EINDHOVEN UNIVERSITY OF TECHNOLOGY
Department of Mathematics and Computing Science

Afstudeerverslag

Galois Connections Presented Calculationally.

by
C.J. Aarts

Supervisor: Roland Backhouse

July 7, 1992

Contents

Chapter 1

Introduction

Although computing science is a relatively new branch of science, the subject of this report is in fact an old one. The concept of a *Galois connection* was first investigated by E. Galois back in 1830. He discovered that, for a field K there was a connection between the subfields of a field extension on K which contain K and the collection of automorphisms on the field extension which leave K pointwise fixed. The properties of that connection remain valid in a much broader setting.

In 1940 G. Birkhoff [Bir67] found that any relation gave rise to a connection which he called a polarity. It was in fact an instance of a Galois connection. The actual generalisation of these connections was done by O. Ore [Ore44]. He coined the term *Galois connexion*. Nowadays Ore's peculiar spelling of *connexion* has been replaced by *connection*.

Now, what is a Galois connection? Let's present a first definition. A Galois connection involves two ordered sets $(\mathcal{A}, \leq_{\mathcal{A}})$ and $(\mathcal{B}, \leq_{\mathcal{B}})$, a mapping $F : \mathcal{A} \leftarrow \mathcal{B}$ and a mapping in the opposite direction $G : \mathcal{B} \leftarrow \mathcal{A}$. We will say (F, G) *is a Galois connection* iff for all $x \in \mathcal{B}$ and $y \in \mathcal{A}$ the following holds

$$F.x \ \leq_{\mathcal{A}} \ y \ \equiv \ x \ \leq_{\mathcal{B}} \ G.y \ .$$

This compact definition of a Galois connection was first introduced in [Sch53]. We refer to F as the *lower adjoint* and to G as the *upper adjoint*.

As might be anticipated from the names given to F and G, Galois connections are related to the categorical notion of an adjunction[1]. When considering a set with an order as a category, Galois connections and adjunctions coincide. So we can study Galois connections by studying adjunctions. Adjunctions have been extensively studied by several people, one of the most comprehensive accounts of adjunctions being [Mac71], so why bother to study them separately? There are several reasons why Galois connections are interesting in their own right.

The notion of an adjunction is more complex than the notion of a Galois connection. At best an adjunction involves two categories, two functors and two mappings between the

[1] All remarks referring to category theory can be skipped if you're not familiar with it.

hom-sets. Other definitions require two natural transformations instead of the mappings between hom-sets, or one natural transformation and a universality property. On top of that, there are properties of Galois connections which are not valid for adjunctions in general. This last observation prompted Herrlich and Hušek to introduce four levels of Galois connections, ranging from polarities to a restricted form of adjunctions [HH85].

Galois connections have very nice calculational properties. This is based on two things. Because of the equivalence in the definition of a Galois connection, one can use the side that is easier to manipulate. If one tries to prove some property for G, it might be advantageous to use the Galois connection to get rid of G, thereby introducing an F for which the calculation is easy.

Things get even better. It is known which conditions a mapping F has to satisfy in order to ensure existence of an adjoint. So one can write down the Galois connection and derive properties for the adjoint of F, or calculate with F by using the Galois connection without actually giving an explicit formula for the adjoint! One only uses its calculational properties, or rather its *specification*. This means one can give specifications of a mapping and know that there exists a mapping that satisfies that specification without having to construct such a mapping. This way of defining new operators is used in [BVvdW91]; e.g. the factors are defined that way.

Unfortunately not all mappings can be expressed in terms of a Galois connection. The functions that can be expressed that way are the mappings that define some sort of extremal value, i.e. the functions that give the least, or greatest, element such that a certain property holds. Nevertheless this class of mappings is sufficiently large to be interesting.

Apart from being not new, Galois connections appeared frequently in the literature. But in all articles about Galois connections, the calculational properties are not exploited. In general one recognises that something is an instance of a Galois connection, but then that observation is hardly ever used. In this report we will focus on the calculational use of Galois connections.

In the next section we will first describe the —mathematical— tools we need, specifically the proof format being used and the language in which we conduct the proofs, the predicate calculus. There is also a description of some elementary lattice theory. We also discuss some properties of relations in general and an axiomatisation of those properties in the form of the spec calculus.

The following section is dedicated to some examples of Galois connections. The examples give a first impression of how to calculate with Galois connections. They also give a first hint as to what properties are common to the Galois connections.

Subsequently we will give an overview of the properties of Galois connections. The properties will not be new but we try to establish them in a calculational way.

Next we will apply the general properties to an application. For that purpose we selected the domain operator in the spec calculus. By using a Galois connection as definition of that operator, we get a number of properties of that operator for free.

Chapter 2

Preliminaries

2.1 Notation

As usual we indicate function application by the lower dot "$.$". If a is an element of type A and F a mapping from A —called the *domain*— to some other type, we denote the unique image element of a by $F.a$. To indicate that F is a mapping to B —called the *range*— from A we write $F : B \leftarrow A$. The choice for the unconventional direction of the arrow is based on the way we denote function application and composition of two mappings. In case of function application, the argument of a function is placed on the right-hand side of the function. Writing the type information as we do, the domain of the function is placed on the right-hand side of the arrow. If G is a mapping to C from B we denote the composite of $G : C \leftarrow B$ and $F : B \leftarrow A$ by $G.F$, with $G.F : C \leftarrow A$. Note that the same symbol is used for function application as for composition of two functions. One can always deduce which operation is understood from typing considerations. As a consequence of this overloading we have no need for letting the lower dot be right associative. Here the lower dot is associative. The composition of functions can be given as an inference rule:

$$\frac{G : C \leftarrow B \qquad F : B \leftarrow A}{G.F : C \leftarrow A}$$

If we use the more conventional notation for the typing of a function, the inference rule is less easy to remember. The lower dot has the highest precedence of all binary operators.

2.2 Meta-language

The meta-language we use is the predicate calculus. We assume the reader is familiar with the predicate calculus, so we content ourselves with a short description. A more extensive one can be found in [DS90]. Just for the benefit of those who have read [DS90], we do not use the *everywhere* operator, denoted by the square brackets. We adopt the convention —unless stated otherwise— that the formulae we give are universally quantified over all free variables.

The predicate calculus, or the calculus of boolean structures, consist of two boolean scalars: true and false. The predicates can be seen as boolean-valued functions. In order to reason about the predicates, some operators are used.

The *equivalence* ($\equiv$) is used to denote boolean equality. It has the least binding power of all binary operators. The boolean scalar true is an identity for the equivalence, the boolean scalar false acts a a zero for the equivalence.

The *disjunction* ($\vee$) is used to model the boolean or, the *conjunction* ($\wedge$) models the and. Both these binary operators are symmetric, associative and idempotent. The scalar true is a zero for the disjunction and an identity for the conjunction. The scalar false acts as an identity for the disjunction and as a zero for the conjunction.

The remaining two binary operators are the *implication* ($\Rightarrow$) and the *follows-from* ($\Leftarrow$). They have equal binding power, higher than the equivalence but less than the disjunction and conjunction. The implication and the follows-from are formally indistinguishable, since $Y \Leftarrow X \;\equiv\; X \Rightarrow Y$. Nevertheless it is nice to have both of them available for constructing proofs. In the expression $Y \Leftarrow X$ or $X \Rightarrow Y$ we refer to X as the *antecedent* and to Y as the *consequent*. From the truth of $Y \Leftarrow X \;\equiv\; (X \vee Y \;\equiv\; X)$, the reader can establish various properties of the follows-from, and thus of the implication.

As a unary operator we have the *negation* ($\neg$). It is written as a prefix operator. We adopt the convention that unary operators have a higher binding power than any binary operator, including function application/composition. Thus the negation has the highest binding power. For the negation we have the Law of Excluded Middle, i.e. $X \vee \neg X$ for any predicate X. Of course we also have $\mathsf{false} \;\equiv\; \neg\mathsf{true}$ and $X \;\equiv\; \neg\neg X$ for any predicate X. When calculating with the negation, the Laws of de Morgan come in handy: $\neg X \vee \neg Y \;\equiv\; \neg(X \wedge Y)$ and $\neg X \wedge \neg Y \;\equiv\; \neg(X \vee Y)$.

The conjunction and disjunction can be generalised. They yield the *universal quantification*, respectively the *existential quantification*. We use $P{\cdot}x$ to indicate that the predicate P might depend on x. For predicates P and Q, that might depend on x, the universal quantification appears as $(\forall\, x : P{\cdot}x : Q{\cdot}x)$ and the existential quantification looks like $(\exists\, x : P{\cdot}x : Q{\cdot}x)$. In those formulae we refer to x as the dummy; it can be replaced by any other variable without changing the truth of the formulae if we replace its occurrences in $P{\cdot}x$ and $Q{\cdot}x$. We call $P{\cdot}x$ the range and $Q{\cdot}x$ the term. Perhaps redundantly, we mention that the predicates P and Q need not depend on x. The range true will be omitted. For the universal quantification we have, among others, the following rules:

- $(\forall\, x : P{\cdot}x : Q{\cdot}x) \;\equiv\; (\forall\, x :: \neg P{\cdot}x \;\vee\; Q{\cdot}x)$ called *trading*,
- $(\forall\, x :: (\forall\, y :: P \cdot x \cdot y)) \;\equiv\; (\forall\, y :: (\forall\, x :: P \cdot x \cdot y))$ called *interchanging quantifications*,
- $X \vee (\forall\, x :: P{\cdot}x) \;\equiv\; (\forall\, x :: X \vee P{\cdot}x)$ called *disjunction over universal quantification*,
- $(\forall\, x :: P{\cdot}x) \wedge (\forall\, x :: Q{\cdot}x) \;\equiv\; (\forall\, x :: P{\cdot}x \wedge Q{\cdot}x)$ called *universal quantification over conjunction* ,

- $(\forall\, x :: \mathsf{true}) \;\equiv\; \mathsf{true}$ called *term true*,
- $(\forall\, x : \mathsf{false} : P{\cdot}x) \;\equiv\; \mathsf{true}$ called *empty range*,
- $(\forall\, x : x = y : P{\cdot}x) \;\equiv\; P{\cdot}y$ called *one-point rule*,
- $(\exists\, x : P{\cdot}x : Q{\cdot}x) \;\equiv\; \neg(\forall\, x : P{\cdot}x : \neg Q{\cdot}x)$ called *de Morgan's Law*.

The reader can, by the use of de Morgan's Law, reformulate the above given rules for the universal quantification in terms of the existential quantification.

2.3 Proofstyle

The proofs in this report are presented in the style introduced by W.H.J. Feijen in [DF88]. It gives a clear overview of a proof and leaves sufficient room for the hints. In general it looks like:

$$
\begin{array}{ll}
 & P \\
= & \qquad \{ \text{ hint 1 } \} \\
 & Q \\
= & \qquad \{ \text{ hint 2 } \} \\
 & R
\end{array}
$$

The expressions P, Q and R can contain one or more free variables. From the above proof we can deduce that $P = Q$ —for all instantiations of free variables— on account of hint 1, and that $Q = R$ on account of hint 2. This proves, because of the transitivity of the equality, $P = R$.

Instead of the *equality* $(=)$, any transitive operator can be used. The *equivalence* $(\equiv)$, *implies* $(\Rightarrow)$ and *follows-from* $(\Leftarrow)$ will be used when calculating with predicates. The *equality* $(=)$, *at most* $(\leq)$ and *at least* $(\geq)$ will be used when calculating with other ordered structures. Occasionally $\sqsubseteq$, respectively $\sqsupseteq$, will be used instead of $\leq$, respectively $\geq$. They will appear when calculating in a *spec algebra*.

2.4 Relations

A Galois connection is concerned with functions. Nevertheless it is worthwhile to look at relations as they can be viewed as a generalisation of functions. The relations provides a means to express things in a more abstract way. In most cases it leads to a formulation of a property with less dummies, or even with no dummies at all.

A relation is any subset of the *cartesian product* of two sets. Given two sets $\mathcal{A}$ and $\mathcal{B}$, their cartesian product is the set $\mathcal{A} \times \mathcal{B} \;\doteq\; \{(y,x) \mid y \in \mathcal{A} \wedge x \in \mathcal{B}\}$. Instead of $(y,x) \in R$ we write $y.R.x$. On relations we now define some elementary operations.

Definition 2.1 The *converse* of a relation R, denoted $R^\cup$, is defined by:

$$x.(R^\cup).y \ \equiv \ y.R.x \ .$$

□

The converse has the same operator precedence as the negation. One can easily observe that $(\neg R)^\cup = \neg(R^\cup)$ for every relation R. We can therefore safely do away with the parentheses. Note that the converse is idempotent and that if $R \subseteq \mathcal{A} \times \mathcal{B}$ then $R^\cup \subseteq \mathcal{B} \times \mathcal{A}$.

Another interesting operation on relations is the following.

Definition 2.2 For relations $R \subseteq \mathcal{C} \times \mathcal{B}$ and $S \subseteq \mathcal{B} \times \mathcal{A}$ we define the the relation $R \circ S \subseteq \mathcal{C} \times \mathcal{A}$, called the *composition of R and S*, by

$$y.(R \circ S).x \ \equiv \ (\exists\, z : z \in \mathcal{B} : y.R.z \wedge z.S.x) \ .$$

□

The composition binds harder than any other binary operator, excluding function application or composition.

We will use $\perp\!\!\!\perp$, called *bottom*, to indicate the empty relation, and $\top\!\!\!\top$, pronounced *top*, to indicate the full relation —in the appropriate universe—. Hence we have for every relation $\perp\!\!\!\perp \subseteq R$ and $R \subseteq \top\!\!\!\top$.

If we consider relations on $\mathcal{A} \times \mathcal{A}$ instead of $\mathcal{A} \times \mathcal{B}$, we can identify a special relation: the *identity*, sometimes referred to as the *diagonal*, denoted I . The identity is defined as $I \doteq \{(x,x) \mid x \in \mathcal{A}\}$. This relation acts as a left and right identity for the composition. Note that the identity on $\mathcal{B} \times \mathcal{B}$ is defined as $I \doteq \{(x,x) \mid x \in \mathcal{B}\}$. Since we won't use different symbols, or tag the identity in order to obtain $I_\mathcal{A}$ and $I_\mathcal{B}$, it should always be clear which identity is meant. In general this poses no problems, since it will always be clear from the context how I should be defined. The correct definition of the identity can be deduced by a process very similar to type inference.

We indicated that relations can be seen as a generalisation of functions. Given a function $f : \mathcal{A} \leftarrow \mathcal{B}$ we define a relation $\tilde{f} \subseteq \mathcal{A} \times \mathcal{B}$ as $y.\tilde{f}.x \ \equiv \ y = f.x$. We will use the same symbol for a function and its relation, so we drop the tilde. The relation arising from a function has some properties not enjoyed by arbitrary relations.

Definition 2.3 For a relation $R \subseteq \mathcal{A} \times \mathcal{B}$ we say

- R is *total* iff $I \subseteq R^\cup \circ R$,
- R is an *imp* (or *functional*) iff $R \circ R^\cup \subseteq I$,
- R is *injective* iff $R^\cup$ is an imp (i.e. $R^\cup \circ R \subseteq I$),
- R is *surjective* iff $R^\cup$ is total (i.e. $I \subseteq R \circ R^\cup$).

□

We now have the following characterisation for relations that can be identified with functions.

Property 2.4 We call a relation $f \subseteq \mathcal{A} \times \mathcal{B}$ a function to $\mathcal{A}$ from $\mathcal{B}$ iff f is a total imp.
□

The above given —short— introduction to the *relational calculus* is not only convenient for reasoning about functions, but also when considering *order (relations)*.

2.5 Order and lattices

The properties of Galois connections depend heavily on the properties of the order in which they are used. An order can, like functions, be seen as a relation with some specific properties. Let's first consider some properties a relation, and thus an order, can have.

Let $\mathcal{P}$ be a set, and R a binary relation on $\mathcal{P}$, i.e. $R \subseteq \mathcal{P} \times \mathcal{P}$. We define the following properties for the relation R.

Definition 2.5

- R is *reflexive* iff $I \subseteq R$,
- R is *transitive* iff $R \circ R \subseteq R$,
- R is *antisymmetric* iff $R \cap R^{\cup} \subseteq I$,
- R is *linear* iff $\top\!\top \subseteq R \cup R^{\cup}$.

□

The reader may wish to extract the perhaps more familiar pointwise definitions. He will then probably appreciate the above given definitions. With these properties we can describe *orders*.

Definition 2.6

- R is called a *pre-order* iff R is reflexive and transitive,
- R is called a *partial order* iff R is reflexive, transitive and antisymmetric.

□

In general, we call a relation an order if it is a pre-order. Traditionally, an order is denoted by $\leq$ or variants thereof. We will conform to that notation for no reason at all. A set $\mathcal{P}$ with a pre-/partial order $\leq$ is denoted by $(\mathcal{P}, \leq)$. If $\leq$ is a partial order, $(\mathcal{P}, \leq)$ is called a *poset*. In general we call $(\mathcal{P}, \leq)$ an ordered set. If $(\mathcal{P}, \leq)$ is a poset and $\leq$ is linear, then $(\mathcal{P}, \leq)$ is called a *chain*. When no confusion arises the order is left implicit.

Since an order is a relation, we can apply the converse to orders. First we observe the following.

