When is a function a fold or an unfold?

Jeremy Gibbons
University of Oxford
WG2.1#57, April 2003

1. Universal property as characterization

Folds:

$$h = \mathsf{fold}_{\mathcal{F}}\ f \quad \Leftrightarrow \quad h \cdot \mathsf{in} = f \cdot \mathcal{F}\ h$$

Unfolds:

$$h = \mathsf{unfold}_{\mathcal{F}}\ f \quad \Leftrightarrow \quad \mathsf{out} \cdot h = \mathcal{F}\ h \cdot f$$

Exact characterizations, but *intensional* rather than *extensional*.
Also require *second-order quantifications*.

2. Partial extensional characterizations

An injection is a fold:

> For injective total function h, there exists a g with $g \cdot h = \mathsf{id}$.
> So $h = \mathsf{fold}_{\mathcal{F}}\ (h \cdot \mathsf{in} \cdot \mathcal{F}\ g)$.

Dually, a surjection is an unfold:

> For surjective function h, there exists a g with $h \cdot g = \mathsf{id}$.
> So $h = \mathsf{unfold}_{\mathcal{F}}\ (\mathcal{F}\ g \cdot \mathsf{out} \cdot h)$.

But these are only implications. Not all folds are injections, nor all unfolds surjections.

3. Earlier results (CMCS2001): Folds

Define $\mathsf{ker}\ f = f^{\circ} \cdot f$.

Say 'f is an $\mathcal{F}$-congruence for g' if $g \cdot \mathcal{F}\ f \subseteq f \cdot g$.
(Usually used when f is an equivalence.)

Theorem:

> Total function h is a fold iff $\mathsf{ker}\ h$ is an $\mathcal{F}$-congruence for in.

For example, 'safe tail' function

$$stail\ xs = \mathbf{if}\ null\ xs\ \mathbf{then}\ xs\ \mathbf{else}\ tail\ xs$$

is not a fold, because lists with equal safe-tails are not closed under cons.

Results dualize too.

4. Last meeting (#56, September 2001)

Result for folds generalizes to partial functions too.

But the elegant relational proof I had did not generalize.

5. Quotients and kernels

Define quotients $\backslash$ and $/$ by

$$X \subseteq R \backslash S \quad \Leftrightarrow \quad R \cdot X \subseteq S$$
$$X \subseteq S \,/\, R \quad \Leftrightarrow \quad X \cdot R \subseteq S$$

Revise definition of kernel to:

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

(Coincides with earlier definition for simple and entire R.)

Define

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

6. When is a partial function a fold?

Theorem:

For simple R, exists simple S with $R = \mathsf{fold}_{\mathcal{F}}\ S$ iff

$$\mathsf{ker}\ (\mathcal{F}\ R) \subseteq \mathsf{ker}\ (R \cdot \mathsf{in}) \quad \wedge \quad \mathsf{dom}\ (\mathcal{F}\ R) \supseteq \mathsf{dom}\ (R \cdot \mathsf{in})$$

6.1. Lemma: Simple postfactors

Theorem is a direct corollary of this lemma:

For simple R, T, exists simple S with $T = S \cdot R$ iff

$$\mathsf{ker}\ R \subseteq \mathsf{ker}\ T \quad \wedge \quad \mathsf{dom}\ R \supseteq \mathsf{dom}\ T$$

(with $R := \mathcal{F}\ R$ and $T := R \cdot \mathsf{in}$).

6.2. Sublemma

Kernel has a universal property (from definition of quotient):

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

(ie $\mathsf{ker}\ R$ is largest S with $R \supseteq R \cdot S \cap R \cdot S^{\circ}$).

