power construction and let

$$\begin{array}{ll} + = \uplus : & [\mathcal{P}\mathbf{X} \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}] \\ 0 = \theta : & \mathcal{P}\mathbf{X} \\ \cdot = \lambda(a,\, S).\, ext\,(\lambda\diamond.\, S)\, a : & [\mathcal{P}\mathbf{1} \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}] \\ 1 = \{|\diamond|\} : & \mathcal{P}\mathbf{1} \end{array}$$

Then $\mathcal{P}\mathbf{1}$ with these operations is a semiring domain, and $\mathcal{P}\mathbf{X}$ is a $\mathcal{P}\mathbf{1}$-module for all domains $\mathbf{X}$. For $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$, the extension $\overline{f} : [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ is linear, and $\overline{f} \circ \iota = f$ holds.

The semiring $\mathcal{P}\mathbf{1}$ is called the *characteristic semiring* of the power construction $\mathcal{P}$. Generalizing a bit, a power construction $\mathcal{P}$ is said to have characteristic semiring R iff $\mathcal{P}\mathbf{1}$ and R are isomorphic semirings where the isomorphism is assumed to be fixed (cf. section 11.3).

Different power constructions may have the same characteristic semiring. For instance, the construction of the set of all subsets and the construction of the set of finite subsets for the class of discrete domains both have characteristic semiring $\{0, 1\}$ with $1 + 1 = 1$.

Conversely, one may wonder whether there is a power construction for every given semiring. The answer is yes; in chapters 14 and 15, two distinguished constructions with given semiring are presented.

11.2 Examples for characteristic semirings

In this section, we informally present some examples for power constructions and their characteristic semirings.

- The *lower power construction* has characteristic semiring $\{0 < 1\}$, or logically $\{\mathsf{F} < \mathsf{T}\}$ where $\mathsf{T} \curlyvee \mathsf{T} = \mathsf{T}$. In this logic, F is unstable because it may become T while the computation proceeds. Thus, F actually means 'don't know' since only positive answers are reliable.
- The *upper power construction* has the dual semiring $\{1 < 0\}$, or logically $\{\mathsf{T} < \mathsf{F}\}$. Here, T is unstable and may change to F in the course of a computation. Only negative answers are reliable.

- The convex or *Plotkin power construction* has semiring $\{0, 1\}$ with $1 + 1 = 1$. The elements are not comparable. Logically, T and F are both stable here. The semiring is discrete, whence computations with logical result cannot proceed. They have immediately to decide whether the result is T or F, and cannot change their 'opinion' afterwards.

  The constructions of the set of all subsets and of the set of finite subsets have the same characteristic semiring as Plotkin's construction. Indeed, the construction of finite subsets is just a special instance of Plotkin's.

The three examples above show the importance of the empty set in our algebraic theory. Without empty set resp. 0, all three semirings would collapse to $\{1\}$ and could not be distinguished.

- A power construction with a more reasonable logic should have the Boolean domain $\mathbf{B} = \{\bot, \mathsf{F}, \mathsf{T}\}$ as semiring. Such constructions are called set domain constructions in [Hec90c]. The interpretation of $\bot$ is 'I do not (yet) know'. Computations with logical results start in this state which may change to F or T if the computation proceeds.

  The *sandwich power construction* [BDW88] or *big set domain construction* [Hec90c] and the *mixed power construction* [Gun89b, Gun90] or *small set domain construction* [Hec90c] both have characteristic semiring $\mathbf{B}$ with parallel conjunction and disjunction.

- *Multi-power domain constructions* containing formal multi-sets should have the natural numbers as their semiring. There are several ways how to arrange the naturals to form a semiring domain:
  - $\mathbf{N}_0^\infty = \{0 < 1 < 2 < \cdots < \infty\}$ with addition extended by $n + \infty = \infty$ and multiplication extended by $0 \cdot \infty = 0$ and $n \cdot \infty = \infty$ for $n > 0$.
  - The order dual $\mathbf{N}_\infty^0 = \{0 > 1 > 2 > \cdots > \infty\}$ of the semiring above.
  - '∞' is not needed here. Thus, $\mathbf{N}^0 = \{0 > 1 > 2 > \cdots\}$ with usual arithmetic is also a semiring domain.
  - $\mathbf{N}_0 = \{0, 1, 2, \ldots\}$ with usual arithmetic and discrete order.
  - The flat domain $\mathbf{N}_\bot = \{\bot, 0, 1, 2, \ldots\}$ with usual arithmetic extended by $n + \bot = \bot$, $0 \cdot \bot = 0$, and $n \cdot \bot = \bot$ for $n > 0$.
  - The domain of 'lazy naturals'.
  - The only multi-power construction that was ever proposed occurs in [Bro82] and is defined for algebraic ground domains. It excludes the empty set as many other proposals do. If the empty set is added properly, then the characteristic semiring becomes $\{0, 1 < 2 < 3 < \cdots < \infty\}$, i.e. 0 is totally uncomparable as in Plotkin's construction, and the remaining numbers form an infinite ascending chain.
- In [Mai85], *discrete probabilistic non-determinism* is modeled by a power construction with characteristic semiring $\mathbf{R}_0^\infty$ — the non-negative reals including infinity ordered as usual with ordinary addition and multiplication.
- In [Mai85] again, *oracle non-determinism* is modeled by a construction whose semiring is the power set of a fixed set. The power set is ordered by inclusion '$\subseteq$', addition is union, and multiplication is intersection.

- A third construction in [Mai85] models *ephemeral non-determinism*. Its semiring is the so-called *tropical semiring* $\mathbf{T} = \{t_0 < t_1 < t_2 < \cdots < t_\infty\}$ where $t_n + t_k = t_{min\,(n,\,k)}$, $0 = t_\infty$, $t_n \cdot t_k = t_{n+k}$, and $1 = t_0$, i.e. addition in $\mathbf{T}$ is minimum, and multiplication in $\mathbf{T}$ is arithmetic addition.

11.3 Power constructions with semirings

It is generally useful not to stick to the fact that the characteristic semiring be exactly $\mathcal{P}\mathbf{1}$. It is better to be more flexible and let the characteristic semiring be some isomorphic copy of $\mathcal{P}\mathbf{1}$. In this case, it is important to fix an isomorphism.

Definition 11.3.1 A tuple $(\mathcal{P}, R, \varphi)$ is a power construction with semiring R, or shortly an R-construction, iff $\mathcal{P}$ is a power construction, R a semiring, and $\varphi : [R \to \mathcal{P}\mathbf{1}]$ is a semiring isomorphism.

If R allows non-trivial automorphisms, then there are several different isomorphisms between $\mathcal{P}\mathbf{1}$ and R. Hence, we fix an isomorphism in the definition. The importance of this fixing will be seen in the subsequent chapters. Nevertheless, we shall mostly use the sloppy notation '$\mathcal{P}$ is an R-construction' without explicitly mentioning the fixed isomorphism $\varphi : [R \to \mathcal{P}\mathbf{1}]$.

Various derived power operations involved the power domain $\mathcal{P}\mathbf{1}$ in their functionality. By means of the isomorphisms φ and φ^{-1}, they may be turned into operations involving R instead. For the sake of clarity, we mark the original operations by an asterisk in the following, and denote the original products by '$*$'.

$\cdot :$	$[R \times \mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}]$	$r \cdot A = \varphi r * A$
$\cdot :$	$[\mathcal{P}\mathbf{X} \times R \to \mathcal{P}\mathbf{X}]$	$A \cdot r = A * \varphi r$
$ex :$	$[[\mathbf{X} \to R] \to [\mathcal{P}\mathbf{X} \to R]]$	$ex\, p = \varphi^{-1} \circ ex^*\,(\varphi \circ p)$
$ne :$	$[\mathcal{P}\mathbf{X} \to R]$	$ne = \varphi^{-1} \circ ne^*$
$\mathcal{E} :$	$[\mathcal{P}\mathbf{X} \to [[\mathbf{X} \to R] \to R]]$	$\mathcal{E}\,A\,p = \varphi^{-1}\,(\mathcal{E}^*A\,(\varphi \circ p))$
$filter :$	$[[\mathbf{X} \to R] \to [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}]]$	$filter\, p = filter^*\,(\varphi \circ p)$

These new operations enjoy the same algebraic properties as the original operations. The proofs may be performed by simple equational reasoning. In the sequel, we shall mostly use the new operations.

11.4 Finite linear combinations

In section 9.4, we already defined finite formal sets in a power domain $\mathcal{P}\mathbf{X}$ by $\{\!|x_1, \ldots, x_n|\!\} = \{\!|x_1|\!\} \uplus \cdots \uplus \{\!|x_n|\!\}$. This notion may be generalized by employing multiplication. If $\mathcal{P}$ is an R-construction, we define *finite linear combinations* in a power domain $\mathcal{P}\mathbf{X}$ by

$$\{\!|r_1 \cdot x_1, \ldots, r_n \cdot x_n|\!\} = r_1 \cdot \{\!|x_1|\!\} \uplus \cdots \uplus r_n \cdot \{\!|x_n|\!\}$$

where the coefficients r_i are in R and the points x_i are in $\mathbf{X}$.

The coefficients indicate the degree of membership of the corresponding point in the formal set. A coefficient $0 = \mathsf{F}$ at some point x means this point is not in the formal set, whereas $1 = \mathsf{T}$ means it is. Other coefficients have other meanings depending on the structure of R. For instance, if $R = \{\bot, \mathsf{F}, \mathsf{T}\}$, then a coefficient $\bot$ denotes an uncertain membership because of $\bot \leq \mathsf{T}$ and $\bot \leq \mathsf{F}$.

We now show how the power operations act on such finite linear combinations.

- $\theta \;=\; \{\!|\}$
- $\{\!|x|\!\} \;=\; \{\!|1 \cdot x|\!\}$
- $\{\!|r_1 \cdot x_1, \ldots, r_n \cdot x_n|\!\} \uplus \{\!|s_1 \cdot y_1, \ldots, s_m \cdot y_m|\!\} \;=\; \{\!|r_1 \cdot x_1, \ldots, r_n \cdot x_n, s_1 \cdot y_1, \ldots, s_m \cdot y_m|\!\}$
- $ext\, f\, \{\!|r_1 \cdot x_1, \ldots, r_n \cdot x_n|\!\} \;=\; r_1 \cdot f x_1 \uplus \cdots \uplus r_n \cdot f x_n$
- $map\, f\, \{\!|r_1 \cdot x_1, \ldots, r_n \cdot x_n|\!\} \;=\; \{\!|r_1 \cdot f x_1, \ldots, r_n \cdot f x_n|\!\}$
- $\mathcal{E}\, \{\!|r_1 \cdot x_1, \ldots, r_n \cdot x_n|\!\} \;=\; \lambda p.\, (r_1 \barwedge p\, x_1) \barvee \cdots \barvee (r_n \barwedge p\, x_n)$
- $s \cdot \{\!|r_1 \cdot x_1, \ldots, r_n \cdot x_n|\!\} \;=\; \{\!|(s \cdot r_1) \cdot x_1, \ldots, (s \cdot r_n) \cdot x_n|\!\}$
- $\{\!|r_1 \cdot x_1, \ldots, r_n \cdot x_n|\!\} \cdot s \;=\; \{\!|(r_1 \cdot s) \cdot x_1, \ldots, (r_n \cdot s) \cdot x_n|\!\}$
- $filter\, p\, \{\!|r_1 \cdot x_1, \ldots, r_n \cdot x_n|\!\} \;=\; \{\!|(r_1 \cdot p\, x_1) \cdot x_1, \ldots, (r_n \cdot p\, x_n) \cdot x_n|\!\}$
- $\{\!|r_1 \cdot x_1, \ldots, r_n \cdot x_n|\!\} \overrightarrow{\times} \{\!|s_1 \cdot y_1, \ldots, s_m \cdot y_m|\!\} \;=\; \{\!|(r_i \cdot s_j) \cdot (x_i, y_j) \mid 1 \leq i \leq n, 1 \leq j \leq m|\!\}$
- $\{\!|r_1 \cdot x_1, \ldots, r_n \cdot x_n|\!\} \overleftarrow{\times} \{\!|s_1 \cdot y_1, \ldots, s_m \cdot y_m|\!\} \;=\; \{\!|(s_j \cdot r_i) \cdot (x_i, y_j) \mid 1 \leq i \leq n, 1 \leq j \leq m|\!\}$

The equation for the right product is due to Prop. 10.10.2 (9): $\{\!|x|\!\} \cdot s = s \cdot \{\!|x|\!\}$. Hence, the left product operates from the outside, whereas the right product operates at the inside.

The formulae for the Cartesian products are derived by

$$\begin{array}{lcl}
(r \cdot \{\!|x|\!\}) \overrightarrow{\times} (s \cdot \{\!|y|\!\}) & = & ext\, (\lambda a.\, ext\, (\lambda b.\, \{\!|(a, b)|\!\})\, (s \cdot \{\!|y|\!\}))\, (r \cdot \{\!|x|\!\}) \\
(\mathrm{S4}\cdot): & = & r \cdot ext\, (\lambda a.\, ext\, (\lambda b.\, \{\!|(a, b)|\!\})\, (s \cdot \{\!|y|\!\}))\, \{\!|x|\!\} \\
(\mathrm{P3}): & = & r \cdot ext\, (\lambda b.\, \{\!|(x, b)|\!\})\, (s \cdot \{\!|y|\!\}) \\
(\mathrm{S4}\cdot): & = & r \cdot s \cdot ext\, (\lambda b.\, \{\!|(x, b)|\!\})\, \{\!|y|\!\} \\
(\mathrm{P3}): & = & r \cdot s \cdot \{\!|(x, y)|\!\}
\end{array}$$

and

$$\begin{array}{lcl}
(r \cdot \{\!|x|\!\}) \overleftarrow{\times} (s \cdot \{\!|y|\!\}) & = & ext\, (\lambda b.\, ext\, (\lambda a.\, \{\!|(a, b)|\!\})\, (r \cdot \{\!|x|\!\}))\, (s \cdot \{\!|y|\!\}) \\
(\mathrm{S4}\cdot): & = & s \cdot ext\, (\lambda b.\, ext\, (\lambda a.\, \{\!|(a, b)|\!\})\, (r \cdot \{\!|x|\!\}))\, \{\!|y|\!\} \\
(\mathrm{P3}): & = & s \cdot ext\, (\lambda a.\, \{\!|(a, y)|\!\})\, (r \cdot \{\!|x|\!\}) \\
(\mathrm{S4}\cdot): & = & s \cdot r \cdot ext\, (\lambda a.\, \{\!|(a, y)|\!\})\, \{\!|x|\!\} \\
(\mathrm{P3}): & = & s \cdot r \cdot \{\!|(x, y)|\!\}
\end{array}$$

In our opinion, these results show that '$\overrightarrow{\times}$' is more natural than '$\overleftarrow{\times}$'.

According to the algebraic laws of the power operations, syntactically different linear combinations may yield equal values, e.g. $\{\!|r \cdot x, s \cdot y|\!\} = \{\!|s \cdot y, r \cdot x|\!\}$, $\{\!|0 \cdot x, s \cdot y|\!\} = \{\!|s \cdot y|\!\}$, and $\{\!|r \cdot x, s \cdot x|\!\} = \{\!|(r + s) \cdot x|\!\}$ hold.

In addition, there are equalities among linear combinations that cannot be explained by algebraic laws only. They result from constraints due to monotonicity. Assume for instance

that R be a semiring where $1+1 = 1$ holds. Then in every R-powerdomain, $x \leq y \leq z$ implies $\{\!|x, y, z|\!\} = \{\!|x, z|\!\}$ because of $\{\!|x, z|\!\} = \{\!|x, x, z|\!\} \leq \{\!|x, y, z|\!\} \leq \{\!|x, z, z|\!\} = \{\!|x, z|\!\}$.

Besides the finite linear combinations, a power domain usually contains limits of directed sets of these. These limits cannot always be conceived as infinite linear combinations. Worse, many power domains contain 'junk elements' that are neither finite linear combinations nor limits of these. Power domains that do not contain junk are called *reduced*; this topic is further explored in chapter 14.

11.5 Real power constructions

The subsequent sections are devoted to the definition and investigation of various classes of power constructions characterized by additional properties. We always try to attribute these properties to the characteristic semiring.

A *real power construction* is characterized by the additional property $A \uplus A = A$ for all A in $\mathcal{P}\mathbf{X}$ for all domains $\mathbf{X}$ in D. An equivalent criterion is $1 + 1 = 1$ in the characteristic semiring $\mathcal{P}\mathbf{1}$ since this is a special instance of the general property, and on the other hand, it implies $A \uplus A = 1 \cdot A \uplus 1 \cdot A = (1 + 1) \cdot A = 1 \cdot A = A$. Hence, it is sufficient to consider $\mathcal{P}\mathbf{1}$ to decide whether union in all power domains $\mathcal{P}\mathbf{X}$ is idempotent.

11.6 Symmetry and commutativity

We first repeat the definitions and introduce a new notion in between:

Definition 11.6.1 Let $\mathcal{P}$ be a power construction.

- $\mathcal{P}$ is *symmetric* iff for all domains $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$ in D, and all A in $\mathcal{P}\mathbf{X}$, B in $\mathcal{P}\mathbf{Y}$, and $\star : [\mathbf{X} \times \mathbf{Y} \to \mathcal{P}\mathbf{Z}]$:

  $$ext\,(\lambda a.\, ext\,(\lambda b.\, a \star b)\, B)\, A = ext\,(\lambda b.\, ext\,(\lambda a.\, a \star b)\, A)\, B$$

- $\mathcal{P}$ is *commutative* iff for all domains $\mathbf{Y}$ in D and all a in $\mathcal{P}\mathbf{1}$ and B in $\mathcal{P}\mathbf{Y}$:

  $$a \cdot B = B \cdot a$$

- $\mathcal{P}\mathbf{1}$ is *commutative* iff for all a, b in $\mathcal{P}\mathbf{1}$: $a \cdot b = b \cdot a$

Obviously, commutativity of the characteristic semiring is a special instance of commutativity of the construction. The relation between symmetry and commutativity of $\mathcal{P}$ is clarified by expanding left and right multiplication:

$$\begin{aligned} a \cdot B &= ext\,(\lambda\diamond.\, B)\, a = ext\,(\lambda\diamond.\, ext\,(\lambda b.\, \{\!|b|\!\})\, B)\, a \quad \text{by (S3)} \\ B \cdot a &= ext\,(\lambda b.\, a \cdot \{\!|b|\!\})\, B = ext\,(\lambda b.\, ext\,(\lambda\diamond.\, \{\!|b|\!\})\, a)\, B \end{aligned}$$

Thus, commutativity is a special instance of symmetry where $\mathbf{X} = \mathbf{1}$, $\mathbf{Y} = \mathbf{Z}$, and $\diamond \star b = \{\!|b|\!\}$.

Symmetry implies commutativity of $\mathcal{P}$ which in turn implies commutativity of $\mathcal{P}\mathbf{1}$. The opposite implications seem to be false in general; we do not know of examples for this however. The next section provides a special case where they are true.

11.7 Unique extensions

A power construction $\mathcal{P}$ has *unique linear extensions* iff for all linear functions $F_1, F_2 : [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]$, $F_1 \circ \iota = F_2 \circ \iota$ implies $F_1 = F_2$. In other words, two linear functions that coincide for singletons are equal. $\mathcal{P}$ has *unique additive extensions* iff two additive functions that coincide for singletons are equal. Since all linear functions are additive, the property of having unique additive extensions implies unique linear extensions.

Proposition 11.7.1 A power construction with unique linear extensions is symmetric iff its characteristic semiring is commutative. A power construction with unique additive extensions is symmetric.

Proof: For the first statement, we only need to prove the symmetry of the power construction in the case of commutative semiring R; the opposite implication was already handled in the previous section. The proof is done in two steps:

- In the first step, we claim

  $$ext\,(\lambda x.\, r \cdot fx) = \lambda A.\, r \cdot ext\, f\, A$$

  The left hand function is linear as an extension. The right hand function is linear only because of the commutativity of R. A linear factor at A has to be moved across r:

  $$\begin{aligned}(\lambda A.\, r \cdot ext\, f\, A)\,(s \cdot A) &= r \cdot ext\, f\,(s \cdot A) = r \cdot s \cdot ext\, f\, A \\ &= s \cdot r \cdot ext\, f\, A = s \cdot (\lambda A.\, r \cdot ext\, f\, A)\, A\end{aligned}$$

  Both functions map a singleton $\{\!|a|\!\}$ to $r \cdot fa$, whence they are equal.

- Next, we claim

  $$ext\,(\lambda a.\, ext\,(\lambda b.\, a \star b)\, B) = \lambda A.\, ext\,(\lambda b.\, ext\,(\lambda a.\, a \star b)\, A)\, B$$

  Both functions are linear; the function to the right because of the equation proved in the first step. Both functions map a singleton $\{\!|a|\!\}$ to $ext\,(\lambda b.\, a \star b)\, B$.

For the second statement, we only have to show commutativity of $\mathcal{P}\mathbf{1}$, then the first statement applies. For all a in $\mathcal{P}\mathbf{1}$, we claim $\lambda x.\, a \cdot x = \lambda x.\, x \cdot a$ where x ranges over $\mathcal{P}\mathbf{1}$. Because of distributivity, both functions are additive. Applied to the only singleton $\{\!|\diamond|\!\} = 1$, they both yield a. Hence, they are equal. □

11.8 The four kinds of power constructions

According to the relations between empty set and singletons, one may distinguish among four kinds of power constructions: the *lower kind* where the empty set is strictly below all singletons, the *upper kind* where it is strictly above, the *degenerated kind* where all singletons are empty, and the *separated kind* where the empty set is uncomparable to all singletons. The following propositions show that it is impossible that some singletons are strictly below θ whereas others are not. The reason is that the four kinds are completely determined by the characteristic semiring; they correspond to the cases $0 < 1$, $0 > 1$, $0 = 1$, and incomparability of 0 and 1.

Proposition 11.8.1 For power constructions, the following statements are equivalent:

(1) There is a domain $\mathbf{X}$ in D and a point x in $\mathbf{X}$ with $\{\!|x|\!\} = \theta$.

(2) In $\mathcal{P}\mathbf{1}$, $0 = 1$ holds.

(3) For all domains $\mathbf{X}$ in D and all A in $\mathcal{P}\mathbf{X}$, $A = \theta$ holds.

(4) All $\mathcal{P}\mathbf{1}$-modules are isomorphic to $\{0\}$.

Proof:

(1) $\Rightarrow$ (2) : $ne\ \{\!|x|\!\} = 1$ and $ne\ \theta = 0$.

(2) $\Rightarrow$ (1) : Let $\mathbf{X} = \mathbf{1}$ and $x = \diamond$. $0 = \theta$ and $1 = \{\!|\diamond|\!\}$ hold.

(2) $\Rightarrow$ (4) : $A = 1 \cdot A = 0 \cdot A = 0$

(4) $\Rightarrow$ (3) $\Rightarrow$ (2) is obvious. □

Let the *degenerated power construction* be defined by $\mathcal{P}\mathbf{X} = \{\theta\}$ for all domains $\mathbf{X}$. Trivially, this is a symmetric real power construction. Prop. 11.8.1 shows that it is the only construction where $\{\!|x|\!\} = \theta$ is possible for some x in some $\mathbf{X}$.

Proposition 11.8.2 For power constructions, the following statements are equivalent:

(1) There is a domain $\mathbf{X}$ in D and a point x in $\mathbf{X}$ with $\theta \leq \{\!|x|\!\}$.

(2) In $\mathcal{P}\mathbf{1}$, $0 \leq 1$ holds.

(3) For all domains $\mathbf{X}$ in D and all A in $\mathcal{P}\mathbf{X}$, $\theta \leq A$ holds.

(4) In all $\mathcal{P}\mathbf{1}$-modules, 0 is the least element.

The dual equivalence obtained by replacing '$\leq$' by '$\geq$' and 'least' by 'greatest' also holds.

Proof:

(1) $\Rightarrow$ (2) : $\theta \leq \{\!|x|\!\}$ implies $0 = ne\ \theta \leq ne\ \{\!|x|\!\} = 1$.

(2) $\Rightarrow$ (1) : Let $\mathbf{X} = \mathbf{1}$ and $x = \diamond$. $\theta = 0 \leq 1 = \{\!|\diamond|\!\}$ holds.

(2) $\Rightarrow$ (4) : $0 = 0 \cdot A \leq 1 \cdot A = A$

(4) $\Rightarrow$ (3) $\Rightarrow$ (2) is obvious. □

11.9 Faithful power constructions

Definition 11.9.1 A power domain construction $\mathcal{P}$ is *faithful* iff for all domains $\mathbf{X}$ in D the map $\iota : \mathbf{X} \to \mathcal{P}\mathbf{X}$ is an embedding, i.e. $\{\!|x|\!\} \leq \{\!|x'|\!\}$ implies $x \leq x'$. $\mathcal{P}$ is *injective* iff ι is injective for all domains $\mathbf{X}$ in D.

