TECHNICAL CONTRIBUTIONS

On Induced Congruences

Roland Backhouse
Grant Malcolm

Groningen University

In this note we present a proof of a theorem to be found in Ehrig and Mahr [3]. The theorem states that a relation constructed from a given function is a congruence relation iff that function is a homomorphism: we go on to generalise this result to the relational homomorphisms treated by the first author in [1]. Specifically, we prove that a congruence relation can be constructed from a relational homomorphism. Our construction generalises that of Ehrig and Mahr. The significance of this note lies both in the economy of our calculations and in the novel use we make of weakest prespecifications.

We have been unable to extend the theorem to an equivalence: we offer the remaining half of the equivalence as a challenge to the reader.

We consider a type $\mathcal{T}$ defined according to the paradigm $\mathcal{T} = \mu(\tau : \mathsf{F})$, where F is a *relator* (such types are special cases of "Hagino types", details of which may be found in Hagino [4]). For the purposes of this note, the important properties of a relator F are the following.

- if α is a type, then $\alpha\mathsf{F}$ is a type;
- if $f \in \alpha \leftarrow \beta$ is a function, then there is a function $f\mathsf{F} \in \alpha\mathsf{F} \leftarrow \beta\mathsf{F}$;
- if $R \in \alpha \sim \beta$ is a relation, then there is a relation $R\mathsf{F} \in \alpha\mathsf{F} \sim \beta\mathsf{F}$;
- $R\mathsf{F} \circ S\mathsf{F} = (R \circ S)\mathsf{F}$, for R and S either functions or relations (in fact, we shall adopt the position that functions are special cases of relations, with the property that $x\langle f\rangle y \equiv x = f.y$: hence composition of relations and of functions is the same thing);
- $\mathrm{I}\mathsf{F} = \mathrm{I}$, where I denotes the identity relation of the appropriate type;
- if $R \supseteq S$, then $R\mathsf{F} \supseteq S\mathsf{F}$; and
- $(R\mathsf{F})^{\cup} = (R^{\cup})\mathsf{F}$, where $R^{\cup}$ denotes the reverse of relation R; i.e., for all x and y of the appropriate types, $x\langle R^{\cup}\rangle y \equiv y\langle R\rangle x$.

The type $\mathcal{T}$ can be viewed as the least fixed point of the relator F, whose constructor is the total function $\tau \in \mathcal{T} \leftarrow \mathcal{T}\mathsf{F}$. The type enjoys the following unique extension property: given $R \in \beta \sim \beta\mathsf{F}$, there is a unique relation $(\!|R|\!) \in \beta \sim \mathcal{T}$ which satisfies

$$(\!|R|\!) \circ \tau = R \circ (\!|R|\!)\mathsf{F}. \tag{1}$$

Moreover, if R is a function, so too is $(\!|R|\!)$.

As already remarked, we consider functions to be special cases of relations; their additional properties are captured in the following definition.

Definition 1 (total functions) That f is a function is expressed by

(functionality) $\quad \mathrm{I} \supseteq f \circ f^{\cup}$

and that it is total by

(totality) $\quad f^{\cup} \circ f \supseteq \mathrm{I}.$

Moreover, f is injective iff $f^{\cup}$ is functional, and f is surjective iff $f^{\cup}$ is total. □

Definition 2 For $R \in \alpha \sim \beta$ and $S \in \gamma \sim \delta$, the relation $R \longleftarrow S \in (\alpha \leftarrow \gamma) \sim (\beta \leftarrow \delta)$ is defined by: for all f and g,

$$f(R \longleftarrow S)g \quad \equiv \quad R \circ g \supseteq f \circ S.$$

□

This overloading of the $\leftarrow$ operator as a constructor of both types and relations has been used severally by Wadler, de Bruin and Backhouse [6,2,1] to investigate properties of polymorphic functions. Such overloading encourages us to confuse types and relations yet further and write $\epsilon \in R$ if $\epsilon(R)\epsilon$.

The relational calculus allows us to formulate the following elegant definition of congruence relations.