Property 2.7 If a relation is reflexive, transitive, antisymmetric, respectively linear, then its converse is reflexive, transitive, antisymmetric, respectively linear.

$\square$

This leads to the following observation:

Property 2.8 The converse of a pre-, respectively partial order is a pre-, respectively partial order.

$\square$

Definition 2.9 For $(\mathcal{P}, \leq)$ an ordered set, we define its *dual* by $(\mathcal{P}, \leq^{\cup})$.

$\square$

2.5.1 Extremal values in posets

Given a poset $(\mathcal{P}, \leq)$ one can look at extremal elements of a subset of $\mathcal{P}$.

Definition 2.10 For $Y \subseteq \mathcal{P}$, x is called a *least* element of Y iff

- $x \in Y$,
- $(\forall\, y : y \in Y : x \leq y)$.

$\square$

Informally, $x \in Y$ is a least element if it is at most any other $y \in Y$. The existence of a least element is in general not assured. But if it exists, one can prove it is unique.

We will denote a least element of a subset Y by $\underline{\mathbf{min}}\, Y$. We will write $(\underline{\mathbf{min}}\, x : P.x : f.x)$ as an alternative for $\underline{\mathbf{min}}\, \{f.x \mid P.x\}$.

In a similar manner one can define a *greatest* element.

Definition 2.11 For $Y \subseteq \mathcal{P}$, x is called a *greatest* element of Y iff

- $x \in Y$,
- $(\forall\, y : y \in Y : y \leq x)$.

$\square$

Note that definition 2.11 is just definition 2.10 in the dual poset.

We will denote the greatest element of a subset Y by $\underline{\mathbf{max}}\, Y$. Occasionally we will use $(\underline{\mathbf{max}}\, x : P.x : f.x)$ instead of $\underline{\mathbf{max}}\, \{f.x \mid P.x\}$.

The definition of these extremal values are, in a sense, local to the subset which contains the extremal element. I.e. in order to conclude that an element x of a subset Y is a least or greatest element, one only needs to compare x with elements of Y. It is not necessary to consider arbitrary elements of the poset $\mathcal{P}$, especially those not in Y.

One can also look at another kind of extremal value.

Definition 2.12 We call z a *lower bound* of Y iff $(\forall y : y \in Y : z \leq y)$.
□

Note that it is not required that $z \in Y$.

Definition 2.13 We call x a *greatest lower bound*, *glb* for short, or —*infimum*—, of Y iff for all $z \in \mathcal{P}$:

$$z \leq x \quad \equiv \quad (\forall y : y \in Y : z \leq y) \ .$$

□

In most, if not all, of the literature, the infimum is defined slightly different. The reader may wish to prove the following.

Theorem 2.14 x is the infimum of Y iff

- $(\forall y : y \in Y : x \leq y)$,
- $(\forall y : y \in Y : z \leq y) \quad \Rightarrow \quad z \leq x$.

□

We prefer definition 2.13 since it is more compact than the alternative formulation as in theorem 2.14. Moreover the formulation given in definition 2.13 is more amenable to manipulation. To be precise, it is a Galois connection! Theorem 2.14 is an instantiation of a general theorem about Galois connections.

We denote the infimum of a set Y by $\sqcap_{\mathcal{P}} Y$. If no confusion arises we will drop the tag, in particular we will drop the subscript when the subscript is equal to the poset. In this notation the infimum is a unary prefix operator. As a result it binds more strongly than function application. As is the case for the minimum and the maximum, we prefer $(\sqcap x : P.x : f.x)$ to $\sqcap \{f.x \mid P.x\}$.

The reason for introducing the tag is that we will later on need some sort of local infimum. Instead of looking at infima relative to the entire poset, one can also define infima relative to a subset of the poset. That subset, with a suitable restriction of the ordering, is a subposet.

Definition 2.15 For $\mathcal{Z} \subseteq \mathcal{P}$ and $Y \subseteq \mathcal{Z}$, we call x the *infimum of* Y *in* $\mathcal{Z}$ iff $x \in \mathcal{Z}$ and for all $z \in \mathcal{Z}$:

$$z \leq x \quad \equiv \quad (\forall y : y \in Y : z \leq y) \ .$$

The unique solution, x, of this equation is denoted by $\sqcap_{\mathcal{Z}} Y$.
□

Note that the defining formula in definition 2.13 and 2.15 is the same. The difference lies in the requirements on x and z that occur in those formula. This observation gives rise to the following

Property 2.16 For $X \subseteq Y \subseteq Z \subseteq \mathcal{P}$ we have, provided $\sqcap_Y X$ and $\sqcap_Z X$ exist,

a $\sqcap_Y X \leq \sqcap_Z X$,

b $\sqcap_Y X \;=\; \sqcap_Z X \;\equiv\; \sqcap_Z X \;\in\; Y$.
$\Box$

We have already observed that the least element can be dualised in order to obtain the greatest element. The infimum also dualises. If we spell this definition out in full detail, we obtain the following.

Definition 2.17 We call z an *upper bound* of Y iff $(\forall\, y : y \,\in\, Y : y \,\leq\, z)$.
$\Box$

Definition 2.18 For $\mathcal{Z} \subseteq \mathcal{P}$ and $Y \subseteq \mathcal{Z}$, we call x a *least upper bound*, *lub* for short —or *supremum*—*of* Y *in* $\mathcal{Z}$ iff $x \in \mathcal{Z}$ and for all $z \in \mathcal{Z}$:

$$x \leq z \quad \equiv \quad (\forall\, y : y \in Y : y \,\leq\, z) \ .$$

The x is denoted $\sqcup_{\mathcal{Z}} Y$.

$\Box$

If no confusion arises, we will drop the tag. For the supremum we observe the following.

Property 2.19 For $X \subseteq Y \subseteq Z \subseteq \mathcal{P}$ we have, when $\sqcup_Z X$ and $\sqcup_Y X$ exist,

a $\sqcup_Z X \;\leq\; \sqcup_Y X$,

b $\sqcup_Z X \;=\; \sqcup_Y X \;\equiv\; \sqcup_Z X \;\in\; Y$.
$\Box$

From the shape of the defining equations of least elements and infima, one might expect that they are related. The same holds for greatest elements and suprema.

Property 2.20 For all $Y \subseteq \mathcal{P}$ and $x \in \mathcal{P}$ we have the following:

a $x \;=\; \underline{\mathbf{min}}\, Y \quad \equiv \quad x \,\in\, Y \;\wedge\; x \;=\; \sqcap Y$,

b $x \;=\; \underline{\mathbf{max}}\, Y \quad \equiv \quad x \,\in\, Y \;\wedge\; x \;=\; \sqcup Y$.
$\Box$

As was the case for least and greatest elements, not every (sub)set of a poset has an infimum or supremum.

2.5.2 Lattices

As was already indicated, a poset can have suprema, respectively infima.

Definition 2.21 A poset $(\mathcal{P}, \leq)$ is called a *lattice* iff every non-empty finite subset of $\mathcal{P}$ has an infimum and a supremum.

□

Instead of $\sqcap\{x, y\}$ one writes $x \sqcap y$. The same can be done for the supremum. Note that we have $x \leq y$ iff $x \sqcap y = x$ iff $x \sqcup y = y$. It is possible to give the definition of a lattice in a more algebraic fashion. The definition is then given in terms of two binary operations. In that case one requires that the two operations are idempotent, commutative, associative and satisfy two absorption laws: —using $\sqcap$ and $\sqcup$ to denote those two operations— $x \sqcap (x \sqcup y) = x$ and $x \sqcup (x \sqcap y) = y$. That approach is completely equivalent. The reason for defining lattices as a special poset is that for Galois connections the ordering on a set is relevant. Had we defined lattices from a more algebraic point of view, the link with orders and thus the possible interactions with Galois connections is less obvious. Nevertheless, the fact that lattices can be treated in an algebraic way, or should we say calculational way, will have bearing on the properties of Galois connections in case the orderings involved are lattice orderings.

Definition 2.22 A poset $(\mathcal{P}, \leq)$ is a *complete lattice* iff every subset of $\mathcal{P}$ has a supremum and an infimum.

□

In particular, if $(\mathcal{P}, \leq)$ is a complete lattice, then $\mathcal{P}$ has a least element —the supremum of the empty set, which equals the infimum of $\mathcal{P}$— and a greatest element —the infimum of the empty set, which equals the supremum of $\mathcal{P}$—.

In order to prove that a poset is a complete lattice, definition 2.22 suggests that one has to prove all suprema and infima exist. However, it is sufficient to prove that all suprema, or dually all infima, exist. If all suprema exist, one can define the infimum of a set X by $\sqcup\{y \mid (\forall x : x \in X : y \leq x)\}$. A dual construction can be applied if all infima exist.

There are some more definitions that can be of interest for lattices.

Definition 2.23 A lattice $(\mathcal{P}, \leq)$ with least element $\perp\!\!\perp$ and greatest element $\top\!\!\top$ is *complemented* iff for every $x \in \mathcal{P}$ there is a y, called a *complement*, such that $x \sqcap y = \perp\!\!\perp$ and $x \sqcup y = \top\!\!\top$.

□

In general the complement of an element need not be uniquely determined. For a lattice with unique complements, the complement of an $x \in \mathcal{P}$ is denoted $\neg x$. The $\neg$ is called the negation. In that case we have that $\neg\neg x = x$ holds.

When a lattice is *distributive*, the complement is unique.

Definition 2.24 A lattice $(\mathcal{P}, \leq)$ is called *distributive* iff for all $x \in \mathcal{P}$ and all non-empty finite $Y \subseteq \mathcal{P}$ we have: $x \sqcup (\sqcap Y) = (\sqcap y : y \in Y : x \sqcup y)$ and $x \sqcap (\sqcup Y) = (\sqcup y : y \in Y : x \sqcap y)$.
$\Box$

It is possible that the distributivity property holds for every subset of a lattice.

Definition 2.25 A lattice $(\mathcal{P}, \leq)$ is called *completely distributive* iff for all $x \in \mathcal{P}$ and all $Y \subseteq \mathcal{P}$ we have: $x \sqcup (\sqcap Y) = (\sqcap y : y \in Y : x \sqcup y)$ and $x \sqcap (\sqcup Y) = (\sqcup y : y \in Y : x \sqcap y)$.
$\Box$

Note that the predicate calculus is a calculus in a complete, completely distributive, complemented lattice. The ordering is the implication, the supremum is the disjunction and the infimum is the conjunction.

2.6 Functions between ordered sets

A function between ordered sets is just a function that maps elements of one ordered set into another ordered set. Since the sets involved have an order, a function can satisfy some properties which are meaningless for functions between mere sets.

Let F be a mapping to an ordered set $(\mathcal{A}, \leq_{\mathcal{A}})$ from an ordered set $(\mathcal{B}, \leq_{\mathcal{B}})$, hence $F : \mathcal{A} \leftarrow \mathcal{B}$.

Definition 2.26 F is called *$\mathcal{A}$ from $\mathcal{B}$ monotonic* iff $F.x \leq_{\mathcal{A}} F.y \Leftarrow x \leq_{\mathcal{B}} y$.
$\Box$

For endofunctions, i.e. $F : \mathcal{B} \leftarrow \mathcal{B}$, we abbreviate "$\mathcal{B}$ from $\mathcal{B}$ monotonic" to simply "monotonic". Actually, even for a mapping to $\mathcal{A}$ from $\mathcal{B}$ it is sufficient to say "F is monotonic" since it is possible to deduce which orderings are meant from typing considerations. So why go to the trouble of introducing a non-standard baroque terminology? The reason for doing so, is because we want to emphasize that there are two different orderings that play a rôle. In the case of monotonicity the typing of F is probably sufficient even for those who do not have a high degree of familiarity with these matters. But for other properties, in which the ordering meant is left implicit, our experience is that one can easily get confused.

Definition 2.27 Given a poset $(\mathcal{B}, \leq_{\mathcal{B}})$, an ordered set $(\mathcal{A}, \leq_{\mathcal{A}})$ and a mapping $F : \mathcal{A} \leftarrow \mathcal{B}$, we call F *existentially cup $\mathcal{A}$ from $\mathcal{B}$ junctive* iff for every $X \subseteq \mathcal{B}$ whose supremum exists, i.e. $\sqcup X$ exists, we have $\sqcup (F.X) = F.(\sqcup X)$. So the supremum in $\mathcal{A}$ of $\{F.x \mid x \in X\}$ exists and is equal to $F.(\sqcup X)$.
$\Box$

Instead of writing "F is existentially cup $\mathcal{A}$ from $\mathcal{B}$ junctive" we write "F is existentially $\sqcup_{\mathcal{A} \leftarrow \mathcal{B}}$ junctive". In effect we tag the symbol denoting the supremum with the typing of the involved function.
There are some other kinds of junctivity.

Definition 2.28 Let $\mathcal{B}$ be a complete lattice, $\mathcal{A}$ an poset and F a mapping to $\mathcal{A}$ from $\mathcal{B}$. We then define:

- F is *universally* $\sqcup_{\mathcal{A}\leftarrow\mathcal{B}}$ junctive iff for all $X \subseteq \mathcal{B}$ we have $\sqcup(F.X) = F.(\sqcup X)$,
- F is *positively* $\sqcup_{\mathcal{A}\leftarrow\mathcal{B}}$ junctive iff for all non-empty $X \subseteq \mathcal{B}$ we have $\sqcup(F.X) = F.(\sqcup X)$,
- F is $\sqcup_{\mathcal{A}\leftarrow\mathcal{B}}$ junctive iff for all non-empty, finite $X \subseteq \mathcal{B}$ we have $\sqcup(F.X) = F.(\sqcup X)$.

□

Instead of cup junctivity, which is concerned with suprema, one can also look at cap junctivity, which is concerned with infima. One can easily obtain the corresponding notions from definition 2.27 and 2.28 by replacing every occurrence of cup by cap, supremum by infimum and $\sqcup$ by $\sqcap$. If we restrict our attention to endofunctions, the different notions of junctivity from definition 2.28 coincide with the definitions of junctivity in [DS90].

In order to prove that a function is existentially $\sqcup$-junctive or existentially $\sqcap$-junctive, it is sufficient to prove that the function is an *order-isomorphism*.

Definition 2.29 A function $F : \mathcal{A} \leftarrow \mathcal{B}$ is called an *order-monomorphism* iff $F.x \leq_{\mathcal{A}} F.y \equiv x \leq_{\mathcal{B}} y$. A function is called an *order-isomorphism* iff it is a surjective order-monomorphism.

□

When the orderings involved in definition 2.29 are partial orders then one usually speaks of a *poset-monomorphism*, respectively *poset-isomorphism*, instead of an order-monomorphism, respectively order-isomorphism.

Property 2.30 If $\mathcal{B}$ and $\mathcal{A}$ are posets with $F : \mathcal{A} \leftarrow \mathcal{B}$ then

a if F is an order-monomorphism then F is injective,

b if F is an order-isomorphism then F is existentially $\sqcup_{\mathcal{A}\leftarrow\mathcal{B}}$ junctive and existentially $\sqcap_{\mathcal{A}\leftarrow\mathcal{B}}$ junctive.

□

The proof of these properties is left as an exercise for the reader.

If we have a function between lattices which both have unique complements, one can define another function which has some sort of dual junctivity properties.

Definition 2.31 Let $\mathcal{A}$ and $\mathcal{B}$ be two lattices with unique complements. Given an $F : \mathcal{A} \leftarrow \mathcal{B}$, we define the *conjugate* of F, denoted $F^\star$ with $F^\star : \mathcal{A} \leftarrow \mathcal{B}$, by $F^\star.x = \neg(F.\neg x)$. The postfix star binds stronger than function application.

□

Note that taking the conjugate is its own reverse, i.e. $(F^\star)^\star = F$. If F has some type of junctivity, then something can be said about $F^\star$'s type of junctivity.

Property 2.32 F has a type of cup junctivity iff $F^\star$ is cap junctive of that same type. □

For a proof of this, the reader can consult [DS90], in which it is proven for an endofunction. The general case is not harder to prove and we trust the reader can do that himself.

2.7 Spec algebra

The spec algebra, and with it the spec calculus, can be seen as an axiomatisation of the endorelations over some anonymous universe. A complete description can be found in [BVvdW91].

The spec calculus can be described in three layers, each layer with its own operations and its own interfaces to the other layers. Let $\mathcal{A}$ be a set. We refer to elements of $\mathcal{A}$ as specs, hence the name for the algebra and calculus. One can read, for this introduction, "relation" instead of "spec".

The first layer of the spec algebra is the lattice layer. The set $\mathcal{A}$ is ordered by $\sqsubseteq$. To be precise, we require that $(\mathcal{A}, \sqsubseteq)$ is a complete, completely distributive, complemented lattice. We denote the supremum by $\sqcup$, the infimum by $\sqcap$, the complement by the prefix $\neg$, and the least, respectively greatest, elements by $\perp\!\!\perp$, respectively $\top\!\!\top$.