If $\mathcal{P}$ is a faithful construction, then $\mathbf{X}$ may be considered a subdomain of $\mathcal{P}\mathbf{X}$. There is a useful criterion for faithfulness:

Lemma 11.9.2 Let $\mathcal{P}$ be a power construction defined for a class D. If there is a domain $\mathbf{Y}$ in D such that $\mathcal{P}\mathbf{Y}$ is not discrete, then $\mathcal{P}$ is faithful.

Here, being discrete means $a \leq b$ implies $a = b$. Hence, a domain is not discrete iff there are points a and b with $a < b$ in it.

Proof: Let $\mathbf{Y}$ be a (fixed) domain such that $\mathcal{P}\mathbf{Y}$ is not discrete. Let B and B' be two fixed members of $\mathcal{P}\mathbf{Y}$ with $B < B'$.
Let $\mathbf{X}$ be an arbitrary domain in D, and let x and x' be two points of $\mathbf{X}$ such that $\{\!|x|\!\} \leq \{\!|x'|\!\}$ holds. We have to show $x \leq x'$. Applying Prop. 4.3.1, let O be an open set with $x \in O$. Then we must show $x' \in O$.

Let $f : \mathbf{X} \to \mathcal{P}\mathbf{Y}$ be defined by $fu = \begin{cases} B' & \text{if } u \in O \\ B & \text{otherwise} \end{cases}$

f is continuous by Lemma 3.7.1, and may be extended to the continuous function $\overline{f} : [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]$. $x \in O$ implies $\overline{f}\{\!|x|\!\} = fx = B'$. By monotonicity of $\overline{f}$, $fx' = \overline{f}\{\!|x'|\!\} \geq \overline{f}\{\!|x|\!\} = B'$ holds. f is able to produce only the two values B and B', whence $fx' = B'$ follows, i.e. x' is in O. □

By this theorem, a total power construction is not faithful iff all power domains $\mathcal{P}\mathbf{X}$ are discrete.

The non-discrete power domain $\mathcal{P}\mathbf{Y}$ may well be $\mathcal{P}\mathbf{1}$. Thus, we obtain

Corollary 11.9.3
A power domain construction with a non-discrete characteristic semiring is faithful.

The final theorem tells that being injective and being faithful is almost the same.

Theorem 11.9.4 Let $\mathcal{P}$ be a power construction that is defined for at least one non-discrete domain $\mathbf{X}$. Then, the following statements are equivalent:

(1) $\mathcal{P}$ is faithful.

(2) $\mathcal{P}$ is injective.

(3) $\mathcal{P}\mathbf{X}$ is not discrete.

(4) There is a domain $\mathbf{Y}$ in D such that $\mathcal{P}\mathbf{Y}$ is not discrete.

Proof:

(1) ⇒ (2): Every embedding is injective.

(2) ⇒ (3): Let a and b be two points of $\mathbf{X}$ with $a < b$. By monotonicity, $\{\!|a|\!\} \leq \{\!|b|\!\}$ holds. The two singletons are different because of injectivity. Thus, $\{\!|a|\!\} < \{\!|b|\!\}$ holds, and $\mathcal{P}\mathbf{X}$ is not discrete.

(3) ⇒ (4): is obvious; let $\mathbf{Y} = \mathbf{X}$.

(4) ⇒ (1): Immediately by Lemma 11.9.2. □

11.10 Ground domains as sub-domains of power domains

If $\mathcal{P}$ is a faithful power construction, then power domains $\mathcal{P}\mathbf{X}$ contain an isomorphic image of the ground domain $\mathbf{X}$ as a sub-domain. If $\mathcal{P}$ is not faithful, then this statement is wrong. Even in this case however, $\mathcal{P}\mathbf{X}$ contains a sub-domain $\mathbf{Y}$ such that $\mathcal{P}\mathbf{X}$ is isomorphic to $\mathcal{P}\mathbf{Y}$. The alternative ground domain $\mathbf{Y}$ is the image of $\mathbf{X}$ in $\mathcal{P}\mathbf{X}$.

Theorem 11.10.1 Let $\mathbf{X}$ be a ground domain and $\mathcal{P}$ a power domain construction defined for $\mathbf{X}$. Then the image $\mathbf{Y} = \iota[\mathbf{X}]$ of $\mathbf{X}$ by the singleton mapping is a sub-domain of $\mathcal{P}\mathbf{X}$ and the two power domains $\mathcal{P}\mathbf{X}$ and $\mathcal{P}\mathbf{Y}$ are isomorphic by a $\mathcal{P}\mathbf{1}$-linear mapping.

Proof: If $\mathcal{P}$ is faithful, then $\mathbf{Y}$ is isomorphic to $\mathbf{X}$ by ι, whence it is a sub-domain of $\mathcal{P}\mathbf{X}$. Otherwise, the power domain $\mathcal{P}\mathbf{X}$ is discrete by Lemma 11.9.2, whence $\mathbf{Y}$ is also discrete and a sub-domain of $\mathcal{P}\mathbf{X}$.

Let $\iota_{\mathbf{X}} : [\mathbf{X} \to \mathcal{P}\mathbf{X}]$ and $\iota_{\mathbf{Y}} : [\mathbf{Y} \to \mathcal{P}\mathbf{Y}]$ be the two singleton mappings. $\iota_{\mathbf{X}}$ may be co-restricted to a surjective mapping $e : [\mathbf{X} \to \mathbf{Y}]$. By composition with $\iota_{\mathbf{Y}}$, one obtains $f = \iota_{\mathbf{Y}} \circ e : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$. The natural inclusion map of $\mathbf{Y}$ into $\mathcal{P}\mathbf{X}$ is denoted by $g : [\mathbf{Y} \to \mathcal{P}\mathbf{X}]$. Extension yields a pair of functions $\overline{f} : [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ and $\overline{g} : [\mathcal{P}\mathbf{Y} \to \mathcal{P}\mathbf{X}]$. We show that $\overline{f}$ and $\overline{g}$ are inverse to each other.

One part of the proof is fairly easy:

$$\overline{g} \circ \overline{f} \overset{(S4)}{=} \overline{\overline{g} \circ f} = \overline{\overline{g} \circ \iota_{\mathbf{Y}} \circ e} \overset{(P3)}{=} \overline{g \circ e} = \overline{\iota_{\mathbf{X}}} \overset{(S3)}{=} id_{\mathcal{P}\mathbf{X}}$$

using the equation $g \circ e = \iota_{\mathbf{X}}$.

Similarly, $\overline{f} \circ \overline{g} = \overline{\overline{f} \circ g}$ holds by (S4). If we are able to prove $\overline{f} \circ g = \iota_{\mathbf{Y}}$, then $\overline{f} \circ \overline{g} = id_{\mathcal{P}\mathbf{Y}}$ follows by (S3).

Let y be a point of $\mathbf{Y}$. Then $y = ex$ holds for some x in $\mathbf{X}$, and $\overline{f}\,(g\,y) = \overline{f}\,(g\,(e\,x)) = \overline{f}\,(\iota_{\mathbf{X}} x) = fx = \iota_{\mathbf{Y}}\,(e\,x) = \iota_{\mathbf{Y}}\,y$ follows. □

11.11 Modules over rings

A *ring* is a semiring that has a member -1 such that $1 + (-1) = 0$ holds. One might believe that power constructions whose characteristic semiring is a ring have particularly nice properties. Because we consider domains and continuous operations, the contrary is true however.

Proposition 11.11.1 If R is a ring, then every R-module is discrete.

Hence, power constructions with a characteristic ring cannot be faithful if they are defined for some non-discrete ground domain.

Proof: Let M be an R-module where R is a ring. Then for all c in M, $c + (-1) \cdot c = (1 + (-1)) \cdot c = 0 \cdot c = 0$ holds.

Now assume $a \leq b$ holds for some points a and b of M. By monotonicity of the external product, $(-1) \cdot a \leq (-1) \cdot b$ follows. By monotonicity of addition, we obtain $a + b + (-1) \cdot a \leq a + b + (-1) \cdot b$. By the equation above, the left hand side equals b and the right hand side equals a. Thus, $a \leq b$ implies $b \leq a$, whence $a = b$. □

11.12 Additive semirings

Modules M over a semiring R were defined as commutative monoids with an external product. A morphism $f : [M_1 \to M_2]$ between two R-modules is *additive* iff $f\,(0) = 0$ and

$f(a+b) = fa + fb$, and *linear* iff $f(a+b) = fa + fb$ and $f(r \cdot a) = r \cdot fa$. Every linear map is additive by $f(0) = f(0 \cdot 0) = 0 \cdot f0 = 0$. The opposite implication not being generally true, it however holds for many common cases. We attribute this property to the semiring and define:

Definition 11.12.1 A semiring domain R is *additive* iff all additive morphisms between any two R-modules are linear.

The quantification over all additive *morphisms* makes this notion depend on the underlying domains. There are semirings where continuity is necessary to derive linearity from additivity.

Some examples will clarify the situation:

- A semiring R with carrier $\{0, 1\}$ with any order is additive since $f(0 \cdot x) = f(0) = 0 = 0 \cdot fx$ holds by additivity of f, and also $f(1 \cdot x) = fx = 1 \cdot fx$ holds anyway.
- $\mathbf{N}_0^\infty = \{0 < 1 < 2 < \cdots < \infty\}$ with usual addition and multiplication extended by $n + \infty = \infty$ for all n, and $0 \cdot \infty = 0$, and $n \cdot \infty = \infty$ for all $n > 0$ becomes a semiring domain. It is additive since $f(n \cdot x) = n \cdot fx$ may be shown by induction for $n < \infty$:

  $$f((n+1) \cdot x) = f(n \cdot x + x) = f(n \cdot x) + fx = n \cdot fx + fx = (n+1) \cdot fx$$

  and follows from continuity of f and '$\cdot$' in case $n = \infty$.

  The monotonic, but non-continuous map

  $$g : \mathbf{N}_0^\infty \to \mathbf{N}_0^\infty, \quad g\,n = \begin{cases} 0 & \text{if } n < \infty \\ \infty & \text{if } n = \infty \end{cases}$$

  is additive, but not linear because of $g(\infty \cdot 1) = g(\infty) = \infty$, but $\infty \cdot g(1) = \infty \cdot 0 = 0$.
- The 'tropical semiring' is $\mathbf{T} = \{t_0 < t_1 < \cdots < t_\infty\}$ with $t_n + t_k = t_{min\,(n,\,k)}$, $0 = t_\infty$, $t_n \cdot t_k = t_{n+k}$, and $1 = t_0$. The operation of doubling $d(t_n) = t_{2 \cdot n}$ is continuous and additive, but not linear since $d(t_1 \cdot t_1) = d(t_2) = t_4$, whereas $t_1 \cdot d(t_1) = t_1 \cdot t_2 = t_3$. Hence, the tropical semiring is not additive.

Proposition 11.12.2 (Consequences of additivity)

(1) Every additive semiring is commutative.

(2) A power construction with additive characteristic semiring is commutative.

Proof: We show only (2); the proof of (1) is similar.

Let S be a member of $\mathcal{P}\mathbf{X}$ for some $\mathbf{X}$ in D. The map $f = \lambda r.\, S \cdot r : [\mathcal{P}\mathbf{1} \to \mathcal{P}\mathbf{X}]$ is additive, whence linear because of additivity of $\mathcal{P}\mathbf{1}$. Thus,

$$S \cdot r = S \cdot (r \cdot 1) = f(r \cdot 1) = r \cdot f(1) = r \cdot (S \cdot 1) = r \cdot S \qquad \square$$

Chapter 12

Power homomorphisms

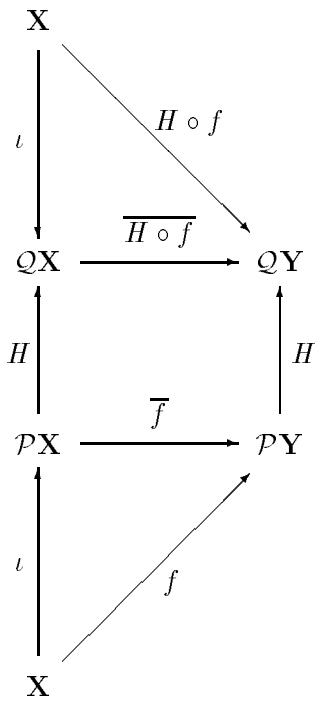
Homomorphisms between algebraic structures are mappings preserving all operations of these structures. Power constructions may be considered algebraic structures on a higher level. Thus, it is also possible and useful to define corresponding homomorphisms.

Power homomorphisms are defined in section 12.1. In section 12.2, power isomorphisms are considered. In section 12.3, the behavior of the derived power operations under power homomorphisms is studied. It turns out that power homomorphisms are usually not linear. The linear ones are investigated in section 12.4. They can be used to define initial and final power constructions (section 12.5). A power construction with semiring R is *initial* iff there is exactly one linear power homomorphism from it to every other construction with semiring R. *Finality* is the dual notion. The existence of initial and final power constructions for every semiring is shown in chapters 14 and 15 respectively.

12.1 Definition

A *power homomorphism* $H : \mathcal{P} \dot{\to} \mathcal{Q}$ between two power constructions $\mathcal{P}$ and $\mathcal{Q}$ with $def\ \mathcal{P} \subseteq def\ \mathcal{Q}$ is a 'family' of morphisms $H = (H_{\mathbf{X}})_{\mathbf{X} \in def\ \mathcal{P}} : [\mathcal{P}\mathbf{X} \to \mathcal{Q}\mathbf{X}]$ commuting over all power operations, i.e.

- The empty set in $\mathcal{P}\mathbf{X}$ is mapped to the empty set in $\mathcal{Q}\mathbf{X}$: $H\theta = \theta$.
- The image of a union is the union of the images: $H(A \uplus B) = (HA) \uplus (HB)$.
  This axiom and the previous one together mean H is additive.
- Singletons in $\mathcal{P}\mathbf{X}$ are mapped to singletons in $\mathcal{Q}\mathbf{X}$: $H\{\!|x|\!\}_{\mathcal{P}} = \{\!|x|\!\}_{\mathcal{Q}}$, or: $H \circ \iota_{\mathcal{P}} = \iota_{\mathcal{Q}}$.
- Let $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$. Then $H \circ f : [\mathbf{X} \to \mathcal{Q}\mathbf{Y}]$, and $H(ext_{\mathcal{P}}\, f\, A) = ext_{\mathcal{Q}}\,(H \circ f)(HA)$ has to hold for all A in $\mathcal{P}\mathbf{X}$. This axiom may also be written $H \circ (ext_{\mathcal{P}}\, f) = ext_{\mathcal{Q}}(H \circ f) \circ H$ (see the figure to the right).



Obviously, there is an identity power homomorphism $I : \mathcal{P} \dot{\to} \mathcal{P}$ where all morphisms $I_{\mathbf{X}}$ are identities. Furthermore, two power homomorphisms $G : \mathcal{P} \dot{\to} \mathcal{Q}$ and $H : \mathcal{Q} \dot{\to} \mathcal{R}$ may be composed 'pointwise', i.e. $(H \circ G)_{\mathbf{X}} = H_{\mathbf{X}} \circ G_{\mathbf{X}}$. It is easy to show that the outcome is again a power homomorphism $H \circ G : \mathcal{P} \dot{\to} \mathcal{R}$.

12.2 Power isomorphisms

A *power isomorphism* between two constructions $\mathcal{P}$ and $\mathcal{Q}$ is a family of isomorphisms $H = H_{\mathbf{X}} : [\mathcal{P}\mathbf{X} \to \mathcal{Q}\mathbf{X}]$ such that both $(H_{\mathbf{X}})_{\mathbf{X} \in def\, \mathcal{P}}$ and $(H_{\mathbf{X}}^{-1})_{\mathbf{X} \in def\, \mathcal{Q}}$ are power homomorphisms. Hence, two isomorphic constructions are defined for the same class of domains.

In contrast to continuity, the inverse of a bijective power homomorphism is again a power homomorphism.

Proposition 12.2.1 Let $H : \mathcal{P} \dot{\to} \mathcal{Q}$ be a power homomorphism such that the individual maps $H_{\mathbf{X}} : [\mathcal{P}\mathbf{X} \to \mathcal{Q}\mathbf{X}]$ are all bijective, and their inverses are monotonic. Then H is a power isomorphism.

Proof: The inverses are continuous by Prop. 2.5.3. They satisfy the axioms of a power homomorphism:

- $H^{-1}(\theta_{\mathcal{Q}}) = H^{-1}(H(\theta_{\mathcal{P}})) = \theta_{\mathcal{P}}$.
- $H^{-1}(A \uplus B) = H^{-1}((H(H^{-1}A)) \uplus (H(H^{-1}B))) = H^{-1}(H(H^{-1}A \uplus H^{-1}B)) = H^{-1}A \uplus H^{-1}B$.
- $H^{-1}\{\!|x|\!\}_{\mathcal{Q}} = H^{-1}(H\{\!|x|\!\}_{\mathcal{P}}) = \{\!|x|\!\}_{\mathcal{P}}$.
- $H^{-1} \circ ext_{\mathcal{Q}} f = H^{-1} \circ ext_{\mathcal{Q}}(H \circ H^{-1} \circ f) \circ H \circ H^{-1} = H^{-1} \circ H \circ ext_{\mathcal{Q}}(H^{-1} \circ f) \circ H^{-1} = ext_{\mathcal{Q}}(H^{-1} \circ f) \circ H^{-1}$ □

12.3 Some properties of power homomorphisms

Since power homomorphisms preserve all basic power operations, it is not surprising that they also preserve the derived operations.

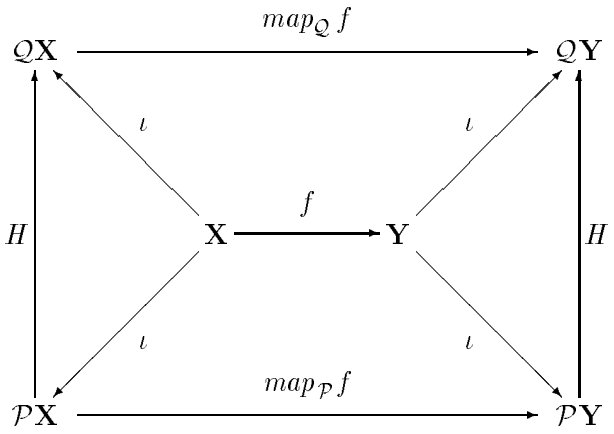
Proposition 12.3.1 Let $H : \mathcal{P} \dot{\rightarrow} \mathcal{Q}$ be a power homomorphism.

(1) Let $f : [\mathbf{X} \to \mathbf{Y}]$. Then $H \circ (map_{\mathcal{P}} f) = (map_{\mathcal{Q}} f) \circ H : [\mathcal{P}\mathbf{X} \to \mathcal{Q}\mathbf{Y}]$ (see the figure).

(2) Let b be in $\mathcal{P}\mathbf{1}$ and S in $\mathcal{P}\mathbf{X}$. Then $H(b \cdot S) = Hb \cdot HS$ and $H(S \cdot b) = HS \cdot Hb$.

(3) $H_{\mathbf{1}} : [\mathcal{P}\mathbf{1} \to \mathcal{Q}\mathbf{1}]$ is a semiring homomorphism.

(4) Let $p : [\mathbf{X} \to \mathcal{P}\mathbf{1}]$ and A in $\mathcal{P}\mathbf{X}$. Then $H\,(filter_{\mathcal{P}}\, p\, A) = filter_{\mathcal{Q}}\,(H \circ p)\,(HA)$. Using composition, one may also write $H \circ (filter_{\mathcal{P}}\, p) = (filter_{\mathcal{Q}}\,(H \circ p)) \circ H$.



In categorical terms, (1) means H is a *natural transformation* between the functors $\mathcal{P}$ and $\mathcal{Q}$.

Proof:

(1)
$$\begin{aligned} H \circ (map_{\mathcal{P}}\, f) &= H \circ (ext_{\mathcal{P}}\, (\iota_{\mathcal{P}} \circ f)) \\ &= (ext_{\mathcal{Q}}\, (H \circ \iota_{\mathcal{P}} \circ f)) \circ H \\ &= (ext_{\mathcal{Q}}\, (\iota_{\mathcal{Q}} \circ f)) \circ H \\ &= (map_{\mathcal{Q}}\, f) \circ H \end{aligned}$$

(2) $H(b \cdot S) = H(ext\,(\lambda\diamond.\, S)\, b) = ext\,(\lambda\diamond.\, HS)\,(Hb) = (Hb) \cdot (HS)$

(4)
$$\begin{aligned} H(filter\, p\, A) &= H(ext\,(\lambda x.\, p\, x \cdot \{\!|x|\!\}_{\mathcal{P}})\, A) \\ &= ext\,(\lambda x.\, H(p\, x \cdot \{\!|x|\!\}_{\mathcal{P}}))\,(HA) \\ (2): \quad &= ext\,(\lambda x.\, H(p\, x) \cdot \{\!|x|\!\}_{\mathcal{Q}})\,(HA) \\ &= filter\,(H \circ p)\,(HA) \end{aligned}$$

(2) $H(S \cdot b) = H(filter\,(\lambda x.\, b)\, S) = filter\,(\lambda x.\, Hb)\,(HS) = (HS) \cdot (Hb)$

(3) $H_{\mathbf{1}}$ respects $+ = \uplus$, $0 = \theta$, and $1 = \{\!|\diamond|\!\}$ by the definition of power homomorphisms. It respects '$\cdot$' by (2). □

12.4 Linear power homomorphisms

In the following, we want to compare power constructions with the same characteristic semiring by means of power homomorphisms. For fixed semiring, the notion of linearity of a power homomorphism makes sense.

Definition 12.4.1 Let $(\mathcal{P}, R, \varphi)$ and $(\mathcal{P}', R, \varphi')$ be two power constructions with the same characteristic semiring. A power homomorphism $H : \mathcal{P} \dot{\to} \mathcal{Q}$ is called *linear* iff the morphisms $H_{\mathbf{X}} : [\mathcal{P}\mathbf{X} \to \mathcal{P}'\mathbf{X}]$ are R-linear.

Remember that we always fix a semiring isomorphism $\varphi : [R \to \mathcal{P}\mathbf{1}]$ when considering a power construction $\mathcal{P}$ with semiring R.

Linearity of the morphisms is not a matter of course. Prop. 12.3.1 (2) tells $H(b \cdot S) = Hb \cdot HS$ instead for b in $\mathcal{P}\mathbf{1}$. From this, it becomes evident that a power homomorphism is linear iff it acts on R as an identity.

Proposition 12.4.2 Let $(\mathcal{P}, R, \varphi)$ and $(\mathcal{P}', R, \varphi')$ be two power constructions with the same characteristic semiring. A power homomorphism $H : \mathcal{P} \dot{\to} \mathcal{Q}$ is linear iff the composition $\varphi'^{-1} \circ H_{\mathbf{1}} \circ \varphi : [R \to R]$ is the identity.

Proof: To be sufficiently distinctive, we denote the product with members of $\mathcal{P}\mathbf{1}$ and $\mathcal{P}'\mathbf{1}$ by '$*$' in this proof.

Let H be a linear power homomorphism. Then for all r in R,

$$\begin{array}{rcll}
\varphi'^{-1}(H_{\mathbf{1}}(\varphi r)) & = & \varphi'^{-1}(H_{\mathbf{1}}(\varphi r * \{\!|\diamond|\!\})) & \{\!|\diamond|\!\} \text{ is neutral in } \mathcal{P}\mathbf{1} \\
& = & \varphi'^{-1}(H_{\mathbf{1}}(r \cdot \{\!|\diamond|\!\})) & R\text{-product '}\cdot\text{' defined by } \varphi \\
& = & \varphi'^{-1}(r \cdot H_{\mathbf{1}}\{\!|\diamond|\!\}) & H \text{ is linear} \\
& = & \varphi'^{-1}(\varphi' r * \{\!|\diamond|\!\}') & H \text{ is power homomorphism} \\
& = & \varphi'^{-1}(\varphi' r) \;=\; r &
\end{array}$$

Conversely,

$$H(r \cdot S) = H(\varphi r * S) = H(\varphi r) * HS = \varphi'^{-1}(H(\varphi r)) \cdot HS = r \cdot HS$$

holds applying the definition of '$\cdot$' in terms of '$*$'. □

Hence, if R allows non-trivial automorphisms there are non-linear power homomorphisms besides the linear ones.

12.5 Initial and final constructions

Initial and final power constructions are defined relative to the characteristic semiring by means of *linear* power homomorphisms. Without the assumption of linearity, their existence could not be guaranteed.

A construction $\mathcal{P}$ is initial if for all constructions $\mathcal{Q}$ with the same characteristic semiring there is exactly one linear power homomorphism $\mathcal{P} \dot{\to} \mathcal{Q}$. Finality is dual. The exact definitions however are more complex. To prevent a construction from being initial simply because it is almost undefined, we concentrate on total constructions defined for all domains.