Hence $Q^{\circ} \cdot Q \subseteq \mathsf{ker}\ Q$ for simple Q:

$$\begin{array}{ll} & Q^{\circ} \cdot Q \subseteq \mathsf{ker}\ Q \\ \Leftrightarrow & \quad \{\text{UP of kernel}\} \\ & Q \supseteq Q \cdot Q^{\circ} \cdot Q \wedge Q \supseteq Q \cdot Q^{\circ} \cdot Q \\ \Leftarrow & \quad \{\text{monotonicity}\} \\ & \mathsf{id} \supseteq Q \cdot Q^{\circ} \\ \Leftrightarrow & \\ & Q \text{ is simple} \end{array}$$

6.3. Another sublemma

$$
\begin{array}{ll}
 & Q \cdot \mathsf{ker}\ Q \subseteq Q \\
\Leftrightarrow & \quad \{\text{quotient}\} \\
 & \mathsf{ker}\ Q \subseteq Q \setminus Q \\
\Leftrightarrow & \quad \{\text{kernel}\} \\
 & \mathsf{true}
\end{array}
$$

6.4. Proof of lemma: Right to left

Let $S = T \cdot R^\circ$.

Then

$$T = T \cdot \mathsf{dom}\ T \subseteq T \cdot \mathsf{dom}\ R \subseteq T \cdot R^\circ \cdot R \quad (= S \cdot R)$$

and

$$T \cdot R^\circ \cdot R \subseteq T \cdot \mathsf{ker}\ R \subseteq T \cdot \mathsf{ker}\ T \subseteq T$$

Moreover, S is simple:

$$S \cdot S^\circ = S \cdot R \cdot T^\circ = T \cdot T^\circ \subseteq \mathsf{id}$$

6.5. Proof of lemma: Left to right

Conversely, suppose R, S simple, and let $T = S \cdot R$. Then

$$
\begin{array}{ll}
 & \mathsf{ker}\ R \subseteq \mathsf{ker}\ T \\
\Leftrightarrow & \\
 & \mathsf{ker}\ R \subseteq \mathsf{ker}\ (S \cdot R) \\
\Leftrightarrow & \qquad \{\text{UP of kernel}\} \\
 & S \cdot R \cdot \mathsf{ker}\ R \subseteq S \cdot R \quad \wedge \quad S \cdot R \cdot \mathsf{ker}\ R \subseteq S \cdot R \\
\Leftarrow & \qquad \{\text{symmetry; monotonicity}\} \\
 & R \cdot \mathsf{ker}\ R \subseteq R \\
\Leftrightarrow & \qquad \{\text{lemma; } R \text{ simple}\} \\
 & \mathsf{true}
\end{array}
$$

and

$$
\mathsf{dom}\ R \supseteq \mathsf{dom}\ T \quad \Leftrightarrow \quad \mathsf{dom}\ R \supseteq \mathsf{dom}\ (S \cdot R) \quad \Leftrightarrow \quad \mathsf{true}
$$

7. When is a partial function an unfold?

Define $\mathsf{ran}\ R = R \cdot R^{\circ} \cap \mathsf{id}$.

Lemma (simple prefactors):

For simple R, T, exists simple S with $T = R \cdot S$ iff

$$\mathsf{ran}\ R \supseteq \mathsf{ran}\ T$$

Theorem (a corollary):

For simple R, exists simple S with $R = \mathsf{unfold}\ S$ iff

$$\mathsf{ran}\ (\mathcal{F}\ R) \supseteq \mathsf{ran}\ (\mathsf{out} \cdot R)$$

(Generalizes ‘surjective function is an unfold’.)

7.1. Proof of lemma: Right to left

By symmetry, we'd expect to let $S = R^\circ \cdot T$, but in general this is not simple.

Instead, choose $Q \subseteq R^\circ$ such that Q is simple yet $\mathsf{dom}\ Q = \mathsf{dom}\ R^\circ$, and let $S = Q \cdot T$.

(By Axiom of Choice, any relation has a simple domain-preserving refinement).

We'll show that $T = R \cdot S = R \cdot Q \cdot T$.

7.2. Sublemma

For simple relations, equality follows from inclusion and common domain:

For simple R, S,

$$R = S \quad \Leftarrow \quad R \subseteq S \wedge \mathsf{dom}\ R \supseteq \mathsf{dom}\ S$$

(Note that domain inclusion is equivalent to domain equality here.)