We also have a composition for the specs, with an identity denoted I, as is the case for relations. This constitutes the second layer: $(\mathcal{A}, \circ, I)$ is a monoid. As interface with the first layer, we take the composition to be universally $\sqcup$-junctive. This means that for all $\mathcal{V}, \mathcal{W} \subseteq \mathcal{A}$ we have $(\sqcup \mathcal{V}) \circ (\sqcup \mathcal{W}) \;=\; (\sqcup V, W : V \in \mathcal{V} \wedge W \in \mathcal{W} : V \circ W)$. As a result of this we have:

- $\perp\!\!\perp$ is a left and right zero for $\circ$,
- $\circ$ is monotonic (with respect to $\sqsubseteq$),
- $\top\!\!\top \circ \top\!\!\top \;=\; \top\!\!\top$.

The third layer, is the converse structure. On $\mathcal{A}$ we postulate the unary postfix operator woc, denoted by $^\cup$. As interface with the first layer we have $P^\cup \sqsubseteq Q \;\equiv\; P \sqsubseteq Q^\cup$. For the interface with the second layer we have $(R \circ S)^\cup \;=\; S^\cup \circ R^\cup$.

In addition to these layers and interfaces, we have another axiom: for all $R, S, T \in \mathcal{A}$ we have $R \circ S \sqcap T \;\sqsubseteq\; R \circ (R^\cup \circ T \sqcap S)$. We occasionally use this rule in a slightly different formulation: for all $R, S, T, U \in \mathcal{A}$ we have $R \circ S \sqcap T \;\sqsubseteq\; R \circ U \;\;\Leftarrow\;\; S \sqcap R^\cup \circ T \;\sqsubseteq\; U$. We refer to this rule as the dedekind rule. This rule was first formulated by Riguet in [Rig48].

These are not the only axioms for the spec calculus, but they are sufficient for what is needed here. For a full account, the reader is referred to [BVvdW91].

Chapter 3

Elementary Examples

One may wonder if and where Galois connections occur in computing science or mathematics. They do occur in various parts, but they are not often recognised as such. As a consequence proofs we have encountered are either complicated or unnecessarily long, whereas exploitation of the Galois connection can immediately suggest compact and straightforward proofs. In this section we give some elementary examples of Galois connections and their use in constructing elegant calculations.

3.1 Floor and ceiling

Our first example of a Galois connection is in the realm of mathematics. In most mathematical texts the function *floor*, denoted $\lfloor x \rfloor$, from reals to integers is defined as follows: for all real x we take $\lfloor x \rfloor$ to be the greatest integer at most x. Likewise the *ceiling*, denoted $\lceil x \rceil$, is defined for all real x as the least integer at least x.

With these definitions various properties of the two functions can be verified, but it is very difficult to actually calculate with them. A possible way to improve this is to give the definition as a Galois connection. Let's first consider the floor-function.

$\lfloor x \rfloor$ is defined as the greatest integer satisfying some property. To be precise, it has the property that it is at most x. Hence if we have another integer n that satisfies the same property —i.e. $n \leq x$—, n cannot be greater than $\lfloor x \rfloor$, since $\lfloor x \rfloor$ is defined to be the greatest such integer. This gives the following Galois connection as definition:

Definition 3.1 For all real x and integer n

$$n \leq \lfloor x \rfloor \;\equiv\; n \leq x \;\; .$$

□

In a similar way we find a Galois connection for the ceiling-function.

Definition 3.2 For all real x and integer n

$$\lceil x \rceil \leq n \;\equiv\; x \leq n \;\; .$$

□

One might complain that definition 3.1 and definition 3.2 are not genuine Galois connections, since they involve only one function, namely the floor-, respectively ceiling-, function from reals to integer. A Galois connection involves two functions in opposite directions. But in both specifications there is a second, invisible, function present that maps integers to reals. In this case that is a very trivial function, since integers can be embedded in a straightforward way in the reals. If we take U to be that embedding, we can reformulate definition 3.1 as

$$n \leq \lfloor x \rfloor \;\equiv\; U.n \leq x \;\; . \tag{3.3}$$

A similar rewriting can be done for definition 3.2. As long as we note that n is an integer, we can safely omit the U.

It has already been noted that the specifications of floor and ceiling can be given in the shape of a Galois connection, see [GKP89] and [RB88]. But that fact is not used in any calculation. Even worse, in [GKP89] they don't consider it useful at all to recognise a Galois connection since they have difficulty remembering the Galois connection! In order to show the usefulness of the given Galois connection, let's calculate some properties.

We know that the floor-function maps reals to integer. By the instantiation $n := \lfloor x \rfloor$ in definition 3.1 this reduces to $\lfloor x \rfloor \leq x$. Likewise, using definition 3.2, one finds $x \leq \lceil x \rceil$.

In [GKP89] the following theorem is mentioned.

Theorem 3.4 $\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor \;=\; \lfloor \sqrt{x} \rfloor$, for all $0 \leq x$.

Proof For any integer n we derive

$$\begin{array}{ll}
 & n \leq \left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor \\
\equiv & \qquad \{ \;\; n \text{ is an integer, definition 3.1} \;\; \} \\
 & n \leq \sqrt{\lfloor x \rfloor} \\
\equiv & \qquad \{ \;\; \text{arithmetic} \;\; \} \\
 & n^2 \leq \lfloor x \rfloor \quad \vee \quad n < 0 \\
\equiv & \qquad \{ \;\; n^2 \text{ is an integer, definition 3.1} \;\; \} \\
 & n^2 \leq x \quad \vee \quad n < 0 \\
\equiv & \qquad \{ \;\; \text{arithmetic} \;\; \} \\
 & n \leq \sqrt{x} \\
\equiv & \qquad \{ \;\; n \text{ is an integer, definition 3.1} \;\; \} \\
 & n \leq \lfloor \sqrt{x} \rfloor
\end{array}$$

By instantiating n to $\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor$ we obtain $\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor \leq \lfloor \sqrt{x} \rfloor$, and by instantiating n to $\lfloor \sqrt{x} \rfloor$ we find $\lfloor \sqrt{x} \rfloor \leq \left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor$, from which the theorem now follows.

□

Note that the decision on how to prove the theorem, i.e. the introduction of the integer n, is entirely inspired by the shape of definition 3.1. The only way we can calculate something about the floor-function is to use its specification. That specification allows one to rewrite the floor-function only when it is in some special shape. In this case: it is on the *greater* side of the $\leq$ and on the *smaller* side there is an integer. So the only way one can hope to be able to prove something from its specification is to manipulate the demonstrandum in such a way that the specification can be used.

The reader is cordially invited to compare the above proof of theorem 3.4 with the proof given in [GKP89]. You may also wish to prove $\lfloor x+m \rfloor = \lfloor x \rfloor + m$, and $\lfloor x \rfloor \, \underline{\mathbf{min}} \lfloor y \rfloor = \lfloor x \, \underline{\mathbf{min}} \, y \rfloor$ for all real x and y, and integer m, or $\lfloor x/m \rfloor = \lfloor \lfloor x \rfloor /m \rfloor$ for all real x and positive integer m in the same calculational style. You should observe a general pattern, which might even give rise to a general theorem.

If we negate both sides of definition 3.1 and definition 3.2, the equivalence still holds. We find:

Corollary 3.5 $n > \lfloor x \rfloor \;\equiv\; n > x$.

□

Corollary 3.6 $\lceil x \rceil > n \;\equiv\; x > n$.

□

This observation leads to the proof of

Theorem 3.7 $\lceil x \rceil = n \;\equiv\; n-1 < x \leq n$.

Proof For any integer n we have

$$
\begin{array}{ll}
 & \lceil x \rceil = n \\
\equiv & \qquad \{ \text{ calculus } \} \\
 & \lceil x \rceil \leq n \;\wedge\; n \leq \lceil x \rceil \\
\equiv & \qquad \{ \text{ definition 3.2 } \} \\
 & x \leq n \;\wedge\; n \leq \lceil x \rceil
\end{array}
$$

Calculating with the second conjunct, we obtain:

$$
\begin{array}{ll}
 & n \leq \lceil x \rceil \\
\equiv & \qquad \{ \text{ integer arithmetic } \} \\
 & n-1 < \lceil x \rceil \\
\equiv & \qquad \{ \; n-1 \text{ is integer corollary 3.6 } \} \\
 & n-1 < x
\end{array}
$$

□

From theorem 3.7 we obtain, by taking $x := n$ the following:

Corollary 3.8 $\lceil n \rceil = n$ for any integer n.

□

A theorem similar to theorem 3.7 can be given for the floor-function.

3.2 Galois connection for relations

As was noted in the preliminaries, section 2.4, we can see relations as a generalisation of functions. But one can also view a relation as a set-valued function. To be precise, every relation gives rise to two set-valued functions.

Definition 3.9 For $R \subseteq \mathcal{X} \times \mathcal{Y}$, a mapping to $\mathbb{P}(\mathcal{X})$ from $\mathcal{Y}$ is defined by taking for every $y \in \mathcal{Y}$:

$$R.y \doteq \{x \mid x.R.y\} \ .$$

□

By elementary set calculus, we observe that $x \in R.y \ \equiv \ x.R.y$.
In the same vein we make the following definition.

Definition 3.10 For $R \subseteq \mathcal{X} \times \mathcal{Y}$ we define a mapping to $\mathbb{P}(\mathcal{Y})$ from $\mathcal{X}$ by defining for every $x \in \mathcal{X}$:

$$x.R \doteq \{y \mid x.R.y\} \ .$$

□

Note that a relation is fully determined by either one of these mappings. Furthermore we observe the following connection

$$x.R \ni y \quad \equiv \quad x \in R.y \ ,$$

for every $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. When we view $x.R$ as a predicate on $\mathbb{P}(\mathcal{Y})$ and $R.y$ as a predicate on $\mathbb{P}(\mathcal{X})$, this connection translates into

$$x.R.y \quad = \quad (x.R).y \quad = \quad x.(R.y) \ ,$$

for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$.

A similar description, but with different notation, of the Galois connections for relations can also be found in [Sch53].

3.2.1 Polarities

Our second example is by now a classic. It was first introduced by G. Birkhoff in 1940 and can be viewed as a starting point for the interest in Galois connections. The description given here is based upon the description given in [Bir67].

Let R be a relation between sets $\mathcal{X}$ and $\mathcal{Y}$. The mappings $x.R$ and $R.y$ can be *lifted* to mappings to $\mathbb{P}(\mathcal{Y})$ from $\mathbb{P}(\mathcal{X})$, respectively to $\mathbb{P}(\mathcal{X})$ from $\mathbb{P}(\mathcal{Y})$. These mappings are called *polars* in [Bir67].

Definition 3.11 For every $X \in \mathbb{P}(\mathcal{X})$ define the *right polar* as

$$\{\!|X|\!\}R \doteq (\cap\, x : x \in X : x.R) \ .$$

□

Definition 3.12 For every $Y \in I\!P(\mathcal{Y})$ define the *left polar* as

$$R\{\!\!\{Y\}\!\!\} \doteq (\cap\, y : y \in Y : R.y) \ .$$

□

If we take $x \in \mathcal{X}$ then $\{\!\!\{\{x\}\}\!\!\}R = x.R$. A similar property holds for the left polar. Hence a relation is fully determined by either one of its polars.

These two polars are connected. Indeed, they are Galois connected. For $R \subseteq \mathcal{X} \times \mathcal{Y}$, $X \in I\!P(\mathcal{X})$ and $Y \in I\!P(\mathcal{Y})$ we have

Theorem 3.13 $X \subseteq R\{\!\!\{Y\}\!\!\} \quad \equiv \quad \{\!\!\{X\}\!\!\}R \supseteq Y$.

Proof

$$\begin{array}{ll}
 & X \subseteq R\{\!\!\{Y\}\!\!\} \\
\equiv & \qquad \{ \text{ calculus } \} \\
 & (\forall\, x : x \in X : x \in R\{\!\!\{Y\}\!\!\}) \\
\equiv & \qquad \{ \text{ definition 3.12 } \} \\
 & (\forall\, x : x \in X : (\forall\, y : y \in Y : x.R.y)) \\
\equiv & \qquad \{ \text{ interchanging quantifications } \} \\
 & (\forall\, y : y \in Y : (\forall\, x : x \in X : x.R.y)) \\
\equiv & \qquad \{ \text{ definition 3.11 } \} \\
 & (\forall\, y : y \in Y : \{\!\!\{X\}\!\!\}R \ni y) \\
\equiv & \qquad \{ \text{ calculus } \} \\
 & \{\!\!\{X\}\!\!\}R \supseteq Y
\end{array}$$

□

Most of the formal properties of polars can easily be deduced by instantiating the general properties of the Galois connections, see section 4. For more properties, especially the applicability of polars to other examples, in the field of: geometry, theory of rings and groups, the reader is referred to [Bir67].

Recently, the polars have acquired a new jacket. They popped up in the field of *formal concept analysis* [DP90]. Let's give a brief description to see the connection with polars.

A *context* is a triple $(\mathsf{G}, \mathsf{M}, R)$, where G, called the objects, and M, called the attributes, are sets and $R \subseteq \mathsf{G} \times \mathsf{M}$. Hence R relates objects and attributes. For $G \subseteq \mathsf{G}$, $\{\!\!\{G\}\!\!\}R$ is the set of attributes common to all objects in G . Similarly for $M \subseteq \mathsf{M}$, $R\{\!\!\{M\}\!\!\}$ is the set of objects possessing all the attributes in M.

In this context, a *concept* is a pair (G, M) with $G = R\{\!\!\{M\}\!\!\}$ and $M = \{\!\!\{G\}\!\!\}R$. The set of all concepts in a context $(\mathsf{G}, \mathsf{M}, R)$ is denoted $\mathcal{B}(\mathsf{G}, \mathsf{M}, R)$. On this set one can define an ordering $\leq$ as follows:

$$(g_0, m_0) \leq (g_1, m_1) \ \equiv\ g_0 \subseteq g_1 \ .$$

It is easy to show that $g_0 \subseteq g_1$ is equivalent to $m_1 \subseteq m_0$. With this ordering, the set $\mathcal{B}(\mathsf{G}, \mathsf{M}, R)$ forms a complete lattice: the concept lattice. Without going into further details, all the properties of *formal concepts* are easily proven by using general properties of Galois connections, specifically by the properties of the polars. This was also noted in [DP90].

The polars arise in another important disguise. They form a pointwise basis for *factors*. Factors will be discussed after the next example, the weakest liberal precondition.

3.2.2 The weakest liberal precondition

There is another way of lifting a relation S on $\mathcal{X} \times \mathcal{Y}$ into a mapping to $I\!\!P(\mathcal{Y})$ from $I\!\!P(\mathcal{X})$, or to $I\!\!P(\mathcal{X})$ from $I\!\!P(\mathcal{Y})$. Like the previous example, the mappings $x.S$ and $S.y$ can be lifted but in a different way. For lack of standard nomenclature, these mappings will be called *image* mappings.

Definition 3.14 For $X \in I\!\!P(\mathcal{X})$ define the *right image* of the relation $S \subseteq \mathcal{X} \times \mathcal{Y}$ by

$$[X]S \doteq (\cup x : x \in X : x.S) \ ,$$

□

Definition 3.15 For $Y \in I\!\!P(\mathcal{Y})$ define the *left image* of the relation $S \subseteq \mathcal{X} \times \mathcal{Y}$ by

$$S[Y] \doteq (\cup y : y \in Y : S.y) \ .$$

□

For functions, the notion of an image is well known. When we consider a function as a relation, the left image of that relation is the image of the function. That is the reason for the name image mapping.

As is the case for polar mappings, any one of these image mappings fully determines the relation, since for any $x \in \mathcal{X} : [\{x\}]S = x.S$. A dual equality holds for the left image mapping.

Knowing the Galois connection for polar maps, one might anticipate a similar result for the image mappings. There is indeed a connection between the image mappings, even a Galois connection.

Theorem 3.16 For all $X \in I\!\!P(\mathcal{X})$ and $Y \in I\!\!P(\mathcal{Y})$:

$$[X]S \subseteq Y \quad \equiv \quad X \subseteq S^{\star}[Y] \ .$$

Proof Since $[X]S \subseteq Y$ is equivalent to $(\forall x : x \in X : x.S \subseteq Y)$, it is sufficient to prove $x.S \subseteq Y \equiv x \in S^{\star}[Y]$. We derive for any $x \in X$

$$
\begin{array}{ll}
 & x \in S^\star[Y] \\
\equiv & \quad \{ \text{ definition left image, calculus } \} \\
 & x \notin (\cup\, y : y \notin Y : S.y) \\
\equiv & \quad \{ \text{ calculus } \} \\
 & (\forall\, y : y \notin Y : x \notin S.y) \\
\equiv & \quad \{ \text{ calculus } \} \\
 & (\forall\, y : y \notin Y : \neg(x.S.y)) \\
\equiv & \quad \{ \text{ trading } \} \\
 & (\forall\, y : x.S.y : y \in Y) \\
\equiv & \quad \{ \text{ calculus } \} \\
 & x.S \subseteq Y
\end{array}
$$

□

By instantiating $X, Y := \neg X, \neg Y$ in theorem 3.16 and some simplifications of the resulting expression, we find

Corollary 3.17 $X \supseteq S[Y] \quad \equiv \quad [X]S^\star \supseteq Y$.
□

The relation $S^\star$ is well studied in computing science, albeit in a somewhat narrower setting and, of course, under a different name.