Definition 3 (congruence) Relation $R \in \mathcal{T} \sim \mathcal{T}$ is a congruence relation if it is an equivalence relation and respects the structure of $\mathcal{T}$: that is, if R is reflexive: $R \supseteq \mathrm{I}$, transitive: $R \supseteq R \circ R$, symmetric: $R = R^{\cup}$, and furthermore $\tau \in R \longleftarrow R^{\mathsf{F}}$.
□

Elementary properties of equivalence relations will be assumed, namely: R is reflexive iff $R^{\cup}$ is reflexive, and R is transitive iff $R^{\cup}$ is transitive.

We now prove the theorem on congruence relations from Ehrig and Mahr ([3], p. 77).

Theorem 4 (induced congruences) For total functions $f \in B \leftarrow \mathcal{T}$, $f^{\cup} \circ f$ is a congruence relation if and only if f is a homomorphism.

Proof: by mutual implication.

($\Leftarrow$): It is straightforward to show that $f^{\cup} \circ f$ is an equivalence relation, for all functions f; we prove only that a homomorphism $f = (\!|g|\!)$ respects the structure of $\mathcal{T}$; i.e., $\tau \in (f^{\cup} \circ f) \longleftarrow (f^{\cup} \circ f)^{\mathsf{F}}$. By definition 2, this means we have to show that

$$f^{\cup} \circ f \circ \tau \supseteq \tau \circ (f^{\cup} \circ f)^{\mathsf{F}}.$$

We calculate as follows:

$$\begin{array}{ll} & f^{\cup} \circ f \circ \tau \\ \supseteq & \quad \{ \text{ functionality of } \tau \ \} \\ & \tau \circ \tau^{\cup} \circ f^{\cup} \circ f \circ \tau \\ = & \quad \{ \text{ reverse } \} \\ & \tau \circ (f \circ \tau)^{\cup} \circ f \circ \tau \\ = & \quad \{ (1), \text{ twice } \} \\ & \tau \circ (g \circ f^{\mathsf{F}})^{\cup} \circ g \circ f^{\mathsf{F}} \\ = & \quad \{ \text{ reverse } \} \\ & \tau \circ f^{\mathsf{F}\cup} \circ g^{\cup} \circ g \circ f^{\mathsf{F}} \\ \supseteq & \quad \{ \text{ totality of } g; \text{ relators } \} \\ & \tau \circ (f^{\cup} \circ f)^{\mathsf{F}} \end{array}$$

($\Rightarrow$): Suppose now that $f^{\cup} \circ f$ is a congruence relation; i.e.

(2) $$f^{\cup} \circ f \circ \tau \supseteq \tau \circ (f^{\cup} \circ f)^{\mathsf{F}}.$$

We have to find $g \in \beta \leftarrow \beta^{\mathsf{F}}$ such that $(\!|g|\!) = f$. From type considerations alone we are led to the following choice: $g \triangleq f \circ \tau \circ (f^{\cup})^{\mathsf{F}}$ and we must show

(3) $$f \circ \tau = g \circ f^{\mathsf{F}}$$

whence by the unique extension property, $(\!|g|\!) = f$, and thus f is a homomorphism. We prove (3) by mutual inclusion:

$$\begin{array}{ll} & g \circ f^{\mathsf{F}} \\ = & \quad \{ \text{ defn. } g \ \} \\ & f \circ \tau \circ (f^{\cup})^{\mathsf{F}} \circ f^{\mathsf{F}} \\ = & \quad \{ \text{ relators } \} \\ & f \circ \tau \circ (f^{\cup} \circ f)^{\mathsf{F}} \\ \supseteq & \quad \{ \text{ totality of } f; \text{ monotonicity; identity } \} \\ & f \circ \tau \end{array}$$

So far we have not used that $f^{\cup} \circ f$ is a congruence; we do need that assumption to prove the other inclusion:

$$\begin{array}{ll} & g \circ f^{\mathsf{F}} \\ = & \quad \{ \text{ defn. } g, \text{ relators } \} \\ & f \circ \tau \circ (f^{\cup} \circ f)^{\mathsf{F}} \\ \subseteq & \quad \{ (2) \ \} \\ & f \circ f^{\cup} \circ f \circ \tau \\ \subseteq & \quad \{ \text{ functionality of } f \ \} \\ & f \circ \tau \end{array}$$

Note that, in general, g need not be a total function, since it makes use of $f^{\cup}$. However, functionality of g follows straightforwardly from the property that $f^{\cup} \circ f$ is a congruence; a sufficient condition for g to be total is that f be surjective.
□

In the above, a congruence relation was constructed from a functional homomorphism; we now turn to the question of whether it is possible to generalise this to the construction of a congruence relation from a *relational* homomorphism. We formulate the generalised construction with the aid of the following definition.