Definition 12.5.1

A total power construction $(\mathcal{P}, R, \varphi)$ is *initial* for semiring R if for all total R-constructions $(\mathcal{Q}, R, \varphi')$ there is exactly one linear power homomorphism $H : \mathcal{P} \dot{\rightarrow} \mathcal{Q}$.

A total power construction $(\mathcal{P}, R, \varphi)$ is *final* for semiring R if for all R-constructions $(\mathcal{Q}, R, \varphi')$ there is exactly one linear power homomorphism $H : \mathcal{Q} \dot{\rightarrow} \mathcal{P}$.

These definitions imply the existence and uniqueness of an initial and a final construction for every given semiring domain R, as pointed out in chapters 14.5 and 15. If the definitions did not refer to *linear* power homomorphisms, there would be no initial and final constructions for semirings with non-trivial automorphisms.

Next, we state some simple properties of initial and final constructions.

Proposition 12.5.2 If $\mathcal{P}$ is isomorphic to an initial (a final) power construction $\mathcal{P}'$ for R, then $\mathcal{P}$ is also an initial (a final) power construction for R.

Proposition 12.5.3 For given semiring R, initial and final power constructions are unique up to isomorphism.

Note that this proposition does not claim the existence of initial and final constructions.

The proofs of the propositions are done by standard algebraic arguments — provided that 'isomorphic' is understood as isomorphic by a linear power isomorphism.

The main result is the following theorem:

Theorem 12.5.4 For every semiring R, initial and final power constructions exist.

In chapter 14, we demonstrate the initial construction. Chapter 15 is then devoted to the final construction. Before introducing the initial construction, we first investigate the theory of R-**X**-*modules* because the results of this theory are used when considering the initial construction.

Chapter 13

R-X-Modules

Before introducing the initial and final power constructions for a semiring R, we consider R-$\mathbf{X}$-*modules* in this chapter. R-$\mathbf{X}$-modules are R-modules together with a map from $\mathbf{X}$. Power domains are R-$\mathbf{X}$-modules by the singleton map. The theory of R-$\mathbf{X}$-modules allows to prove a host of theorems that are applied to the theory of power domain constructions in the next chapter.

The chapter starts by the definition of R-$\mathbf{X}$-modules and R-$\mathbf{X}$-linear maps in section 13.1. In section 13.2, we introduce the *core* of an R-$\mathbf{X}$-module as its least subset that still admits all operations. R-$\mathbf{X}$-modules that coincide with their core are called *reduced*. They have particularly nice properties, which are presented in section 13.3. An R-$\mathbf{X}$-module is *free* iff there is a unique R-$\mathbf{X}$-linear map to every other R-$\mathbf{X}$-module. The existence of free R-$\mathbf{X}$-modules is generally shown in section 13.5. Section 13.6 then provides a more explicit construction of the free R-$\mathbf{X}$-module in case of algebraic R and $\mathbf{X}$.

13.1 Definition

An R-$\mathbf{X}$-module is an R-module together with a mapping from $\mathbf{X}$ to it.

Definition 13.1.1 An R-$\mathbf{X}$-*module* $\mathbf{M}$ is a pair $\mathbf{M} = (M, \eta)$ of an R-module domain M and a morphism $\eta : [\mathbf{X} \to M]$.

A morphism $f : (M, \eta) \to (M', \eta')$ is R-$\mathbf{X}$-*linear* iff $f : [M \to M']$ is R-linear and $f \circ \eta = \eta'$, i.e. $f(\eta x) = \eta' x$ for all x in $\mathbf{X}$.

We already met examples for such R-$\mathbf{X}$-modules and R-$\mathbf{X}$-linear mappings. If $H : \mathcal{P} \dot{\to} \mathcal{Q}$ is a linear power homomorphism between two power constructions with the same semiring R, then for every ground domain $\mathbf{X}$, the instance $H_{\mathbf{X}}$ is an R-$\mathbf{X}$-linear mapping between the two R-$\mathbf{X}$-modules $(\mathcal{P}\mathbf{X}, \iota_{\mathcal{P}})$ and $(\mathcal{Q}\mathbf{X}, \iota_{\mathcal{Q}})$. If $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$, then the extension $ext\, f$ is R-$\mathbf{X}$-linear between the R-$\mathbf{X}$-modules $(\mathcal{P}\mathbf{X}, \iota)$ and $(\mathcal{P}\mathbf{Y}, f)$ since $ext\, f \circ \iota = f$. Thus, the R-$\mathbf{X}$-modules with R-$\mathbf{X}$-linear mappings provide a common abstraction of extension and power homomorphisms.

In the sequel, we need some more definitions.

Definition 13.1.2 Let $\mathbf{M} = (M, \eta)$ where $M = (M, +, 0, \cdot)$ is an R-module. A subset S of (the carrier of) M is called an R-$\mathbf{X}$-*submodule* of $\mathbf{M}$ iff

(1) ηx is in S for all $x \in \mathbf{X}$, i.e. $\eta[\mathbf{X}] \subseteq S$.

(2) 0 is in S.

(3) If a and b are in S, then so is $a + b$.

(4) If a is in S, then $r \cdot a$ is in S for all $r \in R$.

(5) S is a subdomain of M, i.e. if D is a directed subset of S, then the limit of D w.r.t. M is in S.

By definition, S may be assumed to be an R-$\mathbf{X}$-module again, and the natural inclusion map $e : S \to M$ is an R-$\mathbf{X}$-linear morphism.

13.2 The core of an R-X-module

It is easily verified that the intersection of a family of R-$\mathbf{X}$-submodules of a fixed R-$\mathbf{X}$-module is again an R-$\mathbf{X}$-submodule. Hence, the R-$\mathbf{X}$-submodules form a complete lattice, and there is a least R-$\mathbf{X}$-submodule for every given R-$\mathbf{X}$-module $\mathbf{M}$. We call it the *core* $\mathbf{M}^c$ of $\mathbf{M}$. In the following, we develop a more explicit description of the core.

Theorem 13.2.1

If $\mathbf{M} = (M, \eta)$ is an R-$\mathbf{X}$-module, then its core is given by $\mathbf{M}^c = \overline{\mathbf{M}^\#}$ where

$$\mathbf{M}^\# = \{r_1 \cdot \eta x_1 + \cdots + r_n \cdot \eta x_n \mid n \in \mathbf{N}_0, r_i \in R, x_i \in \mathbf{X}\}$$

and $\overline{B}$ is the least d-closed superset of B.

The size of $\mathbf{M}^c$ is bounded by $|\mathbf{M}^c| \leq 2^{(|R|^{|\mathbf{X}|})}$.

The proof of the theorem is split into a sequence of propositions and their proofs.

Proposition 13.2.2 $\mathbf{M}^\#$ satisfies the properties (1) through (4) of Def. 13.1.2.

Proof:

(1) $\eta x = 1 \cdot \eta x$ implies $\eta[\mathbf{X}] \subseteq \mathbf{M}^\#$.

(2) $r_1 \cdot \eta x_1 + \cdots + r_n \cdot \eta x_n = 0$ in case $n = 0$.

(3) Obvious.

(4) $r \cdot (r_1 \cdot \eta x_1 + \cdots + r_n \cdot \eta x_n) = (r \cdot r_1) \cdot \eta x_1 + \cdots + (r \cdot r_n) \cdot \eta x_n$. □

Proposition 13.2.3 $|\mathbf{M}^\#| \leq |R|^{|\mathbf{X}|}$

Proof: Because of $r \cdot \eta x + r' \cdot \eta x = (r + r') \cdot \eta x$, one can arrange $r_1 \cdot \eta x_1 + \cdots + r_n \cdot \eta x_n$ such that every x in $\mathbf{X}$ occurs at most once. Those x that do not occur may be added as $0 \cdot x$. Thus, $|\mathbf{M}^\#| \leq |\mathbf{X} \to R| = |R|^{|\mathbf{X}|}$. □

Proposition 13.2.4 $\overline{\mathbf{M}^\#}$ satisfies properties (1) through (5) of Def. 13.1.2, i.e. it is an R-$\mathbf{X}$-submodule of $\mathbf{M}$.

Proof: (1) and (2) hold because of Prop. 13.2.2 and $\mathbf{M}^{\#} \subseteq \overline{\mathbf{M}^{\#}}$. Property (3) for $\mathbf{M}^{\#}$ means this set is closed w.r.t. the binary continuous operation '+', whence $\overline{\mathbf{M}^{\#}}$ is also closed w.r.t. '+' by Prop. 4.8.4 (2).

For $r \in R$, let $p_r : [M \to M]$ be given by $p_r\, m = r \cdot m$. Property (4) for $\mathbf{M}^{\#}$ means this set is closed w.r.t. the unary continuous operation p_r, whence $\overline{\mathbf{M}^{\#}}$ is also closed w.r.t. p_r by Prop. 4.8.4 (1) for all r. □

Proposition 13.2.5 $\mathbf{M}^c = \overline{\mathbf{M}^{\#}}$

Proof: By Prop. 13.2.4, $\overline{\mathbf{M}^{\#}}$ is an R-$\mathbf{X}$-submodule of $\mathbf{M}$. Since $\mathbf{M}^c$ is the least such set, $\mathbf{M}^c \subseteq \overline{\mathbf{M}^{\#}}$ holds. Conversely, $\mathbf{M}^c$ being d-closed and $\mathbf{M}^{\#} \subseteq \mathbf{M}^c$ implies $\overline{\mathbf{M}^{\#}} \subseteq \mathbf{M}^c$. □

Proposition 13.2.6 $|\mathbf{M}^c| \leq 2^{(|R|^{|\mathbf{X}|})}$

Proof: By Prop. 13.2.3, $|\mathbf{M}^{\#}| \leq |R|^{|\mathbf{X}|}$ holds, and Prop. 3.5.9 yields $|\overline{B}| \leq 2^{|B|}$. □

13.3 Reduced R-X-modules

Definition 13.3.1 An R-$\mathbf{X}$-module is *reduced* iff it coincides with its core.

Equivalently, an R-$\mathbf{X}$-module is reduced iff it does not allow proper R-$\mathbf{X}$-submodules.

For every R-$\mathbf{X}$-module $\mathbf{M}$, the core $\mathbf{M}^c$ is reduced. Hence, every R-$\mathbf{X}$-module contains a reduced R-$\mathbf{X}$-submodule.

Reduced R-$\mathbf{X}$-modules enjoy many interesting properties listed in the sequel.

Lemma 13.3.2 Let $\mathbf{M} = (M, \eta)$ be a reduced R-$\mathbf{X}$-module, and M' an R-module. If $F, G : [M \to M']$ are two R-linear morphisms with $F(\eta x) \leq G(\eta x)$ for all $x \in \mathbf{X}$, then $F \leq G$ holds.

Proof: Let $S = \{a \in M \mid Fa \leq Ga\}$. We show that S satisfies the properties of Def. 13.1.2 whence $S = M$ follows because $\mathbf{M}$ admits no proper R-$\mathbf{X}$-submodules.

(1) For $x \in \mathbf{X}$, ηx is in S since $F(\eta x) \leq G(\eta x)$.

(2) $F(0) = 0_{M'} = G(0)$ whence $0 \in S$.

(3) Let $a, b \in S$. Then $F(a + b) = Fa + Fb \leq Ga + Gb = G(a + b)$.

(4) Let $a \in S$ and $r \in R$. Then $F(r \cdot a) = r \cdot Fa \leq r \cdot Ga = G(r \cdot a)$.

(5) Let D be a directed subset of S with limit a w.r.t. M. Then for all $d \in D$, $Fd \leq Gd \leq Ga$ holds, whence $Fa \leq Ga$ by continuity of F. □

The Lemma allows several conclusions:

Proposition 13.3.3 In Lemma 13.3.2, '$\leq$' may be replaced by '=':
Let $\mathbf{M} = (M, \eta)$ be a reduced R-$\mathbf{X}$-module, and M' an R-module. If $F, G : [M \to M']$ are two R-linear morphisms with $F(\eta x) = G(\eta x)$ for all $x \in \mathbf{X}$, then $F = G$ holds.

Proof: By anti-symmetry: $a = b$ iff $a \leq b$ and $b \leq a$. □

As a special instance of this proposition, one obtains:

Proposition 13.3.4 If $\mathbf{M}$ is a reduced R-$\mathbf{X}$-module, then there is at most one R-$\mathbf{X}$-linear mapping from $\mathbf{M}$ to any other R-$\mathbf{X}$-module $\mathbf{M}'$.

Proof: If F and G are two R-$\mathbf{X}$-linear morphisms, then they are in particular linear, and $F(\eta_{\mathbf{M}}x) = \eta_{\mathbf{M}'}x = G(\eta_{\mathbf{M}}x)$ holds for all x in $\mathbf{X}$. □

Proposition 13.3.5 If the semiring R has a least element $\bot_R$ and $\mathbf{X}$ has a least element $\bot_{\mathbf{X}}$, then every reduced R-$\mathbf{X}$-module $\mathbf{M} = (M, \eta)$ has a least element, namely $\bot_R \cdot \eta(\bot_{\mathbf{X}})$.

Proof: Let $S = \{a \in M \mid a \geq \bot_R \cdot \eta(\bot_{\mathbf{X}})\}$.

(1) Let $x \in \mathbf{X}$. Then $\eta x = 1 \cdot \eta x \geq \bot_R \cdot \eta(\bot_{\mathbf{X}})$.

(2) $0 = 0 \cdot \eta(\bot_{\mathbf{X}}) \geq \bot_R \cdot \eta(\bot_{\mathbf{X}})$.

(3) Let $a, b \in S$. Then $a + b \geq \bot_R \cdot \eta(\bot_{\mathbf{X}}) + \bot_R \cdot \eta(\bot_{\mathbf{X}}) = (\bot_R + \bot_R) \cdot \eta(\bot_{\mathbf{X}}) \geq \bot_R \cdot \eta(\bot_{\mathbf{X}})$.

(4) For $r \in R$ and $a \in S$, $r \cdot a \geq r \cdot \bot_R \cdot \eta(\bot_{\mathbf{X}}) \geq \bot_R \cdot \eta(\bot_{\mathbf{X}})$.

(5) S is obviously closed w.r.t. limits of directed sets in M.

Hence, S satisfies the conditions of Def. 13.1.2. Thus, $S = M$ holds. □

The following Lemma will be needed in the next chapter.

Lemma 13.3.6 Let $\mathbf{M} = (M, \eta)$ and $\mathbf{M}' = (M', \eta')$ be two R-$\mathbf{X}$-modules, and $F : [M \to M']$ an R-linear morphism that maps all points ηx into the core of $\mathbf{M}'$. If $\mathbf{M}$ is reduced, then F maps all points of $\mathbf{M}$ into the core of $\mathbf{M}'$.

Proof: Let $S = \{a \in \mathbf{M} \mid FA \in \mathbf{M}'^c\}$. We show that S satisfies conditions (1) through (5) of Def. 13.1.2. This implies $S = \mathbf{M}$ whence the claim of the proposition follows.

(1) $F(\eta_{\mathbf{M}}x) \in \mathbf{M}'^c$ by precondition.

(2) $F(0) = 0 \in \mathbf{M}'^c$.

(3) If a and b are in S, then $F(a + b) = Fa + Fb$ is in $\mathbf{M}'^c$.

(4) If a is in S, then $F(r \cdot a) = r \cdot Fa \in \mathbf{M}'^c$.

(5) If D is a directed set in S, then $F(\bigsqcup D) = \bigsqcup F[D] \in \mathbf{M}'^c$. □

13.4 Free R-X-modules

By Prop. 13.3.4, there is at most one R-$\mathbf{X}$-linear mapping from every reduced R-$\mathbf{X}$-module. In this section, we consider an even more special class of R-$\mathbf{X}$-modules.

Definition 13.4.1 An R-$\mathbf{X}$-module $\mathbf{F}$ is *free* iff for every R-$\mathbf{X}$-module $\mathbf{M}$, there is exactly one R-$\mathbf{X}$-linear morphism from $\mathbf{F}$ to $\mathbf{M}$.

The existence of free R-$\mathbf{X}$-modules is shown in section 13.5. For algebraic R and $\mathbf{X}$, a more explicit construction is provided in section 13.6. In this section, we study the properties of free R-$\mathbf{X}$-modules.

Proposition 13.4.2 All free R-$\mathbf{X}$-modules are isomorphic to each other.

Proof: Let $\mathbf{F}_1$ and $\mathbf{F}_2$ be two free R-$\mathbf{X}$-modules. Then there are R-$\mathbf{X}$-linear morphisms $f_1 : \mathbf{F}_1 \to \mathbf{F}_2$ and $f_2 : \mathbf{F}_2 \to \mathbf{F}_1$. Their composition $f_2 \circ f_1$ is an R-$\mathbf{X}$-linear morphism from $\mathbf{F}_1$ to itself. Identity is another such. By uniqueness, $f_2 \circ f_1 = id$ follows. The dual equation $f_1 \circ f_2 = id$ is shown analogously. □

Proposition 13.4.3 Every free R-$\mathbf{X}$-module is reduced.

Proof:
Let $\mathbf{F}$ be a free R-$\mathbf{X}$-module and S an R-$\mathbf{X}$-submodule of $\mathbf{F}$. We have to show $S = \mathbf{F}$.

The embedding $\epsilon : S \to \mathbf{F}$ is R-$\mathbf{X}$-linear since S is an R-$\mathbf{X}$-submodule. Since $\mathbf{F}$ is free, there is an R-$\mathbf{X}$-linear morphism $\zeta : [\mathbf{F} \to S]$. The composition $\epsilon \circ \zeta$ is R-$\mathbf{X}$-linear and maps $\mathbf{F}$ to itself as the identity does. By freedom, $\epsilon \circ \zeta = id$ holds. Hence, for every y in $\mathbf{F}$, $y = \epsilon\,(\zeta y) \in S$ holds. □

If $\mathbf{F}$ is a free R-$\mathbf{X}$-module, then for every morphism $f : [\mathbf{X} \to M]$ from $\mathbf{X}$ to some R-module M, there is a unique R-$\mathbf{X}$-linear extension $\overline{f} : [\mathbf{F} \to (M, f)]$ to the R-$\mathbf{X}$-module (M, f). Thus, '$\overline{\ }$' itself is a function from $[\mathbf{X} \to M]$ to $[\mathbf{F} \to M]$.

Theorem 13.4.4 If $\mathbf{F}$ is a free R-$\mathbf{X}$-module, then for every R-module M, the mapping $\overline{\ } : [\mathbf{X} \to M] \to [\mathbf{F} \to M]$ as introduced above is continuous.

Proof: '$\overline{\ }$' is monotonic by Lemma 13.3.2 telling that $f \leq g$ implies $\overline{f} \leq \overline{g}$.

Now, we show the continuity of '$\overline{\ }$'. Let η be the morphism from $\mathbf{X}$ to $\mathbf{F}$. Let $\mathcal{D}$ be a directed set of morphisms from $\mathbf{X}$ to M, and let f be its limit. We have to show $\overline{f} = \bigsqcup_{d \in \mathcal{D}} \overline{d}$. The function on the right hand side is R-linear by continuity of '$+$' and '$\cdot$'. It maps ηx to fx by continuity of application and $\overline{d}\,(\eta x) = d\,x$. By uniqueness, it thus equals $\overline{f}$. □

In the special case $\mathbf{X} = \mathbf{1}$, R itself is a free R-$\mathbf{X}$-module:

Proposition 13.4.5 $(R, \lambda x.\, 1)$ is a free R-$\mathbf{1}$-module.

Proof: Let $\mathbf{M} = (M, \eta)$ be an R-$\mathbf{1}$-module. Let $f : [R \to M]$ be given by $f\,(r) = r \cdot \eta \diamond$. This mapping is R-linear because of the module axioms. For instance, $f\,(r \cdot r') = (r \cdot r') \cdot \eta \diamond = r \cdot (r' \cdot \eta \diamond) = r \cdot f\,(r')$ holds. f is R-$\mathbf{1}$-linear since $f\,((\lambda x.\, 1) \diamond) = f\,(1) = 1 \cdot \eta \diamond = \eta \diamond$.

Let F be an arbitrary R-$\mathbf{1}$-linear map from $(R, \lambda x.1)$ to $\mathbf{M}$. Then $F\,(r) = F\,(r \cdot 1) = r \cdot F\,(1) = r \cdot F\,((\lambda x.\, 1) \diamond) = r \cdot \eta \diamond = f\,(r)$ holds, i.e. f is unique. □

13.5 Existence of free modules

In this section, we show the existence of the free R-$\mathbf{X}$-module for arbitrary semiring domains R and ground domains $\mathbf{X}$. The proof follows the lines of [Hoo87] who proved the existence of the free commutative idempotent monoid over $\mathbf{X}$. Hoofman used the categorical Freyd Adjoint Functor Theorem. We avoid its usage for the sake of a slightly more explicit construction. Our proof looks much simpler than that of Hoofman because we apply the notion of R-$\mathbf{X}$-modules.

We first construct the so-called solution set required by the Adjoint Functor Theorem. Instead of applying this theorem after verifying its remaining preconditions and thus obtaining

the mere existence of the free module, we present a simple explicit construction based on the solution set.

The problem with the class of all R-$\mathbf{X}$-modules is that it is not a set. The problem is solved by providing a set of R-$\mathbf{X}$-modules $\{\mathbf{M}_i \mid i \in I\}$ that may be used as representatives for all R-$\mathbf{X}$-modules.

Let c be the cardinal number $2^{(|R|^{|\mathbf{X}|})}$, and let C be a set of cardinality c. From C, we construct the set

$$D = \bigcup_{A \subseteq C} \{A\} \times (A \times A \to 2) \times (A \times A \to A) \times A \times (R \times A \to A) \times (\mathbf{X} \to A)$$

where $2 = \{0, 1\}$. Next, let I be the set of all tuples $(A, \leq, +, 0, \cdot, f)$ in D such that $\mathbf{A} = (A, \leq)$ is a domain, $M = (\mathbf{A}, +, 0, \cdot)$ is an R-module domain, and $f : \mathbf{X} \to \mathbf{A}$ is continuous, i.e. (M, f) is an R-$\mathbf{X}$-module. By construction, I contains isomorphic copies of all R-$\mathbf{X}$-modules up to cardinality c. Indexing I by itself, we obtain a family $(\mathbf{M}_i)_{i \in I}$ of R-$\mathbf{X}$-modules.

Now let $\mathbf{M} = (M, f)$ be an arbitrary R-$\mathbf{X}$-module. Let $\mathbf{M}^c$ be the core of $\mathbf{M}$ and $e : [\mathbf{M}^c \to \mathbf{M}]$ the natural inclusion. Note that e is R-$\mathbf{X}$-linear.

By Th. 13.2.1, $|\mathbf{M}^c| \leq 2^{(|R|^{|\mathbf{X}|})} = c$ holds. Hence, there is an isomorphic copy $\mathbf{M}_i$ of $\mathbf{M}^c$ in I. Let $\varphi : [\mathbf{M}_i \to \mathbf{M}^c]$ be the R-$\mathbf{X}$-linear isomorphism between $\mathbf{M}_i$ and $\mathbf{M}^c$.

Given the 'solution set' $(\mathbf{M}_i)_{i \in I}$, it is now easy to construct the free module. Let $\mathbf{P} = \prod_{i \in I} \mathbf{M}_i$. The operations in $\mathbf{P}$ are defined as follows:

- $a \leq b$ iff $a_i \leq b_i$ for all i in I,
- $a + b = (a_i + b_i)_{i \in I}$,
- $r \cdot a = (r \cdot a_i)_{i \in I}$ for r in R,
- $\eta x = (\eta_i\, x)_{i \in I}$ for $x \in \mathbf{X}$.

It is not difficult to see that all these functions are continuous, and make $\mathbf{P}$ into an R-$\mathbf{X}$-module. The projections $\pi_i : [\mathbf{P} \to \mathbf{M}_i]$ are R-$\mathbf{X}$-linear.

Finally, let $\mathbf{F}$ be the core of $\mathbf{P}$. Then the inclusion $p : \mathbf{F} \to \mathbf{P}$ is R-$\mathbf{X}$-linear. Summarizing, we get for each R-$\mathbf{X}$-module $\mathbf{M}$ the following chain of R-$\mathbf{X}$-linear mappings for some i:

$$\mathbf{F} \xrightarrow{\ p\ } \mathbf{P} \xrightarrow{\ \pi_i\ } \mathbf{M}_i \xrightarrow{\ \varphi\ } \mathbf{M}^c \xrightarrow{\ e\ } \mathbf{M}$$

Thus, we get an R-$\mathbf{X}$-linear map f from $\mathbf{F}$ to every R-$\mathbf{X}$-module $\mathbf{M}$. f is unique since $\mathbf{F}$ is reduced (Prop. 13.3.3).

13.6 Free modules in the algebraic case

A more explicit construction of the free R-$\mathbf{X}$-module is possible at least in the case of *structurally algebraic* semiring R and *algebraic* domain $\mathbf{X}$.

