A note on the equational calculus for many-sorted algebras with possibly empty carrier sets

A 85/01

by Jacques Loeckx and Bernd Mahr

Jacques Loeckx
Fachrichtung 10.2 Informatik
Universität des Saarlandes
6600 Saarbrücken

Bernd Mahr
Fachbereich 20
Technische Universität Berlin
Franklinstraße 28/29
1000 Berlin 10

Submitted for publication in EATCS Bulletin

January 1985

A NOTE ON THE EQUATIONAL CALCULUS FOR MANY-SORTED ALGEBRAS WITH POSSIBLY EMPTY CARRIER SETS

Jacques Loeckx
Fachbereich 10
Universität des Saarlandes
D - 6600 Saarbrücken

Bernd Mahr
Fachbereich 20
Technische Universität Berlin
Franklinstraße 28/29
D - 1000 Berlin 10

Many-sorted algebras form a useful and adequate concept which allows for a mathematical modelling of "data types". As such, many-sorted algebras are often admitted to contain empty carrier sets. While this is not a source of problems from an algebraic, respectively a categorical point of view, empty carrier sets are a nuisance if it comes to logic. This has been recognized by many authors (see e.g. [KR 71], [M 76], [GM 81]). Actually, Goguen and Meseguer proposed in [GM 81] to attach "variable declarations" to equations, and to extend the equational calculus accordingly. Their solution to the "empty carriers problem" is indeed elegant and has been widely adopted. The appropriate extension of the equational calculus, however, does not seem to be well understood. In several papers Goguen and Meseguer discuss the extension of this calculus to many-sorted algebras with possibly empty carrier sets, but most of their proposals are misleading or incorrect. We feel that it is therefore justified to discuss the matter again, hoping that this helps clarifying the situation.

Given a signature SIG = (S, OP) we write equations as

$(X,\ L = R)$

where $X = (X_s)_{s \in S}$ is a (possibly infinite) S-sorted set of variables, and $L, R \in T_{OP}(X)$ are SIG-terms of the same sort built over X. Informally, $(\{x_1, x_2, \ldots\},\ L = R)$ stands for $\forall x_1, x_2, \ldots\ .\ (L = R)$. The key problem in extending the classical equational calculus to many-sorted algebras with possibly empty carrier sets, is to provide rules allowing the set X of *variable declarations* to shrink or grow.

The following observations reflect a solution to this problem:

(1) a set of variable declarations can always grow without affecting validity, i.e.:
If the equation $(X,\ L = R)$ is valid in a SIG-algebra A, and if $X \subseteq Y$, then the equation $(Y,\ L = R)$ is also valid in A.

(2) the shrinking of a set of variable declarations does not affect validity if and only if the shrinking does not lead to a "dying-out" of sorts, i.e.:
If the equation $(X,\ L = R)$ is valid in a SIG-algebra A, if $Y \subseteq X$, if $L, R \in T_{OP}(Y)$ and, finally, if

$$\text{for all } s \in S: \quad X_s \neq \emptyset \ \text{ implies } \ T_{OP,s}(Y) \neq \emptyset \qquad (*)$$

then the equation $(Y,\ L = R)$ is also valid in A.
Conversely, if the equations $(X,\ L = R)$ and $(Y,\ L = R)$ do not satisfy the condition (*), then there is a SIG-algebra A in which $(X,\ L = R)$ is valid but not $(Y,\ L = R)$. Note that the condition (*) is trivially satisfied for any sort s with $Y_s \neq \emptyset$.

These two observations lead to the following equational calculus for many-sorted algebras with possibly empty carrier sets:

