Journal of Logical and Algebraic Methods in Programming 85 (2016) 921–930

Contents lists available at ScienceDirect

Journal of Logical and Algebraic Methods in Programming

www.elsevier.com/locate/jlamp

Kernels, in a nutshell

Jeremy Gibbons

Department of Computer Science, University of Oxford, United Kingdom

ARTICLE INFO

Article history:
Received 11 June 2015
Received in revised form 11 October 2015
Accepted 17 October 2015
Available online 10 November 2015

For José Nuno Oliveira, on his 60th birthday

ABSTRACT

A classical result in algebraic specification states that a total function defined on an initial algebra is a homomorphism if and only if the kernel of that function is a congruence. We expand on the discussion of that result from an earlier paper: extending it from total to *partial functions*, simplifying the proofs using *relational calculus*, and generalising the setting to *regular categories*.

1. Introduction

When is a function a fold? In one sense, the definition of *fold* says it all:

$$\begin{aligned}&\mathit{fold} : \mathit{Functor}\,\mathsf{F} \Rightarrow (\mathsf{F}\,A \to A) \to \mu\mathsf{F} \to A\\&\mathit{fold}_{\mathsf{F}}\,f\,(\mathrm{in}_{\mathsf{F}}\,x) = f\,(\mathsf{F}\,(\mathit{fold}_{\mathsf{F}}\,f)\,x)\end{aligned}$$

A function $h : \mu\mathsf{F} \to a$ can be written in the form of a fold precisely when there exists an $f : \mathsf{F}\,A \to A$ such that $h = \mathit{fold}_{\mathsf{F}}\,f$. For example, with $\mathsf{L}\,A = 1 + \mathit{Nat} \times A$ as the shape functor for lists of naturals, $\mathit{sum} : \mu\mathsf{L} \to \mathit{Nat}$ is a fold: indeed, $\mathit{sum} = \mathit{fold}_{\mathsf{L}}\,\mathit{add}$ where

$$\begin{aligned}&\mathit{add}\,(\mathit{Inl}\,()) &&= 0\\&\mathit{add}\,(\mathit{Inr}\,(m, n)) &&= m + n\end{aligned}$$

But $\mathit{allEqual} : \mu\mathsf{L} \to \mathit{Bool}$, the predicate testing that all elements of a list have the same value, is not a fold: with a little effort (for example, considering lists of length 0, 1, and 2), one can convince oneself that there exists no f with $\mathit{allEqual} = \mathit{fold}_{\mathsf{L}}\,f$.

However, this criterion is a little unsatisfying. One can use the existence of f as a criterion to prove that h is a fold, by exhibiting the f; but it is harder to use it to disprove that h is a fold, since it is harder to provide evidence for the non-existence of any such f. The criterion is *intensional*, referring to some property f of the implementation of h, which we may not yet have to hand. We might hope for an *extensional* criterion instead, expressed purely in terms of the behaviour of h rather than of any possible implementation.

An extensional but incomplete answer is given by the observation that if h is injective, so that there exists a post-inverse h' with $h' \circ h = \mathit{id}$, then

$$h = \mathit{fold}_{\mathsf{F}}\,(h \circ \mathrm{in}_{\mathsf{F}} \circ \mathsf{F}\,h')$$

E-mail address: jeremy.gibbons@cs.ox.ac.uk.
URL: http://www.cs.ox.ac.uk/jeremy.gibbons/.

http://dx.doi.org/10.1016/j.jlamp.2015.10.006

and so h is a fold. But injectivity is only a sufficient condition, not a necessary one—indeed, *sum* is a fold, despite not being injective. So again this observation is no help in showing that a function is not a fold.

In this paper, we discuss a necessary and sufficient condition for h to be a fold. The result was presented in an earlier paper [6]. It turns out to be a standard result in algebraic specification; see for example [4, §3.10]. We elaborate on that earlier work here. Our original presentation was purely in set-theoretic terms, treating functions as sets of pairs, and limited to total functions. Here, we point out a straightforward extension to *partial functions*, and we consider an *allegorical* (that is, axiomatic relational) presentation, which turns out to be rather simpler, and one in terms of *regular categories*, which is a bit more flexible.

In the interests of brevity, we talk only about folds and postfactors. There's a dual story about prefactors, but the most useful connection with unfolds isn't quite one of duality (because dualising 'partial function' isn't very helpful). We leave the details for the curious reader to explore for themselves.

2. Totally

In this section, we work in the category $\mathcal{S}et$, in which the objects are sets and the arrows are total functions between sets. In particular, a function $f : A \to B$ is a triple consisting of the source A, the target B, and the graph, the set of pairs $\{(a,b) \mid a \in A \wedge b = f\,a \in B\}$. We write $\mathsf{ran}\,f \subseteq B$ for the range of f.

A crucial ingredient in the construction is the notion of the *kernel* of a function, that is, the set of pairs of arguments identified by the function.

Definition 1. The kernel $\mathsf{ker}\,f$ of a total function $f : A \to B$ is the set of pairs

$$\mathsf{ker}\,f = \{(a,a') \mid a, a' \in A \wedge f\,a = f\,a'\} \qquad \diamond$$

It is easy to see that this definition yields an equivalence relation on A.