Let's call $\mathcal{X}$ the statespace. Take $\perp \notin \mathcal{X}$ and define for any $X \in I\!P(\mathcal{X}) : X_\perp \doteq X \cup \{\perp\}$. A program S can be modelled by a relation $S \subseteq \mathcal{X} \times \mathcal{X}_\perp$. The $\perp$ is used to represent a nonterminating computation. Hence a program *maps* states from $\mathcal{X}$ onto states in $\mathcal{X}_\perp$. This means it either terminates in some state of $\mathcal{X}$, or it doesn't terminate, which is modelled by $\perp$. Note that, since S is a relation and not necessarily a function, non-determinancy can easily be dealt with in this framework.

A well-established method in showing the correctness of programs is by way of so-called Hoare-triples. For $P, Q \subseteq \mathcal{X}$ this means showing the validity of $\{P\}\, S\, \{Q\}$; i.e. show that the program S, when started in a state belonging to P, either terminates in a state belonging to Q or doesn't terminate at all. In the relational setting this amounts to the validity of $[P]S \subseteq Q_\perp$. Using the Galois connection theorem 3.16 this is equivalent to $P \subseteq S^\star[Q_\perp]$.

In computing science one writes $\mathsf{wlp}.S.Q$ instead of $S^\star[Q_\perp]$. So the connection between the weakest liberal precondition and Hoare triples

$$P \subseteq \mathsf{wlp}.S.Q \quad \equiv \quad \{P\}\, S\, \{Q\}$$

is a Galois connection. It was already noted in [DS90] that $\mathsf{wlp}.S.Q$ is an extremal solution of an equation involving a Hoare triple. To be precise, it is the greatest —or in the terminology used in [DS90]; the weakest— solution of $X :: \{X\}\, S\, \{Q\}$.

3.3 Factors

One very fine example of a Galois connection is provided by the factors. They first appeared in [Dil39] under the name *residuals*. They are used under the same name in [Bir67]. The name *factor* is used by [Con71] in the context of regular languages and finite machines. They also, more recently, were used in program specification by [HJ86] under the names *weakest pre-* and *postspecifications*. They are also used in [BVvdW91] since they have nice calculational properties.

The approach given here is based on the polarities. This approach has a drawback. It is very *low-level*, in the sense that it defines factors in terms of their elements. It is very well possible to define factors without using elements, as is done in [HJ86] and [BVvdW91]. The advantage of using polarities to define factors, and hence the reason for choosing the outlined approach, is that it may help in recognising a factor in a pointwise definition. One cannot recognise a factor in an expression involving elements if one is unaware of the pointwise definition of factors.

It is definitely not suggested that the pointwise definition of factors is used for calculational purposes. The Galois connection for factors is much more convenient. For a multitude of examples on how factors can be used in calculations, the reader might want to consult [BVvdW91]. Let's first look at the factors in a relational framework.

The notation used in this section is introduced in the section about polarities, see section 3.2. All the relations used here are subsets of $\mathcal{X} \times \mathcal{X}$.

Definition 3.18 For R and S relations, define the *right factor* $R\backslash S$ by

$$x.(R\backslash S) \doteq \{\!\!\{R.x\}\!\!\}S \ ,$$

for all $x \in \mathcal{X}$.
□

Definition 3.19 For relations T and S the *left factor* S/T is defined by

$$(S/T).y \doteq S\{\!\!\{y.T\}\!\!\} \ ,$$

for all $y \in \mathcal{X}$.
□

Since there is a Galois connection between the polars, one might anticipate a Galois connection for the factors. Indeed, one can prove:

Theorem 3.20 $R \subseteq S/T \quad \equiv \quad R\backslash S \supseteq T$.

Proof

$$\begin{array}{ll} & R \subseteq S/T \\ \equiv & \qquad \{ \text{ calculus } \} \\ & (\forall\, z :: R.z \subseteq (S/T).z) \\ \equiv & \qquad \{ \text{ definition 3.19 } \} \\ & (\forall\, z :: R.z \subseteq S\{\!\!\{z.T\}\!\!\}) \end{array}$$

$$\begin{array}{ll}
\equiv & \quad \{ \text{ Galois connection for polars, theorem 3.13 } \} \\
& (\forall\, z :: \llbracket R.z \rrbracket S \;\supseteq\; z.T) \\
\equiv & \quad \{ \text{ definition 3.18 } \} \\
& R\backslash S \;\supseteq\; T
\end{array}$$

□

This Galois connection is not the only one that can be given for the factors. There is a more interesting one. Before embarking on that one, let's first give a lemma that is interesting in its own right.

Lemma 3.21 For R, S and T relations:

a $x.(R\backslash S).y \quad \equiv \quad R.x \subseteq S.y$,

b $x.(S/T).y \quad \equiv \quad x.S \supseteq y.T$.

Proof Only **(a)** is proven; **(b)** can be proven likewise.

$$\begin{array}{ll}
& x.(R\backslash S).y \\
\equiv & \quad \{ \text{ definition 3.18 } \} \\
& \llbracket R.x \rrbracket S \ni y \\
\equiv & \quad \{ \text{ calculus } \} \\
& \llbracket R.x \rrbracket S \;\supseteq\; \{y\} \\
\equiv & \quad \{ \text{ Galois connection for polars, theorem 3.13 } \} \\
& R.x \;\subseteq\; S\llbracket \{y\} \rrbracket \\
\equiv & \quad \{ \text{ definition polar } \} \\
& R.x \;\subseteq\; S.y
\end{array}$$

□

In [HJ86] it is observed that for factors the following holds

$$x.(R\backslash S).y \quad \equiv \quad (\forall\, z :: z.R.x \Rightarrow z.S.y) \ .$$

Our notation eliminates the dummy z.

Now let's give a more interesting Galois connection for factors.

Theorem 3.22 For R, S and T relations

$$R \circ S \;\subseteq\; T \quad \equiv \quad R \;\subseteq\; T/S \ .$$

Proof

$$\begin{array}{ll}
& R \circ S \;\subseteq\; T \\
\equiv & \quad \{ \text{ calculus } \} \\
& (\forall\, x :: x.(R \circ S) \;\subseteq\; x.T) \\
\equiv & \quad \{ \text{ calculus } \}
\end{array}$$

$$
\begin{array}{ll}
 & (\forall\, x,y : x.R.y : y.S \subseteq x.T) \\
\equiv & \qquad \{ \text{ lemma 3.21}(\mathbf{b}) \ \} \\
 & (\forall\, x,y : x.R.y : x.(T/S).y) \\
\equiv & \qquad \{ \text{ calculus } \} \\
 & R \subseteq T/S
\end{array}
$$

□

Combining theorem 3.20 and theorem 3.22 leads to:

Theorem 3.23 For R, S and T relations

$$R \circ S \subseteq T \ \equiv\ S \subseteq R \backslash T \ .$$

□

Theorem 3.22 is used in [HJ86] as the definition of the weakest prespecification. Although there they write $P \backslash R$ instead of R/P. The reason for preferring the latter is that factors —like any component of a Galois connection— enjoy a *cancellation* property. Taking $R := T/S$ in theorem 3.22 gives the cancellation property:

$$(T/S) \circ S \subseteq T \ .$$

In this expression the two adjacent occurrences of S cancel one another. Using the notation suggested in [HJ86], this property would read as:

$$(S \backslash T) \circ S \subseteq T \ ,$$

in which the two occurrences of S that cancel are not adjacent. This makes it more difficult to remember the property or to see that cancellation is applicable, especially when S or T is a long formula. The choice for the notation of the factors is based upon economy of calculation. A similar argument can be given against the notation used in [Bir67].

Again note that the approach used here to introduce factors by giving an expression for them, and subsequently proving the Galois connections hold —i.e. theorem 3.22 and 3.23—, is a roundabout way. One could also, even better, give the Galois connections and then prove that these are valid definitions. This is done in [HJ86] and [BVvdW91]. That approach is dealt with when describing the abstract properties of Galois connections.

So much for the factors in a relational setting. The factors also appear in another setting: the theory of regular languages. In [Con71] they were introduced as a tool for expressing a regular expression E as a regular function of F_1, F_2, ... with the F_i to be determined. We will define the factors for regular languages in the same vein as is done for the relations. Notice the analogy with the factors in a relational setting. The reader is urged to translate the theorems about the factors for regular languages into a relational setting.

It is tacitly assumed that the reader has some knowledge of the theory of regular languages. The symbol $\cdot$ will be used to denote the *concatenation*-operator, $\cup$ stands for set union and the $\leq$ is the complete lattice ordering on regular languages, to be precise: $F \leq E \equiv E = E \cup F$. We will not distinguish between a one-element language and a word, as is common practise.

One of the standard operations for regular languages is the *derivative*.

Definition 3.24 For a regular language E and a word w, the *word-derivative* E_w is defined by $E_w \doteq \{v \mid w \cdot v \in E\}$.
□

Another frequently appearing notation for the word-derivative E_w is $\partial_w E$. The word-derivative can be seen as a function which maps a word onto a regular language. This function can be generalised in order to obtain a function that maps a regular language onto a regular language.

Definition 3.25 For regular languages E and F we define the *derivative* by $\partial_F E \doteq (\cup w : w \in F : E_w)$.
□

By taking $F = \{w\}$ one easily sees that the derivative is indeed a generalisation of the word-derivative. A more familiar, but completely equivalent way of defining the derivative is by $\partial_F E = \{v \mid F{\cdot}v \cap E \neq \emptyset\}$.

Although the notation for the derivative suggests that it is a function of E, it can also be seen as a function of F. These functions are very useful for regular languages. They are (e.g.) used to efficiently construct a finite machine that accepts a given regular language.

The word-derivative can be generalised in another way.

Definition 3.26 For regular languages E and F, the *right factor* is defined by $F \backslash E \doteq (\cap w : w \in F : E_w)$.
□

Even for those who are familiar with regular languages, it might be the first time they have came across factors.

As was the case for relations, there is a Galois connection for the right factor.

Theorem 3.27 For E, F and G regular languages we have $F \cdot G \leq E \equiv G \leq F \backslash E$.

Proof We observe for any $v \in G$

$$
\begin{array}{ll}
 & v \in F \backslash E \\
\equiv & \qquad \{ \text{ definition 3.26 } \} \\
 & v \in (\cap w : w \in F : E_w) \\
\equiv & \qquad \{ \text{ calculus } \} \\
 & (\forall w : w \in F : v \in E_w) \\
\equiv & \qquad \{ \text{ definition 3.24 } \}
\end{array}
$$

$$
\begin{array}{ll}
 & (\forall\, w : w \in F : w \cdot v \in E) \\
\equiv & \qquad \{ \text{ calculus } \} \\
 & F \cdot v \leq E
\end{array}
$$

□

There is an intimate relation between the right factor and the derivative. To that end, we first prove a small lemma which we will need later on.

Lemma 3.28 For any regular language E and word w, we have $\neg(E_w) = (\neg E)_w$.

Proof For any word v we calculate:

$$
\begin{array}{ll}
 & v \in (\neg E)_w \\
\equiv & \qquad \{ \text{ definition 3.24 } \} \\
 & w \cdot v \in \neg E \\
\equiv & \qquad \{ \text{ calculus } \} \\
 & w \cdot v \notin E \\
\equiv & \qquad \{ \text{ definition 3.24 } \} \\
 & v \notin E_w \\
\equiv & \qquad \{ \text{ calculus } \} \\
 & v \in \neg(E_w)
\end{array}
$$

□

This lemma enables us to prove that the derivative and the right factor are each other's conjugates.

Theorem 3.29 For regular languages E and F:

$$(\partial_F)^\star E = F \backslash E \ .$$

Proof For any word v we derive:

$$
\begin{array}{ll}
 & v \in (\partial_F)^\star E \\
\equiv & \qquad \{ \text{ definition conjugate } \} \\
 & v \notin \partial_F(\neg E) \\
\equiv & \qquad \{ \text{ definition 3.25 } \} \\
 & v \notin (\cup\, w : w \in F : (\neg E)_w) \\
\equiv & \qquad \{ \text{ calculus } \} \\
 & (\forall\, w : w \in F : v \notin (\neg E)_w) \\
\equiv & \qquad \{ \text{ lemma 3.28 } \} \\
 & (\forall\, w : w \in F : v \in E_w) \\
\equiv & \qquad \{ \text{ calculus } \} \\
 & v \in (\cap\, w : w \in F : E_w) \\
\equiv & \qquad \{ \text{ definition 3.26 } \} \\
 & v \in F \backslash E
\end{array}
$$

□

Hence right factors and derivatives are in a one to one correspondence. The properties of the one can immediately be transcribed into properties of the other. So, formally it doesn't matter which one of the two is studied. In most of the literature concerning regular languages the derivative is defined as is done above, i.e. by explicitly stating its elements. The factor is most easily expressed in the form of the Galois connection, see definition 3.27. This means that proofs involving the derivative will be in terms of elements, while proofs involving factors will be element-free —although it can be done using elements, see the beginning of this section—.

There is also a left factor. The conjugate of the left factor is called the the *antiderivative*. The properties of that one are dual to the properties of the derivative, since properties of the left factor are dual to the properties of the right factor.

Chapter 4

Abstract properties of Galois connections

After seeing the previous examples, it is time to take a more formal approach. The theory presented here is not new. One of the earliest contributions is by G. Birkhoff with the introduction of polarities, see section 3.2.1. C.J. Everett proved that every Galois connection between powersets arises from a polarity [Eve44]. The actual generalisation to the Galois connections as we use them here was done by O. Ore [Ore44]. J. Schmidt introduced a very concise formula for describing a Galois connection [Sch53]. That formula is used here as the definition of a Galois connection. In [HH85] there are four kinds of "Galois connections" introduced, ranging from polarities to a restricted form of adjunctions. A comprehensive overview of the theory of Galois connections can be found in [GHK+80].

In what follows we take $\mathcal{A}$ and $\mathcal{B}$ to be sets with some ordering, at least a pre-order, imposed on them: $(\mathcal{A}, \leq_{\mathcal{A}})$ and $(\mathcal{B}, \leq_{\mathcal{B}})$. We let F be a mapping to $\mathcal{A}$ from $\mathcal{B}$ and G a mapping in the opposite direction, so $F : \mathcal{A} \leftarrow \mathcal{B}$ and $G : \mathcal{B} \leftarrow \mathcal{A}$. For such an F and G we have the following definition.

Definition 4.1 (F, G) is a Galois connection iff for all $x \in \mathcal{B}$ and $y \in \mathcal{A}$

$$F.x \ \leq_{\mathcal{A}} \ y \ \equiv \ x \ \leq_{\mathcal{B}} \ G.y \ \ .$$

□

In order to make the formulae more readable, we will drop the subscripts from the orderings. This will not lead to confusion, since it can always be deduced which ordering is meant from type considerations.

For (F, G) a Galois connection we refer to F as the lower adjoint, since it is on the *lower* side of an order, and to G as the upper adjoint, since it is on the *upper* side of an order.

In category theory the names left- and right adjoint are more common, but they are more amenable to be interchanged. But then again the names lower and upper adjoint are also easily mixed up, since the lower adjoint is the upper adjoint in the dual ordering.

Theorem 4.2 (F, G) is a Galois connection iff (G, F) is a Galois connection, where the orderings of $\mathcal{A}$ and $\mathcal{B}$ are reversed.

Proof We have for any $x \in \mathcal{A}$ and $y \in \mathcal{B}$:

$$
\begin{array}{ll}
 & G.y \leq^{\cup} x \\
\equiv & \quad \{ \text{ dual order } \} \\
 & x \leq G.y \\
\equiv & \quad \{ \ (F, G) \text{ is a Galois connection } \} \\
 & F.x \leq y \\
\equiv & \quad \{ \text{ dual order } \} \\
 & y \leq^{\cup} F.x
\end{array}
$$

□

A result of this is that all statements about one of the adjoints of a Galois connection have a dual statement for the other adjoint. That is, any theorem concerning a lower adjoint gives rise to a theorem about the upper adjoint, since that one is the lower adjoint when we reverse the ordering. So with one proof, we get two theorems. In general we mention the dual of a theorem, but we won't have to prove it.

All properties that can be derived from definition 4.1 depend heavily on the properties of the orderings of $\mathcal{A}$, respectively $\mathcal{B}$. We try to disentangle the theorems about Galois connections by starting with pre-orders and subsequently imposing more structure on the orderings.

Most properties are already well-documented, just look at the references mentioned at the beginning of this section. Those properties and their proofs are not in a calculational style but in a more "traditional" style. We will give the proofs here in the calculational fashion. We don't explicitly define what we mean when talking about a calculational style. We trust that this report in its whole will convey what we deem to be calculational.

4.1 Pre-orders

For the time being, we only require that the orderings on $\mathcal{A}$ and $\mathcal{B}$ are pre-orders, i.e. reflexive and transitive.

We will first introduce some calculation rules for pre-orders and subsequently give some equivalent definitions. It turns out that the equivalent definitions are just reformulations of the calculation rules. In the literature one easily finds the alternative definitions of a Galois connection, but the calculation rules that one uses are not explicitly mentioned.

4.1.1 Calculating in pre-orders

The first theorem arises frequently when calculating with Galois connections, as will be seen throughout this chapter. We refer to this theorem as a cancellation law.

Theorem 4.3 [cancellation] If (F, G) is a Galois connection, then we have

a $x \leq G.F.x$ for all $x \in \mathcal{B}$,

b $F.G.y \leq y$ for all $y \in \mathcal{A}$.

