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

A R T I C L E I N F O

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

A B S T R A C T

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). □

From this follows the main result of [6]:

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

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

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

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