In this section, we construct the free R-$\mathbf{X}$-module from a structurally algebraic semiring domain R and an algebraic ground domain $\mathbf{X}$. We first build up an unordered set of finite linear combinations from the bases R^0 and $\mathbf{X}^0$. This set is then pre-ordered and finally completed to an algebraic domain.

Definition 13.6.1 A semiring domain R is *structurally algebraic* if it is algebraic and its base R^0 contains 0 and 1 and is closed w.r.t. '$+$' and '$\cdot$'.

Examples:

- Every finite and every discrete semiring domain R is structurally algebraic since $R^0 = R$ holds in these cases.
- $\mathbf{N}_0^\infty$ is structurally algebraic since sum and product of finite numbers are finite.
- The tropical semiring $\mathbf{T}$ is algebraic but not structurally algebraic since t_∞ is the neutral element of its addition.
- The powerset of an infinite set X ordered by inclusion with union as addition and intersection as multiplication is algebraic by Prop. 6.3.3, but not structurally algebraic since $1 = X$ is infinite.

Now, let R be a fixed structurally algebraic semiring and $\mathbf{X}$ a fixed algebraic ground domain. As a first step, we consider the set $\widehat{X}$ of finite linear combinations over $\mathbf{X}^0$.

Definition 13.6.2 For functions $\alpha : \mathbf{X}^0 \to R^0$, let $|\alpha| = \{x \in \mathbf{X}^0 \mid \alpha x \neq 0\}$. Then $\widehat{X} = \{\alpha : \mathbf{X}^0 \to R^0 \mid |\alpha| \text{ is finite}\}$.

$\widehat{X}$ consists of arbitrary functions; it is not restricted to continuous or even monotonic functions. For the moment, no order is assumed for $\widehat{X}$. The elements of $\widehat{X}$ stand for finite linear combinations over $\mathbf{X}^0$ where $\alpha\, x$ is the coefficient of x. Consequently, the following operations are defined in $\widehat{X}$:

- $\widehat{0} = \lambda x.\, 0$. It is in $\widehat{X}$ since $|\widehat{0}| = \emptyset$.
- $\alpha \mathbin{\widehat{+}} \beta = \lambda x.\, \alpha\, x + \beta\, x$. $|\alpha \mathbin{\widehat{+}} \beta| \subseteq |\alpha| \cup |\beta|$ holds.
- $r \mathbin{\hat{\cdot}} \alpha = \lambda x.\, r \cdot \alpha\, x$ for $r \in R^0$. $|r \mathbin{\hat{\cdot}} \alpha| \subseteq |\alpha|$ holds.
- $\hat{\imath} a = \lambda x. \begin{cases} 1 & \text{if } x = a \\ 0 & \text{otherwise} \end{cases}$ for $a \in \mathbf{X}^0$. $|\hat{\imath} a| = \{a\}$ holds.
- Let (M, f) be an R-$\mathbf{X}$-module. Then let $\widetilde{f} : \widehat{X} \to M$ be defined by $\widetilde{f}\alpha = \sum_{x \in |\alpha|} \alpha\, x \cdot fx$.

The operations (and $\widehat{X}$ itself) are well defined because R is *structurally* algebraic. The sum in $\widetilde{f}\alpha$ may also be assumed to range over $x \in \mathbf{X}^0$ since αx is 0 outside of $|\alpha|$.

$\widetilde{f}$ is R-$\mathbf{X}$-linear, i.e. is a linear extension of f:

- $\widetilde{f}(\alpha \mathbin{\widehat{+}} \beta) = \sum(\alpha\, x + \beta\, x) \cdot fx = \sum \alpha\, x \cdot fx + \sum \beta\, x \cdot fx = \widetilde{f}\alpha + \widetilde{f}\beta$
  using commutativity and associativity of '$+$' in M.
- $\widetilde{f}(r \mathbin{\hat{\cdot}} \alpha) = \sum(r \cdot \alpha\, x) \cdot fx = r \cdot \sum \alpha\, x \cdot fx = r \cdot \widetilde{f}\alpha$
- $\widetilde{f}(\hat{\imath} a) = \sum(\hat{\imath} a)\, x \cdot fx = 1 \cdot fa = fa$

Function $\widetilde{f}$ is unique with these properties since $|\alpha| = \{x_1, \ldots, x_n\}$ implies $\alpha = \alpha\, x_1 \mathbin{\hat{\cdot}} \hat{\imath} x_1 \mathbin{\widehat{+}} \cdots \mathbin{\widehat{+}} \alpha\, x_n \mathbin{\hat{\cdot}} \hat{\imath} x_n$.

The next step is pre-ordering $\widehat{X}$. Let '$\preceq$' the least binary relation in $\widehat{X}$ with the following properties:

(1) $\alpha \preceq \alpha$.

(2) If $\alpha \preceq \beta$ and $\beta \preceq \gamma$, then $\alpha \preceq \gamma$.

(3) If $x \leq x'$ in $\mathbf{X}^0$, then $\hat{\iota}x \preceq \hat{\iota}x'$.

(4) If $\alpha \preceq \alpha'$ and $\beta \preceq \beta'$, then $\alpha \mathbin{\hat{+}} \beta \preceq \alpha' \mathbin{\hat{+}} \beta'$.

(5) If $r \leq r'$ in R^0 and $\alpha \preceq \alpha'$, then $r \mathbin{\hat{\cdot}} \alpha \preceq r' \mathbin{\hat{\cdot}} \alpha'$.

More formally, '$\preceq$' is the intersection of all subsets of $\hat{X} \times \hat{X}$ with the indicated properties. One easily verifies that the intersection then also has these properties.

'$\preceq$' is a pre-order by (1) and (2), and the operations $\hat{\iota}$, '$\hat{+}$', and '$\hat{\cdot}$' are monotonic by (3) through (5). The extended functions $\tilde{f}$ are also monotonic.

Proof:
For fixed $f : [\mathbf{X} \to M]$, define a relation '$\preceq_f$' in $\hat{X}$ by $\alpha \preceq_f \beta$ iff $\tilde{f}\alpha \leq \tilde{f}\beta$. Then '$\preceq_f$' obviously is reflexive and transitive, and it also satisfies the properties (3) through (5) above:

(3) $x \leq x'$ implies $\tilde{f}(\hat{\iota}x) = fx \leq fx' = \tilde{f}(\hat{\iota}x')$, whence $\hat{\iota}x \preceq_f \hat{\iota}x'$.

(4) $\tilde{f}(\alpha \mathbin{\hat{+}} \beta) = \tilde{f}\alpha + \tilde{f}\beta \leq \tilde{f}\alpha' + \tilde{f}\beta' = \tilde{f}(\alpha' \mathbin{\hat{+}} \beta')$

(5) $\tilde{f}(r \mathbin{\hat{\cdot}} \alpha) = r \cdot \tilde{f}\alpha \leq r' \cdot \tilde{f}\alpha' = \tilde{f}(r' \mathbin{\hat{\cdot}} \alpha')$

Since '$\preceq$' is the least relation with these properties, $\alpha \preceq \beta$ implies $\alpha \preceq_f \beta$, i.e. $\tilde{f}\alpha \leq \tilde{f}\beta$. □

As a next step, we turn the pre-ordered set $\hat{X}$ into the poset $\hat{X}^*$ by forming classes w.r.t. the equivalence relation '$\alpha \preceq \beta$ and $\beta \preceq \alpha$'. All operations of $\hat{X}$ may also be defined for $\hat{X}^*$ because they are monotonic. The resulting operations on $\hat{X}^*$ are monotonic again.

As final step, let $\overline{X}$ be the ideal completion of the poset $\hat{X}^*$. Hence, $\overline{X}$ is an algebraic domain whose base is isomorphic to $\hat{X}^*$. All the monotonic functions $\hat{+} : \hat{X}^* \times \hat{X}^* \to \hat{X}^*$, $\hat{\cdot} : R^0 \times \hat{X}^* \to \hat{X}^*$, and $\tilde{f} : \hat{X}^* \to M$ for every $f : [\mathbf{X} \to M]$ have unique continuous extensions $+ : [\overline{X} \times \overline{X} \to \overline{X}]$, $\cdot : [R \times \overline{X} \to \overline{X}]$, and $\overline{f} : [\overline{X} \to M]$ for every $f : [\mathbf{X} \to M]$. These operations possess the necessary algebraic properties such as associativity and linearity because they are inherited from the base. The linear extension $\overline{f}$ of f on $\overline{X}$ is unique because $\overline{X}$ trivially is a reduced R-$\mathbf{X}$-module. Thus, $\overline{X}$ is the free R-$\mathbf{X}$-module.

The results above allow to state the following theorem:

Theorem 13.6.3 If R is a structurally algebraic semiring domain and $\mathbf{X}$ is algebraic, then the free R-$\mathbf{X}$-module is algebraic.

Problem 9 What happens if R is algebraic without being structurally algebraic?

Proposition 13.6.4 If R and $\mathbf{X}$ are discrete, then so is the free R-$\mathbf{X}$-module. It equals $\hat{X}$, the set of finite R-linear combinations over $\mathbf{X}$.

Proof: Discrete semirings are structurally algebraic. Consider the set $\hat{X}$. We claim $\alpha \preceq \beta$ iff $\alpha = \beta$.

$\alpha = \beta$ implies $\alpha \preceq \beta$ by reflexivity. For the opposite direction, note that the relation '$=$' satisfies the properties (1) through (5) of '$\preceq$'. In proving this, discreteness of $\mathbf{X}$ is needed for (3), and discreteness of R for (5). Hence, $\hat{X}$ is a discrete poset and coincides with its ideal completion. □

Proposition 13.6.5 If R and $\mathbf{X}$ are finite, then so is the free R-$\mathbf{X}$-module. It equals $\widehat{X}^*$, the poset of equivalence classes of R-linear combinations over $\mathbf{X}$.

Proof: Finite semirings are structurally algebraic. Because the restriction that $|\alpha|$ be finite is satisfied always, $\widehat{X}$ is the set of all functions from $\mathbf{X}$ to R. This set is finite. Thus, $\widehat{X}^*$ is also finite, whence it is isomorphic to its ideal completion. □

Chapter 14

Sub-constructions, reduced and initial constructions

In this chapter, we consider some notions that were already introduced and investigated for R-$\mathbf{X}$-modules in the previous chapter. Here, we abstract from the ground domain $\mathbf{X}$ and apply the notions to power constructions.

A power construction $\mathcal{Q}$ is a sub-construction of $\mathcal{P}$ if the power domains $\mathcal{Q}\mathbf{X}$ are subsets of $\mathcal{P}\mathbf{X}$ such that $\mathcal{Q}$ inherits all operations of $\mathcal{P}$ (see section 14.1). Sub-constructions of $\mathcal{P}$ may or may not have the same characteristic semiring as $\mathcal{P}$. The *core* is the least sub-construction of $\mathcal{P}$ with the same semiring (section 14.2). *Reduced power constructions* coincide with their core, whence they do not possess proper sub-constructions with the same characteristic semiring. Their properties are investigated in sections 14.3 and 14.4. The initial power construction for semiring R is introduced in section 14.5. It results from mapping every ground domain $\mathbf{X}$ to the free R-$\mathbf{X}$-module. If R' is a sub-semiring of $\mathcal{P}\mathbf{1}$, then there is a greatest sub-construction of $\mathcal{P}$ that has characteristic semiring R'. In section 14.6, this sub-construction is explicitly characterized in terms of formal existential quantification on $\mathcal{P}$.

If $\mathcal{P}$ is an R-construction, then the power domains $\mathcal{P}\mathbf{X}$ induce R-$\mathbf{X}$-modules $(\mathcal{P}\mathbf{X}, \iota_{\mathbf{X}})$. In the sequel, we always refer to this R-$\mathbf{X}$-module when saying $\mathcal{P}\mathbf{X}$ is reduced or $\mathcal{P}\mathbf{X}$ and $\mathcal{Q}\mathbf{X}$ are isomorphic. Consequently, isomorphisms between two power domains $\mathcal{P}\mathbf{X}$ and $\mathcal{Q}\mathbf{X}$ are R-$\mathbf{X}$-linear maps.

14.1 Sub-constructions

Let $\mathcal{P}$ be a given power construction. $\mathcal{Q}$ is called a *sub-construction* of $\mathcal{P}$ iff $\mathcal{Q}$ maps ground domains $\mathbf{X}$ into subsets of $\mathcal{P}\mathbf{X}$ such that

- $\mathcal{Q}\mathbf{X}$ is closed w.r.t. lubs of directed sets,
- $\theta \in \mathcal{Q}\mathbf{X}$,
- If A and B are in $\mathcal{Q}\mathbf{X}$, then $A \uplus B$ is in $\mathcal{Q}\mathbf{X}$,
- $\{\!|x|\!\}$ is in $\mathcal{Q}\mathbf{X}$ for all x in $\mathbf{X}$,
- If $f : [\mathbf{X} \to \mathcal{Q}\mathbf{Y}]$ and A in $\mathcal{Q}\mathbf{X}$, then $\mathit{ext}\, f\, A$ is in $\mathcal{Q}\mathbf{Y}$.

In shorter terms, $\mathcal{Q}\mathbf{X}$ is closed w.r.t. all power operations of $\mathcal{P}$.

$\mathcal{Q}$ is obviously a power construction since the validity of the power axioms for $\mathcal{Q}$ is inherited from $\mathcal{P}$. By the same argument, one concludes

Proposition 14.1.1
If $\mathcal{P}$ is commutative / symmetric / faithful, then every sub-construction of $\mathcal{P}$ is so.

One easily verifies that the intersection of a family of sub-constructions of a power construction $\mathcal{P}$ is again a sub-construction of $\mathcal{P}$, if we define $(\bigcap_{i\in I}\mathcal{Q}_i)\mathbf{X} = \bigcap_{i\in I}(\mathcal{Q}_i\mathbf{X})$. Hence, the sub-constructions of $\mathcal{P}$ form a complete lattice.

Sub-semirings are defined analogously to sub-constructions.

Definition 14.1.2
Let $(R, +, 0, \cdot, 1)$ be a semiring domain. A subset R' of R is a *sub-semiring* of R iff

(1) 0 is in R';

(2) if a and b are in R', then $a + b$ is in R';

(3) 1 is in R';

(4) if a and b are in R', then $a \cdot b$ is in R';

(5) if D is a directed set in R' with limit x w.r.t. R, then x is in R'.

Because the operations in the characteristic semiring are derived from the power operations, the semiring of a sub-construction $\mathcal{Q}$ of $\mathcal{P}$ is a sub-semiring of the semiring of $\mathcal{P}$. Similarly, the semiring of an intersection of sub-constructions is the intersection of the semirings of the sub-constructions. In section 14.6, a method is presented to obtain a sub-construction for every given semiring.

The sub-constructions with the same characteristic semiring attract special interest.

Proposition 14.1.3 Let $\mathcal{Q}$ be a sub-construction of a power construction $\mathcal{P}$. Then $\mathcal{Q}\mathbf{1} = \mathcal{P}\mathbf{1}$ holds iff all power domains $\mathcal{Q}\mathbf{X}$ are closed w.r.t. $\mathcal{P}\mathbf{1}$-multiplication.

Proof: Assume $\mathcal{Q}\mathbf{1} = \mathcal{P}\mathbf{1}$ holds. Let A be in $\mathcal{Q}\mathbf{X}$ and r in $\mathcal{P}\mathbf{1}$, whence it is also in $\mathcal{Q}\mathbf{1}$. Extension yields $r \cdot A = ext\,(\lambda\diamond.\, A)\,r$ in $\mathcal{Q}\mathbf{X}$ by the definition of sub-constructions.

If all power domains $\mathcal{Q}\mathbf{X}$ are closed w.r.t. $\mathcal{P}\mathbf{1}$-multiplication, then in particular $\mathcal{Q}\mathbf{1}$ is so. Hence, for all r in $\mathcal{P}\mathbf{1}$, $r = r \cdot 1$ is in $\mathcal{Q}\mathbf{1}$ since 1 is in $\mathcal{Q}\mathbf{1}$. □

If $\mathcal{Q}$ is a sub-construction of $\mathcal{P}$, then the natural inclusion maps $E_{\mathbf{X}} : \mathcal{Q}\mathbf{X} \to \mathcal{P}\mathbf{X}$ yield a power homomorphism $E : \mathcal{Q}\dot{\to}\mathcal{P}$. If $\mathcal{Q}$ moreover has the same characteristic semiring as $\mathcal{P}$, then E is a linear power homomorphism.

14.2 The core of a power construction

Let $\mathcal{P}$ be a power construction with characteristic semiring R. Then the power domains $\mathcal{P}\mathbf{X}$ form R-$\mathbf{X}$-modules together with the singleton mappings $\iota : [\mathbf{X} \to \mathcal{P}\mathbf{X}]$. We denote the core of $(\mathcal{P}\mathbf{X}, \iota)$ by $(\mathcal{P}^c\mathbf{X}, \iota)$ and show that $\mathcal{P}^c$ induces a power domain construction with the same characteristic semiring as $\mathcal{P}$.

The operations θ, '$\uplus$', and $\{\!|.|\!\}$ obviously cut down to operations for $\mathcal{P}^c$ because $\mathcal{P}^c\mathbf{X}$ was defined to allow these operations together with R-multiplication. We only have to provide an extension satisfying the power axioms.

For every $f : [\mathbf{X} \to \mathcal{P}^c\mathbf{Y}]$, the linear extension $ext_{\mathcal{P}}\, f$ maps singletons $\{\!|x|\!\}$ of $\mathcal{P}^c\mathbf{X}$ into $\mathcal{P}^c\mathbf{Y}$ since $ext_{\mathcal{P}}\{\!|x|\!\} = fx$. Hence by Lemma 13.3.6, $ext_{\mathcal{P}}\, f$ maps all members of $\mathcal{P}^c\mathbf{X}$ to $\mathcal{P}^c\mathbf{Y}$. Thus, the extension of $\mathcal{P}$ cuts down to the extension of $\mathcal{P}^c$. It satisfies the power axioms because $ext_{\mathcal{P}}$ did. Because the power operations for $\mathcal{P}^c$ are derived from those of $\mathcal{P}$ by restriction and corestriction, the embeddings $E : \mathcal{P}^c\mathbf{X} \to \mathcal{P}\mathbf{X}$ form a power homomorphism.

$\mathcal{P}^c\mathbf{1}$ equals $\mathcal{P}\mathbf{1}$ since every member b of $\mathcal{P}\mathbf{1}$ equals $b \cdot \{\!|\diamond|\!\}$, whence $b \in \mathcal{P}^c\mathbf{1}$. Thus, $\mathcal{P}^c$ has the same characteristic semiring as $\mathcal{P}$.

If $\mathcal{Q}$ is another sub-construction of $\mathcal{P}$ with semiring $\mathcal{P}\mathbf{1}$, then the power domains $(\mathcal{Q}\mathbf{X}, \iota)$ form R-$\mathbf{X}$-submodules of $(\mathcal{P}\mathbf{X}, \iota)$ by the definition of sub-constructions and by Prop. 14.1.3. Hence, $\mathcal{P}^c\mathbf{X} \subseteq \mathcal{Q}\mathbf{X}$ holds for all ground domains $\mathbf{X}$. Thus, $\mathcal{P}^c$ is the least sub-construction of $\mathcal{P}$ that still has characteristic semiring $\mathcal{P}\mathbf{1}$.

Let $\mathcal{P}$ and $\mathcal{Q}$ be two power constructions with the same characteristic semiring. For every power homomorphism $H : \mathcal{P} \dot{\to} \mathcal{Q}$, $H\{\!|x|\!\}_{\mathcal{P}} = \{\!|x|\!\}_{\mathcal{Q}}$ is in $\mathcal{Q}^c\mathbf{X}$. If H is linear, then H cuts down to a power homomorphism $H^c : \mathcal{P}^c \dot{\to} \mathcal{Q}^c$ by Lemma 13.3.6.

All results of this section are collected in the following theorem:

Theorem 14.2.1 For every power construction $\mathcal{P}$, the core $\mathcal{P}^c$ is the least sub-construction of $\mathcal{P}$ with the same characteristic semiring. The embeddings of the cores $\mathcal{P}^c\mathbf{X}$ into the power domains $\mathcal{P}\mathbf{X}$ provide a linear power homomorphism $E : \mathcal{P}^c \dot{\to} \mathcal{P}$.

For every linear power homomorphism $H : \mathcal{P} \dot{\to} \mathcal{Q}$, there is a linear homomorphism $H^c : \mathcal{P}^c \dot{\to} \mathcal{Q}^c$ with $E \circ H^c = H^c \circ E$.

14.3 Reduced power constructions

Definition 14.3.1 A power construction is *reduced* iff it coincides with its core.

For every power construction $\mathcal{P}$, the core $\mathcal{P}^c$ is reduced. Hence, every power construction contains a reduced sub-construction.

Since the core construction $\mathcal{P}^c$ maps ground domains $\mathbf{X}$ to the core modules $(\mathcal{P}\mathbf{X}, \iota)^c$, a power construction is reduced iff all R-$\mathbf{X}$-modules $(\mathcal{P}\mathbf{X}, \iota)$ are reduced. Thus, all results of the previous chapter about reduced R-$\mathbf{X}$-modules apply.

Proposition 14.3.2 Let $\mathcal{P}$ be a reduced R-construction, $\mathbf{X}$ a ground domain, and M an R-module. Two linear morphisms $F, G : [\mathcal{P}\mathbf{X} \to M]$ that coincide on singletons are equal.

Proof: If $F, G : [\mathcal{P}\mathbf{X} \to M]$ are two linear morphisms that coincide on singletons, i.e. $F \circ \iota = G \circ \iota$, then F and G induce two R-$\mathbf{X}$-linear morphisms from $(\mathcal{P}\mathbf{X}, \iota)$ to $(M, F \circ \iota)$. By Prop. 13.3.3, $F = G$ follows. □

Furthermore, we obtain the following properties:

Proposition 14.3.3

(1) Reduced power constructions have unique linear extensions.

(2) Every reduced power construction with a commutative semiring is symmetric.

(3) Every reduced power construction with finite semiring preserves FIN, F-ALG, and F-CONT.

(4) Let $\mathcal{P}$ be a reduced power construction with a semiring R that has a least element $\bot_R$. If $\mathbf{X}$ has a least element $\bot_{\mathbf{X}}$, then $\mathcal{P}\mathbf{X}$ has a least element, namely $\bot_R \cdot \{\!|\bot_{\mathbf{X}}|\!\}$.

Proof:

(1) By Prop. 14.3.2 in case $M = \mathcal{P}\mathbf{Y}$.

(2) From (1) by Prop. 11.7.1.

(3) Since $(\mathcal{P}\mathbf{X}, \iota)$ is reduced, its cardinality is bounded by $2^{|R|^{|\mathbf{X}|}}$ by Th. 13.2.1. Hence, $\mathcal{P}\mathbf{X}$ is finite if R and $\mathbf{X}$ are finite, i.e. $\mathcal{P}$ preserves FIN. Preservation of F-ALG and F-CONT is then due to Th. 7.4.4.

(4) directly follows from Prop. 13.3.5. □

Finally, we investigate the behavior of reduced power constructions w.r.t. power homomorphisms. First, linear power homomorphisms are nothing else but families of linear mappings.

Proposition 14.3.4 Let $\mathcal{P}$ be a reduced power construction for semiring R, and $\mathcal{Q}$ a power construction with the same semiring. If $L_{\mathbf{X}} : [\mathcal{P}\mathbf{X} \to \mathcal{Q}\mathbf{X}]$ is a family of linear mappings indexed by domains $\mathbf{X}$ such that $L_{\mathbf{X}}\{\!|x|\!\}_{\mathcal{P}} = \{\!|x|\!\}_{\mathcal{Q}}$ holds for every x in every $\mathbf{X}$, then $L : \mathcal{P} \dot{\to} \mathcal{Q}$ is a linear power homomorphism.

Proof: We only have to show $L \circ (ext_{\mathcal{P}}\, f) = ext_{\mathcal{Q}}\,(L \circ f) \circ L$. Since L and all extensions are linear, both sides are linear morphisms from $\mathcal{P}\mathbf{X}$ to $\mathcal{Q}\mathbf{Y}$. They coincide on singletons: $L\,(ext_{\mathcal{P}}\, f\, \{\!|x|\!\}_{\mathcal{P}}) = L\,(fx)$ and $ext_{\mathcal{Q}}\,(L \circ f)\,(L\{\!|x|\!\}_{\mathcal{P}}) = ext_{\mathcal{Q}}\,(L \circ f)\,\{\!|x|\!\}_{\mathcal{Q}} = L(fx)$ hold. By Prop. 14.3.2, both sides are equal. □

Proposition 14.3.5 Let $\mathcal{P}$ be a reduced power construction, and $\mathcal{Q}$ an arbitrary power construction with the same semiring as $\mathcal{P}$.

(1) There is at most one linear power homomorphism $\mathcal{P} \dot{\to} \mathcal{Q}$.