Proof Since **a** and **b** are dual, only **a** is proven.

$$
\begin{array}{ll}
 & x \leq G.F.x \\
\equiv & \quad \{ \ (F,G) \text{ is a Galois connection } \} \\
 & F.x \leq F.x \\
\equiv & \quad \{ \ \text{reflexivity } \} \\
 & \mathsf{true}
\end{array}
$$

□

With this theorem it is straightforward to prove the following

Corollary 4.4 If (F, G) is a Galois connection, then both F and G are monotonic.

Proof For monotonicity of F we observe

$$
\begin{array}{ll}
 & F.x \leq F.z \\
\equiv & \quad \{ \ (F,G) \text{ is a Galois connection } \} \\
 & x \leq G.F.z \\
\Leftarrow & \quad \{ \ \mathsf{cancellation}, \text{ transitivity } \} \\
 & x \leq z
\end{array}
$$

Monotonicity of G follows by duality.
□

Apart from the encountered cancellation law we have another property that is prominent in calculations, the Galois connection itself. It is very useful for transcribing something with an F on the lower side of the ordering, into some expression with a G on the upper side of an ordering and vice-versa. This kind of equivalence between expressions is used very often when calculating. One only has to look at the various proofs in this report.

Nevertheless, the Galois connection has only limited use for direct calculations. It only gives a means for transcribing some particular expressions into another one. One would like to have equivalent expressions for a broader class of expressions. That will be the content of the next few theorems.

Theorem 4.5 If (F, G) is a Galois connection then the following are equivalent:

a $x \leq G.y$,

b $F.x \leq F.G.y$,

c $F.x \leq y$,

d $G.F.x \leq G.y$.

Proof The proof is by cyclic implication.

$$
\begin{array}{ll}
 & x \le G.y \\
\Rightarrow & \quad \{ \ F \text{ is monotonic } \} \\
 & F.x \le F.G.y \\
\Rightarrow & \quad \{ \ \textsf{cancellation}, \text{ transitivity } \} \\
 & F.x \le y \\
\Rightarrow & \quad \{ \ G \text{ monotonic } \} \\
 & G.F.x \le G.y \\
\Rightarrow & \quad \{ \ \textsf{cancellation}, \text{ transitivity } \} \\
 & x \le G.y
\end{array}
$$

□

By instantiating $x := G.x$ in theorem 4.5, and subsequently making some simplifications, we obtain

Corollary 4.6 If (F, G) is a Galois connection then the following are equivalent:

a $G.x \le G.y$,

b $F.G.x \le F.G.y$,

c $F.G.x \le y$.

□

Instantiating $y := F.y$ in theorem 4.5 leads to the following

Corollary 4.7 If (F, G) is a Galois connection then the following are equivalent:

a $F.x \le F.y$,

b $G.F.x \le G.F.y$,

c $x \le G.F.y$.

□

These last two corollaries tell us something about the two adjoints when they are restricted to $F.\mathcal{B}$ and $G.\mathcal{A}$. In case $\mathcal{B}$ and $\mathcal{A}$ are posets a stronger result holds, see theorem 4.17.

Theorem 4.8 If (F, G) is a Galois connection then

a $F : \mathcal{A} \leftarrow G.\mathcal{A}$ is an order-monomorphism,

b $G : \mathcal{B} \leftarrow F.\mathcal{B}$ is an order-monomorphism.

Proof Assume (F, G) is a Galois connection. For part **a** we have to prove that $F.x \le F.z \equiv x \le z$ for all $x, z \in G.\mathcal{A}$. This follows directly from corollary 4.6.

Part **b** is the dual of part **a** and thus already proven.

□

As an immediate result we have

Corollary 4.9 If (F, G) is a Galois connection then

a $F : F.\mathcal{B} \leftarrow G.\mathcal{A}$ is an order-isomorphism,

b $G : G.\mathcal{A} \leftarrow F.\mathcal{B}$ is an order-isomorphism.

□

With the tools we now have, we will now look at some equivalent formulations of a Galois connection.

4.1.2 Alternative definitions

The earliest definition of a Galois connection is the one introduced by O. Ore in [Ore44].

Theorem 4.10 (F, G) is a Galois connection iff the following two clauses hold:

a $x \leq G.F.x$ and $F.G.y \leq y$,

b F and G are monotonic.

Proof The proof is by mutual implication.
The $\Rightarrow$ part follows immediately from theorem 4.3 and corollary 4.4.
The $\Leftarrow$ part is already proven, see the proof of theorem 4.5.
□

The alternative formulation of a Galois connection given in theorem 4.10 resembles the original one more closely. In the original definition of a Galois connection the ordering on $\mathcal{B}$ is reversed. We prefer definition 4.1, proposed by J. Schmidt [Sch53], for two reasons. It is easier to remember Schmidt's definition since it consist of only one clause, whereas the alternative formulation requires two clauses. More importantly, Schmidt's definition is more calculational than the original definition.

There is also a sort of mixed form of definition 4.1 and theorem 4.10 that defines a Galois connection.

Theorem 4.11 (F, G) is a Galois connection iff the following three clauses hold

- F is monotonic,
- $F.G.y \leq y$,
- $F.x \leq y \Rightarrow x \leq G.y$.

Proof The proof is by mutual implication.
The $\Rightarrow$ part is a direct result of theorem 4.3(**b**), corollary 4.4 and the definition of a Galois connection.
For the $\Leftarrow$ part we prove F and G satisfy definition 4.1. We only have to prove $F.x \leq y \Leftarrow x \leq G.y$.

$$
\begin{array}{ll}
 & x \le G.y \\
\Rightarrow & \quad \{ \ F \text{ is monotonic } \} \\
 & F.x \le F.G.y \\
\Rightarrow & \quad \{ \ F.G.y \le y \ \} \\
 & F.x \le y
\end{array}
$$

□

And its dual

Theorem 4.12 (F, G) is a Galois connection iff the following three clauses hold

a G is monotonic,

b $x \le G.F.x$,

c $F.x \le y \Leftarrow x \le G.y$.

□

These last two theorems give the definition of a Galois connection in terms of a (co-)universal mapping property [Mac71, pages 55–59,80–82].

4.1.3 Uniqueness of adjoints in a pre-order

Because of the generality of a pre-order, the statements that can be proven are fairly weak. It is rather difficult, in general, to prove equality for elements of a pre-ordered set. Often one has to be content with an equivalence.

Theorem 4.13 If (F_0, G_0) and (F_1, G_1) are Galois connections, then $F_0 \cong F_1 \ \equiv \ G_0 \cong G_1$.

Proof

$$
\begin{array}{ll}
 & F_0 \cong F_1 \\
\equiv & \quad \{ \text{ definition } \} \\
 & (\forall\, x :: F_0.x \cong F_1.x) \\
\equiv & \quad \{ \text{ calculus } \} \\
 & (\forall\, x, y :: F_0.x \le y \ \equiv \ F_1.x \le y)
\end{array}
$$

Dually we obtain $G_0 \cong G_1 \ \equiv \ (\forall\, x, y :: x \le G_0.y \ \equiv \ x \le G_1.y)$. Using the Galois connection on the terms in the quantifications completes the proof.

□

A direct result of this theorem is that all adjoints of a given function are equivalent.

It is possible to derive more theorems for Galois connections involving pre-orders. These theorems are very general, or should we say weak. In fact, they are so weak that it is hard to prove equality of things. It is in most cases only possible to prove equivalence. One can be satisfied with this, or one can strengthen the requirements imposed on the orderings. That is what we now propose.

4.2 Partial orders

We now focus on partial orders, i.e. pre-orders with anti-symmetry. All the theorems one can derive for Galois connections with pre-orders are valid when considering partial orders. But most of these can be strengthened, since equivalence turns into equality.

Before embarking on the more traditional theorems, we first examine what calculation rules can be deduced. Since we now have anti-symmetry we focus on calculation rules that give us an equality.

Next we will derive existence theorems for adjoints. Subsequently we will give an equivalent way of studying Galois connections, by means of the so-called closure operators. Interesting as that is, it is not calculational. Luckily we can extract some calculational properties from that observation, by which we end this section.

4.2.1 More cancellation laws

When using the symmetry present in the first two clauses of corollary 4.6 and corollary 4.7, we can deduce

Corollary 4.14 If (F, G) is a Galois connection then

a $G.x = G.y \equiv F.G.x = F.G.y$,

b $F.x = F.y \equiv G.F.x = G.F.y$.

□

The mappings of a Galois connection are not only each others' duals, but they are also in a way inverse to each other. Sometimes, this property is referred to by calling F and G each others' *semi-inverse* or *quasi-inverse*. We adopt the former name.

Theorem 4.15 [semi-inverse] If (F, G) is a Galois connection then

a $F.x = F.G.F.x$,

b $G.y = G.F.G.y$.

Proof We only prove **a**, the statement **b** being the dual.

$$
\begin{array}{ll}
 & F.x = F.G.F.x \\
\Leftarrow & \quad \{ \ \textsf{cancellation} \text{ with } y := F.x \ \} \\
 & F.x \leq F.G.F.x \\
\equiv & \quad \{ \ (F,G) \text{ is a Galois connection } \} \\
 & G.F.x \leq G.F.x \\
\Leftarrow & \quad \{ \ \text{reflexivity } \} \\
 & \textsf{true}
\end{array}
$$

□
This theorem could also have been proven for pre-orders; instead of the equality one then obtains an equivalence.

As a result we have the following

Corollary 4.16 If (F, G) is a Galois connection then $F.G$ and $G.F$ are idempotent.

Proof Follows directly from semi-inverse and the use of Leibniz with F, respectively G .
□

The previous theorems are very useful in calculations. They are best referred to as cancellation laws. We have already observed one cancellation law, cancellation. In that one there is still an order present. In the newly-encountered cancellation laws, we have a genuine equality.

We already observed that F and G when restricted to each others' images, are both order-isomorphisms. For partial orders we can do better.

Theorem 4.17 If (F, G) is a Galois connection then $G.\mathcal{A}$ and $F.\mathcal{B}$ are isomorphic posets.

Proof That $F.\mathcal{B}$ and $G.\mathcal{A}$ are posets is trivial. The mappings $F : F.\mathcal{B} \leftarrow G.\mathcal{A}$ and $G : G.\mathcal{A} \leftarrow F.\mathcal{B}$ are both order-isomorphisms, see theorem 4.9. This immediately gives that $G.\mathcal{A}$ and $F.\mathcal{B}$ are isomorphic posets.
□

As an immediate corollary we have (see property 2.30(**b**))

Corollary 4.18 If (F, G) is a Galois connection then

a F is existentially $\sqcup_{G.\mathcal{A} \leftarrow F.\mathcal{B}}$ junctive and existentially $\sqcap_{G.\mathcal{A} \leftarrow F.\mathcal{B}}$ junctive,

b G is existentially $\sqcup_{F.\mathcal{B} \leftarrow G.\mathcal{A}}$ junctive and existentially $\sqcap_{F.\mathcal{B} \leftarrow G.\mathcal{A}}$ junctive.

□

With the added anti-symmetry we can strengthen theorem 4.13.

Theorem 4.19 Each adjoint in a Galois connection determines uniquely its other adjoint.
□

From this theorem one might anticipate that each adjoint is expressible in terms of the other. This will be the concern of the next section.

4.2.2 Existence of adjoints

Before we look for conditions which ensure the existence of an adjoint, let's first give a formulation of a Galois connection in which one adjoint is expressed in terms of the other adjoint.

Theorem 4.20 The following are equivalent:

a (F, G) is a Galois connection,

b F is monotonic and $G.y \;=\; (\underline{\mathbf{max}}\, x : F.x \;\leq\; y : x)$,

c G is monotonic and $F.x \;=\; (\underline{\mathbf{min}}\, y : x \;\leq\; G.y : y)$.

Proof The fact that **a** equivales **b** is just a reformulation of theorem 4.11. For **a** equivales **c** use theorem 4.12.
□
Since being a least element is a stronger property then being an infimum, we obtain the following

Corollary 4.21 If (F, G) is a Galois connection then the following two hold

a $G.y \;=\; (\sqcup\, x : F.x \;\leq\; y : x)$,

b $F.x \;=\; (\sqcap\, y : x \;\leq\; G.y : y)$.

□

From theorem 4.20 one can extract necessary and sufficient conditions for a mapping to have an upper, respectively lower, adjoint.

Theorem 4.22 A mapping $F : \mathcal{A} \leftarrow \mathcal{B}$ has an upper adjoint iff F is monotonic and for every $y \in \mathcal{A}$ the equation $x \;::\; F.x \;\leq\; y$ has a greatest solution.

Proof The proof is by mutual implication.
The $\Rightarrow$ part follows directly from theorem 4.20(**b**), the greatest solution of $x \;::\; F.x \;\leq\; y$ is given by $G.y$ for every $y \in \mathcal{A}$.
For the $\Leftarrow$ part define $G.y$, for any $y \in \mathcal{A}$, to be the greatest solution of $x \;::\; F.x \;\leq\; y$, i.e. $G.y \;=\; (\underline{\mathbf{max}}\, x : F.x \;\leq\; y : x)$. Since F is monotonic, the result follows from theorem 4.20.
□
As a dual we have:

Theorem 4.23 A mapping $G : \mathcal{B} \leftarrow \mathcal{A}$ has a lower adjoint iff G is monotonic and for every $x \in \mathcal{B}$ the equation $y \;::\; x \;\leq\; G.y$ has a least solution.
□

These theorems provide a nice answer as to when a mapping has a lower, respectively upper adjoint. But requiring that a subset of a poset has a least or greatest element, is quite a strong requirement. In fact, if we require that every non-empty subset of a poset has a least (or greatest) element, it means that the poset is linear. In general, this is too strong. Take for example two arbitrary sets. There is a good chance that these will be incomparable, it is not the case that one of them is a subset of the other. So one doesn't have a least, or greatest, set. But any two sets do have an infimum, the intersection of the sets, and a supremum, the union of the sets.

From corollary 4.21 we know that an adjoint can be expressed as an infimum, respectively supremum of a set. In order to extract some kind of existence theorem using infima and suprema, we first observe the following. From theorem 4.20 we see that a mapping has an upper adjoint if it is monotonic and some particular set has a greatest element. If a mapping is monotonic, it means that it preserves greatest elements. But the converse also holds, if a mapping preserves greatest elements then it is monotonic.

If we want to give an existence theorem for an upper adjoint, using suprema, it might be worthwhile to first focus on the preservation of suprema by the mapping. In other words, we want to establish the junctivity type of the mappings involved in a Galois connection. From corollary 4.18 we know something about the type of junctivity with respect to $G.\mathcal{A}$ and $F.\mathcal{B}$, but this says nothing about the elements outside those sets. We need something stronger for that.

Lemma 4.24 If (F, G) is a Galois connection then

a F is existentially $\sqcup_{\mathcal{A}\leftarrow\mathcal{B}}$ junctive,

b G is existentially $\sqcap_{\mathcal{B}\leftarrow\mathcal{A}}$ junctive.

Proof We only prove **a**, since **b** is its dual. Take any $X \subseteq \mathcal{B}$ and assume $\sqcup_{\mathcal{B}} X$ exists. We have to show that $F. \sqcup_{\mathcal{B}} X$ solves the defining equation of $\sqcup_{\mathcal{A}} (F.X)$. For any $y \in \mathcal{A}$ we derive:

$$
\begin{array}{ll}
 & F. \sqcup_{\mathcal{B}} X \leq y \\
\equiv & \qquad \{ \ (F,G) \text{ is a Galois connection } \} \\
 & \sqcup_{\mathcal{B}} X \leq G.y \\
\equiv & \qquad \{ \ G.y \in \mathcal{B} \text{ , definition supremum } \} \\
 & (\forall x : x \in X : x \leq G.y) \\
\equiv & \qquad \{ \ (F,G) \text{ is a Galois connection } \} \\
 & (\forall x : x \in X : F.x \leq y) \\
\equiv & \qquad \{ \ \text{calculus } \} \\
 & (\forall z : z \in F.X : z \leq y)
\end{array}
$$

□

Now we are in a position to express a Galois connection in terms of suprema and infima.

Theorem 4.25 The following three are equivalent:

a (F, G) is a Galois connection,

b F is existentially $\sqcup_{\mathcal{A}\leftarrow\mathcal{B}}$ junctive and $G.y = (\sqcup x : F.x \leq y : x)$,

c G is existentially $\sqcap_{\mathcal{B}\leftarrow\mathcal{A}}$ junctive and $F.x = (\sqcap y : x \leq G.y : y)$.