Definition 5 For a relation $R \in \alpha \sim \beta$, the relation $R\dagger \in \beta \sim \beta$ is defined by the following property: for all S,

$$R\dagger \supseteq S \quad \equiv \quad R \supseteq R \circ S.$$

□

The relation $R\dagger$ is the "weakest prespecification" $R \backslash R$ of Hoare and He Jifeng (see [5]); its equational presentation lends itself well to the sort of calculational style of proof in which we are interested.

Theorem 6 $f\cup \circ f = f\dagger$.
Proof: we first note that for all R, $f\cup \circ f \supseteq R \quad \equiv \quad f \supseteq f \circ R$:

$$\begin{array}{ll} & f \supseteq f \circ R \\ \Rightarrow & \quad \{ \text{ monotonicity } \} \\ & f\cup \circ f \supseteq f\cup \circ f \circ R \\ \Rightarrow & \quad \{ \text{ totality of } f \} \\ & f\cup \circ f \supseteq R \\ \Rightarrow & \quad \{ \text{ monotonicity } \} \\ & f \circ f\cup \circ f \supseteq f \circ R \\ \Rightarrow & \quad \{ \text{ functionality of } f \} \\ & f \supseteq f \circ R \end{array}$$

Hence, by definition 5, $f\cup \circ f = f\dagger$.
□

Property 7 $R\dagger$ is reflexive.
Proof: $R \supseteq R \circ \mathrm{I}$, hence by definition 5, $R\dagger \supseteq \mathrm{I}$.
□

Property 8 $R \supseteq R \circ R\dagger$.
Proof: $R\dagger \supseteq R\dagger$, hence by definition 5, $R \supseteq R \circ R\dagger$.
□

Property 9 $R\dagger$ is transitive.
Proof:

$$\begin{array}{ll} & R\dagger \supseteq R\dagger \circ R\dagger \\ \equiv & \quad \{ \text{ defn. 5 } \} \\ & R \supseteq R \circ R\dagger \circ R\dagger \\ \Leftarrow & \quad \{ \text{ property 8, twice } \} \\ & R \supseteq R \\ \equiv & \\ & \mathsf{true} \end{array}$$

□

Corollary 10 $(R\dagger) \cap (R\dagger)\cup$ is an equivalence relation.
Proof: intersection preserves reflexivity and transitivity.
□

Since $R\dagger$ is not in general symmetric, we have had to take the intersection of $R\dagger$ with its own reverse to obtain symmetry. Note however that if R is a total function, then $(R\dagger) \cap (R\dagger)\cup = R\dagger$, so taking the intersection is simply a generalisation of the previous construction. We have, then, constructed an equivalence relation, but is it also a congruence relation? The following lemmata allow us to give a positive answer.

Lemma 11 $\tau \in R \longleftarrow R\mathsf{F} \quad \equiv \quad \tau \in R\cup \longleftarrow (R\cup)\mathsf{F}$.
Proof:

$$\begin{array}{ll} & \tau \in R \longleftarrow R\mathsf{F} \\ \equiv & \quad \{ \text{ defn. 2 } \} \\ & R \circ \tau \supseteq \tau \circ R\mathsf{F} \\ \equiv & \quad \{ \text{ reverse; relators } \} \\ & \tau\cup \circ R\cup \supseteq (R\cup)\mathsf{F} \circ \tau\cup \\ \Leftarrow & \quad \{ \text{ monotonicity; functionality and totality of } \tau \} \\ & R\cup \circ \tau \supseteq \tau \circ (R\cup)\mathsf{F} \\ \equiv & \quad \{ \text{ defn. 2 } \} \\ & \tau \in R\cup \longleftarrow (R\cup)\mathsf{F} \end{array}$$