(2) For every linear power homomorphism $H : \mathcal{P} \dot{\to} \mathcal{Q}$, there is a unique linear power homomorphism $H' : \mathcal{P} \dot{\to} \mathcal{Q}^c$ such that $E \circ H' = H$ where $E : \mathcal{Q}^c \dot{\to} \mathcal{Q}$ is the natural inclusion.

Proof:

(1) Let H_1 and H_2 be two linear power homomorphisms from $\mathcal{P}$ to $\mathcal{Q}$. Then for every ground domain $\mathbf{X}$, the mappings H_1 and H_2 are linear and coincide for singletons: $H_1\{\!|x|\!\}_{\mathcal{P}} = \{\!|x|\!\}_{\mathcal{Q}} = H_2\{\!|x|\!\}_{\mathcal{P}}$, whence they are equal by Prop. 14.3.2.

(2) H' is the power homomorphism H^c of Prop. 14.2.1. It is unique because of (1). □

14.4 Reduced constructions and retracts

In section 7.5, we introduced the notion of *retracts*. A domain $\mathbf{Y}$ is a retract of a domain $\mathbf{X}$ iff there are morphisms $r : [\mathbf{X} \to \mathbf{Y}]$ and $e : [\mathbf{Y} \to \mathbf{X}]$ with $r \circ e = id_{\mathbf{Y}}$. Theorem 7.5.3 stated that every continuous domain is a retract of some algebraic domain.

In this section, we show two theorems about retracts. The first theorem states that reducedness carries over to retracts, whereas the second theorem handles isomorphisms between power domains of different power constructions.

Theorem 14.4.1 Let $\mathcal{P}$ be an R-construction defined for two domains $\mathbf{X}$ and $\mathbf{Y}$ where $\mathbf{Y}$ is a retract of $\mathbf{X}$. If $\mathcal{P}\mathbf{X}$ is reduced, then $\mathcal{P}\mathbf{Y}$ is reduced, too.

Proof: Let S be an R-$\mathbf{X}$-submodule of the R-$\mathbf{X}$-module $(\mathcal{P}\mathbf{Y}, \iota_{\mathbf{Y}})$. We have to show $S = \mathcal{P}\mathbf{Y}$. The two morphisms $r : [\mathbf{X} \to \mathbf{Y}]$ and $e : [\mathbf{Y} \to \mathbf{X}]$ are raised to $R = map\, r : [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ and $E = map\, e : [\mathcal{P}\mathbf{Y} \to \mathcal{P}\mathbf{X}]$. These mappings are linear and satisfy $R \circ E = id_{\mathcal{P}\mathbf{X}}$ because of the properties of '*map*'. Let $T = R^{-1}[S]$ be the inverse image of S in $\mathcal{P}\mathbf{X}$. We show that T is an R-$\mathbf{X}$-submodule of $\mathcal{P}\mathbf{X}$.

(1) For x in $\mathbf{X}$, $R\{\!|x|\!\} = \{\!|r\, x|\!\} \in S$ holds, whence $\{\!|x|\!\}$ is in T.

(2) θ is in T by $R\theta = \theta \in S$.

(3) If A and B are in T, then $A \uplus B$ also is in T by $R\,(A \uplus B) = RA \uplus RB \in S$.

(4) Similarly, A in T implies $r \cdot A$ in T for all r in R.

(5) T is d-closed by Prop. 3.5.6 since S is d-closed.

Since $\mathcal{P}\mathbf{X}$ is reduced, T equals $\mathcal{P}\mathbf{X}$. If A is an arbitrary member of $\mathcal{P}\mathbf{Y}$, then EA is in $\mathcal{P}\mathbf{X} = T$, whence $A = R\,(EA)$ is in S. Thus, S equals $\mathcal{P}\mathbf{Y}$. □

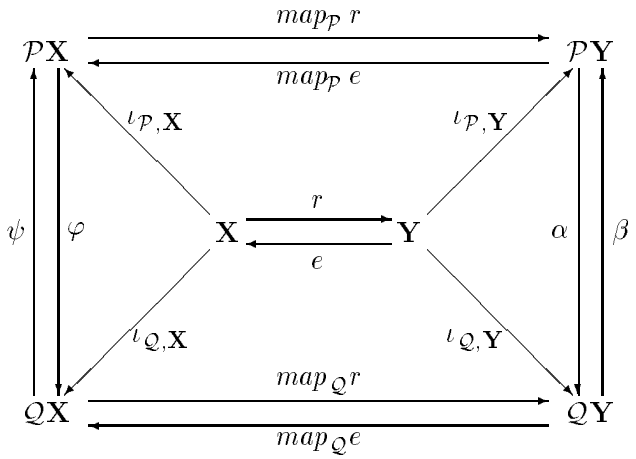
The Theorem immediately implies the following corollary:

Corollary 14.4.2
Let $\mathcal{P}$ be a power construction defined for continuous domains. If $\mathcal{P}\mathbf{X}$ is reduced for all algebraic domains $\mathbf{X}$, then $\mathcal{P}\mathbf{Y}$ is also reduced for all continuous domains $\mathbf{Y}$.

Now we turn to isomorphisms between power constructions.

Theorem 14.4.3
Let $\mathcal{P}$ and $\mathcal{Q}$ be two power constructions with the same semiring R defined for two domains $\mathbf{X}$ and $\mathbf{Y}$ where $\mathbf{Y}$ is a retract of $\mathbf{X}$. If the power domains $\mathcal{P}\mathbf{X}$ and $\mathcal{Q}\mathbf{X}$ are reduced and isomorphic, then the power domains $\mathcal{P}\mathbf{Y}$ and $\mathcal{Q}\mathbf{Y}$ are also reduced and isomorphic.

Proof: The retract mappings $r : [\mathbf{X} \to \mathbf{Y}]$ and $e : [\mathbf{Y} \to \mathbf{X}]$, and the pair of isomorphisms $\varphi : [\mathcal{P}\mathbf{X} \to \mathcal{Q}\mathbf{X}]$ and $\psi : [\mathcal{Q}\mathbf{X} \to \mathcal{P}\mathbf{X}]$ induce the following diagram of mappings:



Here, α and β are given by $\alpha = map_{\mathcal{Q}}r \circ \varphi \circ map_{\mathcal{P}}e$ and $\beta = map_{\mathcal{P}}r \circ \psi \circ map_{\mathcal{Q}}e$. Both α and β are R-linear as compositions of R-linear maps. They are also R-$\mathbf{X}$-linear:

$$\begin{aligned}
\alpha \circ \iota_{\mathcal{P},\mathbf{Y}} &= map_{\mathcal{Q}}r \circ \varphi \circ map_{\mathcal{P}}e \circ \iota_{\mathcal{P},\mathbf{Y}} \\
&= map_{\mathcal{Q}}r \circ \varphi \circ \iota_{\mathcal{P},\mathbf{X}} \circ e \\
&= map_{\mathcal{Q}}r \circ \iota_{\mathcal{Q},\mathbf{X}} \circ e \\
&= \iota_{\mathcal{Q},\mathbf{Y}} \circ r \circ e \\
&= \iota_{\mathcal{Q},\mathbf{Y}}
\end{aligned}$$

The R-$\mathbf{X}$-linearity of β, i.e. $\beta \circ \iota_{\mathcal{Q},\mathbf{Y}} = \iota_{\mathcal{P},\mathbf{Y}}$, is shown analogously. The composition $\beta \circ \alpha$ forms an R-$\mathbf{X}$-linear map from $\mathcal{P}\mathbf{Y}$ to itself. Identity is another such map. By Th. 14.4.1, $\mathcal{P}\mathbf{Y}$ is reduced. By Prop. 13.3.4, $\beta \circ \alpha = id$ follows. Analogously, $\alpha \circ \beta = id$ is shown. □

Corollary 14.4.4 If $\mathcal{P}$ and $\mathcal{Q}$ are two power constructions defined for continuous domains such that $\mathcal{P}\mathbf{X}$ and $\mathcal{Q}\mathbf{X}$ are reduced and isomorphic for all algebraic ground domains $\mathbf{X}$, then $\mathcal{P}\mathbf{Y}$ and $\mathcal{Q}\mathbf{Y}$ are also reduced and isomorphic for all continuous ground domains $\mathbf{Y}$.

14.5 Initial constructions

In this section, the existence of the initial construction for given semiring R is shown and its properties are studied. The idea to consider initial power constructions dates back to [HP79]. Hoofman [Hoo87] showed the existence of the initial construction for semiring $\{0, 1\}$. Main [Mai85] then proposed initial constructions for some fancy semirings as indicated in section 11.2. In contrast to our work, he requires the singleton mapping to be strict without telling exactly why. Our singleton mappings are generally non-strict as indicated by Prop. 13.3.5 and 15.7.4. The singleton maps of mixed and sandwich power domain are also non-strict.

For every domain $\mathbf{X}$ and every semiring R, there is a free R-$\mathbf{X}$-module $R \odot \mathbf{X}$. The construction $\mathbf{X} \mapsto R \odot \mathbf{X}$ is the initial power construction for semiring R as will be shown in the sequel.

Principally, 'the' free R-$\mathbf{X}$-module is only determined up to isomorphism. Henceforth, we assume that $R \odot \mathbf{X}$ is a fixed member of the class of all free R-$\mathbf{X}$-modules. In the special case $\mathbf{X} = \mathbf{1}$, one may choose $R \odot \mathbf{1} = R$ by Prop. 13.4.5.

Theorem 14.5.1

Let R be a semiring. The power construction $\mathcal{P}$ defined by $\mathcal{P}\mathbf{X} = R \odot \mathbf{X}$ is an initial power construction for semiring R. The a priori given external product of the modules $\mathcal{P}\mathbf{X}$ coincides with the external product derived from the power operations. $\mathcal{P}$ is reduced.

Proof: We first show that $\mathcal{P}$ is a power construction. Empty set and union are given by the module operations: $\theta = 0$ and $A \uplus B = A + B$. Singleton is the morphism $\eta : [\mathbf{X} \to R \odot \mathbf{X}]$, i.e. $\{\!|x|\!\} = \eta x$. For every $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$, the extension ext is given by the unique R-$\mathbf{X}$-linear map from $R \odot \mathbf{X}$ to $(\mathcal{P}\mathbf{Y}, f)$. Function ext is continuous by Theorem 13.4.4. We have to demonstrate that it satisfies the power axioms.

The primary axioms of extension are satisfied by definition of ext. Linearity of $ext\, f$ implies additivity, i.e. (P1) and (P2), and $ext\, f \circ \eta = f$ is (P3). The secondary axioms are consequences of the uniqueness of the extended map (cf. Prop. 14.3.2).

(S1) $ext\,(\lambda a.\, \theta) = \lambda A.\, \theta$

The function to the right is linear and maps singletons to θ. The function to the left behaves equally, whence they are equal.

(S2) $ext\,(\lambda x.\, f x \uplus g x) = \lambda A.\, ext\, f\, A \uplus ext\, g\, A$

Both functions are linear, and both map a singleton $\{\!|a|\!\}$ to $fa \uplus ga$. Note that commutativity of the addition in a module is required to prove the additivity of the function ρ to the right because $\rho(A \uplus B) = \overline{f}A + \overline{f}B + \overline{g}A + \overline{g}B$, whereas $\rho A \uplus \rho B = \overline{f}A + \overline{g}A + \overline{f}B + \overline{g}B$.

(S3) $ext\, \iota = id$

Again, both sides are linear and coincide on singletons since both map $\{\!|a|\!\}$ to $\{\!|a|\!\}$.

(S4) $ext\, g \circ ext\, f = ext\,(ext\, g \circ f)$

Once more, both sides are linear — the left hand side as composition of linear maps. They both map a singleton $\{\!|a|\!\}$ to $ext\, g\,(fa)$.

Next, we show that the primarily given external product of the R-module $\mathcal{P}\mathbf{X}$ coincides with the derived external product of the power construction. The latter is denoted by '$*$' for the moment.

$$\begin{aligned} r * A &= ext\,(\lambda\diamond.\, A)\, r = ext\,(\lambda\diamond.\, A)\,(r \cdot 1) \\ &= r \cdot ext\,(\lambda\diamond.\, A)\,(\eta\diamond) = r \cdot A \end{aligned}$$

At the line break, the linearity of extended maps is used.

The power construction $\mathcal{P}$ is reduced since all power domains $\mathcal{P}\mathbf{X}$ are reduced by Prop. 13.4.3.

To show initiality of $\mathcal{P}$, let $\mathcal{Q}$ be another power construction with characteristic semiring R. We have to demonstrate the existence of a unique linear power homomorphism $H : \mathcal{P} \dot{\to} \mathcal{Q}$.

For every domain $\mathbf{X}$, $(\mathcal{Q}\mathbf{X}, \iota_{\mathcal{Q}})$ is an R-$\mathbf{X}$-module. Since $(\mathcal{P}\mathbf{X}, \iota_{\mathcal{P}})$ is a free R-$\mathbf{X}$-module, there is a (unique) R-linear morphism $H : [\mathcal{P}\mathbf{X} \to \mathcal{Q}\mathbf{X}]$ with $H \circ \iota_{\mathcal{P}} = \iota_{\mathcal{Q}}$. By linearity, H is additive, i.e. $H\theta = \theta$ and $H(A \uplus B) = HA \uplus HB$ hold. Since $\mathcal{P}$ is reduced, these properties allow to apply Prop. 14.3.4, whence $H : \mathcal{P} \dot{\to} \mathcal{Q}$ is a linear power homomorphism. It is unique by Prop. 14.3.5 since $\mathcal{P}$ is reduced. □

Since the initial power construction is reduced, it enjoys all properties of reduced power constructions as enumerated in the previous section. In addition, we are able to prove some more properties:

Theorem 14.5.2 If R is structurally algebraic, then the initial power construction for R preserves ALG and CONT.

Proof: Preservation of ALG is due to Th. 13.6.3. Preservation of CONT follows from Prop. 7.5.6. □

Lemma 14.5.3
If there is a non-discrete R-module, then the initial construction for R is faithful.

Proof: The proof is analogous to that of Lemma 11.9.2. One only has to replace the non-discrete power domain $\mathcal{P}\mathbf{Y}$ by the non-discrete R-module. □

14.6 Existential restriction of power constructions

So far, we mainly considered sub-constructions of $\mathcal{P}$ with characteristic semiring $\mathcal{P}\mathbf{1}$. The least such construction is given by the core $\mathcal{P}^c$. In this section, we consider a different problem. Given a specific sub-semiring R' of $\mathcal{P}\mathbf{1}$, we derive sub-constructions of $\mathcal{P}$ with just this characteristic semiring. The principal method to do this is *existential restriction*.

Let $\mathcal{P}$ be an R-construction. According to section 11.3, existential quantification may be defined w.r.t. R and then has type $\mathcal{E} : [\mathcal{P}\mathbf{X} \to [[\mathbf{X} \to R] \to R]]$. The existential restriction of $\mathcal{P}\mathbf{X}$ now is defined as the set of all those formal sets where quantification may be restricted to result in a second order predicate in $[[\mathbf{X} \to R'] \to R']$.

Definition 14.6.1
Let R be a semiring with a sub-semiring R', and let $\mathcal{P}$ be an R-construction. Then we define for all ground domains $\mathbf{X}$ the *existential restriction* of $\mathcal{P}\mathbf{X}$ to R':

$$\mathcal{P}'\mathbf{X} = \{A \in \mathcal{P}\mathbf{X} \mid \forall p : [\mathbf{X} \to R'] : \mathcal{E}\, A\, p \in R'\}$$

In the following, we verify that $\mathcal{P}'$ is a power construction with characteristic semiring R'.

- $\mathcal{E}\,\theta\, p = 0 \in R'$ implies $\theta \in \mathcal{P}'\mathbf{X}$.
- If A and B are in $\mathcal{P}'\mathbf{X}$, then for all $p : [\mathbf{X} \to R']$, $\mathcal{E}\, A\, p$ and $\mathcal{E}\, B\, p$ are in R', whence $\mathcal{E}\,(A \uplus B)\, p = \mathcal{E}\, A\, p + \mathcal{E}\, B\, p$ is in R'.
- For x in $\mathbf{X}$ and $p : [\mathbf{X} \to R']$, $\mathcal{E}\{\!|x|\!\}\, p = p\, x$ is in R'. Hence, $\{\!|x|\!\}$ is in $\mathcal{P}'\mathbf{X}$ for all x in $\mathbf{X}$.
- Let $f : [\mathbf{X} \to \mathcal{P}'\mathbf{Y}]$ and $A \in \mathcal{P}'\mathbf{X}$. We have to show $ext\, f\, A$ in $\mathcal{P}'\mathbf{Y}$.

  For all $p : [\mathbf{Y} \to R']$, $\mathcal{E}\,(ext\, f\, A)\, p = \mathcal{E}\, A\, (\lambda a.\mathcal{E}(f a)\, p)$ holds by the results of section 10.5. $f a \in \mathcal{P}'\mathbf{Y}$ implies $\mathcal{E}(f a)\, p \in R'$. Thus, $(\lambda a.\, \mathcal{E}(f a)\, p) : [\mathbf{X} \to R']$, whence the value of the whole term is in R'.
- Finally, we have to verify that $\mathcal{P}'\mathbf{X}$ is a sub-domain of $\mathcal{P}\mathbf{X}$. Let $(A_i)_{i \in I}$ be a directed family of members of $\mathcal{P}'\mathbf{X}$ with limit A. Then for all $p : [\mathbf{X} \to R']$, $\mathcal{E}(\bigsqcup_{i \in I} A_i)\, p = \bigsqcup_{i \in I}(\mathcal{E}\, A_i\, p) \in R'$ by continuity of $\mathcal{E}$.

Thus, the power operations of $\mathcal{P}$ imply power operations for $\mathcal{P}'$ by restriction and co-restriction. The power axioms thus are directly inherited from $\mathcal{P}$. Note that we only used parts (1), (2), and (5) of the definition of sub-semirings so far.

Next, we show $\mathcal{P}'\mathbf{1} = R'$. For $p : [\mathbf{1} \to R]$ and $a \in R = \mathcal{P}\mathbf{1}$, we may simplify $\mathcal{E}\, a\, p = ext\,(\lambda\diamond.\, p\,\diamond)\, a = a \cdot p\,\diamond$. Hence, $\mathcal{P}'\mathbf{1} = \{a \in \mathcal{P}\mathbf{1} \mid \forall p : [\mathbf{1} \to R'] : \mathcal{E}\, a\, p \in R'\} = \{a \in R \mid \forall r \in R' : a \cdot r \in R'\}$. This set is a subset of R', since $a \in \mathcal{P}'\mathbf{1}$ and $1 \in R'$ implies $a = a \cdot 1 \in R'$. Conversely, if r' is in R', then for all r in R', $r' \cdot r$ is in R', whence r' is in $\mathcal{P}'\mathbf{1}$.

Thus, $\mathcal{P}'\mathbf{1} = R'$ is proven. Here, we needed the remaining parts (3) and (4) of the definition of sub-semirings.

If $\mathcal{Q}$ is an arbitrary sub-construction of $\mathcal{P}$ with $\mathcal{Q}\mathbf{1} = R'$, then $\mathcal{Q}\mathbf{X} \subseteq \mathcal{P}'\mathbf{X}$ holds for all ground domains $\mathbf{X}$ since existential quantification in $\mathcal{Q}$ maps $\mathcal{Q}\mathbf{1}$-predicates to $\mathcal{Q}\mathbf{1}$.

Summarizing, we obtain

Theorem 14.6.2 If $\mathcal{P}$ is an R-construction, and R' is a sub-semiring of R, then the existential restriction $\mathcal{P}'$ of $\mathcal{P}$ to semiring R' is the greatest sub-construction of $\mathcal{P}$ with semiring R'. The core of $\mathcal{P}'$ is the least sub-construction of $\mathcal{P}$ with semiring R'.

In the special case $R' = R$, the existential restriction of $\mathcal{P}$ is $\mathcal{P}$ itself. Since the existential restriction $\mathcal{P}'$ is a sub-construction of $\mathcal{P}$, it is commutative, symmetric, or faithful whenever $\mathcal{P}$ is so. It however need not be reduced even if $\mathcal{P}$ is; section 22.1 provides an example.

Let $H : \mathcal{P} \dot{\to} \mathcal{Q}$ be a linear power homomorphism between two R-constructions, and let R' be a sub-semiring of R. Does H cut down to a power homomorphism between the existential restrictions $\mathcal{P}'$ and $\mathcal{Q}'$ of $\mathcal{P}$ and $\mathcal{Q}$?

The answer is yes. We only need to show $H\,A \in \mathcal{Q}'\mathbf{X}$ for $A \in \mathcal{P}'\mathbf{X}$. Linear power homomorphisms act as identity on the characteristic semiring by Prop. 12.4.2. Hence, for all $p : [\mathbf{X} \to R']$, $\mathcal{E}(H\,A)\,p = ext\,(H \circ p)\,(H\,A) = H\,(ext\,p\,A) = \mathcal{E}\,A\,p \in R'$ holds. Thus, we obtain

Proposition 14.6.3 Let R be a semiring with sub-semiring R', and let ^{e} be the method of existential restriction to R'. Then every R-linear power homomorphism $H : \mathcal{P} \dot{\to} \mathcal{Q}$ between two R-constructions $\mathcal{P}$ and $\mathcal{Q}$ cuts down to an R'-linear power homomorphism $H^e : \mathcal{P}^e \dot{\to} \mathcal{Q}^e$.

Chapter 15

Final power constructions

In contrast to the initial power construction, the final one may be explicitly constructed. As indicated in section 10.5, existential quantification leads to a mapping $\mathcal{E}$ from $\mathcal{P}\mathbf{X}$ to $[[\mathbf{X} \to \mathcal{P}\mathbf{1}] \to \mathcal{P}\mathbf{1}]$ for every power construction $\mathcal{P}$. This suggests to define $\mathcal{P}\mathbf{X}$ as $[[\mathbf{X} \to R] \to R]$ if $R = \mathcal{P}\mathbf{1}$ is given. The equations in section 10.5 also indicate how to define the power operations.

One has to prove that these operations satisfy the axioms of chapter 9, and that the derived semiring $\mathcal{P}\mathbf{1}$ is isomorphic to the original semiring R. For proving the axioms, the outer, second order mappings have to be additive, and for proving the isomorphism between $\mathcal{P}\mathbf{1}$ and R, they even have to be right linear. Thus, the actual definition is $\mathcal{P}\mathbf{X} = [[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$.

The main theorem about the final power construction for semiring R and its power operations is presented in section 15.1. The proof of the main theorem is spread over the subsequent 4 sections. In section 15.6, the derived operations of the final power construction are computed. Properties of the final construction such as preservation of domain classes are studied in section 15.7. Linear functions on final power domains are not generally uniquely determined by their values on singletons. In section 15.8, we present a necessary and sufficient criterion for this. The core of the final construction is briefly looked at in section 15.9.

15.1 The main theorem

Let R be a given semiring, and let $\mathbf{X}$ and $\mathbf{Y}$ be two right R-modules. Remember a mapping $F : [\mathbf{X} \to \mathbf{Y}]$ is right linear iff $F(x + x') = Fx + Fx'$ and $F(x \cdot r) = Fx \cdot r$ for all $x, x' \in \mathbf{X}$ and $r \in R$. The set $\{F : [\mathbf{X} \to \mathbf{Y}] \mid F \text{ is right linear } \}$ is denoted by $[\mathbf{X} \stackrel{rlin}{\to} \mathbf{Y}]$. Ordered as subset of $[\mathbf{X} \to \mathbf{Y}]$, it becomes a domain because the lub of a directed set of linear functions is linear again by continuity of application, sum, and external product.

Every semiring R becomes a right R-module in a canonical way. For given domain $\mathbf{X}$, the function space $[\mathbf{X} \to R]$ also becomes a right R-module by defining $f \cdot r = \lambda x.\,(fx) \cdot r$. Thus, the notation $[[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$ makes sense and denotes a domain.

Theorem 15.1.1 The *final power construction* belonging to a given semiring R is defined by $(\mathcal{P}, R, \varphi)$ where $\mathcal{P}\mathbf{X} = \mathcal{P}_f^R\mathbf{X} = [[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$. Its operations are defined by

- $\theta = \lambda g.\, 0$
- $A \uplus B = \lambda g.\, Ag + Bg$
- $\{\!|x|\!\} = \lambda g.\, gx \quad$ for $x \in \mathbf{X}$.
- $ext\, f\, A = \lambda g.\, A\,(\lambda a.\, fag) \quad$ for $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ and $A \in \mathcal{P}\mathbf{X}$.
- The isomorphism $\varphi : [R \to \mathcal{P}\mathbf{1}]$ is given by $\varphi\,(r) = \lambda g.\, r \cdot g\diamond$. Its inverse is $\psi\,(A) = A(\lambda\diamond.\, 1)$.