Proof We only prove **a** equivales **b**. The equivalence of **a** and **c** follows by duality. The proof is by mutual implication.
a$\Rightarrow$**b**: This is the conjunction of corollary 4.21(**a**) and lemma 4.24(**a**).
a$\Leftarrow$**b**: From $G.y = (\sqcup x : F.x \leq y : x)$ we deduce that the supremum of $\{x \mid F.x \leq y\}$ for every $y \in \mathcal{A}$ exists. We prove $F.z \leq y \equiv z \leq G.y$ by a ping-pong argument.

$$
\begin{array}{ll}
 & F.z \le y \\
\Rightarrow & \quad \{\ S \le \sqcup S \text{ for all sets } S\ \} \\
 & z \le (\sqcup x : F.x \le y : x) \\
\Rightarrow & \quad \{\ F \text{ is monotonic }\ \} \\
 & F.z \le F.(\sqcup x : F.x \le y : x) \\
\equiv & \quad \{\ F \text{ is existentially } \sqcup_{\mathcal{A} \leftarrow \mathcal{B}} \text{ junctive }\ \} \\
 & F.z \le (\sqcup x : F.x \le y : F.x) \\
\Rightarrow & \quad \{\ \text{see below, } \le \text{ is transitive }\ \} \\
 & F.z \le y
\end{array}
$$

Which uses the fact that $(\sqcup x : F.x \le y : F.x) \le y$ and is proven as follows

$$
\begin{array}{ll}
 & (\sqcup x : F.x \le y : F.x) \le y \\
\equiv & \quad \{\ \text{definition supremum }\ \} \\
 & (\forall x : F.x \le y : F.x \le y) \\
\equiv & \quad \{\ \text{calculus }\ \} \\
 & \mathsf{true}
\end{array}
$$

□

This enables us to formulate an alternative existence theorem for a lower, respectively upper, adjoint.

Theorem 4.26 A mapping $F : \mathcal{A} \leftarrow \mathcal{B}$ has an upper adjoint iff F is existentially $\sqcup_{\mathcal{A} \leftarrow \mathcal{B}}$ junctive and the set $\{x \mid F.x \le y\}$ has a supremum for every $y \in \mathcal{A}$.

Proof The proof is by mutual implication.
The $\Rightarrow$ part follows directly from theorem 4.25.
For the $\Leftarrow$ part: define for all $y \in \mathcal{A}$, $G.y$ as $(\sqcup x : F.x \le y : x)$. This supremum is well defined, by assumption. The rest follows from theorem 4.25.
□
As a dual we have

Theorem 4.27 A mapping $G : \mathcal{B} \leftarrow \mathcal{A}$ has a lower adjoint iff G is existentially $\sqcap_{\mathcal{B} \leftarrow \mathcal{A}}$ junctive and the set $\{y \mid x \le G.y\}$ has an infimum for every $x \in \mathcal{B}$.
□

The theorems in this section are used to establish the existence of an adjoint, and thus a Galois connection, without giving an explicit formula for the adjoint. Yet it is possible to give an expression for the adjoint, in terms of an extremal element. In general that expression is not amenable to manipulation, so it is hardly ever used.

We already observed that the sets $F.\mathcal{B}$ and $G.\mathcal{A}$ are isomorphic posets. The elements of these sets have some special properties. In order to derive these properties and to look at Galois connections in another way we first discuss a related topic.

4.2.3 The closure connection

The composites $G.F$ and $F.G$ are interesting in their own right. In order to show why, we first examine a particular class of mappings.

Definition 4.28 For f an endofunction over a poset, we call f a *closure operator* iff the following two clauses hold

- $x \leq f.x$ for all x,
- $x \leq f.y \Rightarrow f.x \leq f.y$ for all x and y.

□

As a dual to the closure operators, we have the following

Definition 4.29 For f an endofunction over a poset, we call f a *co-closure* or a *interior operator* iff the following two clauses hold

- $f.x \leq x$ for all x,
- $f.x \leq y \Rightarrow f.x \leq f.y$ for all x and y.

□

In [GHK⁺80] an interior operator is called a *kernel*. For f a closure or an interior operator, we call an element z *closed* iff $f.z = z$. It is common practice to refer to the closed elements of interior operators as *open* elements. We don't adhere to existing practice, because the closed and open elements are defined by the same equation.

The ceiling function, see section 3.1, can be seen as a closure operator. Consider the ceiling function as a mapping from reals to reals. We then have $x \leq \lceil x \rceil$ and $x \leq \lceil y \rceil \Rightarrow \lceil x \rceil \leq \lceil y \rceil$ as can be verified easily. The closed elements in this case are precisely the integers. The floor function can in the same way be seen as a co-closure operator.

In fact, every Galois connection gives rise to a closure and an interior operator.

Theorem 4.30 If (F, G) is a Galois connection then

a $G.F$ is a closure operator,

b $F.G$ is an interior operator.

Proof Only **a** is proven since **b** is its dual. In order to conclude that $G.F$ is a closure operator, we have to prove two things. First $x \leq G.F.x$, which follows directly from cancellation. Secondly, we have to prove $x \leq G.F.y \Rightarrow G.F.x \leq G.F.y$.

$$
\begin{array}{ll}
 & G.F.x \leq G.F.y \\
\Leftarrow & \qquad \{\ G \text{ is monotonic } \} \\
 & F.x \leq F.y \\
\equiv & \qquad \{\ (F, G) \text{ is a Galois connection } \} \\
 & x \leq G.F.y
\end{array}
$$

□

Just for completeness we also give the converse of this theorem. Every (co-)closure operator gives a Galois connection. So instead of studying (co-)closure operators one can also study Galois connections.

Theorem 4.31 If f is a closure, respectively co-closure, then there is a Galois connection such that $f = G.F$, respectively $f = F.G$.

Proof We only prove the theorem for f a closure operator. Let f be a closure over the poset $(\mathcal{P}, \leq)$, hence $f : \mathcal{P} \leftarrow \mathcal{P}$. Take $\overline{\mathcal{P}}$ to be the set of closed elements, i.e. $\overline{\mathcal{P}} = f.\mathcal{P}$. We construct a Galois connection between $\overline{\mathcal{P}}$ and $\mathcal{P}$. Let F be f but typed as $F : \overline{\mathcal{P}} \leftarrow \mathcal{P}$. Take $G : \mathcal{P} \leftarrow \overline{\mathcal{P}}$ to be the inclusion, i.e. $G.x = x$ for all $x \in \overline{\mathcal{P}}$. Now observe that $G.F = f$ and $F.G$ is the identity on $\overline{\mathcal{P}}$. It is easy to check that F and G satisfy the clauses of theorem 4.12.

□

These are all nice well-documented results. But not quite satisfactory. The reason for our interest in Galois connections is because they have good calculational properties. The observation that there is a one-to-one correspondence between Galois connections and (co-)closure operators is fine, but one can not calculate with that observation.

4.2.4 "Perfect" connections

In case of a Galois connection, there is an alternative way to characterise the closed elements of $G.F$ and $F.G$. They are precisely the elements that are an image of some element under G, respectively F.

Theorem 4.32 If (F, G) is a Galois connection then

a $G.F.x = x \equiv x \in G.\mathcal{A}$,

b $F.G.y = y \equiv y \in F.\mathcal{B}$.

Proof Again only **a** is proven, since **b** is its dual. We prove **a** by mutual implication
For the $\Rightarrow$: this is trivial, since $F.x \in \mathcal{A}$.
For the $\Leftarrow$: since $x \in G.\mathcal{A}$ we have $x = G.y$ for some $y \in \mathcal{A}$.

$$
\begin{array}{ll}
 & x = G.y \\
\equiv & \quad \{ \text{ calculus, semi-inverse } \} \\
 & x = G.y \quad \wedge \quad x = G.F.G.y \\
\Rightarrow & \quad \{ \text{ calculus } \} \\
 & x = G.F.x
\end{array}
$$

□

Although theorem 4.32 was introduced to give an alternative formulation for the closed elements of $G.F$, respectively $F.G$, it is mostly used in the opposite direction. It provides an alternative expression for an element of $G.\mathcal{A}$, respectively $F.\mathcal{B}$. That alternative expression lends itself better for calculations. For an element of $G.\mathcal{A}$ we can freely introduce or remove an application of $G.F$. A similar property holds for the elements of $F.\mathcal{B}$. These can also be viewed as some sort of cancellation properties.

For a Galois connection we have the cancellation laws $x \leq G.F.x$ for any $x \in \mathcal{B}$ and $F.G.y \leq y$ for any $y \in \mathcal{A}$. Using this we obtain from theorem 4.32 the following

Corollary 4.33 If (F, G) is a Galois connection then

a $G.F.x \leq x \equiv x \in G.\mathcal{A}$,

b $y \leq F.G.y \equiv y \in F.\mathcal{B}$.

□

It is possible that all elements of $\mathcal{B}$ are closed under $G.F$. Ore would say: the Galois connection is *perfect* in $\mathcal{B}$. In [MSS86] this is called a *Galois insertion from $\mathcal{B}$ to $\mathcal{A}$*. There are several equivalent expressions to indicate that all elements of $\mathcal{B}$ are closed.

Theorem 4.34 For (F, G) a Galois connection the following are equivalent

a $(\forall x : x \in \mathcal{B} : F.x = (\underline{\mathbf{min}}\, y : x = G.y : y))$,

b $(\forall x : x \in \mathcal{B} : G.F.x = x)$,

c G is surjective,

d F is a poset-monomorphism,

e F is injective.

Moreover, any one of the above implies

- $(\forall x : x \in \mathcal{B} : F.x = (\sqcap y : x = G.y : y))$.

Proof We first prove the equivalence between **a** and **b**. The rest is proven by cyclic implication. Assume (F, G) is a Galois connection.

$$
\begin{array}{ll}
 & (\forall x : x \in \mathcal{B} : F.x = (\underline{\mathbf{min}}\, y : x = G.y : y)) \\
\equiv & \qquad \{ \text{ definition } \underline{\mathbf{min}} \text{ } \} \\
 & (\forall x : x \in \mathcal{B} : x = G.F.x \wedge (\forall y : x = G.y : F.x \leq y)) \\
\equiv & \qquad \{ \text{ } (F,G) \text{ is a Galois connection } \} \\
 & (\forall x : x \in \mathcal{B} : G.F.x = x)
\end{array}
$$

We now prove **b**⇒ **c**⇒ **d**⇒**e**⇒**b**.

$$
\begin{array}{ll}
 & (\forall x : x \in \mathcal{B} : G.F.x = x) \\
\equiv & \qquad \{ \text{ theorem 4.32}(\mathbf{a}) \ \} \\
 & (\forall x : x \in \mathcal{B} : x \in G.\mathcal{A}) \\
\equiv & \qquad \{ \text{ calculus } \} \\
 & \mathcal{B} = G.\mathcal{A} \\
\Rightarrow & \qquad \{ \text{ theorem 4.8}(\mathbf{a}), \text{ restriction to } G.\mathcal{A} \text{ is vacuous } \} \\
 & F \text{ is a poset-monomorphism} \\
\Rightarrow & \qquad \{ \text{ calculus } \} \\
 & F \text{ is injective} \\
\Rightarrow & \qquad \{ \text{ definition of injective } \} \\
 & (\forall x : x \in \mathcal{B} : F.G.F.x = F.x \equiv G.F.x = x) \\
\equiv & \qquad \{ \textsf{ semi-inverse } \} \\
 & (\forall x : x \in \mathcal{B} : G.F.x = x)
\end{array}
$$

The fact that any of the clauses **a** through **e** implies $F.x = (\sqcap y : x = G.y : y)$ for all $x \in \mathcal{B}$ is trivial.

□

By duality we obtain

Theorem 4.35 For (F, G) a Galois connection the following are equivalent

a $(\forall y : y \in \mathcal{A} : G.y = (\underline{\mathbf{max}}\, x : F.x = y : x))$,

b $(\forall y : y \in \mathcal{A} : F.G.y = y)$,

c F is surjective,

d G is a poset-monomorphism,

e G is injective.

And any one of the above implies

- $(\forall y : y \in \mathcal{A} : G.y = (\sqcup x : F.x = y : x))$.

□

So much for Galois connections for partial orders. The theorems encountered so far form a substantial part of the known, or rather documented, theorems about Galois connections. In particular we have introduced most of the theorems that are useful for calculational purposes.

Some of the theorems depend on the existence of suprema or infima. If we have a structure where the existence of those extremal elements is trivial, one might be able to improve some of the results stated in this section.

4.3 Complete lattices

In case of a Galois connection, there are two orderings that play a rôle. If we want to adhere to the symmetry between these orderings and the theorems, it would be advantageous to take both orderings to be complete lattices. However, that is quite a strong requirement. We will only assume —unless stated otherwise — that just one of the orderings is a complete lattice. When we give the dual of a theorem, we will have to require that the other ordering is a complete lattice.

In this section we will merely give an improvement on some of the theorems already mentioned.

Assume that $\mathcal{B}$ is a complete lattice. We can now characterise the mappings that have an upper adjoint in the following concise way.

Theorem 4.36 A mapping $F : \mathcal{A} \leftarrow \mathcal{B}$ has an upper adjoint iff F is universally $\sqcup_{\mathcal{A}\leftarrow\mathcal{B}}$ junctive.

Proof Since $\mathcal{B}$ is a complete lattice, we know the set $\{x \mid F.x \leq y\}$ has a supremum in $\mathcal{B}$ for every $y \in \mathcal{A}$. From theorem 4.26 we deduce that F has an upper adjoint iff F is existentially $\sqcup_{\mathcal{A}\leftarrow\mathcal{B}}$ junctive. With $\mathcal{B}$ being a complete lattice, this is equivalent to F being universally $\sqcup_{\mathcal{A}\leftarrow\mathcal{B}}$ junctive which completes the proof.
$\square$
For the dual, assume $\mathcal{A}$ is a complete lattice. We then obtain the following:

Theorem 4.37 A mapping $G : \mathcal{B} \leftarrow \mathcal{A}$ has a lower adjoint iff G is universally $\sqcap_{\mathcal{B}\leftarrow\mathcal{A}}$ junctive.
$\square$

The previous two theorems can be used in two different ways. If one wants to prove that a mapping is universally $\sqcup$-junctive, one only has to prove that the mapping has an upper adjoint. This is known in the predicate calculus as the junctivity lemma. The two orderings are then instantiated to the ordering of the predicates, the implication.

On the other hand, if one wants to establish that a mapping has an upper adjoint, it is sufficient to prove that the mapping is universally $\sqcup$-junctive. This gives a nice existence theorem. It is this theorem that can be used to prove the existence of the factors, as is done in [BVvdW91].

We now focus our attention on the closed elements of F and G. We already know that they are isomorphic posets. With $\mathcal{B}$ being a complete lattice, we can do better.

Theorem 4.38 If $\mathcal{B}$ is a complete lattice, the poset $G.\mathcal{A}$ is a complete lattice. Moreover the infima in $G.\mathcal{A}$ coincide with the infima of $\mathcal{B}$.

Proof To show that $G.\mathcal{A}$ is a complete lattice, it is sufficient to show all infima exist. Take any $X \subseteq G.\mathcal{A}$. We have to show that $\sqcap_{G.\mathcal{A}} X$ exist. We do that by demonstrating it is equal to $\sqcap_{\mathcal{B}} X$, which exists. By property 2.16(**b**) it is sufficient to show that $\sqcap_{\mathcal{B}} X \in G.\mathcal{A}$.

$$
\begin{array}{ll}
& \sqcap_{\mathcal{B}} X \in G.\mathcal{A} \\
\equiv & \qquad \{ \text{ corollary } 4.33(\mathbf{a}) \ \} \\
& G.F. \sqcap_{\mathcal{B}} X \le \sqcap_{\mathcal{B}} X \\
\Leftarrow & \qquad \{ \ G.F \text{ is monotonic, hence } G.F. \sqcap_{\mathcal{B}} X \le \sqcap_{\mathcal{B}} (G.F.X) \ \} \\
& \sqcap_{\mathcal{B}} (G.F.X) \le \sqcap_{\mathcal{B}} X \\
\equiv & \qquad \{ \ X \subseteq G.\mathcal{A} \text{ theorem } 4.32(\mathbf{a}) \ \} \\
& \sqcap_{\mathcal{B}} X \le \sqcap_{\mathcal{B}} X \\
\equiv & \qquad \{ \text{ calculus } \} \\
& \mathsf{true}
\end{array}
$$

□

Given the fact that $\mathcal{B}$ is a complete lattice, we now know that $G.\mathcal{A}$ is a complete lattice and the infima in $G.\mathcal{A}$ coincide with the infima in $\mathcal{B}$. We also know the suprema in $G.\mathcal{A}$ always exist. Alas, the suprema in $G.\mathcal{A}$ do not, in general, coincide with the suprema of $\mathcal{B}$.

Theorem 4.39 If $\mathcal{B}$ is a complete lattice, then for any $X \subseteq G.\mathcal{A}$ the supremum in $G.\mathcal{A}$, $\sqcup_{G.\mathcal{A}} X$, is $G.F. \sqcup_{\mathcal{B}} X$.

Proof Take any $X \subseteq G.\mathcal{A}$. We prove that $G.F. \sqcup_{\mathcal{B}} X = \sqcup_{G.\mathcal{A}} X$ by mutual containment.

$$
\begin{array}{ll}
& \sqcup_{G.\mathcal{A}} X \\
\le & \qquad \{ \ X = G.F.X \le G.F. \sqcup_{\mathcal{B}} X \text{ since } G.F \text{ monotonic } \} \\
& G.F. \sqcup_{\mathcal{B}} X \\
\le & \qquad \{ \ G.F \text{ monotonic, } \sqcup_{\mathcal{B}} X \le \sqcup_{G.\mathcal{A}} X \ \} \\
& G.F. \sqcup_{G.\mathcal{A}} X \\
= & \qquad \{ \ \sqcup_{G.\mathcal{A}} X \in G.\mathcal{A} \text{ theorem } 4.32(\mathbf{a}) \ \} \\
& \sqcup_{G.\mathcal{A}} X
\end{array}
$$

□

As a dual to theorem 4.38 and theorem 4.39 we have the following

Theorem 4.40 If $\mathcal{A}$ is a complete lattice, the poset $F.\mathcal{B}$ is a complete lattice. The suprema in $F.\mathcal{B}$ coincide with the suprema in $\mathcal{A}$, and for any $Y \subseteq F.\mathcal{B}$ the infimum in $F.\mathcal{B}$, i.e. $\sqcap_{F.\mathcal{B}} Y$, is given by $F.G. \sqcap_{\mathcal{A}} Y$.