Given $h : A \to C$ and $f : A \to B$, when can h be factorised into $g \circ f$ for some $g : B \to C$? It is clearly necessary for the function space $B \to C$ to be non-empty, that is, either $C \neq \emptyset$ or $B = \emptyset$; otherwise, there can be no such g. Given that proviso, a necessary and sufficient condition for the existence of such a postfactor g is for the kernel of h to include the kernel of f:

Theorem 2. *Given $h : A \to C$ and $f : A \to B$ such that $B \to C \neq \emptyset$,*

$$(\exists g : B \to C \,.\, h = g \circ f) \quad \Leftrightarrow \quad \mathsf{ker}\,h \supseteq \mathsf{ker}\,f \qquad \diamond$$

Proof. From left to right, suppose that $h = g \circ f$. Then

$$\begin{array}{ll} & (a,a') \in \mathsf{ker}\,h \\ \Leftrightarrow & [\![\text{ definition of kernel }]\!] \\ & h\,a = h\,a' \\ \Leftrightarrow & [\![\; h = g \circ f \;]\!] \\ & g\,(f\,a) = g\,(f\,a') \\ \Leftarrow & [\![\text{ Leibniz }]\!] \\ & f\,a = f\,a' \\ \Leftrightarrow & [\![\text{ definition of kernel }]\!] \\ & (a,a') \in \mathsf{ker}\,f \end{array}$$

which establishes the inclusion. From right to left, suppose that $\mathsf{ker}\,h \supseteq \mathsf{ker}\,f$; we construct g as follows. For $b \in \mathsf{ran}\,f$, pick any a such that $f\,a = b$, and define $g\,b = h\,a$; by the hypothesis, the choice of a does not affect the value of $g\,b$. For $b \notin \mathsf{ran}\,f$, define $g\,b$ arbitrarily; by the assumption that $B \to C \neq \emptyset$, this is possible (classically). $\square$

From this follows the main result of [6]:

Corollary 3. *For functor F such that the initial algebra $(\mu\mathsf{F}, \mathsf{in}_\mathsf{F})$ exists, and for $h : \mu\mathsf{F} \to A$,*

$$(\exists g \,.\, h = \mathit{fold}_\mathsf{F}\, g) \quad \Leftrightarrow \quad \mathsf{ker}\,(h \circ \mathsf{in}_\mathsf{F}) \supseteq \mathsf{ker}\,(\mathsf{F}\,h) \qquad \diamond$$

Proof. The connection to Theorem 2 comes from the universal property of *fold*:

$$\begin{array}{ll} & \exists g \,.\, h = \mathit{fold}_\mathsf{F}\, g \\ \Leftrightarrow & [\![\text{ universal property of fold }]\!] \\ & \exists g \,.\, h \circ \mathsf{in}_\mathsf{F} = g \circ \mathsf{F}\,h \end{array}$$

$$\begin{array}{ll} \Leftrightarrow & [\![\text{ Theorem 2 }]\!] \\ & \mathsf{ker}\,(h \circ \mathsf{in}_\mathsf{F}) \supseteq \mathsf{ker}\,(\mathsf{F}h) \end{array}$$

(Note that the side condition $\mathsf{F}A \to A \neq \emptyset$ follows from $\mu\mathsf{F} \to A \neq \emptyset$ [6], which follows in turn from the existence of h.) □

Remark 4. One can show that $\mathsf{ker}\,(\mathsf{F}h) = \mathsf{Rel}_\mathsf{F}(\mathsf{ker}\,h)$, where $\mathsf{Rel}_\mathsf{F}R$ denotes the *relational lifting* of the relation R on A to a relation acting pointwise on $\mathsf{F}A$. Moreover, since in_F is a bijection, $\mathsf{ker}\,(h \circ \mathsf{in}_\mathsf{F})$ is equivalent to just $\mathsf{ker}\,h$. Finally, given an F-algebra $f : \mathsf{F}A \to A$, we say that a relation R is an F-*congruence for* f if pointwise-related arguments are taken by f to related results:

$$(x, x') \in \mathsf{Rel}_\mathsf{F}R \quad \Rightarrow \quad (f\,x, f\,x') \in R$$

Then the condition $\mathsf{ker}\,(h \circ \mathsf{in}_\mathsf{F}) \supseteq \mathsf{ker}\,(\mathsf{F}h)$ in Corollary 3 is equivalent to saying that $\mathsf{ker}\,h$ is an F-congruence for in_F, which is the more traditional but less manipulable formulation. ◇

3. Partially

The simple characterisation above of the kernel of a total function needs adaptation, if it is to continue to serve as an equivalence relation on the source of a *partial* function:

Definition 5. The kernel $\mathsf{ker}\,f \subseteq A \times A$ of a partial function $f : A \nrightarrow B$ is the set of pairs

$$\begin{array}{l} \mathsf{ker}\,f = \{(a, a') \mid a, a' \in \mathsf{dom}\,f \wedge f\,a = f\,a'\} \\ \qquad \cup \{(a, a') \mid a, a' \in A - \mathsf{dom}\,f\} \end{array}$$ ◇

(writing $\mathsf{dom}\,f \subseteq A$ for the domain of definition of f). This denotes an equivalence relation again: two elements are equivalent iff they are treated equivalently by f. When f is in fact total, $\mathsf{dom}\,f = A$ and Definition 5 reduces to Definition 1.