To understand the definition of *ext*, note that a ranges over $\mathbf{X}$. Then a in $\mathbf{X}$ and $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ imply $fa \in \mathcal{P}\mathbf{Y} = [[\mathbf{Y} \to R] \stackrel{rlin}{\to} R]$. g ranges over $[\mathbf{Y} \to R]$, whence $fag \in R$ and $\lambda a.\, fag : [\mathbf{X} \to R]$. Thus, $A \in \mathcal{P}\mathbf{X} = [[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$ implies $A\,(\lambda \ldots) \in R$.

The proof of the theorem proceeds in four steps: First, it is shown that the power operations defined above always create right linear maps when applied to such maps. Second, the validity of the power axioms is shown by λ-conversions. Third, an isomorphism between $\mathcal{P}\mathbf{1}$ and R is established. Fourth, the power construction $\mathcal{P}_f^R$ is demonstrated to be final. These steps are done in the next four sections.

15.2 Proof step 1: Right linearity

In this section, we show that the power operations defined above always preserve right linearity.

- $\theta = \lambda g.\, 0$
  Additive: $\theta\,(g + g') = 0 = 0 + 0 = \theta\, g + \theta\, g'$
  Linear: $\theta\,(g \cdot r) = 0 = 0 \cdot r = (\theta\, g) \cdot r$
- $A \uplus B = \lambda g.\, Ag + Bg$

  $$\begin{aligned}\text{Additive}: \quad (A \uplus B)(g + g') &= A\,(g + g') + B\,(g + g') = Ag + Ag' + Bg + Bg' \\ &= Ag + Bg + Ag' + Bg' = (A \uplus B)\,g + (A \uplus B)\,g'\end{aligned}$$

  Note that for the equality at the line break, commutativity of '+' is needed, which is ensured by the definition of semirings.

  $$\begin{aligned}\text{Linear}: \quad (A \uplus B)(g \cdot r) &= A\,(g \cdot r) + B\,(g \cdot r) = (Ag) \cdot r + (Bg) \cdot r \\ &= (Ag + Bg) \cdot r = (A \uplus B)\,g \cdot r\end{aligned}$$

- $\{\!|x|\!\} = \lambda g.\, g\, x$ for $x \in \mathbf{X}$.
  Additive: $\{\!|x|\!\}\,(g + g') = (g + g')\,x = g\,x + g'\,x = \{\!|x|\!\}\,g + \{\!|x|\!\}\,g'$
  Linear: $\{\!|x|\!\}\,(g \cdot r) = (g \cdot r)\,x = (gx) \cdot r = (\{\!|x|\!\}\,g) \cdot r$
- $ext\, f\, A = \lambda g.\, A\,(\lambda a.\, fag) \quad$ for $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ and $A \in \mathcal{P}\mathbf{X}$.
  Here, the linearity of fa and A is used.

  $$\begin{aligned}\text{Linear}: \quad (ext\, f\, A)\,(g \cdot r) &= A\,(\lambda a.\, f\, a\,(g \cdot r)) \\ &= A\,(\lambda a.\, (fag \cdot r)) = A\,((\lambda a.\, fag) \cdot r) \\ &= (A\,(\lambda a.\, fag)) \cdot r = ((ext\, f\, A)\,g) \cdot r\end{aligned}$$

  Additivity is shown analogously.

15.3 Proof step 2: The power axioms

In this section, we prove the validity of the power axioms for the new construction.

By the definition $A \uplus B = \lambda g.\, Ag + Bg$, the operation '$\uplus$' trivially is commutative, associative, and has neutral element $\theta = \lambda g.\, 0$. The axioms of extension are less easy to prove.

Def.: $ext\, f\, A = \lambda p.\, A\, (\lambda a.\, fap)$

(P1) $ext\, f\, \theta = \lambda p.\, \theta\, (\lambda a.\, fap) = \lambda p.\, 0 = \theta$

(P2)
$$\begin{aligned} ext\, f\, (A \uplus B) &= \lambda p.\, (A \uplus B)\, (\lambda a.\, fap) \\ &= \lambda p.\, A\, (\lambda a.\, fap) + B\, (\lambda a.\, fap) \\ &= ext\, f\, A \uplus ext\, f\, B \end{aligned}$$

(P3)
$$\begin{aligned} ext\, f\, \{\!|x|\!\} &= \lambda p.\, \{\!|x|\!\}\, (\lambda a.\, fap) \\ &= \lambda p.\, (\lambda a.\, fap)\, x \\ &= \lambda p.\, fxp \;=\; fx \end{aligned}$$

(S1)
$$\begin{aligned} ext\, (\lambda x.\, \theta)\, A &= \lambda p.\, A\, (\lambda a.\, (\lambda x.\, \theta)\, a\, p) \\ &= \lambda p.\, A\, (\lambda a.\, \theta\, p) \\ &= \lambda p.\, A\, (\lambda a.\, 0) \\ &= \lambda p.\, 0 \;=\; \theta \end{aligned}$$

At the last line break, the additivity of A is used.

(S2)
$$\begin{aligned} ext\, (f \uplus g)\, A &= \lambda p.\, A\, (\lambda a.\, (f \uplus g)\, a\, p) \\ &= \lambda p.\, A\, (\lambda a.\, (fa \uplus ga)\, p) \\ &= \lambda p.\, A\, (\lambda a.\, fap + gap) \qquad \text{using additivity of } A \text{ here} \\ &= \lambda p.\, A\, (\lambda a.\, fap) + A\, (\lambda a.\, gap) \\ &= ext\, f\, A \uplus ext\, g\, A \end{aligned}$$

(S3)
$$\begin{aligned} ext\, \iota\, A &= \lambda p.\, A\, (\lambda a.\, \iota ap) \;=\; \lambda p.\, A\, (\lambda a.\, \{\!|a|\!\}\, p) \\ &= \lambda p.\, A\, (\lambda a.\, pa) \;=\; \lambda p.\, Ap \;=\; A \end{aligned}$$

(S4) The claim is $ext\, g \circ ext\, f = ext\, (ext\, g \circ f)$, or $ext\, g\, (ext\, f\, A) \;=\; ext\, (\lambda x.\, ext\, g\, (fx))\, A$

$$\begin{aligned} ext\, g\, (ext\, f\, A) &= \lambda p.\, (ext\, f\, A)\, (\lambda b.\, gbp) \\ &= \lambda p.\, (\lambda q.\, A\, (\lambda a.\, faq))\, (\lambda b.\, gbp) \\ &= \lambda p.\, A\, (\lambda a.\, f\, a\, (\lambda b.\, gbp)) \\ ext\, (\lambda x.\, ext\, g\, (fx))\, A &= \lambda p.\, A\, (\lambda a.\, (\lambda x.\, ext\, g\, (fx))\, a\, p) \\ &= \lambda p.\, A\, (\lambda a.\, (ext\, g\, (fa))\, p) \\ &= \lambda p.\, A\, (\lambda a.\, (\lambda q.\, (fa)\, (\lambda b.\, gbq))\, p) \\ &= \lambda p.\, A\, (\lambda a.\, f\, a\, (\lambda b.\, gbp)) \end{aligned}$$

15.4 Proof step 3: The characteristic semiring

In this section, we show the power domain $\mathcal{P}\mathbf{1}$ and the original semiring R to be isomorphic. To this end, we first consider how the semiring operations in $\mathcal{P}\mathbf{1}$ are defined.

- $\mathcal{P}\mathbf{1} \;=\; [[\mathbf{1} \to R] \stackrel{rlin}{\to} R]$
- $0 \;=\; \theta \;=\; \lambda p.\, 0$
- $A + B \;=\; A \uplus B \;=\; \lambda p.\, Ap + Bp$
- $1 \;=\; \{\!|\diamond|\!\} \;=\; \lambda p.\, p\,\diamond$
- $$\begin{aligned} A \cdot B \;=\; ext\,(\lambda\diamond.\, B)\,A \;&=\; \lambda p.\, A\,(\lambda a.\, (\lambda\diamond.\, B)\,a\,p) \\ &=\; \lambda p.\, A\,(\lambda a.\, B\,p) \\ &=\; \lambda p.\, A\,(\lambda\diamond.\, B\,p) \end{aligned}$$

  For the last equality, note that a ranges over $\mathbf{1}$.

There is one obvious choice for a mapping $\psi : [\mathcal{P}\mathbf{1} \to R]$, namely $\psi A = A\,(\lambda\diamond.\, 1)$. This mapping is a semiring homomorphism:

- $\psi\,(0) \;=\; (\lambda p.\, 0)\,(\lambda\diamond.\, 1) \;=\; 0$
- $\psi\,(A + B) \;=\; (\lambda p.\, Ap + Bp)\,(\lambda\diamond.\, 1) \;=\; \psi A + \psi B$
- $\psi\,(1) \;=\; (\lambda p.\, p\,\diamond)\,(\lambda\diamond.\, 1) \;=\; (\lambda\diamond.\, 1)\,\diamond \;=\; 1$
- $$\begin{aligned} \psi\,(A \cdot B) \;&=\; (\lambda p.\, A\,(\lambda\diamond.\, Bp))\,(\lambda\diamond.\, 1) \\ &=\; A\,(\lambda\diamond.\, B\,(\lambda\diamond.\, 1)) \\ &=\; A\,(\lambda\diamond.\, \psi B) \;=\; A\,(\lambda\diamond.\, 1 \cdot \psi B) \qquad \text{use right linearity of } A \text{ now} \\ &=\; A\,(\lambda\diamond.\, 1) \cdot \psi B \;=\; \psi A \cdot \psi B \end{aligned}$$

As announced in the introduction of this chapter, right linearity of the second order functions in $\mathcal{P}\mathbf{X}$ is needed here. With left linearity, the result would be $\psi\,(A \cdot B) = \psi B \cdot \psi A$ instead.

The mapping ψ is shown to be an isomorphism by specifying its inverse. Let $\varphi : [R \to \mathcal{P}\mathbf{1}]$ be defined by $\varphi r = \lambda p.\, r \cdot p\,\diamond$. The second order mapping φr is right linear in p because

$$\begin{aligned} &\varphi r\,(p + p') \;=\; r \cdot (p + p')\,\diamond \;=\; r \cdot (p\,\diamond + p'\,\diamond) \;=\; r \cdot p\,\diamond + r \cdot p'\,\diamond \;=\; \varphi r\,(p) + \varphi r\,(p') \\ &\varphi r\,(p \cdot a) \;=\; r \cdot (p \cdot a)\,\diamond \;=\; r \cdot (p\,\diamond \cdot a) \;=\; (r \cdot p\,\diamond) \cdot a \;=\; \varphi r\,(p) \cdot a \end{aligned}$$

φ is the inverse of ψ since

$$\begin{aligned} \psi\,(\varphi r) \;&=\; (\lambda p.\, r \cdot p\,\diamond)\,(\lambda\diamond.\, 1) \;=\; r \cdot (\lambda\diamond.\, 1)\,\diamond \;=\; r \cdot 1 \;=\; r \\ \varphi\,(\psi A) \;&=\; \lambda p.\, \psi A \cdot p\,\diamond \\ &=\; \lambda p.\, A\,(\lambda\diamond.\, 1) \cdot p\diamond \qquad \text{and by right linearity of } A \\ &=\; \lambda p.\, A\,(\lambda\diamond.\, 1 \cdot p\,\diamond) \\ &=\; \lambda p.\, A\,(\lambda\diamond.\, p\,\diamond) \;=\; \lambda p.\, Ap \;=\; A \end{aligned}$$

15.5 Proof step 4: Finality

Let $(\mathcal{Q}, R, \rho)$ be an arbitrary power construction with semiring R and let $(\mathcal{P}, R, \varphi)$ be the existential construction for R. We have to construct a linear power homomorphism $H : \mathcal{Q} \dot{\to} \mathcal{P}$ and then show it is unique. H is given by existential quantification $\mathcal{E} : [\mathcal{Q}\mathbf{X} \to [[\mathbf{X} \to R] \stackrel{rlin}{\to} R]]$ as defined in section 11.3.

Existential quantification in $\mathcal{Q}$ would map functions in $[\mathbf{X} \to \mathcal{Q}\mathbf{1}]$ into elements of $\mathcal{Q}\mathbf{1}$. It can be used to define H if semiring elements can be translated into elements of $\mathcal{Q}\mathbf{1}$ and vice versa by means of ρ and ρ^{-1}. Hence we define for A in $\mathcal{Q}\mathbf{X}$

$$H\,A = \lambda p.\, \rho^{-1}\,(ext_{\mathcal{Q}}\,(\rho \circ p)\,A)$$

Here, p ranges over $[\mathbf{X} \to R]$, whence $\rho \circ p : [\mathbf{X} \to \mathcal{Q}\mathbf{1}]$. Thus, $(ext_{\mathcal{Q}}\,(\rho \circ p)\,A)$ is in $\mathcal{Q}\mathbf{1}$, whence its value by ρ^{-1} is in R. Hence, $H : [\mathcal{Q}\mathbf{X} \to [[\mathbf{X} \to R] \to R]]$.

Adopting this definition of H, we have to show that $H\,A$ is right linear, that H is a linear power homomorphism, and finally that H is unique. We tackle these statements one by one.

$H\,A\,(p_1 + p_2)$ equals $\rho^{-1}\,(ext\,(\rho \circ (p_1 + p_2))\,A)$. Using additivity of ρ^{-1} and ρ, and axiom (S2), the operator '+' may be moved to the outermost level.

$$\begin{array}{rcll} H\,A\,(p \cdot r) & = & \rho^{-1}\,(ext\,(\rho \circ (\lambda x.\, p\,x \cdot r))\,A) & \\ & = & \rho^{-1}\,(ext\,((\rho \circ p) \cdot \rho r)\,A) & \text{use Prop. 10.10.2, (6) now} \\ & = & \rho^{-1}\,((ext\,(\rho \circ p)\,A) \cdot \rho r) & \\ & = & \rho^{-1}\,(ext\,(\rho \circ p)\,A) \cdot \rho^{-1}\,(\rho r) \;=\; (H\,A\,p) \cdot r & \end{array}$$

Now the right linearity of $H\,A$ has been proved. Next, we show that H is a power homomorphism:

- $H\,\theta_{\mathcal{Q}} = \lambda p.\, \rho^{-1}\,(ext\,(\rho \circ p)\,\theta_{\mathcal{Q}}) \overset{(P1)}{=} \lambda p.\, \rho^{-1}\,(0) = \lambda p.\, 0 = \theta_{\mathcal{P}}$
- $\begin{array}{rcl} H\,(A \uplus B) & = & \lambda p.\, \rho^{-1}\,(ext\,(\rho \circ p)\,(A \uplus B)) \\ & = & \lambda p.\, \rho^{-1}\,(ext\,(\rho \circ p)\,A) \uplus \rho^{-1}\,(ext\,(\rho \circ p)\,B) \;=\; H\,A \uplus H\,B \end{array}$

  using axiom (P2) and additivity of ρ^{-1} at the equality sign in the middle.
- $H\,\{\!|x|\!\}_{\mathcal{Q}} = \lambda p.\, \rho^{-1}\,(ext\,(\rho \circ p)\,\{\!|x|\!\}_{\mathcal{Q}}) \overset{(P3)}{=} \lambda p.\, \rho^{-1}\,(\rho\,(p\,x)) = \lambda p.\, p\,x = \{\!|x|\!\}_{\mathcal{P}}$
- $\begin{array}{rcl} H\,(ext\,f\,A) & = & \lambda p.\, \rho^{-1}\,(ext\,(\rho \circ p)\,(ext\,f\,A)) \\ & \overset{(S4)}{=} & \lambda p.\, \rho^{-1}\,(ext\,(\lambda x.\, ext\,(\rho \circ p)\,(f\,x))\,A) \\ & = & \lambda p.\, \rho^{-1}\,(ext\,(\lambda x.\, \rho\,(\rho^{-1}\,(ext\,(\rho \circ p)\,(f\,x))))\,A) \\ & = & \lambda p.\, \rho^{-1}\,(ext\,(\lambda x.\, \rho\,(H\,(f\,x)\,p))\,A) \\ & = & \lambda p.\, H\,A\,(\lambda x.\, H\,(f\,x)\,p) \\ & = & \lambda p.\, H\,A\,(\lambda x.\, (H \circ f)\,x\,p) \\ & = & ext_{\mathcal{P}}\,(H \circ f)\,(H\,A) \end{array}$

Now we know H is a power homomorphism. To show its linearity, we have to prove $\psi\,(H_{\mathbf{1}}\,(\rho r)) = r$ for all $r \in R$ by Prop. 12.4.2 where $\psi = \lambda S.\, S\,(\lambda \diamond.\, 1)$ is the isomorphism from $\mathcal{P}\mathbf{1}$ to R.

$$\begin{array}{rcll} \psi\,(H_{\mathbf{1}}\,(\rho r)) & = & (\lambda p.\, \rho^{-1}\,(ext_{\mathcal{Q}}\,(\rho \circ p)\,(\rho r)))\,(\lambda \diamond.\, 1) & \\ & = & \rho^{-1}\,(ext_{\mathcal{Q}}\,(\rho \circ (\lambda \diamond.\, 1))\,(\rho r)) & \\ & = & \rho^{-1}\,(ext_{\mathcal{Q}}\,(\lambda \diamond.\, \{\!|\diamond|\!\}_{\mathcal{Q}})\,(\rho r)) & \text{since } \rho\,(1) = \{\!|\diamond|\!\}_{\mathcal{Q}} \\ & \overset{(S3)}{=} & \rho^{-1}\,(\rho r) \;=\; r & \end{array}$$

The last property to be shown is that H is the only linear power homomorphism from $\mathcal{Q}$ to $\mathcal{P}$. Let G be another linear power homomorphism. Then $\psi \circ G_{\mathbf{1}} \circ \rho = id_R$ holds.

$$\begin{array}{lcll}
HA & = & \lambda p.\, \rho^{-1}\,(ext_{\mathcal{Q}}\,(\rho \circ p)\,A) & \\
& = & \lambda p.\, \psi\,(G_{\mathbf{1}}\,(ext_{\mathcal{Q}}\,(\rho \circ p)\,A)) & \text{since } \rho^{-1} = \psi \circ G_{\mathbf{1}} \\
& = & \lambda p.\, \psi\,(ext_{\mathcal{P}}\,(G_{\mathbf{1}} \circ \rho \circ p)\,(GA)) & \text{because } G \text{ is a power homomorphism} \\
& = & \lambda p.\, (ext_{\mathcal{P}}\,(\psi^{-1} \circ p)\,(GA))\,(\lambda \diamond.\, 1) & \text{since } G_{\mathbf{1}} \circ \rho = \psi^{-1}, \text{ and } \psi S = S\,(\lambda \diamond.\, 1) \\
& = & \lambda p.\, (GA)\,(\lambda x.\, (\psi^{-1} \circ p)\,x\,(\lambda \diamond.\, 1)) & \text{by definition of } ext_{\mathcal{P}} \\
& = & \lambda p.\, (GA)\,(\lambda x.\, \psi\,(\psi^{-1}\,(p\,x))) & \text{since } S(\lambda \diamond.\, 1) = \psi S \\
& = & \lambda p.\, GA\,(\lambda x.\, p\,x) \;=\; \lambda p.\, GA\,p \;=\; GA &
\end{array}$$

Now, the theorem is completely proved.

15.6 Derived operations

The definition of the existential construction provides realizations for the principal power operations in terms of higher order functions. The derived operations may also be expressed in functional form.

- $UA = ext\ id\ A = \lambda p.\, A\,(\lambda a.\, id\,a\,p) = \lambda p.\, A\,(\lambda a.\, a\,p)$
- $$\begin{array}{lcl}
  map\,f\,A & = & ext\,(\iota \circ f)\,A \\
  & = & \lambda p.\, A\,(\lambda a.\, (\iota \circ f)\,a\,p) \\
  & = & \lambda p.\, A\,(\lambda a.\, \{\!|fa|\!\}\,p) \\
  & = & \lambda p.\, A\,(\lambda a.\, p\,(fa)) \\
  & = & \lambda p.\, A\,(p \circ f)
  \end{array}$$
- Existential quantification $\mathcal{E} : \mathcal{P}\mathbf{X} \to [[\mathbf{X} \to R] \to R]$ in terms of the semiring R instead of $\mathcal{P}\mathbf{1}$ is simply given by $\mathcal{E}\,A\,p = A\,p$. The reason is that $\mathcal{E}$ is a linear power homomorphism from $\mathcal{P}$ to $\mathcal{P}$ as we saw in the previous section. Identity also is a linear power homomorphism. Because of the uniqueness result of the previous section, they coincide.
- $ne\ A = \mathcal{E}\,A\,(\lambda x.\, 1) = A\,(\lambda x.\, 1)$
- As indicated in section 11.3, the external product is defined for elements of R by means of φ.

  $$\begin{array}{lcl}
  r \cdot A & = & ext\,(\lambda \diamond.\, A)\,(\varphi r) \\
  & = & \lambda p.\, (\varphi r)\,(\lambda a.\, (\lambda \diamond.\, A)\,a\,p) \\
  & = & \lambda p.\, (\lambda q.\, r \cdot q\,\diamond)\,(\lambda a.\, Ap) \\
  & = & \lambda p.\, r \cdot (\lambda a.\, Ap)\,\diamond \\
  & = & \lambda p.\, r \cdot Ap
  \end{array}$$
- $r \cdot \{\!|x|\!\} \;=\; \lambda p.\, r \cdot \{\!|x|\!\}\,p \;=\; \lambda p.\, r \cdot p\,x$

- Similar to the external product, we define *filter* for mappings $f : [\mathbf{X} \to R]$ instead of $f : [\mathbf{X} \to \mathcal{P}\mathbf{1}]$.

$$\begin{aligned} \mathit{filter}\, f\, A &= \mathit{ext}\,(\lambda x.\, fx \cdot \{\!|x|\!\})\, A \\ &= \lambda p.\, A\,(\lambda a.\,(\lambda x.\, fx \cdot \{\!|x|\!\})\, a\, p) \\ &= \lambda p.\, A\,(\lambda a.\,(fa \cdot \{\!|a|\!\})\, p) \\ &= \lambda p.\, A\,(\lambda a.\,(\lambda q.\, fa \cdot q\, a)\, p) \\ &= \lambda p.\, A\,(\lambda a.\, fa \cdot p\, a) \end{aligned}$$

- $$\begin{aligned} A \cdot r &= \mathit{filter}\,(\lambda x.\, r)\, A \\ &= \lambda p.\, A\,(\lambda a.\,(\lambda x.\, r)\, a \cdot p\, a) \\ &= \lambda p.\, A\,(\lambda a.\, r \cdot p\, a) \end{aligned}$$

Strangely, both $r \cdot A$ and $A \cdot r$ denote an expression where r is a left factor. The difference is that with $\mathcal{P}\mathbf{X} = [[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$, the left product $r \cdot A$ operates at the outer occurrence of R, whereas the right product $A \cdot r$ operates at the inner occurrence.

Proposition 15.6.1
If the semiring R is commutative, then the construction $\mathcal{P}_f^R$ is commutative.

Proof:

$$\begin{aligned} A \cdot r &= \lambda p.\, A\,(\lambda a.\, r \cdot pa) \\ \text{by commutativity of } R: \quad &= \lambda p.\, A\,(\lambda a.\, pa \cdot r) \\ \text{by right linearity of } A: \quad &= \lambda p.\, A\,(\lambda a.\, pa) \cdot r \\ \text{by commutativity of } R: \quad &= \lambda p.\, r \cdot Ap = r \cdot A \end{aligned}$$ □

Concerning symmetry, one has to show $A \stackrel{\rightarrow}{\times} B = A \stackrel{\leftarrow}{\times} B$ for all A in $\mathcal{P}\mathbf{X}$ and B in $\mathcal{P}\mathbf{Y}$ because of Cor. 10.3.2.

$$\begin{aligned} A \stackrel{\rightarrow}{\times} B &= \mathit{ext}\,(\lambda a.\, \mathit{ext}\,(\lambda b.\, \{\!|(a, b)|\!\})\, B)\, A \\ &= \lambda p.\, A\,(\lambda a.\, \mathit{ext}\,(\lambda b.\, \{\!|(a, b)|\!\})\, B\, p) \\ &= \lambda p.\, A\,(\lambda a.\, B\,(\lambda b.\, \{\!|(a, b)|\!\}\, p)) \\ &= \lambda p.\, A\,(\lambda a.\, B\,(\lambda b.\, p\,(a, b))) \end{aligned}$$

and analogously

$$A \stackrel{\leftarrow}{\times} B = \lambda p.\, B\,(\lambda b.\, A\,(\lambda a.\, p\,(a, b)))$$

The usual equational reasoning does not help in proving $A \stackrel{\rightarrow}{\times} B = A \stackrel{\leftarrow}{\times} B$.

Problem 10 Is $\mathcal{P}_f^R$ symmetric whenever R is commutative?

15.7 Further properties

This section is a collection of some simple properties of the final construction.

Proposition 15.7.1 If R is discrete, then $\mathcal{P}_f^R\mathbf{X}$ is discrete for all domains $\mathbf{X}$.