□

So far we have proved that if $\mathcal{B}$ is a complete lattice then so is $G.\mathcal{A}$. A dual result holds for $\mathcal{A}$ and $F.\mathcal{B}$. Now is the time to claim that when $\mathcal{B}$ and $\mathcal{A}$ are complete lattices then so are $F.\mathcal{B}$ and $G.\mathcal{A}$. In fact they are isomorphic complete lattices, since $F : F.\mathcal{B} \leftarrow G.\mathcal{A}$ and $G : G.\mathcal{A} \leftarrow F.\mathcal{B}$ are both poset-isomorphisms; see also corollary 4.18.

But we can do better. For $F.\mathcal{B}$ being a complete lattice it is not necessary that $\mathcal{A}$ is a complete lattice. By using corollary 4.18, we can construct suprema and infima of $F.\mathcal{B}$ even when $\mathcal{A}$ is not a complete lattice.

Theorem 4.41 If $\mathcal{B}$ is a complete lattice, then $F.\mathcal{B}$ is a complete lattice. For $Y \subseteq F.\mathcal{B}$ we have

a $\sqcup_{F.\mathcal{B}} Y = F.\sqcup_{G.\mathcal{A}} (G.Y) = F.\sqcup_{\mathcal{B}} (G.Y)$,

b $\sqcap_{F.\mathcal{B}} Y = F.\sqcap_{G.\mathcal{A}} (G.Y) = F.\sqcap_{\mathcal{B}} (G.Y)$.

Proof For any $Y \subseteq F.\mathcal{B}$ we observe

$$\begin{array}{ll} & F.\sqcup_{\mathcal{B}} (G.Y) \\ = & \qquad \{ \text{ semi-inverse } \} \\ & F.G.F.\sqcup_{\mathcal{B}} (G.Y) \\ = & \qquad \{ \text{ theorem 4.39 } \} \\ & F.\sqcup_{G.\mathcal{A}} (G.Y) \\ = & \qquad \{ \text{ corollary 4.18}(\mathbf{a}) \} \\ & \sqcup_{F.\mathcal{B}} (F.G.Y) \\ = & \qquad \{ Y \subseteq G.\mathcal{A}, \text{ theorem 4.32}(\mathbf{a}) \} \\ & \sqcup_{F.\mathcal{B}} Y \end{array}$$

And

$$\begin{array}{ll} & F.\sqcap_{\mathcal{B}} (G.Y) \\ = & \qquad \{ \text{ theorem 4.38 } \} \\ & F.\sqcap_{G.\mathcal{A}} (G.Y) \\ = & \qquad \{ \text{ corollary 4.18}(\mathbf{a}) \} \\ & \sqcap_{F.\mathcal{B}} (F.G.Y) \\ = & \qquad \{ Y \subseteq G.\mathcal{A}, \text{ theorem 4.32}(\mathbf{a}) \} \\ & \sqcap_{F.\mathcal{B}} Y \end{array}$$

□

As a dual we have

Theorem 4.42 If $\mathcal{A}$ is a complete lattice, then $G.\mathcal{A}$ is a complete lattice. For $X \subseteq G.\mathcal{A}$ we have

a $\sqcup_{G.\mathcal{A}} X = G.\sqcup_{F.\mathcal{B}} (F.X) = G.\sqcup_{\mathcal{A}} (F.X)$,

b $\sqcap_{G.\mathcal{A}} X = G.\sqcap_{F.\mathcal{B}} (F.X) = G.\sqcap_{\mathcal{A}} (F.X)$.

□

So we have the following result.

Theorem 4.43 If $\mathcal{A}$ or $\mathcal{B}$ is a complete lattice then $F.\mathcal{B}$ and $G.\mathcal{A}$ are isomorphic complete lattices.

□

This theorem is rarely cited in the literature. Only [MSS92] mentions this result.

Chapter 5

Application: The Domain Operator

We will now present a definition of what is called the *domain operator* in the spec calculus. In order to define such an operator, we first investigate what the domain operator in the relational calculus should do.

For a relation $R \subseteq \mathcal{A} \times \mathcal{B}$ we can identify two domains, the *left* and the *right* domain. —When restricted to functions, the left domain is usually called the range and the right domain is referred to as the domain. This asymmetrical naming convention for a function is induced by the asymmetrical properties of functions. The most prominent property is the direction of a function. For relations, there is no reason to impose such a distinction or to associate a direction. We therefore adopt the more anonymous names left and right domain.— A $y \in \mathcal{B}$ is in the right domain of the relation R iff there is an $x \in \mathcal{A}$ such that $x.R.y$ holds. In this setting, the domain of a relation is a set. In the spec calculus the sets are absent. One can model sets by subsets of the identity relation, called the *monotypes*. For A a subset of $\mathcal{A}$, we can define the monotype $\{(x,x) \mid x \in A\}$. So the domain operator that we want to construct maps arbitrary specs to monotypes. Before defining the domain operator, we first investigate the monotypes.

5.1 Monotypes

We call A a monotype iff $A \sqsubseteq I$. We adopt the convention that uppercase letters from the beginning of the alphabet denote monotypes. For monotypes we have the following properties.

Property 5.1 For A and B monotypes we have

a $A = A^{\cup}$,

b $A \circ B = A \sqcap B$.

□

These properties are easily seen when monotypes are interpreted in a relational setting. But they can also be proven from the axioms of the spec algebra, see [BVvdW91].

The monotypes form a subposet of the spec algebra. They even form a complete lattice with that ordering, although not a proper sublattice of the spec algebra. The supremum in the monotype lattice is the same as the supremum in the spec algebra. The infimum of a non-empty set of monotypes coincides with the infimum of the spec algebra. The neutral element of the infimum in the monotype lattice is the identity, whereas in the spec algebra this is the top. If we denote the supremum, respectively infimum, in the monotype lattice by $\sqcup_m$, respectively $\sqcap_m$, we have for every set of monotypes $\mathcal{V}$:

$$\sqcup_m \mathcal{V} \;=\; \sqcup \mathcal{V} \ ,$$

$$\sqcap_m \mathcal{V} \;=\; I \sqcap (\sqcap \mathcal{V}) \ .$$

We can safely drop the subscripts for the supremum. We will also drop the subscripts of the infimum for non-empty sets of monotypes. In case of a possibly-empty set of monotypes we will retain the subscript.

5.2 The monotype domain

Now it's time to formally define the right domain operator. We have already observed that our right domain operator should map arbitrary specs into monotypes and we have given an informal definition of the right domain at the beginning of the chapter. We now give an equivalent definition that lends itself better to be translated in the spec calculus in the form of a Galois connection. Let R be an endorelation over some universe, say $\mathcal{X}$. For a set A that contains the right domain of a spec R, we can embed the spec R in the set $\mathcal{X} \times A$. The right domain should be the least set with that property. Reading sets as monotypes, we arrive at the following definition.

Definition 5.2 For every spec R we define its right domain, the monotype $R{>}$, by:

$$R{>} \ \sqsubseteq_m \ A \quad \equiv \quad R \ \sqsubseteq \ \top\!\!\top \circ A \ ,$$

for all monotypes A.
□

The ordering of the monotypes coincides with the ordering of the specs, since the monotypes form a subposet of the specs. We will therefore drop the subscript indicating the monotype ordering.

The definition is given in the shape of a Galois connection. The lower adjoint is the domain operator, the upper adjoint is the function that maps a monotype A to $\top\!\!\top \circ A$. That function will be denoted by $(\top\!\!\top \circ)$. We have to prove that this is indeed a valid definition. Since the monotypes form a complete lattice, we have to show, according to theorem 4.37 that the function $(\top\!\!\top \circ)$ is universally $\sqcap_m$ junctive. That is for all sets of monotypes $\mathcal{V}$ we have to prove the following.

Theorem 5.3 $\top\!\!\top \circ \sqcap_m \ \mathcal{V} \ = \ \sqcap (\top\!\!\top \circ \mathcal{V})$.

Proof By monotonicity we have $\top\!\!\top \circ \sqcap_m \mathcal{V} \sqsubseteq \sqcap(\top\!\!\top \circ \mathcal{V})$. For the other containment we calculate as follows. Assume $Z \sqsubseteq \sqcap(\top\!\!\top \circ \mathcal{V})$, hence $(\forall A : A \in \mathcal{V} : Z \sqsubseteq \top\!\!\top \circ A)$. We have to prove $Z \sqsubseteq \top\!\!\top \circ \sqcap_m \mathcal{V}$.

$$
\begin{array}{ll}
 & Z \\
= & \quad \{ \text{ heading for } \top\!\!\top \circ X, \text{ with } X \sqsubseteq I \ \} \\
 & \top\!\!\top \circ I \sqcap Z \\
\sqsubseteq & \quad \{ \text{ dedekind } \} \\
 & \top\!\!\top \circ (\top\!\!\top \circ Z \sqcap I) \\
\sqsubseteq & \quad \{ \text{ see below } \} \\
 & \top\!\!\top \circ \sqcap_m \mathcal{V}
\end{array}
$$

Which is valid, since we have for any $A \in \mathcal{V}$

$$
\begin{array}{ll}
 & \top\!\!\top \circ Z \sqcap I \\
\sqsubseteq & \quad \{ \text{ assumption, } \top\!\!\top \circ \top\!\!\top = \top\!\!\top \ \} \\
 & \top\!\!\top \circ A \sqcap I \\
\sqsubseteq & \quad \{ \text{ dedekind } \} \\
 & (\top\!\!\top \sqcap I \circ A^{\cup}) \circ A \\
= & \quad \{ \text{ calculus } \} \\
 & A
\end{array}
$$

□

From theorem 5.3 we now conclude that $(\top\!\!\top \circ)$ has a lower adjoint, hence definition 5.2 is indeed a valid definition.

In order to explore the properties of our new operator, let's first make some easy instantiations.

Property 5.4

- **a** $R{>} \sqsubseteq I$,
- **b** $R \sqsubseteq \top\!\!\top \circ R{>}$,
- **c** $(\top\!\!\top \circ A){>} \sqsubseteq A$,
- **d** $R{>} = \perp\!\!\perp \equiv R = \perp\!\!\perp$,
- **e** $\perp\!\!\perp{>} = \perp\!\!\perp$.

Proof All of properties **a** to **e** are obtained by instantiations in definition 5.2. For **a** take $A := I$. This tells us nothing new. We already knew that the right domain operator maps arbitrary specs to monotypes, but it is reassuring that this is formally derivable. For **b** take $A := R{>}$. Property **c** is obtained by instantiating $R := \top\!\!\top \circ A$ and for **d**, respectively **e**, instantiate A, respectively R, to $\perp\!\!\perp$.

□

The properties 5.4(**b**) and 5.4(**c**) are referred to as cancellation properties. They are valid in every Galois connection, see cancellation. For Galois connections we have some more cancellation properties. If we instantiate semi-inverse we obtain the following

Property 5.5

a $(\top\!\!\top \circ R>)> \;=\; R>$,

b $\top\!\!\top \circ (\top\!\!\top \circ A)> \;=\; \top\!\!\top \circ A$.

□

The right domain operator is a mapping to the monotype lattice from a spec algebra. The spec algebra is also a complete lattice. With the use of theorem 4.36 this immediately gives the following

Property 5.6 The right domain operator is universally $\sqcup$-junctive.

□

This also implies that the right domain operator is monotonic. By the mere fact of the way the right domain operator is defined, we know some nice properties without having to prove them.

We still have more properties that we can extract from the general properties of Galois connections. But some of those properties can be improved upon. To that end we first observe some sort of analogue of property 5.4(**b**).

Theorem 5.7 $R> \;\sqsubseteq\; \top\!\!\top \circ R$.

Proof

$$
\begin{array}{ll}
 & R> \;\sqsubseteq\; \top\!\!\top \circ R \\
\equiv & \qquad \{ \text{ heading for the use of the Galois connection } \} \\
 & R> \;\sqsubseteq\; \top\!\!\top \circ R \sqcap I \\
\equiv & \qquad \{ \text{ Galois connection } \} \\
 & R \;\sqsubseteq\; \top\!\!\top \circ (\top\!\!\top \circ R \sqcap I)
\end{array}
$$

And this follows from

$$
\begin{array}{ll}
 & \top\!\!\top \circ (\top\!\!\top \circ R \sqcap I) \\
\sqsupseteq & \qquad \{ \; \top\!\!\top \;=\; \top\!\!\top^{\cup} \text{, dedekind } \} \\
 & \top\!\!\top \circ I \sqcap R \\
= & \qquad \{ \text{ calculus } \} \\
 & R
\end{array}
$$

□

Combining property 5.4(**b**) with theorem 5.7 we obtain the following very useful equality.

Theorem 5.8 $\top\!\!\top \circ R> \;=\; \top\!\!\top \circ R$.

Proof Composing the result of property 5.4(**b**) with $\top\!\!\top$, we obtain $\top\!\!\top \circ R \sqsubseteq \top\!\!\top \circ R>$. In the same way we deduce from theorem 5.7 that $\top\!\!\top \circ R> \sqsubseteq \top\!\!\top \circ R$ which completes the proof.

□

With this theorem we can also simplify the cancellation law mentioned in property 5.5(**a**).

Corollary 5.9 $(\top\!\top \circ R)> \;=\; R>$.
□

But we can get more out of theorem 5.8. We can now formulate and prove almost trivially some rewriting rules.

Theorem 5.10 The following three are equivalent:

- **a** $R> \;\sqsubseteq\; S>$,
- **b** $\top\!\top \circ R \;\sqsubseteq\; \top\!\top \circ S$,
- **c** $R \;\sqsubseteq\; \top\!\top \circ S$.

Proof From corollary 4.7 we obtain an equivalence between the following three statements

- $R> \;\sqsubseteq\; S>$,
- $\top\!\top \circ R> \;\sqsubseteq\; \top\!\top \circ S>$,
- $R \;\sqsubseteq\; \top\!\top \circ S>$.

The use of theorem 5.8 completes the proof.
□
As a result of this theorem, or instantiating corollary 4.14(**b**), we obtain the following

Corollary 5.11 $S> \;=\; R> \;\equiv\; \top\!\top \circ S \;=\; \top\!\top \circ R$.
□

What about the closed elements of the two adjoints? One set of closed elements is the range of the function $(\top\!\top \circ)$. A spec R is a closed element iff $\top\!\top \circ R> \;=\; R$. On account of theorem 5.8 this is equivalent to $\top\!\top \circ R \;=\; R$. A spec R for which this holds is called a *right condition*.

The other closed elements are an element of the range of the right domain operator. Actually every monotype is closed. In order to prove that this is the case, it is according to theorem 4.35 sufficient to prove that $(\top\!\top \circ)$ is a poset-monomorphism from monotypes.

Theorem 5.12 The function $(\top\!\top \circ)$ is a poset-monomorphism from monotypes. Or expressed differently, for all monotypes A and B we have

$$A \;\sqsubseteq\; B \quad\equiv\quad \top\!\top \circ A \;\sqsubseteq\; \top\!\top \circ B \;.$$

Proof

$$
\begin{array}{ll}
 & A \sqsubseteq B \\
\Rightarrow & \qquad \{ \text{ Leibniz with } (\top\!\!\top \circ) \ \} \\
 & \top\!\!\top \circ A \sqsubseteq \top\!\!\top \circ B \\
\Rightarrow & \qquad \{ \ A \sqsubseteq \top\!\!\top \circ A \ \} \\
 & A \sqsubseteq \top\!\!\top \circ B \\
\equiv & \qquad \{ \text{ calculus } \} \\
 & A \sqsubseteq A \sqcap \top\!\!\top \circ B \\
\Rightarrow & \qquad \{ \text{ dedekind } \} \\
 & A \sqsubseteq (\top\!\!\top \sqcap A \circ B^{\cup}) \circ B \\
\equiv & \qquad \{ \text{ calculus, property 5.1 } \} \\
 & A \sqsubseteq B
\end{array}
$$

□

With the aid of theorem 4.35, we can reformulate $(\top\!\!\top \circ)$ being a poset-monomorphism.

Property 5.13

a the right domain operator is surjective,

b the function $(\top\!\!\top \circ)$ is injective on monotypes,

c for all monotypes A we have $(\top\!\!\top \circ A){>} \ = \ A$.

□

The last expression indicates that all monotypes are closed elements of the right domain operator.

Dual to $(\top\!\!\top \circ)$ being a poset-monomorphism, we have that the right domain operator is a poset-monomorphism to monotypes from the right conditions, see corollary 4.9.

Property 5.14 For all right conditions p and q we have $p \sqsubseteq q \ \equiv \ p{>} \sqsubseteq q{>}$.

□

Actually, the right domain operator is a poset-isomorphism to monotypes from right conditions, since we observed in theorem 5.12 that the right domain operator is surjective.

Since the spec calculus is a complete lattice, we deduce from theorem 4.43 the following

Property 5.15 The monotypes and the right conditions form isomorphic complete lattices.