A postfactor theorem similar to Theorem 2 can be proved for partial functions. The conditions need to be strengthened in one sense: clearly now it is necessary for $\mathsf{dom}\,f$ to include $\mathsf{dom}\,h$. But they may be weakened in another sense: we no longer need to assume a non-empty space of results, because partial functions exist even to empty sets.

Theorem 6. *Given partial functions $h : A \nrightarrow C$ and $f : A \nrightarrow B$,*

$$(\exists g : B \nrightarrow C \,.\, h = g \circ f) \quad \Leftrightarrow \quad \mathsf{ker}\,h \supseteq \mathsf{ker}\,f \wedge \mathsf{dom}\,h \subseteq \mathsf{dom}\,f$$ ◇

However, the proof is rather more awkward. It depends on the fact that $\mathsf{dom}\,(g \circ f) = \{a \in \mathsf{dom}\,f \mid f\,a \in \mathsf{dom}\,g\}$.

Proof. From left to right, suppose that $h = g \circ f$. Then

$$\begin{array}{ll} & a \in \mathsf{dom}\,h \\ \Leftrightarrow & [\![\; h = g \circ f \;]\!] \\ & a \in \mathsf{dom}\,(g \circ f) \\ \Leftrightarrow & [\![\text{ domain }]\!] \\ & a \in \mathsf{dom}\,f \wedge f\,a \in \mathsf{dom}\,g \\ \Rightarrow & [\![\text{ weakening }]\!] \\ & a \in \mathsf{dom}\,f \end{array}$$

As for the kernel inclusion, suppose $(a, a') \in \mathsf{ker}\,f$, so either (i) $a, a' \in \mathsf{dom}\,f$ and $f\,a = f\,a'$, or (ii) $a, a' \notin \mathsf{dom}\,f$. In case (i), either $f\,a, f\,a' \in \mathsf{dom}\,g$, when $a, a' \in \mathsf{dom}\,h$ and $h\,a = g\,(f\,a) = g\,(f\,a') = h\,a'$, so $(a, a') \in \mathsf{ker}\,h$; or $f\,a, f\,a' \notin \mathsf{dom}\,g$, when $a, a' \notin \mathsf{dom}\,h$, so $(a, a') \in \mathsf{ker}\,h$. Finally, in case (ii), again $a, a' \notin \mathsf{dom}\,h$ and so $(a, a') \in \mathsf{ker}\,h$.

From right to left, suppose that $\mathsf{ker}\,h \supseteq \mathsf{ker}\,f$ and $\mathsf{dom}\,h \subseteq \mathsf{dom}\,f$; we construct g with $\mathsf{dom}\,g = \{f\,a \mid a \in \mathsf{dom}\,h\}$ as follows. For $b \in \mathsf{dom}\,g$, pick any $a \in \mathsf{dom}\,h$ such that $f\,a = b$, and define $g\,b = h\,a$; by the hypothesis, the choice of a does not affect the result (for if $a, a' \in \mathsf{dom}\,h \subseteq \mathsf{dom}\,f$ with $f\,a = f\,a'$, then $(a, a') \in \mathsf{ker}\,f \subseteq \mathsf{ker}\,h$ and so $h\,a = h\,a'$). Of course, we do not have to consider $b \notin \mathsf{dom}\,g$, so we need no longer resort to classical reasoning. □

4. Allegorically

The construction in the proof of Theorem 2 essentially involves inverting f; this suggests that it might be worth exploring a presentation in terms of the relational calculus [2]. Rather than work concretely with relations as sets of pairs, as we did in Section 2 and in [6], we use the axiomatic presentation of a *division allegory* [5], falling back on sets of pairs only for the purposes of illustration. Formally, we consider typed relations $R : A \sim B$ 'from A to B'; intersection $R \cap S$ forming a semi-lattice, and inducing inclusion $R \subseteq S$ as a preorder on relations of a common type; identity *id* and composition $R \circ S$, forming a monoid, with composition monotonic with respect to $\subseteq$; converse R° forming an involution, contravariant with respect to composition and monotonic with respect to inclusion; and division operators R/S, $R\backslash S$ discussed in more detail below. One additional and non-obvious axiom is required, the so-called *modular law* $(R \circ S) \cap T \subseteq (R \cap (T \circ S^\circ)) \circ S$.

Four special classes of relations are identified as follows:

$$\begin{array}{llll} R \text{ injective:} & R^\circ \circ R \subseteq id & R \text{ simple:} & R \circ R^\circ \subseteq id \\ R \text{ entire:} & R^\circ \circ R \supseteq id & R \text{ surjective:} & R \circ R^\circ \supseteq id \end{array}$$

We say that R is *coreflexive* if $R \subseteq id$. The *domain* of a relation is defined by

$$\mathsf{dom}\, R = (R^\circ \circ R) \cap id$$

with the universal property that $\mathsf{dom}\, R$ is the smallest coreflexive S that may be extracted as a prefactor:

$$\mathsf{dom}\, R \subseteq S \quad \Leftrightarrow \quad R \subseteq R \circ S \qquad \text{– for coreflexive } S$$