Proof: $\mathcal{P}_f^R\mathbf{X}$ is $[[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$ ordered pointwise, i.e. $A \leq B$ iff $Ap \leq Bp$ in R for all $p : [\mathbf{X} \to R]$. □

Proposition 15.7.2 The final construction $\mathcal{P}_f^R$ is faithful iff R is non-discrete.

Proof: If R is non-discrete, then $\mathcal{P}_f^R$ is faithful by Cor. 11.9.3. If R is discrete, then $\mathcal{P}_f^R\mathbf{X}$ is discrete even for non-discrete domains $\mathbf{X}$. Hence, embeddings from non-discrete domains $\mathbf{X}$ into $\mathcal{P}_f^R\mathbf{X}$ are impossible. □

Proposition 15.7.3 If R is finite, then $\mathcal{P}_f^R$ preserves FIN, F-ALG, and F-CONT.

Proof: If R and $\mathbf{X}$ are finite, then so is $[[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$. According to Th. 7.4.4, $\mathcal{P}_f^R$ then maps finitely algebraic (continuous) domains into finitely algebraic (continuous) domains. □

Problem 11 If R and $\mathbf{X}$ are finitely algebraic (R not necessarily being finite), is $\mathcal{P}_f^R\mathbf{X}$ finitely algebraic?

Problem 12 If R and $\mathbf{X}$ are algebraic, is $\mathcal{P}_f^R\mathbf{X}$ algebraic?

Proposition 15.7.4 If R and $\mathbf{X}$ have least elements $\bot_R$ and $\bot_\mathbf{X}$, then $\mathcal{P}_f^R\mathbf{X}$ has a least element, namely $\bot_R \cdot \{\!|\bot_\mathbf{X}|\!\}$.

Proof: We have to show $Ap \geq (\bot_R \cdot \{\!|\bot_\mathbf{X}|\!\})p$ for all $A : [[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$ and all $p : [\mathbf{X} \to R]$.

$$\begin{aligned} Ap &= A(\lambda x.\, p\,x) \geq A(\lambda x.\, p(\bot_\mathbf{X})) \\ &= A(\lambda x.\, 1 \cdot p(\bot_\mathbf{X})) \stackrel{\text{rlin}}{=} A(\lambda x.\, 1) \cdot p(\bot_\mathbf{X}) \\ &\geq \bot_R \cdot p(\bot_\mathbf{X}) = \bot_R \cdot \{\!|\bot_\mathbf{X}|\!\}p = (\bot_R \cdot \{\!|\bot_\mathbf{X}|\!\})p \end{aligned}$$ □

Because of its definition in terms of existential quantification, one might believe that the existential restriction of a final construction for R is a final construction for R'. However this is not true as we shall see in section 23.4. There are two reasons for this. First, two distinct second order predicates in $[[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$ may produce equal results for predicates in $[\mathbf{X} \to R']$. They are then still different in the restriction of the final construction for R, but equal in $[[\mathbf{X} \to R'] \stackrel{rlin}{\to} R']$. Second, there may be additional members in $[[\mathbf{X} \to R'] \stackrel{rlin}{\to} R']$ that cannot be obtained by restricting predicates in $[[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$.

Despite of this general result, we also meet examples for semirings R and R' where the existential restriction of the final construction for R is final for R' — see Th. 23.3.1.

15.8 Unique extensions in final power constructions

Given a power construction $\mathcal{P}$ and two domains $\mathbf{X}$ and $\mathbf{Y}$, one is interested whether mappings $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ have a unique linear extension $\overline{f} : [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{Y}]$. This means, whenever F_1 and F_2 are linear morphisms from $\mathcal{P}\mathbf{X}$ to $\mathcal{P}\mathbf{Y}$, does $F_1 \circ \iota = F_2 \circ \iota$ imply $F_1 = F_2$?

This useful property is not generally true, not even for final constructions. An example for this will be given in section 23.5. However, there is a nice criterion telling that the target domain $\mathbf{Y}$ does not matter; one may substitute $\mathbf{1}$ for it.

Proposition 15.8.1 Let R be an arbitrary semiring domain. For a fixed domain $\mathbf{X}$, the following statements are equivalent:

(1) For every domain $\mathbf{Y}$, $F_1 \circ \iota = F_2 \circ \iota$ implies $F_1 = F_2$ for all linear morphisms $F_1, F_2 : [\mathcal{P}_f^R\mathbf{X} \to \mathcal{P}_f^R\mathbf{Y}]$.

(2) $G_1 \circ \iota = G_2 \circ \iota$ implies $G_1 = G_2$ for all linear morphisms $G_1, G_2 : [\mathcal{P}_f^R\mathbf{X} \to \mathcal{P}_f^R\mathbf{1}]$.

In (2), $\mathcal{P}_f^R\mathbf{1}$ may be replaced by R using the isomorphisms φ and ψ.

Proof: Abbreviating $\mathcal{P}_f^R$ by $\mathcal{P}$, let F_1 and F_2 be two linear maps from $\mathcal{P}\mathbf{X}$ to $\mathcal{P}\mathbf{Y}$ with $F_1 \circ \iota = F_2 \circ \iota$. We have to show $F_1 = F_2$, i.e. $F_1 A\, p = F_2 A\, p$ for all A in $\mathcal{P}\mathbf{X}$ and $p : [\mathbf{Y} \to R]$. For every mapping $p : [\mathbf{Y} \to R]$, the composite $\varphi \circ p$ maps from $\mathbf{Y}$ to $\mathcal{P}\mathbf{1}$, whence its extension maps from $\mathcal{P}\mathbf{Y}$ to $\mathcal{P}\mathbf{1}$. Let $G_i = ext\,(\varphi \circ p) \circ F_i$. Then G_1 and G_2 are linear mappings from $\mathcal{P}\mathbf{X}$ to $\mathcal{P}\mathbf{1}$ with $G_1 \circ \iota = G_2 \circ \iota$. By (2), $G_1 = G_2$ holds, whence $G_1 A\, q = G_2 A\, q$ for all A in $\mathcal{P}\mathbf{X}$ and $q : [\mathbf{1} \to R]$. We use this equation for the special case $q = \lambda\diamond.\, 1$.

$$\begin{aligned} G_i A\, q &= ext\,(\varphi \circ p)\,(F_i A)\, q \\ &= (F_i A)\,(\lambda x.\, (\varphi \circ p)\, x\, q) \qquad \text{by the definition of } ext \\ &= F_i A\,(\lambda x.\, (\varphi\,(p\, x))\,(\lambda\diamond.\, 1)) \\ &= F_i A\,(\lambda x.\, \psi\,(\varphi\,(p\, x))) = F_i A p \end{aligned}$$

Hence, $G_1 A\, q = G_2 A\, q$ implies $F_1 A\, p = F_2 A\, p$. □

15.9 The core of the final construction

Since the final construction need not have unique extensions, it moreover need not be reduced. In this section, we want to consider its core. Being reduced, this core has properties superior to those of the final construction itself. It is symmetric whenever the characteristic semiring is commutative, and it always has unique extensions. Algebraically, it may be characterized as follows:

Proposition 15.9.1
The core of the final construction is final among the reduced constructions.

Proof: Let $\mathcal{P}_f$ be the final construction for semiring R and $\mathcal{P}^c$ its core, and let $\mathcal{Q}$ be a reduced construction with semiring R. Since $\mathcal{P}_f$ is final, there is a linear power homomorphism $H : \mathcal{Q} \dot{\to} \mathcal{P}_f$. By Prop. 14.2.1, it cuts down to a linear power homomorphism $H^c : \mathcal{Q} = \mathcal{Q}^c \dot{\to} \mathcal{P}^c$. This linear homomorphism is unique by Prop. 14.3.5. □

In contrast to this, the initial construction is always reduced by Prop. 13.4.3. Thus, it is not only initial among all constructions, but also initial among the reduced ones.

In the final construction, all power operations and hence all derived operations are representable in terms of λ-expressions involving the semiring operations as constants. Hence, the operations of the final construction may be implemented in a functional language that only has to provide the semiring operations as primitives (usually, these are not sequential). If this implementation is done as an abstract data type that only allows the power operations and nothing else, then the core of the final construction is obtained. This is because the core cannot be left by the power operations including recursion.

Chapter 16

Products of power constructions

The previous chapters showed the existence of three distinguished power constructions for every semiring: the initial construction, the final construction, and the core of the final construction.[1] Now we are going to present a method that allows to produce a power construction $\prod \mathcal{P}_i$ with semiring $\prod R_i$ from given R_i-constructions $\mathcal{P}_i$.

The investigation of the product construction is prepared by investigating products of simpler but related algebraic structures such as modules and semirings in section 16.1. The product construction is then introduced in section 16.2. It is shown that it forms a categorical product in the category of power domain constructions and power homomorphisms. In section 16.3, we prove that the product of final constructions for semirings R_i is final for $\prod_{i \in I} R_i$.

In the remainder of the chapter, we restrict ourselves to binary products. Section 16.4 provides some theory for modules: an $R_1 \times R_2$-module is always isomorphic to a product of an R_1-module and an R_2-module, or more concisely: an $R_1 \times R_2$-module may always be factorized. This result is used to prove that core formation, reducedness, and initiality of power constructions commute over binary products (section 16.5). In section 16.6, we state and prove a necessary and sufficient criterion for the ability to factorize $R_1 \times R_2$-constructions. This criterion holds for large classes of power constructions, e.g. for reduced ones. The final section 16.7 then studies the factorization of linear power homomorphisms.

16.1 Products of algebraic structures

In this section, we consider the products of various algebraic structures we are concerned with: monoids, modules, and semirings. Products of power constructions are then considered in the next section.

Let $(M_i)_{i \in I}$ be a family of monoids, and let $M = \prod_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i \ \forall i \in I\}$ be its Cartesian product. M may be given a monoid structure by defining $0 = (0_i)_{i \in I}$ and $(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I}$. This operation is continuous by Prop. 3.3.5. The algebraic

[1] For particular semirings, two or three of these constructions may well coincide.

laws of associativity and neutrality are obviously satisfied. M is commutative / idempotent iff all M_i are so.

For each $k \in I$, there is an out-going map $\pi_k : M \to M_k$ given by projection onto dimension k, i.e. $\pi_k((m_i)_{i\in I}) = m_k$. All these mappings are continuous and additive. For each $k \in I$, there is also an in-going map $\eta_k : M_k \to M$ defined by $(\eta_k m)_i = \begin{cases} m & \text{if } i = k \\ 0 & \text{otherwise} \end{cases}$ These mappings are also continuous and additive.

Turning to semirings, let R be the Cartesian product of the family $(R_i)_{i\in I}$. By the definitions $1 = (1_i)_{i\in I}$ and $(a_i)_{i\in I} \cdot (b_i)_{i\in I} = (a_i \cdot b_i)_{i\in I}$, R becomes a semiring domain. The projections π_k are semiring homomorphisms whereas the injections η_k are not. This is because $\eta_k(1_k) \neq 1$; the remaining requirements hold: $\eta_k(0_k) = 0$, $\eta_k(a + b) = \eta_k(a) + \eta_k(b)$, and $\eta_k(a \cdot b) = \eta_k(a) \cdot \eta_k(b)$.

Finally, let $(R_i)_{i\in I}$ be a family of semirings and $(M_i)_{i\in I}$ a family of commutative monoids such that for all i in I, M_i is an R_i-module. Let R be the product semiring and M the product monoid. M becomes an R-module by defining $(r_i)_{i\in I} \cdot (m_i)_{i\in I} = (r_i \cdot m_i)_{i\in I}$. The 'small' modules M_k also become R-modules by the definition $r \cdot m = \pi_k(r) \cdot m$ for $r \in R$ and $m \in M_k$. With this definition, both the projection $\pi_k : M \to M_k$ and the injection $\eta_k : M_k \to M$ become R-linear. For the injection, this is proved by

$$\eta_k(r \cdot m) = \begin{pmatrix} r_k \cdot m \\ 0_i \end{pmatrix} = \begin{pmatrix} r_k \cdot m \\ r_i \cdot 0_i \end{pmatrix} = r \cdot \begin{pmatrix} m \\ 0_i \end{pmatrix} = r \cdot \eta_k m$$

where the upper line is the component in dimension k whereas the lower line stands for all other components $i \neq k$.

All these products are also products in a categorical sense. For morphisms $f_i : [\mathbf{X} \to M_i]$, there is a unique $f : [\mathbf{X} \to M]$ such that $\pi_i \circ f = f_i$ for all i in I. This function f is additive / linear / a semiring homomorphism iff the functions f_i are so for all i in I.

16.2 The product power construction

After the preliminaries about semirings and modules, we now turn to the power constructions themselves. Let $(\mathcal{P}_i)_{i\in I}$ be a family of power constructions. Then define $\mathcal{P} = \prod_{i\in I} \mathcal{P}_i$ by $\mathcal{P}\mathbf{X} = \prod_{i\in I} \mathcal{P}_i\mathbf{X}$ for all ground domains $\mathbf{X}$. The power operations in $\mathcal{P}$ are defined 'pointwise':

- $\theta = (\theta_i)_{i\in I}$
- $(A_i)_{i\in I} \uplus (B_i)_{i\in I} = (A_i \uplus B_i)_{i\in I}$
- $\{\!|x|\!\} = (\{\!|x|\!\}_i)_{i\in I}$ for all x in $\mathbf{X}$
- For $f : [\mathbf{X} \to \mathcal{P}\mathbf{Y}]$ let $f_i = \pi_i \circ f$. Then $ext\, f\, (A_i)_{i\in I} = (ext_i\, f_i\, A_i)_{i\in I}$ where ext_i denotes the extension functional of $\mathcal{P}_i$.

The verification of the power axioms for $\mathcal{P}$ is straightforward. For instance, (S4) is shown as follows:

$$\begin{aligned} ext\, f\, (ext\, g\, A) &= (ext_i\, f_i\, \pi_i\, (ext\, g\, A))_{i\in I} \\ &= (ext_i\, f_i\, (ext_i\, g_i\, A_i))_{i\in I} \\ &= (ext_i\, (\lambda x.\, ext_i\, f_i\, (g_i x))A_i)_{i\in I} \\ &= (ext_i\, (\lambda x.\, \pi_i(ext\, f\, (gx)))A_i)_{i\in I} \\ &= ext\, (\lambda x.\, ext\, f\, (gx))\, A \end{aligned}$$

The definition of extension directly implies $\pi_i \circ ext\, f = ext_i\, (\pi_i \circ f) \circ \pi_i$. Together with simple conclusions from the other definitions, one obtains a power homomorphism $\pi_k : \mathcal{P} \dot{\to} \mathcal{P}_k$ for every k in I. In contrast to this, the injections η_k do not create a power homomorphism since $\eta_k\{\!|x|\!\}_k$ has component θ in all dimensions except k, whereas $\{\!|x|\!\}$ has component $\{\!|x|\!\}_i$ in every dimension i.

Let $H_i : \mathcal{Q} \dot{\to} \mathcal{P}_i$ be a family of power homomorphisms. Then define H by $H(A_i)_{i\in I} = (H_i A_i)_{i\in I}$. Then $H_i = \pi_i \circ H$ holds. H is a power homomorphism:

- $H\,\theta_{\mathcal{Q}} = (H_i \theta_{\mathcal{Q}})_{i\in I} = (\theta_i)_{i\in I} = \theta_{\mathcal{P}}$
- $H(A \uplus B) = (H_i(A_i \uplus B_i))_{i\in I} = (H_i A \uplus H_i B)_{i\in I}$ etc.
- $H\,\{\!|x|\!\}_{\mathcal{Q}} = (H_i\{\!|x|\!\}_{\mathcal{Q}})_{i\in I} = (\{\!|x|\!\}_i)_{i\in I} = \{\!|x|\!\}_{\mathcal{P}}$
- $H(ext_{\mathcal{Q}}\, f\, A) = (H_i(ext_{\mathcal{Q}}\, f\, A))_{i\in I} = (ext_i(H_i \circ f)(H_i A))_{i\in I} = ext_{\mathcal{P}}(H \circ f)(HA)$ since $H_i \circ f = \pi_i \circ H \circ f$.

H is unique with $\pi_i \circ H = H_i$. If H' is another one, then $\pi_i(H'A) = H_i A = \pi_i(HA)$ holds for all i in I and A in $\mathcal{Q}\mathbf{X}$, whence $H' = H$.

Now, we determine the characteristic semiring of $\mathcal{P}$. Let $R_i = \mathcal{P}_i\mathbf{1}$ be the characteristic semirings of the factors. Then the characteristic semiring of $\mathcal{P}$ has carrier $R = \prod_{i\in I} R_i$. The operations in R are defined by

- $0 = \theta = (\theta_i)_{i\in I} = (0_i)_{i\in I}$
- $a + b = a \uplus b = (a_i \uplus b_i)_{i\in I} = (a_i + b_i)_{i\in I}$
- $1 = \{\!|\diamond|\!\} = (\{\!|\diamond|\!\}_i)_{i\in I} = (1_i)_{i\in I}$
- $a \cdot b = ext\, (\lambda\diamond.\, b)\, a = (ext_i\, (\lambda\diamond.\, b_i)\, a_i)_{i\in I} = (a_i \cdot b_i)_{i\in I}$

Hence, the characteristic semiring of $\mathcal{P}$ is the product of the semirings of $\mathcal{P}_i$ in the sense of the previous section. Similarly, one shows that the R-module $\mathcal{P}\mathbf{X}$ is the product of the R_i-modules $\mathcal{P}_i\mathbf{X}$.

Summarizing, we obtain the following theorem:

Theorem 16.2.1 For every family $(\mathcal{P}_i)_{i\in I}$ of power constructions with semirings R_i, there is a product construction $\mathcal{P} = \prod_{i\in I} \mathcal{P}_i$ with semiring $R = \prod_{i\in I} R_i$. For every k in I, there is a power homomorphism $\pi_k : \mathcal{P} \dot{\to} \mathcal{P}_k$. For every family of power homomorphisms $H_i : \mathcal{Q} \to \mathcal{P}_i$, there is a unique $H : \mathcal{Q} \dot{\to} \mathcal{P}$ with $\pi_k \circ H = H_k$ for all k in I.

Since all power operations and hence all derived operations are defined componentwise, the following facts become obvious:

Proposition 16.2.2

(1) The product $\prod_{i\in I}\mathcal{P}_i$ is commutative iff all factors are commutative.

(2) The product is symmetric iff all factors are.

(3) If at least one factor is faithful, then the whole product is faithful.

The remainder of the chapter is concerned with more advanced questions, e.g. is the product of reduced / initial / final constructions reduced / initial / final again? Is the core of the product the product of the cores? Is it possible to factorize any power construction with a product semiring? The first question to attack is that of finality.

16.3 Product and finality

This section is concerned with final power constructions. The goal is to prove that the product of final constructions $\mathcal{P}_i$ for semirings R_i is final for the product semiring $R = \prod_{i\in I} R_i$. For this, let $\mathcal{P} = \prod_{i\in I}\mathcal{P}_i$ and let $\mathcal{Q}$ be the final construction for R, i.e. $\mathcal{Q}\mathbf{X} = [[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$. Since $\mathcal{Q}$ is final, there is a (unique) linear power homomorphism $\mathcal{E} : \mathcal{P} \dot{\to} \mathcal{Q}$ defined by $\mathcal{E}A = \lambda p.\, ext\, p\, A$ for A in $\mathcal{P}\mathbf{X}$. Hence, $\mathcal{E}A = \lambda p.\, (ext_i\, p_i\, A_i)_{i\in I} = \lambda p.\, (\mathcal{E}_i\, A_i\, p_i)_{i\in I}$ where $\mathcal{E}_i$ is the unique linear power homomorphism from $\mathcal{P}_i$ to itself, i.e. is the identity. Thus, $\mathcal{E}A = \lambda p.\, (A_i\, p_i)_{i\in I}$. We have to show that $\mathcal{E}$ is a power isomorphism. By Prop. 12.2.1, it suffices to show that $\mathcal{E}$ is a surjective embedding.

Assume $\mathcal{E}A \le \mathcal{E}B$ holds for $A, B \in \mathcal{P}\mathbf{X}$. For all $k \in I$ and all $q : [\mathbf{X} \to R_k]$, let $p = \eta_k \circ q : [\mathbf{X} \to R]$. $\mathcal{E}A \le \mathcal{E}B$ implies $(A_i\, p_i)_{i\in I} = \mathcal{E}Ap \le \mathcal{E}B\, p = (B_i\, p_i)_{i\in I}$. This in particular holds for dimension k. Thus, $A_k\, q \le B_k\, q$ holds for all k in I and $q : [\mathbf{X} \to R_k]$, whence $A_k \le B_k$ for all k, whence $A \le B$.

For surjectivity, let $P : [[\mathbf{X} \to R] \stackrel{rlin}{\to} R]$. Then let $P_i : [[\mathbf{X} \to R_i] \stackrel{rlin}{\to} R_i]$ be defined by $P_i = \lambda q.\, \pi_i\, (P\, (\eta_i \circ q))$. This mapping obviously is additive. Right linearity is shown by the following derivation where $r \in R_i$:

$$\pi_i\,(P\,(\eta_i \circ (q \cdot r))) = \pi_i\,(P\,((\eta_i \circ q) \cdot (\eta_i\, r))) = \pi_i\,(P\,(\eta_i \circ q)) \cdot \pi_i\,(\eta_i\, r) = \pi_i\,(P\,(\eta_i \circ q)) \cdot r$$

Thus, $A = (P_i)_{i\in I}$ is a member of $\mathcal{P}\mathbf{X}$. We claim $\mathcal{E}A = P$.
$\mathcal{E}A\, p = (P_i\, p_i)_{i\in I} = (\pi_i\,(P\,(\eta_i \circ p_i)))_{i\in I}$ holds where $p_i = \pi_i \circ p$. Note that $\eta_i(\pi_i r) = r \cdot \eta_i\, 1_i$ holds for all r in R. Thus,

$$\begin{aligned}\pi_i\,(P\,(\eta_i \circ \pi_i \circ p)) \;&=\; \pi_i\,(P\,(p \cdot \eta_i\, 1_i)) \;=\; \pi_i\,(Pp \cdot \eta_i\, 1_i)\\ &=\; \pi_i\,(Pp) \cdot \pi_i\,(\eta_i\, 1_i) \;=\; \pi_i\,(Pp) \cdot 1_i \;=\; \pi_i\,(Pp)\end{aligned}$$

whence $(\pi_i\,(P\,(\eta_i \circ p_i)))_{i\in I} = Pp$.

Up to now, we proved the following theorem:

Theorem 16.3.1 If $\mathcal{P}_i$ are final power constructions for the semirings R_i for all $i \in I$, then the product $\prod_{i\in I}\mathcal{P}_i$ is a final construction for the product $\prod_{i\in I} R_i$.

16.4 Factorization of modules

Before attacking the remaining questions, we have to consider the product of module domains a bit closer. Thereby, we concentrate on finite products; most of the following results do not hold or are open for infinite ones. Since binary products may be iterated to obtain any desired finite product, we moreover restrict ourselves to products of just two objects.

Let R_1 and R_2 be two semirings with product $R = R_1 \times R_2$. The projections are given in this special case by $\pi_i(r_1, r_2) = r_i$, and the injections by $\eta_1 r = (r, 0)$ and $\eta_2 r = (0, r)$. If it seems appropriate, we also write $(r_i)_{i \in I}$ instead of (r_1, r_2) where I is understood as $\{1, 2\}$.

Given an R_1-module M_1 and an R_2-module M_2, the product $M_1 \times M_2$ is an R-module. We now investigate the opposite direction: given an R-module M, is it possible to find R_i-modules M_i such that M is isomorphic to $M_1 \times M_2$?

The product $R = R_1 \times R_2$ contains two particularly interesting elements: $e_1 = (1, 0)$ and $e_2 = (0, 1)$. They commute with every other semiring element and enjoy the properties $e_1 \cdot e_1 = e_1$, $e_2 \cdot e_2 = e_2$, $e_1 \cdot e_2 = 0$, and $e_1 + e_2 = 1$.

Proposition 16.4.1
Let M be an R-module. For m in M, the following statements are equivalent:

(1) There is an x in M such that $e_1 \cdot x = m$.

(2) $e_1 \cdot m = m$

(3) $e_2 \cdot m = 0$

Proof:

$(1) \Rightarrow (3)$: $e_2 \cdot m = e_2 \cdot e_1 \cdot x = 0 \cdot x = 0$

$(3) \Rightarrow (2)$: $m = 1 \cdot m = (e_1 + e_2) \cdot m = e_1 \cdot m + 0$

$(2) \Rightarrow (1)$: Let $x = m$. □

After these preliminaries, we define

- $M_1 = \{e_1 \cdot x \mid x \in M\} = \{m \in M \mid e_1 \cdot m = m\} = \{m \in M \mid e_2 \cdot m = 0\}$

and analogously M_2.