This shows $\tau \in R\mathsf{F} \longleftarrow R \Leftarrow \tau \in (R\cup)\mathsf{F} \longleftarrow R\cup$; since R was arbitrary, we may replace it by $R\cup$ and so obtain the desired equivalence.
□

Lemma 12 If R is a homomorphism, then $\tau \in R\dagger \longleftarrow (R\dagger)\mathsf{F}$.
Proof: Let R be the homomorphism $(\!|S|\!)$.

$$\begin{array}{ll} & \tau \in R\dagger \longleftarrow (R\dagger)\mathsf{F} \\ \equiv & \quad \{ \text{ defn. 5 } \} \\ & R\dagger \circ \tau \supseteq \tau \circ (R\dagger)\mathsf{F} \\ \Leftarrow & \quad \{ \text{ monotonicity; totality of } \tau \} \\ & R\dagger \supseteq \tau \circ (R\dagger)\mathsf{F} \circ \tau\cup \\ \equiv & \quad \{ \text{ defn. 5 } \} \\ & R \supseteq R \circ \tau \circ (R\dagger)\mathsf{F} \circ \tau\cup \\ \equiv & \quad \{ (1) \} \\ & R \supseteq S \circ R\mathsf{F} \circ (R\dagger)\mathsf{F} \circ \tau\cup \\ \equiv & \quad \{ \text{ relators } \} \\ & R \supseteq S \circ (R \circ R\dagger)\mathsf{F} \circ \tau\cup \\ \Leftarrow & \quad \{ \text{ property 8 } \} \\ & R \supseteq S \circ R\mathsf{F} \circ \tau\cup \\ \Leftarrow & \quad \{ \text{ monotonicity; functionality of } \tau \} \\ & R \circ \tau \supseteq S \circ R\mathsf{F} \\ \equiv & \quad \{ (1) \} \\ & \mathsf{true} \end{array}$$

□

Lemma 13 If $\tau \in R \longleftarrow R_F$ and $\tau \in S \longleftarrow S_F$, then $\tau \in (R \cap S) \longleftarrow (R \cap S)_F$.
Proof: Assume the antecedents; i.e.,

$$R \circ \tau \supseteq \tau \circ R_F \tag{4}$$

$$S \circ \tau \supseteq \tau \circ S_F \tag{5}$$

then we calculate:

$$\begin{array}{ll} & (R \cap S) \circ \tau \\ = & \quad \{ \text{ set theory, } \tau \text{ is a function } \} \\ & (R \circ \tau) \cap (S \circ \tau) \\ \supseteq & \quad \{ (4) \text{ and } (5); \text{ monotonicity } \} \\ & (\tau \circ R_F) \cap (\tau \circ S_F) \\ \supseteq & \quad \{ \text{ set theory } \} \\ & \tau \circ (R_F \cap S_F) \\ \supseteq & \quad \{ \text{ monotonicity of relators } \} \\ & \tau \circ (R \cap S)_F \end{array}$$

□

Corollary 14 If R is a relational homomorphism, then $(R\dagger) \cap (R\dagger)^\cup$ is a congruence relation.
□

The open question that we leave to the reader is whether every congruence relation on T can be expressed in the form $(R\dagger) \cap (R\dagger)^\cup$, where R is a relational homomorphism.

Acknowledgement: Peter de Bruin pointed out to us that the component g of the homomorphism constructed in the proof of theorem 4 is not necessarily total.

References

[1] R.C. Backhouse. Naturality of homomorphisms. Lecture notes, International Summer School on Constructive Algorithmics, vol. 3, 1989.

[2] P.J. de Bruin. Naturalness of polymorphism. 1989. Department of Mathematics and Computing Science, University of Groningen.

[3] H. Ehrig and B. Mahr. *Fundamentals of Algebraic Specification 1. EATCS Monographs on Theoretical Computer Science*, Springer-Verlag Berlin, 1985.

[4] T. Hagino. A typed lambda calculus with categorical type constructors. In D.H. Pitt, A. Poigne, and D.E. Rydeheard, editors. *Category Theory and Computer Science*, pages 140–57, Springer-Verlag Lecture Notes in Computer Science 283, 1988.

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

[6] P. Wadler. Theorems for free! March 1989. Draft report, Dept. Comp. Science, University of Glasgow.