Lemma 7. $R \circ \mathsf{dom}\, R = R$ ◇

Proof. We have:

$$\begin{array}{ll} & R \circ \mathsf{dom}\, R \\ \subseteq & [\![\ \mathsf{dom}\, R \text{ is coreflexive} \ ]\!] \\ & R \\ \subseteq & [\![\ \text{instantiate } S = \mathsf{dom}\, R \text{ in universal property of domain} \ ]\!] \\ & R \circ \mathsf{dom}\, R \end{array}$$

□

Right and left division are characterised by their universal properties

$$\begin{array}{lllll} T \subseteq R/S & \Leftrightarrow & T \circ S \subseteq R & & \\ T \subseteq S\backslash R & \Leftrightarrow & S \circ T \subseteq R & \Leftrightarrow & S \subseteq R/T \end{array}$$

These are the least familiar of the operators of the relational calculus, but they are truly central: $(/S)$ forms a Galois connection with $(\circ S)$, and $(S\backslash)$ with $(S\circ)$, and Galois connections—more generally, adjunctions—underlie most of the structural equivalences we use in program calculation [9].

The appropriate notion of kernel for relations in general is as follows [1]:

Definition 8. The kernel $\mathsf{ker}\, R$ of a relation R is given by

$$\begin{array}{rl} \mathsf{ker}\, R & = (R\backslash R) \cap (R\backslash R)^\circ \\ & = (R\backslash R) \cap (R^\circ / R^\circ) \end{array}$$

◇

In terms of concrete sets of pairs, the quotients reduce to the following constructions:

$$\begin{array}{lll} (a,b) \in R/S & \Leftrightarrow & (\forall c \,.\, (a,c) \in R \Leftarrow (b,c) \in S) \\ (a,c) \in S\backslash R & \Leftrightarrow & (\forall b \,.\, (b,c) \in R \Leftarrow (b,a) \in S) \end{array}$$

and therefore

$$\mathsf{ker}\, R = \{(a,a') \mid \forall b \,.\, (a,b) \in R \Leftrightarrow (a',b) \in R\}$$

In particular, when R is simple, so equivalent to a partial function, this agrees with the definition of kernels in Section 3.

We identify three useful lemmas about kernels, which we will need for the proof of Theorem 12 on postfactors for simple relations, analogous to Theorem 2 and Theorem 6.

Lemma 9. *Kernels enjoy the universal property that*

$$\mathsf{ker}\, R \supseteq S \quad \Leftrightarrow \quad R \supseteq R \circ S \ \wedge \ R \supseteq R \circ S^\circ$$

◇

Proof. This follows from the universal properties of the components:

$$\begin{array}{ll}
& \mathrm{ker}\,R \supseteq S \\
\Leftrightarrow & \llbracket \text{ definition of kernel } \rrbracket \\
& ((R\backslash R) \cap (R\backslash R)^\circ) \supseteq S \\
\Leftrightarrow & \llbracket \text{ universal property of intersection } \rrbracket \\
& (R\backslash R \supseteq S) \wedge ((R\backslash R)^\circ \supseteq S) \\
\Leftrightarrow & \llbracket \text{ converse preserves inclusion } \rrbracket \\
& (R\backslash R \supseteq S) \wedge (R\backslash R \supseteq S^\circ) \\
\Leftrightarrow & \llbracket \text{ universal property of division } \rrbracket \\
& R \supseteq R \circ S \;\wedge\; R \supseteq R \circ S^\circ
\end{array}$$

□

Lemma 10. *$R^\circ \circ R \subseteq \mathrm{ker}\,R$ for simple R.* ◇

Proof. We have

$$\begin{array}{ll}
& \mathrm{ker}\,R \supseteq R^\circ \circ R \\
\Leftrightarrow & \llbracket \text{ universal property of kernel } \rrbracket \\
& R \supseteq R \circ R^\circ \circ R \;\wedge\; R \supseteq R \circ (R^\circ \circ R)^\circ \\
\Leftrightarrow & \llbracket \text{ the conjuncts are equivalent, by contravariance of converse } \rrbracket \\
& R \supseteq R \circ R^\circ \circ R \\
\Leftarrow & \llbracket \text{ monotonicity } \rrbracket \\
& id \supseteq R \circ R^\circ
\end{array}$$

□

Lemma 11. *$R \circ \mathrm{ker}\,R \subseteq R$* ◇

Proof. We have:

$$\begin{array}{ll}
& R \circ \mathrm{ker}\,R \subseteq R \\
\Leftrightarrow & \llbracket \text{ universal property of division } \rrbracket \\
& \mathrm{ker}\,R \subseteq R\backslash R \\
\Leftrightarrow & \llbracket \text{ definition of kernel } \rrbracket \\
& true
\end{array}$$

□

Theorem 12. *For simple $T : A \sim C$ and $R : A \sim B$, there exists simple $S : B \sim C$ with $T = S \circ R$ iff $\mathrm{ker}\,R \subseteq \mathrm{ker}\,T$ and $\mathrm{dom}\,R \supseteq \mathrm{dom}\,T$.* ◇