R1: $$\frac{}{\vdash (X,\ t = t)} \qquad \text{(reflexivity)}$$

for all $t \in T_{OP}(X)$

R2: $$\frac{\vdash (X,\ t1 = t2)}{\vdash (X,\ t2 = t1)} \qquad \text{(symmetry)}$$

for all $t1,\ t2 \in T_{OP}(X)$

R3: $$\frac{\vdash (X,\ t1 = t2) \qquad \vdash (X,\ t2 = t3)}{\vdash (X,\ t1 = t3)} \qquad \text{(transitivity)}$$

for all $t1,\ t2,\ t3 \in T_{OP}(X)$

R4: $$\frac{\vdash (X,\ t1 = t2)}{\vdash (Y,\ \bar{h}(t1) = \bar{h}(t2))} \qquad \text{(substitution)}$$

for all $t1,\ t2 \in T_{OP}(X)$
and for all assignments $h : X \to T_{OP}(Y)$

R5: $$\frac{\vdash (X,\ t1 = t2)}{\vdash (X \cup Y,\ \bar{h}(t) = \bar{g}(t))} \qquad \text{(replacement)}$$

for all $t1,\ t2 \in T_{OP}(X)$ and $t \in T_{OP}(Y)$

and for all assignments $h,\ g : Y \to T_{OP}(X \cup Y)$
such that for all $y \in Y$
either $h(y) = g(y)$
or $h(y) = t1$ and $g(y) = t2$

Here $\bar{h}$ and $\bar{g}$ denote the unique homomorphic extensions of h and g respectively (note, this is just an elegant way of expressing simultaneous substitution). It is shown in [EM 85] that this calculus is correct and complete.

The growing of the set of variable declarations is hidden in the rule R4: Choosing Y such that $X \subset Y$ and h such that $h(x) = x$ for all $x \in X$, we may derive (Y, t1 = t2) from (X, t1 = t2).

The shrinking of the set of variable declarations is also hidden in R4: Suppose $t1, t2 \in T_{OP}(Y)$ with $Y \subset X$. Choose h such that

$$h(y) = \begin{cases} y & \text{if } y \in Y \\ t_y & \text{if } y \in X-Y \end{cases}$$

where t_y denotes an arbitrary term in $T_{OP}(Y)$ which exists by condition (*). We then may derive (Y, t1 = t2) from (X, t1 = t2).

Note that the rule R5 also allows the growing of the set of variable declarations.

Of course it is possible to explicitly express the growing and shrinking of the set of variable declarations by two additional rules:

R6:

$$\frac{\vdash (X,\ t1 = t2)}{\vdash (Y,\ t1 = t2)} \qquad \text{(abstraction)}$$

for all Y with $X \subseteq Y$
and for all $t1, t2 \in T_{OP}(X)$

R7:

$$\frac{\vdash (X,\ t1 = t2)}{\vdash (Y,\ t1 = t2)} \qquad \text{(concretion)}$$

for all $t1, t2 \in T_{OP}(Y)$
and for all Y with $Y \subseteq X$ such that

for all $s \in S$,
$X_s \neq \emptyset$ implies $T_{OP,s}(Y) \neq \emptyset$

but, as we have seen above, these rules do not add to the expressive power of the calculus.

As an example consider the following specification SPEC:

<u>sorts</u>: s, bool, d

<u>opns</u>: $T : \to bool$
$F : \to bool$
$C : s \to bool$
$D : s \to d$

<u>eqns</u>: $(\{x{:}s, y{:}s, z{:}d\}, C(x) = T)$
$(\{x{:}s, y{:}s, z{:}d\}, C(x) = F)$

According to the rules of the equational calculus we can derive the following equations:

e1 : $(\{x{:}s, y{:}s, z{:}d\}, T = F)$
e2 : $(\{x{:}s, z{:}d\}, T = F)$
e3 : $(\{y{:}s, z{:}d\}, T = F)$
e4 : $(\{y{:}s\}, T = F)$

but we can not derive:

e5 : $(\{z{:}d\}, T = F)$
e6 : $(\emptyset, T = F)$

Note, that e4 is derivable (from e3) since there is still a term of sort d, namely D(y), saying that the sort d has not died out. Accordingly e5 cannot be derived since no term of sort s exists, while it existed in e3.
And indeed the algebra A with carrier sets

$$A_s = \emptyset \ , \ A_{bool} = \{\tau, \varphi\} \ , \ A_d = \{\delta\}$$

and operations

$T_A = \tau$, $F_A = \varphi$, C_A and D_A are the empty function

is a SPEC-algebra, but does not satisfy e5. By the same argument e6 is not derivable nor valid in A.