□

The infimum in the lattice of right conditions coincides with the infimum in the spec lattice, see theorem 4.38. In general the suprema in the range of the upper adjoint are not particularly attractive, see theorem 4.39. But in this case it is not so bad.

Theorem 5.16 The suprema in the lattice of right conditions coincide with the suprema in the spec lattice.

Proof For $\mathcal{V}$ a set of right conditions, the supremum in the lattice of right conditions is given by $\top\!\!\top \circ \sqcup\, (\mathcal{V}>)$, see theorem 4.39. We derive

$$\begin{array}{ll}
 & \top\!\!\top \circ \sqcup\, (\mathcal{V}>) \\
= & \quad \{ \text{ composition is universally } \sqcup\text{-junctive } \} \\
 & \sqcup\, (\top\!\!\top \circ \mathcal{V}>) \\
= & \quad \{ \text{ theorem 5.8 } \} \\
 & \sqcup\, (\top\!\!\top \circ \mathcal{V}) \\
= & \quad \{ \ \mathcal{V} \text{ is a set of right conditions } \} \\
 & \sqcup\, \mathcal{V}
\end{array}$$

□

So the lattice of right conditions is a proper sublattice of the spec lattice.

The function $(\top\!\!\top\, \circ)$ preserves all infima in the monotype lattice, see theorem 5.3. It also preserves all suprema in the monotype lattice, since all monotypes are in the range of the right domain. Actually, the function $(\top\!\!\top\, \circ)$ preserves all suprema in a spec lattice.

The right domain operator preserves all suprema in the spec lattice. From corollary 4.18 we deduce that all infima in the lattice of right conditions are preserved. So for every set $\mathcal{V}$ of specs we have

Property 5.17 $\sqcap_m(\mathcal{V}>) \;=\; (\sqcap\, \mathcal{V})> \quad \Leftarrow \quad \top\!\!\top \circ \mathcal{V} \;=\; \mathcal{V}$.

□

In order to conclude something more about the behaviour of the right domain with respect to the infimum of a finite non-empty set we can use the next theorem.

Theorem 5.18 $(R \sqcap S \circ T)> \;=\; (S^{\cup} \circ R \sqcap T)>$.

Proof We only have to prove one containment. The other one follows by some renaming, take $R, S, T := T, S^{\cup}, R$.

$$\begin{array}{ll}
 & (S^{\cup} \circ R \sqcap T)> \;\sqsubseteq\; (R \sqcap S \circ T)> \\
\equiv & \quad \{ \text{ Galois connection } \} \\
 & S^{\cup} \circ R \sqcap T \;\sqsubseteq\; \top\!\!\top \circ (R \sqcap S \circ T)> \\
\Leftarrow & \quad \{ \text{ heading for dedekind } \} \\
 & S^{\cup} \circ R \sqcap T \;\sqsubseteq\; S^{\cup} \circ \top\!\!\top \circ (R \sqcap S \circ T)> \\
\Leftarrow & \quad \{ \text{ dedekind } \} \\
 & R \sqcap S \circ T \;\sqsubseteq\; \top\!\!\top \circ (R \sqcap S \circ T)> \\
\Leftarrow & \quad \{ \text{ property 5.4}(\mathbf{b}) \ \} \\
 & \mathsf{true}
\end{array}$$

□

By the instantiation $T := I$ in theorem 5.18 and using properties of monotypes, especially theorem 5.25, we find the behaviour of the right domain operator with respect to the infimum.

Corollary 5.19 $(R \sqcap S)> \;=\; R^{\cup} \circ S \sqcap I$.

□

But this last corollary gives more properties. Instantiating $S := R$ in corollary 5.19 we get

Corollary 5.20 $R> \;=\; R^{\cup} \circ R \sqcap I$.

□

And instantiating $S := \top\!\!\top$ in corollary 5.19 we find

Corollary 5.21 $R> \;=\; \top\!\!\top \circ R \sqcap I$.

□

Each of the last two corollaries provides a closed expression for the right domain operator. One could also have come up with either one of these as a definition of the right domain operator. However, when subsequently calculating with the right domain operator, one can only replace the occurrences of the domain operator with its definition and then use the calculation rules for the constituents of the right domain operator. In contrast, when the definition is in the shape of a Galois connection calculations tend to be on a higher level of abstraction. The Galois connection provides a useful calculation rule and eliminates the need for a low-level calculation in most cases. The foregoing calculations provide a nice illustration of the calculational benefits of a Galois connection.

The properties of the right domain operator encountered thus far form a substantial part of the theorems about the right domain operator. Other properties about the right domain operator might be less obvious from the Galois connection, but the calculational properties derived from the Galois connection are useful when proving more theorems.

If one is interested in the right domain of a composition $(R \circ S)$, only the right domain of R is of importance.

Theorem 5.22 $(R \circ S)> \;=\; (R> \circ S)>$.

Proof

$$
\begin{array}{ll}
 & (R \circ S)> \;=\; (R> \circ S)> \\
\equiv & \qquad \{ \text{ theorem 5.10 } \} \\
 & \top\!\!\top \circ R \circ S \;=\; \top\!\!\top \circ R> \circ S \\
\equiv & \qquad \{ \text{ theorem 5.8 } \} \\
 & \mathsf{true}
\end{array}
$$

□

Since $R> \sqsubseteq I$ we find, using theorem 5.22, that one cannot enlarge the right domain of a spec by composing another spec to its left.

Corollary 5.23 $S> \;\sqsupseteq\; (R \circ S)>$.

□

This corollary could also be obtained using corollary 5.9.

There is some sort of trade-off between the right conditions and the monotypes. We already observed that they form isomorphic lattices. But instead of the domains in terms of monotypes, one could also use right conditions to model some sort of domain.

Theorem 5.24 $R \sqcap \top\!\!\top \circ S \;=\; R \circ S{>}$.

Proof

$$
\begin{array}{ll}
 & R \sqcap \top\!\!\top \circ S \;=\; R \circ S{>} \\
\equiv & \qquad \{\ \top\!\!\top \circ S = \top\!\!\top \circ S{>} \sqsupseteq R \circ S{>} \text{ and } I \sqsupseteq S{>} \text{ , monotonicity }\ \} \\
 & R \sqcap \top\!\!\top \circ S \sqsubseteq R \circ S{>} \\
\Leftarrow & \qquad \{\ \text{dedekind }\ \} \\
 & I \sqcap R^{\cup} \circ \top\!\!\top \circ S \sqsubseteq S{>} \\
\Leftarrow & \qquad \{\ R^{\cup} \circ \top\!\!\top \sqsubseteq \top\!\!\top \text{ , monotonicity }\ \} \\
 & I \sqcap \top\!\!\top \circ S \sqsubseteq S{>} \\
\equiv & \qquad \{\ \text{corollary 5.21 }\ \} \\
 & \mathsf{true}
\end{array}
$$

□

The Galois connection is in a way asymmetric. It relates monotypes to specs. The monotypes are specs, but specs are in general not monotypes. Hence it is a perfectly valid question to ask what the domain of a monotype is. We expect something extra when combining monotypes and the domain operator. Indeed, monotypes are fix-points of the domain operator.

Theorem 5.25 For all monotypes B we have $B \;=\; B{>}$.

Proof For any monotype A, we derive

$$
\begin{array}{ll}
 & B{>} \sqsubseteq A \\
\equiv & \qquad \{\ \text{Galois connection }\ \} \\
 & B \sqsubseteq \top\!\!\top \circ A \\
\equiv & \qquad \{\ \Rightarrow \text{Leibniz with } (\top\!\!\top \circ);\ \Leftarrow B \sqsubseteq \top\!\!\top \circ B\ \} \\
 & \top\!\!\top \circ B \sqsubseteq \top\!\!\top \circ A \\
\equiv & \qquad \{\ \text{theorem 5.12 }\ \} \\
 & B \sqsubseteq A
\end{array}
$$

□

There is another way of defining the right domain operator. Not by a closed formula but also in the form of an equivalence, however not as a Galois connection. This definition gives a hint as to why it is called the *right domain*.

Theorem 5.26 $R{>} \sqsubseteq A \quad \equiv \quad R \circ A = R$.

Proof Note that the right-hand side of the equivalence can be weakened to $R \sqsubseteq R \circ A$ on account of monotonicity.

$$
\begin{array}{ll}
 & R{>} \sqsubseteq A \\
\equiv & \quad \{ \text{ Galois connection } \} \\
 & R \sqsubseteq \top\!\!\top \circ A \\
\equiv & \quad \{ \text{ calculus } \} \\
 & R \sqsubseteq R \sqcap \top\!\!\top \circ A \\
\equiv & \quad \{ \text{ theorem 5.24, } A = A{>} \ \} \\
 & R \sqsubseteq R \circ A
\end{array}
$$

□

This could also serve as the definition of the right domain operator. In that case one also has to prove that this is a valid definition. For definitions in the form of a Galois connection it is obvious what the proof obligation is, that is the contents of theorem 5.3. For a definition that has the shape of theorem 5.26 it is not clear what that proof obligation is. Well, actually it is clear. One has to prove that there is a least monotype satisfying $A :: R \circ A = R$ for every spec R. But apart from that, there is not, in full generality, some theorem like theorem 4.37 that gives an alternative proof obligation as is the case for Galois connections. On top of that we still have some properties for free in the case of a Galois connection, properties that are not easily seen with another definition.

But there are still some useful properties one can deduce from theorem 5.26. If we instantiate $A := R{>}$ we obtain

Corollary 5.27 $R \circ R{>} = R$.
□

In the beginning of this section, we also mentioned the left domain of a spec. The left domain can be defined in a similar way as has been done for the right domain in theorem 5.2. One can then verify how the left and right domain of a spec are related by the use of the converse. Or one can define the left domain as the right domain of the converse of a relation. One can that easily, if one wants, verify the Galois connection for the left domain. We adopt the former approach.

Definition 5.28 For every spec R we define its left domain, the monotype $R{<}$, by:

$$R{<} \sqsubseteq A \quad \equiv \quad R \sqsubseteq A \circ \top\!\!\top \ ,$$

for every monotype A.
□

The proof that this indeed is a Galois connection follows directly from theorem 5.3 by use of the converse and some simplifying properties.

As already indicated, the left and right domain of a spec are related.

Theorem 5.29 $R_{>} \;=\; (R^{\cup})_{<}$

Proof For any $A \sqsubseteq I$ we derive

$$\begin{array}{ll}
 & (R^{\cup})_{<} \sqsubseteq A \\
\equiv & \qquad \{ \text{ definition 5.28 } \} \\
 & R^{\cup} \;\sqsubseteq\; A \circ \top\!\!\top \\
\equiv & \qquad \{ \text{ property 5.1, } \top\!\!\top^{\cup} \;=\; \top\!\!\top \;\; \} \\
 & R \;\sqsubseteq\; \top\!\!\top \circ A \\
\equiv & \qquad \{ \text{ theorem 5.2 } \} \\
 & R_{>} \sqsubseteq A
\end{array}$$

□

These are not all the properties that are valid for the domain operator(s). But the objective was not to give a complete overview. The purpose of this section is to derive the properties in a smooth calculational way, and to illustrate the point that Galois connections can be used for that.

In retrospect I think both points are proven. By the use of a Galois connection there are some properties that come for free. For other properties and their proof, extensive use is made of the general properties of Galois connections, see for example the proof of theorem 5.10. Instead of trying to find all properties of a new concept by hard work, one can use the Galois connection to obtain properties like cancellation laws, rewrite rules and junctivity theorems for free. This then immediately gives a sound basis for further exploration of the newly-introduced concept.

Chapter 6

Conclusion

In mathematics there is a multitude of abstractions, only some of which are well-chosen and firmly rooted in everyday mathematical knowledge and discourse. Many mathematical abstractions, in contrast, are insignificant either because they are so specific that they have very few applications and hardly deserve the name "abstraction", or because they are so general that their formulation is hideously complex and yet their properties are very weak. The notion of a Galois connection is, in our view, an abstraction that fully deserves a place in the everyday language of mathematics because it has many instances which are easy to recognise, it has a clear, attractive definition, and it has a whole host of properties that make the notion a delight to work with.

We have tried to illustrate these attributes of the notion in this report. We have discussed several applications of the notion, some old, some not so old. In each case our aim has been to show how the definition of a function via a Galois connection combined with a formal syntactic style of calculation can lead to clean, straightforward derivations of significant theorems. The variety of properties enjoyed by Galois connections has been reported on in some depth. That one can manage to discover tens of different, non-trivial, theorems starting with a definition that can be stated in a couple of lines of text is one of the beauties of mathematics. The practical consequences are substantial: recognition of a Galois connection immediately leads to a rich collection of calculationally-useful properties (in particular, the cancellation, semi-inverse and junctivity properties).

We have also tried to illustrate in this report the benefits of a formal, calculational approach to doing mathematics. The observation that suprema and infima are characterised by a Galois connection is possibly the best but not the only example. Of course, the theorems we have presented can and —almost without exception— have been derived in a non-calculational way, but the calculational style, combined with the recognition of the appropriate abstractions, cannot be bettered for elegance, power and simplicity.

Acknowledgements

It would be impossible to give credit to everyone who has had an influence on the making of this report. The list would simply be too long. There are some people who deserve special mentioning.

In the first place I am grateful to Roland Backhouse who guided me during the last couple of months, and made numerous suggestions for improvement of this report and my overall style of producing English text. During the latter stages Jaap van der Woude was a great help. I remember that someone once mentioned that Jaap had the annoying habit of always finding a shorter proof. Several of the short proofs in this report are due to him.

During the "afstudeerperiode" I attended the Mathematics of Programming Club. In those meetings I saw numerous new and interesting things. For me it was the first time to observe research taking place, and I enjoyed it.

The work presented here could not have been done without the continuing support of my parents. They, together with my girl-friend, always managed to cheer me up at times when it didn't go as smoothly as I had anticipated. There is one person who deserves a special mentioning. Without Paul I wouldn't have come this far. I owe him more than he realises, and I thank him for being more than a good friend.

Bibliography

[Bac91] Roland C. Backhouse, editor. *EURICS Workshop : Calculational Theories of Program Structure*. EURICS, 1991.

[Bir67] Garrett Birkhoff. *Lattice Theory*, volume XXV of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Provedence, Rhode Island, third edition, 1967.

[BVvdW91] Roland Backhouse, Ed Voermans, and Jaap van der Woude. A relational theory of datatypes. In Backhouse [Bac91].

[Con71] J. H. Conway. *Regular Algebra and Finite Machines*. Chapman and Hall Mathematics Series. William Clowes & Sons Ltd., London and Colchester, first edition, 1971.

[DF88] Edsger W. Dijkstra and W.H.J. Feijen. *A Method of Programming*. Addison-Wesley, Amsterdam, 1988.

[Dil39] R. P. Dilworth. Non-commutative residuated lattices. *Transactions of the American Mathematical Society*, 46:426–444, 1939.

[DP90] B. A. Davey and H. A. Priestly. *Introduction to Lattices and Order*. Cambridge Mathematical Textbooks. Cambridge University Press, first edition, 1990.

[DS90] Edsger W. Dijkstra and Carel S. Scholten. *Predicate Calculus and Program Semantics*. Text and Monographs in Computer Science. Springer-Verlag, New York, 1990.

[Eve44] C.J. Everett. Closure operators and galois theory in lattices. *Trans. Amer. Math. Soc.*, 55:514–525, 1944.

[GHK+80] G. Gierz, K. H. Hofmann, K. Keimel, J. D. Lawson, M. Mislove, and D. S. Scott. *A Compendium of Continuous Lattices*. Springer-Verlag, 1980.

[GKP89] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics : a Foundation for Computer Science*. Addison-Wesley Publishing Company, 1989.

[HH85] Horst Herrlich and Miroslav Hušek. Galois connections. In *Proc. Math. Foundation of Prog. Semantics*, number 239 in Lecture Notes in Computer Science, pages 122–134, 1985.

[HJ86] C.A.R. Hoare and He Jifeng. The weakest prespecification. *Fundamenta Informaticae*, 9:51–84, 217–252, 1986.

[Mac71] Saunders Mac Lane. *Categories For The Working Mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1971.

[MSS86] A. Melton, D. A. Schmidt, and G. E. Strecker. Galois connections and computer science applications. In David Pitt, Samson Abramsky, Axel Poigné, and David Rydeheard, editors, *Category Theory and Computer Programming*, number 240 in Lecture Notes in Computer Science, pages 299–312. Springer-Verlag, 1986.

[MSS92] Austin Melton, Bernd S.W. Schröder, and George E. Strecker. Connections. In *To appear in: Proc. Math. Foundation of Prog. Semantics*, Lecture Notes in Computer Science, 1992.

[Ore44] Oystein Ore. Galois connexions. *Trans. Amer. Math. Soc.*, 55:493–513, 1944.

[RB88] David E. Rydeheard and Rod M. Burstall. *Computational Category Theory*. Prentice Hall International Series in Computer Science. Prentice Hall, first edition, 1988.

[Rig48] J. Riguet. Relations binaires, fermetures, correspondances de galois. *Bull. Soc. Math. France*, 76:114–155, 1948.

[Sch53] J. Schmidt. Beitrage für filtertheorie. II. *Math. Nachr.*, 10:197–232, 1953.