Proof. From left to right, suppose $T = S \circ R$. Then

$$\begin{array}{ll}
& \mathrm{ker}\,R \subseteq \mathrm{ker}\,T \\
\Leftrightarrow & \llbracket \text{ assumption } \rrbracket \\
& \mathrm{ker}\,R \subseteq \mathrm{ker}\,(S \circ R) \\
\Leftrightarrow & \llbracket \text{ universal property of kernel } \rrbracket \\
& S \circ R \supseteq S \circ R \circ \mathrm{ker}\,R \;\wedge\; S \circ R \supseteq S \circ R \circ (\mathrm{ker}\,R)^\circ \\
\Leftrightarrow & \llbracket\ \mathrm{ker}\,R \text{ is symmetric, so the two conjuncts are equivalent } \rrbracket \\
& S \circ R \supseteq S \circ R \circ \mathrm{ker}\,R \\
\Leftarrow & \llbracket \text{ monotonicity } \rrbracket \\
& R \supseteq R \circ \mathrm{ker}\,R \\
\Leftrightarrow & \llbracket \text{ Lemma 11 } \rrbracket \\
& true
\end{array}$$

and

$$\begin{array}{ll}
& \mathrm{dom}\,R \supseteq \mathrm{dom}\,T \\
\Leftrightarrow & \llbracket \text{ assumption } \rrbracket \\
& \mathrm{dom}\,R \supseteq \mathrm{dom}\,(S \circ R) \\
\Leftrightarrow & \llbracket \text{ universal property of domain } (\mathrm{dom}\,R \text{ is coreflexive}) \rrbracket \\
& S \circ R \circ \mathrm{dom}\,R \supseteq S \circ R \\
\Leftrightarrow & \llbracket \text{ Lemma 7 } \rrbracket \\
& true
\end{array}$$

(We don't actually need the assumption that R, S, and hence T are simple.) Conversely, suppose the kernel and domain inclusions on R, T, and define $S = T \circ R^\circ$. Then $T = S \circ R$:

$$\begin{array}{ll}
& T \\
= & [\![\ \text{Lemma 7}\ ]\!] \\
& T \circ \mathsf{dom}\, T \\
\subseteq & [\![\ \text{assumption}\ ]\!] \\
& T \circ \mathsf{dom}\, R \\
\subseteq & [\![\ \text{definition of domain}\ ]\!] \\
& T \circ R^\circ \circ R \qquad \text{— which is } S \circ R \\
\subseteq & [\![\ \text{Lemma 10—by assumption, } R \text{ is simple}\ ]\!] \\
& T \circ \mathsf{ker}\, R \\
\subseteq & [\![\ \text{assumption}\ ]\!] \\
& T \circ \mathsf{ker}\, T \\
\subseteq & [\![\ \text{Lemma 11}\ ]\!] \\
& T
\end{array}$$

Moreover, S is simple:

$$\begin{array}{ll}
& S \circ S^\circ \\
= & [\![\ \text{definition of } S\ ]\!] \\
& S \circ R \circ T^\circ \\
= & [\![\ \text{by the above, } S \circ R = T\ ]\!] \\
& T \circ T^\circ \\
\subseteq & [\![\ \text{by assumption, } T \text{ is simple}\ ]\!] \\
& id
\end{array}$$

□

Note that this proof establishes the result in the more general setting of simple relations, that is, partial rather than total functions, with no extra fuss. In contrast, the proof of Theorem 6 is rather more complicated than the proof of Theorem 2, with an awkward case analysis.

5. Categorically

One might wonder whether the full structure of a division allegory is necessary for the postfactors result to hold: the proof in Section 4 uses division heavily, but the more concrete one in Section 2 does not. What abstract structure is actually required?

Definition 13 *(Kernel pair).* The categorical analogue of the kernel of a function is the *kernel pair* of an arrow, the pullback of the arrow along itself:

$$\begin{tikzcd}
 & & A \arrow[dr, "f"] & \\
Y \arrow[urr, bend left, "q_0"] \arrow[drr, bend right, "q_1"'] \arrow[r, dashed, "r"] & \mathsf{ker} f \arrow[ur, "p_0"'] \arrow[dr, "p_1"] \arrow[r, phantom, "\rangle"] & & B \\
 & & A \arrow[ur, "f"'] &
\end{tikzcd}$$

That is, the kernel pair of $f : A \to B$ is an object X and arrows $p_0, p_1 : X \to A$ satisfying $f \circ p_0 = f \circ p_1$, with the universal property that, for any other object Y with arrows $q_0, q_1 : Y \to A$ satisfying $f \circ q_0 = f \circ q_1$, there is a unique mediating arrow $r : Y \to X$ such that $q_0 = p_0 \circ r$ and $q_1 = p_1 \circ r$. ◇

Such pullbacks do not always exist. They always do in $\mathcal{S}et$, when the object X is just the set of pairs $\mathsf{ker} f$ from Definition 1, and p_0, p_1 are the left and right projections; that justifies the use of '$\mathsf{ker} f$' for X in the commuting diagram above. More generally, a *finitely complete* category possesses all finite limits, and in particular pullbacks and hence kernel pairs. But for these kernel pairs to be in some sense well behaved, we need a couple of extra conditions as well.