Coming back to the calculi given by Goguen and Meseguer, we have the following situation.

(1) In [GM 81] a 6-rule-calculus is proposed which implicitly assumes that the sets of variable declarations are finite. While being correct and complete the calculus

is misleading. Having remarked that rules (1) to (4) form a correct but incomplete calculus the authors add two rules corresponding to *abstraction* and *concretion* respectively. Actually it turns out that the abstraction rule, which corresponds to our rule R6, is essentially a special case of the authors' rule (4) (called *substitutivity*). The only case which is not covered by rule (4) is the case in which variable declarations are added to an empty set of declarations.

On the other hand, the authors' concretion rule allows the deletion of a single variable declaration, provided the sort in this declaration is *non-void*, i.e. there exists a ground term of this sort. This rule appears to be a strictly weaker version of our rule R7. In fact, our condition (*) above is replaced by the strictly stronger condition

$$\text{for all } s \in S: \quad X_s = Y_s \quad \text{if } s \text{ is void, i.e. } T_{OP,s} = \emptyset \qquad (**)$$

On the other hand, the authors' substitutivity rule is strong enough to allow a derivation of (an equivalent of) our rule R7; this derivation is similar to the derivation of R7 from R4 indicated above. The discussions and proofs in [GM 81] and in [GM 82] suggest that this was not seen by the authors.

As a conclusion, in order to the complete the authors' calculus consisting of the rules (1) to (4) it is sufficient to add a means for covering "abstraction" in the case of an empty set of variable declarations.

(2) [GM 83a] and [GM 83b] essentially present the same calculus as [GM 81] but with a different notation.

The substitutivity rule

$$\frac{\vdash (X, t1=t2), \ \vdash (Y, n1=n2)}{\vdash (X \cup Y - \{x\}, \ t1^{n1}_{x} = t2^{n2}_{x})}$$

- where $x \in X$ is assumed and where t^{n}_{x} denotes the result of the substitution of x by n in t - is incorrect: $X \cup Y - \{x\}$ should be replaced by $(X - \{x\}) \cup Y$ (consider the case n1 = n2 = x).

To prove soundness and completeness of the calculus, the authors present a supposingly equivalent calculus. In this calculus the rules of substitutivity, abstraction and concretion are replaced by two rules (4') and (5') which essentially correspond to our rules R5 and R4 respectively. However, rule (4') is too weak since it can not be applied iteratively. This error may be fixed by replacing variables by terms. More importantly, the equivalence proof of the two calculi is vague at those points where it should be apparent that condition (**) can not replace condition (*).

Conclusion

We have argued that an extension of the classical equational calculus for many-sorted algebras with possibly empty carrier sets essentially has to deal with the appropriate "growing" and "shrinking" of the set of variable declarations. We have presented a set of rules (R1 to R5) which constitutes a sound and complete calculus. Finally, we have discussed the calculi proposed by Goguen and Meseguer. Apart from two minor errors in two of their rules, we found some of their rules misleading.

References:

[EM 85] H. Ehrig, B. Mahr, *Fundamentals of Algebraic Specifications*, EATCS-Monograph-Series, Springer-Verlag, to appear in March 1985

[GM 81] J.A. Goguen, J. Meseguer, Completeness of Many-Sorted Equational Logic, *SIGPLAN NOTICES* 16.7 (1981) pp. 24 - 32

[GM 82] J.A. Goguen, J. Meseguer, Completeness of Many-Sorted Equational Logic, SRI-Technical Report CSL-135, May 1982

[GM 83a] J.A. Goguen, J. Meseguer, An Initiality Primer, draft, March 1983

[GM 83b] J.A. Goguen, J. Meseguer, Initiality, Induction, and Computability, CSL Techn. Rep. 140, SRI Intern., December 1983

[KR 71] H. Kaphengst, H. Reichel, Algebraische Algorithmentheorie, WIB Nr. 1 VEB Kombinat Robotron, Dresden 1971

[M 76] G. Matthiessen, Theorie der heterogenen Algebren, Mathematische-Arbeitspapiere Nr. 3, Universität Bremen, 1976