Proof uses shunting for simpletons.

7.3. Continuing proof of lemma

Want to show that $T = R \cdot Q \cdot T$.

By sublemma, suffices to show:
(i) T, $R \cdot Q \cdot T$ simple,

by construction

(ii) $T \supseteq R \cdot Q \cdot T$,

$T = \mathsf{ran}\ T \cdot T \subseteq \mathsf{ran}\ R \cdot T = R \cdot R^{\circ} \cdot T \subseteq T$ (because R simple)

(iii) $\mathsf{dom}\ T \subseteq \mathsf{dom}\ (R \cdot Q \cdot T)$.

$\mathsf{dom}\ (R \cdot Q \cdot T) = \mathsf{dom}\ ((\mathsf{dom}\ R) \cdot Q \cdot T) \supseteq$
$\mathsf{dom}\ ((\mathsf{ran}\ Q) \cdot Q \cdot T) = \mathsf{dom}\ (Q \cdot T) = \mathsf{dom}\ (\mathsf{dom}\ Q \cdot T) \supseteq$
$\mathsf{dom}\ (\mathsf{ran}\ R \cdot T) = \mathsf{dom}\ (R \cdot R^{\circ} \cdot T) = \mathsf{dom}\ T$

7.4. Proof of lemma: Left to right

Of course, if $T = R \cdot S$ then $\mathsf{ran}\ T \subseteq \mathsf{ran}\ R$.

8. Dualization

We have:

For simple R, exists simple S with $R = \mathsf{fold}_{\mathcal{F}}\ S$ iff

$$\mathsf{ker}\ (\mathcal{F}\ R) \subseteq \mathsf{ker}\ (R \cdot \mathsf{in}) \quad \wedge \quad \mathsf{dom}\ (\mathcal{F}\ R) \supseteq \mathsf{dom}\ (R \cdot \mathsf{in})$$

and

For simple R, exists simple S with $R = \mathsf{unfold}\ S$ iff

$$\mathsf{ran}\ (\mathcal{F}\ R) \supseteq \mathsf{ran}\ (\mathsf{out} \cdot R)$$

They are not each other's duals, because we broke the symmetry by insisting on simplicity.

Therefore their respective duals are worth investigating.

8.1. When is an injection an unfold?

Define $\mathsf{img}\ R = \mathsf{ker}\ R^{\circ} = (R\ /\ R) \cap (R\ /\ R)^{\circ}$.

Lemma (on injective prefactors):

For injective R, T, exists injective S with $T = R \cdot S$ iff

$$\mathsf{img}\ R \subseteq \mathsf{img}\ T \quad \wedge \quad \mathsf{ran}\ R \supseteq \mathsf{ran}\ T$$

(In fact, exists injective such S iff exists *any* such S.)

Theorem (a corollary):

For injective R, exists injective S with $R = \mathsf{unfold}\ S$ iff

$$\mathsf{img}\ (\mathcal{F}\ R) \subseteq \mathsf{img}\ (\mathsf{out} \cdot R) \quad \wedge \quad \mathsf{ran}\ (\mathcal{F}\ R) \supseteq \mathsf{ran}\ (\mathsf{out} \cdot R)$$

8.2. When is an injection a fold?

Lemma (on injective postfactors):

For injective R, T, exists injective S with $T = S \cdot R$ iff

$$\mathsf{dom}\ R \supseteq \mathsf{dom}\ T$$

(Again, 'exists injective' is redundant:
exists injective such S iff exists any such S.)

Theorem (a corollary):

For injective R, exists injective S with $R = \mathsf{fold}_{\mathcal{F}}\ S$ iff

$$\mathsf{dom}\ (\mathcal{F}\ R) \supseteq \mathsf{dom}\ (R \cdot \mathsf{in})$$

(Generalizes 'injective total function is a fold'.)