Definition 14 *(Epimorphism, monomorphism).* An arrow $g : B \to C$ is an *epimorphism* if it is right-cancellable, in the sense that for any $h_0, h_1 : C \to D$, if $h_0 \circ g = h_1 \circ g$ then $h_0 = h_1$.

$$\begin{tikzcd} A \arrow[r, bend left, "f_0"] \arrow[r, bend right, "f_1"'] & B \arrow[r, "g"] & C \arrow[r, bend left, "h_0"] \arrow[r, bend right, "h_1"'] & D \end{tikzcd}$$

Dually, g is a *monomorphism* if it is left-cancellable: for any $f_0, f_1 : A \to B$, if $g \circ f_0 = g \circ f_1$ then $f_0 = f_1$. ◇

In $\mathcal{S}et$, the epimorphisms are the surjections, and the monomorphisms the injections. By convention, we draw epimorphisms in commuting diagrams with double headed arrows $\twoheadrightarrow$ and monomorphisms with hook-tailed arrows $\hookrightarrow$.

Definition 15 *(Coequaliser).* We say that arrow $g : B \to C$ *coequalises* a parallel pair of arrows $f_0, f_1 : A \to B$ if $g \circ f_0 = g \circ f_1$. The *coequaliser* of f_0, f_1 is a universal such C and g—that is, for any other object D and arrow $h : B \to D$ that coequalises f_0, f_1, there is a unique mediating arrow $r : C \to D$ such that $h = r \circ g$.

$$\begin{tikzcd} A \arrow[r, bend left, "f_0"] \arrow[r, bend right, "f_1"'] & B \arrow[r, "g"] \arrow[dr, "h"'] & C \arrow[d, dashed, "r"] \\ & & D \end{tikzcd}$$

◇

In $\mathcal{S}et$, the coequaliser object C is the quotient of B by the smallest equivalence relation $\equiv$ such that $\forall a \in A \,.\, f_0\,a \equiv f_1\,a$; that is, the reflexive, symmetric, transitive closure of the relation induced by f_0, f_1. It is an instructive exercise to verify that the coequaliser is necessarily an epimorphism (whatever the category). Not all epimorphisms arise as coequalisers; those that do are called the *regular epimorphisms*.

Definition 16 *(Regular category).* A *regular category* is one: that is finitely complete (so in particular has all kernel pairs); in which every kernel pair has a coequaliser; and in which regular epimorphisms are stable under pullbacks—that is, if g in the commuting diagram below is a regular epimorphism, then so is p_1.

$$\begin{tikzcd} X \arrow[r, "p_0"] \arrow[d, two heads, "p_1"'] \arrow[dr, phantom, "\lrcorner", very near start] & A \arrow[d, two heads, "g"] \\ A \arrow[r, "f"'] & B \end{tikzcd}$$

The category $\mathcal{S}et$ is regular. ◇

Definition 17 *(Relation).* One can define a notion of 'relation' $R : A \sim B$ via a span $A \leftarrow R \rightarrow B$: in a Cartesian category (that is, one with products), R is modelled as a monomorphism $R \hookrightarrow A \times B$ into the product:

$$\begin{tikzcd} & R \arrow[dl] \arrow[d, hook] \arrow[dr] & \\ A & A \times B \arrow[l, "fst"] \arrow[r, "snd"'] & B \end{tikzcd}$$

(To be more precise, one should consider equivalence classes of such spans under isomorphisms between their apices R. One can also remove the dependence on products by requiring that the two legs of the span are *jointly monic*, suitably defined.) ◇

In $\mathcal{S}et$, this directly corresponds to thinking of R as a subset of $A \times B$. But constructing the composition of relations involves taking a pullback of spans:

$$\begin{tikzcd} & & \bullet \arrow[dl] \arrow[dr] \arrow[dd, phantom, "\lrcorner" rotate=-45, very near start] & & \\ & R \arrow[dl] \arrow[dr] & & S \arrow[dl] \arrow[dr] & \\ A & & B & & C \end{tikzcd}$$

(and then taking the 'image', as discussed above: the arrow from the apex to $A \times C$ is typically not a monomorphism); in order for this composition to be associative, one needs the additional well-behavedness properties of a regular category [5, §1.569]. So regular categories are a somewhat necessary phenomenon in thinking about relational programming; for a recent crisp summary, see [7, Section 2].

Definition 18 *(Partial map).* Similarly, one can define a *partial map* $f : A \nrightarrow B$ in a category as a span with a monomorphic left leg:

$$\begin{tikzcd} & \mathsf{dom} f \arrow[dl, hook'] \arrow[dr, "\bar{f}"] & \\ A & & B \end{tikzcd}$$

writing $\bar{f} : \mathsf{dom} f \to B$ for the restriction of f to its domain (again, up to equivalences arising from isomorphisms on the apices). Composition is again constructed by pullbacks of spans. ◇

Lemma 19 *(Image factorisation). An important result about regular categories is that every arrow $f : A \to B$ factorises into a regular epimorphism followed by a monomorphism.*

$$\begin{tikzcd} \mathsf{ker} f \arrow[r, shift left] \arrow[r, shift right] & A \arrow[rr, "f"] \arrow[dr, two heads, "e"'] & & B \\ & & \mathsf{img} f \arrow[ur, hook, dashed, "m"'] & \end{tikzcd}$$

Indeed, an alternative chacterisation of regular categories is that they have finite limits and image factorisations, stable under pullbacks. ◇

In $\mathcal{S}et$, $\mathsf{img} f$ is $A_{/f}$, the quotient of A into equivalence classes according to f; that is, two elements $a, a' \in A$ are equivalent iff $f\,a = f\,a'$ (in other words, $(a, a') \in \mathsf{ker} f$). So one can think of e as taking an element of A to its equivalence class, and m mapping this class into B. Equivalently, one can think of e as being f but with the target restricted precisely to the range of f, and m as the embedding of the range back into the target: $A_{/f}$ is isomorphic to $\mathsf{ran} f$. For more about image factorisation, see Taylor [13].