Proposition 16.4.2 If M_1 is equipped with the order and the operations of M, then it is an R-module domain. By the definition $r * m = \eta_1 r \cdot m$ for $r \in R_1$ and $m \in M_1$, it also becomes an R_1-module.

Proof:
For the first part, we have to show that M_1 is closed w.r.t. 0, '+', '$\cdot$', and directed limits.

- $e_2 \cdot 0 = 0$, whence $0 \in M_1$
- If $a, b \in M_1$, then $e_2 \cdot (a + b) = e_2 \cdot a + e_2 \cdot b = 0 + 0 = 0$
- If $r \in R$ and $m \in M_1$, then $e_2 \cdot (r \cdot m) = r \cdot (e_2 \cdot m) = r \cdot 0 = 0$
- If D is a directed set in M_1, then $e_2 \cdot (\bigsqcup D) = \bigsqcup_{d \in D} (e_2 \cdot d) = \bigsqcup_{d \in D} 0 = 0$

The necessary algebraic properties are inherited from M.

To demonstrate that M_1 is an R_1-module, we only have to verify the module axioms. Since η_1 is additive and multiplicative, the only problem is with the axiom $1_1 * m = m$. It holds because $1_1 * m = \eta_1 1_1 \cdot m = e_1 \cdot m = m$ holds for all $m \in M_1$. □

Since both M_i are R_i-modules, their product $M_1 \times M_2$ becomes an R-module with multiplication defined as in section 16.1. This multiplication looks like

$$\begin{aligned}
(r_1, r_2) * (m_1, m_2) &= (r_1 * m_1, r_2 * m_2) \\
&= (\eta_1 r_1 \cdot m_1, \eta_2 r_2 \cdot m_2) \\
&= ((r_1, 0) \cdot m_1, (0, r_2) \cdot m_2) \qquad \text{and by } (0, r_2) = (0, r_2) \cdot e_2 \\
&= ((r_1, 0) \cdot m_1 + (0, r_2) \cdot m_1, (r_1, 0) \cdot m_2 + (0, r_2) \cdot m_2) \\
&= ((r_1, r_2) \cdot m_1, (r_1, r_2) \cdot m_2)
\end{aligned}$$

whence $r * (m_1, m_2) = (r \cdot m_1, r \cdot m_2)$.

Next, we claim that M and $M_1 \times M_2$ are isomorphic R-modules. Let $\alpha : [M \to M_1 \times M_2]$ be defined by $\alpha x = (e_1 \cdot x, e_2 \cdot x)$. By definition of M_i, the result really is in $M_1 \times M_2$, and the mapping obviously is continuous. Additivity is simple. For linearity note that

$$\alpha(r \cdot x) = (e_1 \cdot r \cdot x, e_2 \cdot r \cdot x) = (r \cdot e_1 \cdot x, r \cdot e_2 \cdot x) = r * (e_1 \cdot x, e_2 \cdot x) = r * \alpha x$$

using that both e_i commute over all semiring elements.

In the opposite direction, let $\beta : [M_1 \times M_2 \to M]$ be defined by $\beta(m_1, m_2) = m_1 + m_2$. It is continuous because of the continuity of '+'. For linearity, the commutativity of addition in modules is needed:

- $\beta(x_1 + y_1, x_2 + y_2) = x_1 + y_1 + x_2 + y_2 = x_1 + x_2 + y_1 + y_2 = \beta(x_1, x_2) + \beta(y_1, y_2)$
- $\beta(r * (m_1, m_2)) = \beta(r \cdot m_1, r \cdot m_2) = r \cdot m_1 + r \cdot m_2 = r \cdot \beta(m_1, m_2)$

α and β are inverses of each other:

- $\beta(\alpha x) = \beta(e_1 \cdot x, e_2 \cdot x) = e_1 \cdot x + e_2 \cdot x = (e_1 + e_2) \cdot x = 1 \cdot x = x$
- $\alpha(\beta(m_1, m_2)) = \alpha(m_1 + m_2) = (e_1 \cdot (m_1 + m_2), e_2 \cdot (m_1 + m_2))$
  $= (e_1 \cdot m_1 + e_1 \cdot m_2, e_2 \cdot m_1 + e_2 \cdot m_2) = (m_1, m_2)$

Summarizing all results, we proved the following theorem:

Theorem 16.4.3

Every $(R_1 \times R_2)$-module may be factorized into an R_1-module and an R_2-module.

Or more exactly: For every $(R_1 \times R_2)$-module M, there is an R_1-module M_1 and an R_2-module M_2 such that M and $M_1 \times M_2$ are isomorphic R-modules.

This factorization is unique up to isomorphism.

The last statement is proved below.

From modules, we now turn to the corresponding arrows, i.e. to linear morphisms. Let M_1 and M_1' be two R_1-modules, and let M_2 and M_2' be two R_2-modules. Then the products $M = M_1 \times M_2$ and $M' = M_1' \times M_2'$ are R-modules. A pair of R_i-linear mappings $f_i : [M_i \to M_i']$

may be combined to a R-linear $f : [M \to M']$ defined by $f\,(x,\,y) = (f_1\,x,\,f_2\,x)$. We denote f by $f_1 \times f_2$.

Conversely, let $f : [M \to M']$ be a linear morphism. Then $f\,(x,\,0) = f\,((1,\,0)\cdot(x,\,0)) = (1,\,0)\cdot f\,(x,\,0)$ holds, i.e. the M_2'-component of $f\,(x,\,0)$ is 0, i.e. there is a function f_1 such that $f\,(x,\,0) = (f_1 x,\,0)$. f_1 may explicitly built by composition: $f_1 = \pi_1 \circ f \circ \eta_1$. Hence, it is continuous. Additivity is also immediate. f_1 is R_1-linear because of

$$f_1\,(r_1 \cdot x) = \pi_1\,(f\,(r_1 \cdot x,\,0)) = \pi_1\,(f\,((r_1,\,0)\cdot(x,\,0))) = \pi_1\,((r_1,\,0)\cdot(f_1 x,\,0)) = r_1 \cdot f_1 x$$

Obviously, an R_2-linear function f_2 with $f\,(0,\,y) = (0,\,f_2 y)$ also exists.

Finally, $f_1 \times f_2$ is f because of

$$f\,(x,\,y) = f\,((x,\,0) + (0,\,y)) = f\,(x,\,0) + f\,(0,\,y) = (f_1 x,\,0) + (0,\,f_2 y) = (f_1 x,\,f_2 y)$$

It is not difficult to see that $f_1 \times f_2$ is an isomorphism iff f_1 and f_2 are. This proves the uniqueness in the theorem above: if $M_1 \times M_2$ is isomorphic to $M_1' \times M_2'$ by $f_1 \times f_2$, then M_i and M_i' are isomorphic by f_i.

Summarizing, we obtain:

Theorem 16.4.4 Let M_1 and M_1' be R_1-modules and M_2 and M_2' R_2-modules. Then for every pair of R_i-linear functions $f_i : [M_i \to M_i']$, there is an R-linear function $f_1 \times f_2 : [M_1 \times M_2 \to M_1' \times M_2']$ defined by $(f_1 \times f_2)(x,\,y) = (f_1 x,\,f_2 y)$. Conversely, for every R-linear $f : [M_1 \times M_2 \to M_1' \times M_2']$, there are R_i-linear functions $f_i : [M_i \to M_i']$ such that $f = f_1 \times f_2$.

16.5 Product, core, and initiality

This section is concerned with the relations between finite products, core formation, and initiality. The first result is

Theorem 16.5.1 The core of the product of two power constructions equals the product of their cores: $(\mathcal{P}_1 \times \mathcal{P}_2)^c = \mathcal{P}_1^c \times \mathcal{P}_2^c$

Proof: For every ground domain $\mathbf{X}$, $(\mathcal{P}_1^c\mathbf{X} \times \mathcal{P}_2^c\mathbf{X},\,\{\!|.|\!\})$ is an R-$\mathbf{X}$-submodule of $\mathcal{P}_1\mathbf{X} \times \mathcal{P}_2\mathbf{X} = (\mathcal{P}_1 \times \mathcal{P}_2)\mathbf{X}$. Since $C = (\mathcal{P}_1 \times \mathcal{P}_2)^c\mathbf{X}$ is the least such submodule, $C \subseteq \mathcal{P}_1^c\mathbf{X} \times \mathcal{P}_2^c\mathbf{X}$ immediately follows.

Now let $S_1 = \{A \subseteq \mathcal{P}_1\mathbf{X} \mid (A,\,\theta_2) \in C\}$. We show that S_1 is an R-$\mathbf{X}$-submodule of $(\mathcal{P}_1\mathbf{X},\,\{\!|.|\!\}_1)$.

(1) $\{\!|x|\!\}_1 \in S_1$, since $(\{\!|x|\!\}_1,\,\theta_2) = (1_1,\,0_2)\cdot(\{\!|x|\!\}_1,\,\{\!|x|\!\}_2) = e_1 \cdot \{\!|x|\!\} \in C$.

(2) $\theta_1 \in S_1$, since $(\theta_1,\,\theta_2) = \theta \in C$.

(3) If $A, B \in S_1$, then $(A \uplus B,\,\theta_2) = (A,\,\theta_2) \uplus (B,\,\theta_2) \in C$.

(4) If $r_1 \in R_1$ and $A \in S_1$, then $(r_1 \cdot A,\,\theta_2) = (r_1,\,0_2)\cdot(A,\,\theta_2) \in C$.

(5) If D is a directed set in S_1, then $(\bigsqcup D,\,\theta_2) = \bigsqcup_{d\in D}(d,\,\theta_2) \in C$.

Since $\mathcal{P}_1^c\mathbf{X}$ is the least such sub-module, $\mathcal{P}_1^c\mathbf{X} \subseteq S_1$ follows. Similarly, $\mathcal{P}_2^c\mathbf{X} \subseteq S_2$ holds for an analogous set S_2.

Finally, let (A_1, A_2) be in $\mathcal{P}_1^c\mathbf{X} \times \mathcal{P}_2^c\mathbf{X}$. Then, $(A_1, A_2) \in S_1 \times S_2$, whence both (A_1, θ_2) and (θ_1, A_2) are in C. This implies $(A_1, A_2) = (A_1, \theta_2) \uplus (\theta_1, A_2)$ in C. Thus, $\mathcal{P}_1^c\mathbf{X} \times \mathcal{P}_2^c\mathbf{X} \subseteq C$.□

From this theorem, we obtain the following corollary:

Theorem 16.5.2 The product $\mathcal{P}_1 \times \mathcal{P}_2$ is reduced iff both factors $\mathcal{P}_1$ and $\mathcal{P}_2$ are reduced.

Proof: If both $\mathcal{P}_i$ are reduced, then $(\mathcal{P}_1 \times \mathcal{P}_2)^c = \mathcal{P}_1^c \times \mathcal{P}_2^c = \mathcal{P}_1 \times \mathcal{P}_2$, whence the product is reduced.

Conversely, assume $\mathcal{P}_1 \times \mathcal{P}_2$ is reduced. For all $\mathbf{X}$, $\mathcal{P}_1^c\mathbf{X} \times \mathcal{P}_2\mathbf{X}$ is an R-$\mathbf{X}$-submodule of $\mathcal{P}_1\mathbf{X} \times \mathcal{P}_2\mathbf{X}$. Since the product is reduced, $\mathcal{P}_1^c\mathbf{X} \times \mathcal{P}_2\mathbf{X} = \mathcal{P}_1\mathbf{X} \times \mathcal{P}_2\mathbf{X}$ follows, whence $\mathcal{P}_1^c = \mathcal{P}_1$. □

This section is concluded by investigating initiality.

Theorem 16.5.3
If $\mathcal{P}_1$ is initial for R_1 and $\mathcal{P}_2$ initial for R_2, then $\mathcal{P}_1 \times \mathcal{P}_2$ is initial for $R_1 \times R_2$.

Proof: By the results of chapter 14.5, we have to show that $\mathcal{P}_1\mathbf{X} \times \mathcal{P}_2\mathbf{X}$ is a free R-$\mathbf{X}$-module where $R = R_1 \times R_2$. Let $\mathcal{P} = \mathcal{P}_1 \times \mathcal{P}_2$.

Let M be an R-module, and $f : [\mathbf{X} \to M]$ a morphism. By Th. 16.4.3, there are R_i-modules M_i such that M is isomorphic to $M_1 \times M_2$. (In the following, we do not explicitly write down these isomorphisms.) By projection, f splits into morphisms $f_i : [\mathbf{X} \to M_i]$. Since $\mathcal{P}_i\mathbf{X}$ is a free R_i-$\mathbf{X}$-module, there are R_i-linear mappings $F_i : [\mathcal{P}_i\mathbf{X} \to M_i]$ with $F_i \circ \iota_i = f_i$. These mappings may be combined to an R-linear map $F : [\mathcal{P}\mathbf{X} \to M]$. F is an extension of f because of $F\{\!|x|\!\} = (F_i\{\!|x|\!\}_i)_{i\in I} = (f_i x)_{i\in I} = fx$.

Initial constructions are reduced. By Th. 16.5.2, $\mathcal{P}$ is also reduced, whence F is unique by Prop. 14.3.2. □

16.6 Factorization of power constructions

In section 16.4, we saw that every $(R_1 \times R_2)$-module and every $(R_1 \times R_2)$-linear map uniquely factorize into R_i-modules resp. R_i-linear maps. We now investigate to what extent these results hold for power constructions and linear power homomorphisms.

Let $R = R_1 \times R_2$ be a product semiring and let $\mathcal{P}$ be a power construction for R. For every $\mathbf{X}$, $\mathcal{P}\mathbf{X}$ is an R-module. By Th. 16.4.3, it may uniquely be factorized into an R_1-module $\mathcal{P}_1\mathbf{X}$ and an R_2-module $\mathcal{P}_2\mathbf{X}$. These modules are given by $\mathcal{P}_i\mathbf{X} = \{e_i \cdot A \mid A \in \mathcal{P}\mathbf{X}\}$. Members of $\mathcal{P}_1\mathbf{X}$ are equivalently characterized by $e_1 \cdot A = A$ or $e_2 \cdot A = \theta$ by Prop. 16.4.1. $\mathcal{P}\mathbf{X}$ and $\mathcal{P}_1\mathbf{X} \times \mathcal{P}_2\mathbf{X}$ are isomorphic by means of $\alpha A = (e_1 \cdot A, e_2 \cdot A)$ and $\beta(A_1, A_2) = A_1 \uplus A_2$. The question now is whether $\mathcal{P}_i$ are power constructions and whether α and β are inverse power isomorphisms.

Let us check whether $\mathcal{P}_1$ is a power construction. For all $\mathbf{X}$, $\mathcal{P}_1\mathbf{X}$ is a domain equipped with θ and '$\uplus$'. We define $\{\!|x|\!\}_1 = e_1 \cdot \{\!|x|\!\}$. For $f : [\mathbf{X} \to \mathcal{P}_1\mathbf{Y}]$ and A in $\mathcal{P}_1\mathbf{X}$, we simply define $ext_1\, f\, A = ext\, f\, A$. The result is indeed in $\mathcal{P}_1\mathbf{Y}$, since

$$e_1 \cdot ext\, f\, A = ext\, f\, (e_1 \cdot A) = ext\, f\, A$$

Thus, $\mathcal{P}_1$ inherits all power operations of $\mathcal{P}$ except singleton that has a new definition. Hence, all power axioms that do not involve singleton are valid. The only critical axioms are (P3) and (S3).

- $ext\, f\, \{\!|x|\!\}_1 = ext\, f\, (e_1 \cdot \{\!|x|\!\}) = e_1 \cdot ext\, f\, \{\!|x|\!\} = e_1 \cdot fx = fx$
  since fx is in $\mathcal{P}_1\mathbf{X}$.
- $ext\, (\lambda x.\, \{\!|x|\!\}_1)\, A = ext\, (\lambda x.\, e_1 \cdot \{\!|x|\!\})\, A = A \cdot e_1$
  where the last equation is given by the definition of the external product from the right in section 10.10.

  Unfortunately, the factor appears on the wrong side such that one cannot simplify to the desired result A. Remember that $A = e_1 \cdot B$ holds for some $B \in \mathcal{P}\mathbf{X}$ since A is in $\mathcal{P}_1\mathbf{X}$. Thus, one would need the equation $e_1 \cdot B \cdot e_1 = e_1 \cdot B$ for all B in $\mathcal{P}\mathbf{X}$.

Nevertheless, we now check whether α implies a power homomorphism. If so, then α and β are inverse power isomorphisms by Prop. 12.2.1. We know α is linear, whence it respects θ and '$\uplus$'. Singleton and extension remain to be checked.

- $\alpha\{\!|x|\!\} = (e_1 \cdot \{\!|x|\!\}, e_2 \cdot \{\!|x|\!\}) = (\{\!|x|\!\}_1, \{\!|x|\!\}_2)$
  This is the desired outcome.
- $\alpha\, (ext\, f\, A) = (e_i \cdot ext\, f\, A)_{i \in I}$
  On the other hand,
  $ext_{\mathcal{P}_1 \times \mathcal{P}_2}\, (\alpha \circ f)\, (\alpha A) = (ext_i\, (e_i \cdot f)\, (e_i \cdot A))_{i \in I} = (e_i \cdot ext\, (e_i \cdot f)\, A)_{i \in I}$
  As with (S3), there is a problem here: the factor e_i at the function f appears on the wrong side. Left factors at the functional argument of ext cannot generally drawn out, only right factors. A slight generalization of the property needed to prove (S3) helps here, namely $e_i \cdot B = B \cdot e_i$ for all $B \in \mathcal{P}\mathbf{X}$. This equation implies $e_i \cdot B \cdot e_i = e_i \cdot e_i \cdot B = e_i \cdot B$, and also
  $(e_i \cdot ext\, (e_i \cdot f)\, A)_{i \in I} = (e_i \cdot ext\, (f \cdot e_i)\, A)_{i \in I} = (e_i \cdot ext\, f\, A \cdot e_i)_{i \in I} = (e_i \cdot ext\, f\, A)_{i \in I}$
  This is the desired result.

Before formulating the concluding theorem, we consider the additional conditions we need a bit closer. It seems as if we needed both $e_1 \cdot B = B \cdot e_1$ and $e_2 \cdot B = B \cdot e_2$. However, it suffices to explicitly demand only one of these because the other one then holds automatically:

For B in $\mathcal{P}\mathbf{X}$, $e_1 \cdot B = B \cdot e_1$ and $e_2 \cdot B = B \cdot e_2$ are equivalent.

Proof: $e_2 \cdot B = e_2 \cdot B \cdot 1 = e_2 \cdot B \cdot (e_1 + e_2) = e_2 \cdot e_1 \cdot B + e_2 \cdot B \cdot e_2 = e_2 \cdot B \cdot e_2 = B \cdot e_1 \cdot e_2 + e_2 \cdot B \cdot e_2 = (e_1 + e_2) \cdot B \cdot e_2 = B \cdot e_2$ □

Hence, only $e_1 \cdot B = B \cdot e_1$ has to hold to allow factorization. Conversely, if $\mathcal{P}$ may be factorized, then in $\mathcal{P}_1\mathbf{X} \times \mathcal{P}_2\mathbf{X}$, both left and right multiplication operate componentwise, whence

$$e_1 \cdot B = (1, 0) \cdot (B_1, B_2) = (B_1, \theta_2) = (B_1, B_2) \cdot (1, 0) = B \cdot e_1$$

A linear power homomorphism is also right linear, whence this equation carries over to $\mathcal{P}$.

Thus, we obtain the following

Theorem 16.6.1 Let $\mathcal{P}$ be a power domain construction for semiring $R_1 \times R_2$. There are power constructions $\mathcal{P}_1$ for R_1 and $\mathcal{P}_2$ for R_2 such that $\mathcal{P}$ is isomorphic to $\mathcal{P}_1 \times \mathcal{P}_2$ by a linear power isomorphism, if and only if $(1,0) \cdot B = B \cdot (1,0)$ holds for all B in all power domains $\mathcal{P}\mathbf{X}$.

Or in short terms: a power construction for $R_1 \times R_2$ can be factorized if and only if $(1,0)$ commutes over all its formal sets.

It might well be possible that all power constructions for $R_1 \times R_2$ satisfy the criterion and hence may be factorized. However we cannot prove this such that it is an open **problem**. At least, we are able to conclude some interesting corollaries:

Corollary 16.6.2 Every commutative power construction $\mathcal{P}$ for $R_1 \times R_2$ can be factorized. The resulting factors are commutative again. If $\mathcal{P}$ is even symmetric then the factors are symmetric too.

Proof: The first statement is immediate. The remaining ones hold by Prop. 16.2.2. □

Corollary 16.6.3
If $R = R_1 \times R_2$ is additive, then every power construction for R can be factorized.

Proof: By Prop. 11.12.2, every power construction for an additive semiring is commutative.□

Corollary 16.6.4 Every reduced power construction for $R_1 \times R_2$ can be factorized. The resulting factors are reduced again.

Proof: Consider the two functions $F_L, F_R : [\mathcal{P}\mathbf{X} \to \mathcal{P}\mathbf{X}]$ defined by $F_L A = e_1 \cdot A$ and $F_R A = A \cdot e_1$. Both functions obviously are additive. F_R is linear:

$F_R(r \cdot A) = (r \cdot A) \cdot e_1 = r \cdot (A \cdot e_1) = r \cdot F_R A$

F_L is linear since e_1 commutes over all semiring elements:

$F_L(r \cdot A) = e_1 \cdot r \cdot A = r \cdot e_1 \cdot A = r \cdot F_L A$

F_L and F_R coincide for singletons by Prop. 10.10.2 (9). Thus, they are equal by Prop. 14.3.2.

The factors are reduced by Prop. 16.5.2. □

16.7 Factorization of linear power homomorphisms

The goal of this section is to derive a theorem analogous to Th. 16.4.4. This theorem claimed that all linear functions between products of modules can be factorized into linear functions between the factors.

Let $\mathcal{P}_1$ and $\mathcal{P}_1'$ be power constructions with semiring R_1, and let $\mathcal{P}_2$ and $\mathcal{P}_2'$ be power constructions with semiring R_2. Then $\mathcal{P} = \mathcal{P}_1 \times \mathcal{P}_2$ and $\mathcal{P}' = \mathcal{P}_1' \times \mathcal{P}_2'$ are power constructions with semiring $R = R_1 \times R_2$.

Let $H_i : \mathcal{P}_i \dot{\to} \mathcal{P}'_i$ be two linear power homomorphisms. Then define $H = H_1 \times H_2 : \mathcal{P} \dot{\to} \mathcal{Q}$ by $H\,(A_1,\, A_2) = (H_1 A_1,\, H_2 A_2)$. Since the power operations are defined componentwise, H is easily proved to be a linear power homomorphism.

Conversely, if a linear power homomorphism $H : \mathcal{P} \dot{\to} \mathcal{P}'$ is given, it can be split into two families of R_i-linear mappings $H_i : \mathcal{P}_i \dot{\to} \mathcal{P}'_i$ such that $H = H_1 \times H_2$ by Th. 16.4.4. We have to show that both H_i are power homomorphisms.

- $H_1 \{\!|x|\!\}_1 = \pi_1\,(H\,(\{\!|x|\!\}_1,\, \theta_2)) = \pi_1\,(H\,((1,0) \cdot (\{\!|x|\!\}_1,\, \{\!|x|\!\}_2))) = \pi_1\,((1,0) \cdot H\,\{\!|x|\!\}) = \pi_1\,((1,0) \cdot \{\!|x|\!\}') = \{\!|x|\!\}'_1$
  Here, linearity of H is used.
- $H_1\,(ext_1\, f_1\, A_1)) = \pi_1\,(H\,(ext_1\, f_1\, A_1,\, \theta_2)) = \pi_1\,(H\,(ext_i\, f_i\, A_i)_{i \in I})$
  where $f_2 = \lambda x.\, \theta_2$ and $A_2 = \theta_2$. Applying the corresponding property of H, one obtains the desired result.

Summarizing, one gets

Theorem 16.7.1 Let $\mathcal{P}_1$ and $\mathcal{P}'_1$ be power constructions with semiring R_1 and $\mathcal{P}_2$ and $\mathcal{P}'_2$ power constructions with semiring R_2. Then for every pair of R_i-linear power homomorphisms $H_i : \mathcal{P}_i \dot{\to} \mathcal{P}'_i$, there is an R-linear power homomorphism $H_1 \times H_2 : \mathcal{P}_1 \times \mathcal{P}_2 \dot{\to} \mathcal{P}'_1 \times \mathcal{P}'_2$ defined by $(H_1 \times H_2)(A_1,\, A_2) = (H_1 A_1,\, H_2 A_2)$. Conversely, for every R-linear power homomorphism $H : \mathcal{P}_1 \times \mathcal{P}_2 \dot{\to} \mathcal{P}'_1 \times \mathcal{P}'_2$, there are R_i-linear power homomorphisms $H_i : \mathcal{P}_i \dot{\to} \mathcal{P}'_i$ such that $H = H_1 \times H_2$.