Theorem 20. *Given arrows $f : A \to B$ and $h : A \to C$ in a regular category, there exists a partial map $g : B \nrightarrow C$ such that $h = g \circ f$ if and only if there exists an arrow $i : \mathsf{ker} f \to \mathsf{ker}\, h$ satisfying $p_0 = q_0 \circ i$ and $p_1 = q_1 \circ i$, where p_0, p_1 and q_0, q_1 are the kernel pairs of f and h respectively.* ◇

Proof. The situation is illustrated in the diagram below:

$$\begin{tikzcd} & \mathsf{ker} f \arrow[dl, "i"'] \arrow[d, shift right, "p_0"'] \arrow[d, shift left, "p_1"] & \\ \mathsf{ker}\, h \arrow[r, shift left, "q_0"] \arrow[r, shift right, "q_1"'] & A \arrow[r, "h"] \arrow[d, "f"'] \arrow[dr, two heads, "e"] & C \\ & B & \mathsf{img} f \arrow[l, hook', "m"] \arrow[u, dashed, "k"'] \end{tikzcd}$$

From right to left, suppose we are given i making the two upper left triangles commute; we construct g as follows. Let $m \circ e$ be the image factorisation of f (making the lower left triangle commute), so that e is the coequaliser of p_0, p_1. Now h also coequalises p_0, p_1:

$$h \circ p_0 = h \circ q_0 \circ i = h \circ q_1 \circ i = h \circ p_1$$

so by the universal property of the coequaliser there exists a unique mediating arrow $k : \mathsf{img} f \to C$ making the upper right triangle commute. We define partial map $g : B \nrightarrow C$ to be the span $B \xhookleftarrow{m} \mathsf{img} f \xrightarrow{k} C$.

We have to show that $h = g \circ f$ as partial maps. Since f and h are in fact total, their domain coincides with their source, and the monomorphic left legs of the spans are the identity. So for the composition $g \circ f$, we have the following situation:

$$\begin{tikzcd}
 & & X \arrow[dl] \arrow[dr] \arrow[dd, phantom, "\lrcorner" {rotate=-45}, very near start] & & \\
 & A \arrow[dl, equal] \arrow[dr, "f"] & & \mathsf{img}\,f \arrow[dl, hook', "m"'] \arrow[dr, "k"] & \\
A & & B & & C
\end{tikzcd}$$

and we have to show that the outer span equals h. Let us factor f into $m \circ e$, and see what effect this has on the pullback diamond:

$$\begin{tikzcd}
 & & X \arrow[ddll, "a"'] \arrow[dr, "b"] & & \\
 & & & Y \arrow[ddll, "c"'] \arrow[dr, "d"] & \\
A \arrow[dr, two heads, "e"'] & & & & \mathsf{img}\,f \arrow[ddll, hook', "m"] \\
 & \mathsf{img}\,f \arrow[dr, hook, "m"'] & & & \\
 & & B & &
\end{tikzcd}$$

We use two simple standard facts about pullbacks, both of which are straightforward to prove. Firstly, the pullback of a monomorphism along itself is the identity; so $Y = \mathsf{img}\,f$, and $c = d = id$. Secondly, a pullback of the identity (c) is again the identity; so $a = id$, and hence $X = A$ and $b = e$. Therefore, the outer span is indeed $A = A \xrightarrow{k \circ e = h} C$ as required.

Conversely, given $h = g \circ f$, and kernel pairs p_0, p_1 for f and q_0, q_1 for h, we construct the mapping $i : \mathsf{ker}\,f \to \mathsf{ker}\,h$ as follows:

$$\begin{tikzcd}
 & & A \arrow[dr, "h"] \arrow[drr, two heads, "f"] & & \\
\mathsf{ker}\,f \arrow[r, dashed, "i"] \arrow[urr, "p_0"] \arrow[drr, "p_1"'] & \mathsf{ker}\,h \arrow[ur, "q_0"] \arrow[dr, "q_1"'] \arrow[r, phantom, ">"] & & C & B \arrow[l, "g"'] \\
 & & A \arrow[ur, "h"'] \arrow[urr, two heads, "f"'] & &
\end{tikzcd}$$

We have that p_0, p_1 form a cone over $A \xrightarrow{h} C \xleftarrow{h} A$:

$$h \circ p_0 = g \circ f \circ p_0 = g \circ f \circ p_1 = h \circ p_1$$

so by the universal property of the pullback, there exists a (unique) mediating arrow $i : \mathsf{ker}\,f \to \mathsf{ker}\,h$ making the triangles $p_0 = q_0 \circ i$ and $p_1 = q_1 \circ i$ commute. □

Have we gained anything by abstracting from $\mathcal{S}et$ to regular categories? If $\mathcal{S}et$ were the only regular category, the answer would be 'no' (or at least, 'not much': it is still nice to see precisely which axioms are used, even if those axioms admit just one model). However, it is a standard result [3] that any category of Eilenberg–Moore algebras over $\mathcal{S}et$ is also regular. In particular, one can think of partial functions over sets as point-preserving total functions over pointed sets, which are the homomorphisms between algebras for the monad $(1+)$; therefore the category $\mathcal{P}fun$ of sets and partial functions is equivalent to the category of Eilenberg–Moore algebras for this monad, and hence is regular. So the categorical story is more flexible; we can instantiate it for free at least to partial functions.

6. Conclusions

I presented a preliminary version of Section 2 at Meeting #55 of IFIP WG2.1 in Cochabamba in January 2001; Lambert Meertens simplified my proofs there. The work was subsequently published at CMCS 2001 [6], jointly written with Graham

Hutton and Thorsten Altenkirch, whose contributions were invaluable. Bart Jacobs also made some helpful observations about congruences and images, pointing me towards his paper [8].

Thanks to comments received at CMCS, I saw how to generalise from total functions to partial functions; I presented the more general results at Meeting #56 of WG2.1, in Ameland in September 2001—precisely while the tragedy of the twin towers was unfolding. Roland Backhouse encouraged me there to use the relational definition $\mathsf{ker}\,R = (R \backslash R) \cap (R \backslash R)^{\circ}$ of kernels from Section 4, but we didn't manage to complete the proof in the relational style at the meeting. (This notion of kernel turns out to date back at least to 1948 [12]; it is a special case $\mathsf{ker}\,R = \mathsf{syq}(R, R)$ of the 'symmetric quotient' used by Schmidt and by Winter in this volume.) In October 2005, José Oliveira invited me to take part in a PURe Workshop in Braga; that was the spur I needed to complete the relational proofs (helped by Shin-Cheng Mu), which I presented there. José liked the results, because it turned out to be related to work he was doing on pointfree functional dependency theory [10]; he encouraged me to write those results up, but I've never had the excuse to make time for it—until now! (Note that the relational definition of kernels used here is in general incomparable to the definition $\mathsf{ker}\,R = R^{\circ} \circ R$ used by José himself [10,11] as a stepping stone towards his 'injectivity preorder' on relations.)

For help with the categorical construction, I am indebted to Maciej Piróg for pointing me towards regular categories; to James McKinna, Ohad Kammar, and Bob Harper, for enlightening discussions; and especially to Sam Staton, who sketched out the proof of Theorem 20 for me.

Acknowledgements

This work was partially supported by EPSRC grants *Datatype-Generic Programming* (GR/S27078/01) and *A Theory of Least Change for Bidirectional Transformations* (EP/K020919/1).

References

[1] Roland C. Backhouse, Jaap van der Woude, Domain operators and domain kinds, in: STOP Workshop on Galois Connections, Utrecht, 1993. Available from http://www.cs.nott.ac.uk/~rcb/MPC/perorder.ps.gz.

[2] Richard Bird, Oege de Moor, Algebra of Programming, Prentice-Hall, 1997.

[3] Francis Borceux, Handbook of Categorical Algebra, vol. 2, Cambridge University Press, 1994.

[4] Hartmut Ehrig, Bernd Mahr, Fundamental of Algebraic Specification, EATCS Monographs on Theoretical Computer Science, vol. 1, Springer-Verlag, 1985.

[5] Peter J. Freyd, Andre Scedrov, Categories, Allegories, in: Mathematical Library, vol. 39, North-Holland, 1990.

[6] Jeremy Gibbons, Graham Hutton, Thorsten Altenkirch, When is a function a fold or an unfold? Electron. Proc. Theor. Comput. Sci. 44 (1) (April 2001), Coalgebraic Methods in Computer Science.

[7] Chris Heunen, Sean Tull, Categories of relations as models of quantum theory, in: Chris Heunen, Peter Selinger, Jamie Vicary (Eds.), Proceedings of the 12th International Workshop on Quantum Physics and Logic (QPL 2015), Oxford, U.K., July 15–17, 2015, Electron. Proc. Theor. Comput. Sci. 195 (2015) 247–261, http://dx.doi.org/10.4204/EPTCS.195.18, arXiv:1506.05028.

[8] Bart Jacobs, Mongruences and cofree coalgebras, in: V.S. Alagar, M. Nivat (Eds.), Algebraic Methodology and Software Technology, in: LNCS, vol. 936, Springer, 1995, pp. 245–260.

[9] Shin-Cheng Mu, José Nuno Oliveira, Programming from Galois connections, J. Log. Algebr. Program. 81 (6) (2012) 680–704.

[10] José Nuno Oliveira, Functional dependency theory made 'simpler', Technical report DI-PURe-05.01.01, Departamento de Informática da Universidade do Minho, January 2005.

[11] José Nuno Oliveira, Transforming data by calculation, in: Ralf Lämmel, Joost Visser, João Saraiva (Eds.), Generative and Transformational Techniques in Software Engineering II, in: LNCS, vol. 5235, Springer, 2008, pp. 134–195.

[12] Jacques Riguet, Relations binaires, fermetures, correspondances de Galois, Bull. Soc. Math. Fr. 76 (1948) 114–155.

[13] Paul Taylor, Practical Foundations of Mathematics, Studies in Advanced Mathematics, Cambridge University Press, 1999.