On demonic composition

On Demonic Composition

Roland Backhouse

October 28, 1991

Demonic composition has been the subject of at least two recent articles [1, 2]. In both these papers a pointwise definition is given from which, by magic, a — rather ugly — point-free definition is plucked out of the blue. Subsequently, proofs are given of the associativity of the so-defined operator.

Neither proof provided to my mind any justification for point-free reasoning. Rather the opposite: Berghammer's proof [1] struck me as a "machine-code proof" in that the definition of demonic composition was used to expand the two possible ways of composing three specs into — inevitably very long — expressions involving the primitive operators of the plat calculus. These expressions were then laboriously proved to be equal. Van der Woude's proof [2] used exactly the same strategy but was a little better in that his primitives were a little less primitive than Berghammer's and consequently the expressions he had to manipulate were a little shorter. To be fair to van der Woude he made his own dissatisfaction with the proofs explicit by entitling the paper "Free style Specwrestling" and concluding with the words: "Frustating is still the fact that the truth of the statements in the tasks is easily seen with a pointwise interpretation but a rigorous proof on the spec level is still unappealing." In this note I want to take up the challenge of constructing an appealing point-free proof of the associativity of demonic composition.

The task according to van der Woude [2] begins as follows: "Define the demonic composition $R; S$ as the usual composition, provided that it is only defined in states x such that R is defined on all the S-results Sx."

Interpreting this specification literally we are required to specify $R; S$ formally via two clauses: The first clause states that it is "the usual composition" but with a restricted right domain. I.e.

$$(1) \qquad R;S \;=\; R \circ S \circ R\&S$$

where

(2) $\quad monotype.(R\&S)$

Thus $R\&S$ is the "restriction" on the right domain.

The second clause states that the said restriction should include only those "states x such that R is defined on all the S-results Sx." Replacing "states x" by "monotypes B", we formulate this second clause as the requirement that $R\&S$ satisfy the specification:

(3) $\quad A :: \quad \forall(B : monotype.B : A \sqsupseteq B \equiv R\rangle \sqsupseteq (S \circ B)\langle)$

1 Preliminary Analysis

Before embarking on the task of proving that demonic composition is indeed associative let us examine the more elementary consequences.

We begin with the conjunction of (1) and (2). An immediate consequence — at least immediate to the experienced "speculist" — is

(4) $\quad (R;S)\rangle = (R \circ S)\rangle \circ R\&S$

whence also

(5) $\quad R;S = R \circ S \circ (R;S)\rangle$

For the proofs of (4) and (5) we appeal to a slightly more general lemma and its corollary, specifically:

Lemma 6 For all specs S and monotypes A,

$$(S \circ A)\rangle = S\rangle \circ A$$

Proof

$$\begin{array}{ll} & (S \circ A)\rangle \\ = & \quad \{ \text{ domains } \} \\ & (S\rangle \circ A)\rangle \\ = & \quad \{ S\rangle \text{ and } A \text{ are both monotypes. Hence, so is } S\rangle \circ A \} \\ & (S\rangle \circ A) \end{array}$$

□

Corollary 7

$$\exists(A : \mathit{monotype}.A : R = S \circ A) \quad \equiv \quad R = S \circ R{>}$$

Proof Follows-from is obvious. For the implication we have:

$$\begin{array}{ll} & R = S \circ A \\ \equiv & \quad \{\ S = S \circ S{>}\ \} \\ & R = S \circ A = S \circ S{>} \circ A \\ \Rightarrow & \quad \{\ \text{lemma 6}\ \} \\ & R = S \circ R{>} \end{array}$$

□

(Lemmas that have two-step proofs may not be "immediate" to the novice but surely are to the more practised.) Equation (4) is an instance of lemma 6 in which S is instantiated to $R \circ S$ and A to $R\&S$. Similarly, (5) is an application of corollary 7 in which the same assignments are made to S and A, and R is instantiated to $R; S$.

Now we consider (3). The immediate question is whether there is a solution to the specification. To see that this is indeed the case — at a glance — we observe that both the functions $<$ and $S\circ$ are universally $\sqcup$-junctive, hence so is their composition and thus

$$(8) \qquad \sqcup(B : \mathit{monotype}.B \wedge R{>} \sqsupseteq (S \circ B){<} : B)$$

solves (3). As a function of R it is also obviously a monotype transformer (i.e. a function mapping monotypes to monotypes), and we may conclude that the binary operator & does indeed exist.

Knowing this formula is however of little help in any calculations involving $R\&S$ since the inevitable first step in any such calculation will be to return to (3). More progress can be made if one is aware that being universally $\sqcup$-junctive is equivalent to having a certain sort of adjoint. Note that the requirement on $R\&S$ — for all monotypes B and all specs R and S,

$$(9) \qquad R\&S \sqsupseteq B \quad \equiv \quad R{>} \sqsupseteq (S \circ B){<}$$

— is almost a Galois connection between the function $(R \mapsto R\&S)$ and the function $(B \mapsto (S \circ B){<})$. That it is not so can be solely attributed to the occurrence of the right domain operator on the right side of (9).

We can dismiss this obstacle by noting that, for all monotypes A we have $A{>} = A$ and, in particular, $(R{>}){>} = R{>}$. Consequently,

$$(10) \qquad R\&S \;=\; R{>}\&S$$

where, for all monotypes A and B,

$$(11) \qquad A\&S \sqsupseteq B \;\equiv\; A \sqsupseteq (S \circ B){<}$$

Property (10) tells us that the left operand of & may always, without loss of generality, be assumed to be a monotype. Property (11) says that — with the said assumption — the function $\&S$ is adjoint to the function $(B \mapsto (S \circ B){<})$. I.e. in the domain of monotypes there is a Galois connection between $\&S$ and the composition of the two functions $<$ and $S\circ$.

The recognition of a Galois connection is a very crucial observation and unleashes a welcome gush of properties. In order to proceed more quickly to our main task we limit attention to those that prove to be directly relevant. There are just two. The first is the cancellation property:

$$(12) \qquad A \;\sqsupseteq\; (S \circ A\&S){<}$$

Equivalently,

$$(13) \qquad A \circ S \circ A\&S \;=\; S \circ A\&S$$

Comparing (13) with (4) the experienced speculist should spot that

$$(14) \qquad (R;S){>} \;=\; S{>} \circ R\&S$$

which proves to be a crucial lemma in the proof of associativity. The four-step proof of (14) follows:

$$\begin{array}{ll} & (R;S){>} \\ = & \quad \{\ (1)\ \} \\ & (R \circ S \circ R\&S){>} \\ = & \quad \{\ \text{domains}\ \} \\ & (R{>} \circ S \circ R\&S){>} \\ = & \quad \{\ (10),\ (13)\ \} \\ & (S \circ R\&S){>} \\ = & \quad \{\ \text{lemma 6, } R\&S \text{ is a monotype}\ \} \\ & S{>} \circ R\&S \end{array}$$

The second is that the monotype transformer $\&S$ is universally $\sqcap$-junctive.

Since, however, for monotypes the $\sqcap$ operator coincides with composition the monotype transformer $\&S$ is universally composition-junctive and, more particularly, for all monotypes A and B,

$$(15) \qquad (A \circ B)\&S \;=\; A\&S \circ B\&S$$

2 The Proof of Associativity

Now let us turn to the task in hand — proving that demonic composition is associative. We consider the two terms $R;(S;T)$ and $(R;S);T$, and expand each using (1) very cautiously in order not to allow the formulae to grow too big. First, we obtain

$$\begin{array}{ll} & R;(S;T) \\ = & \quad \{\ (1)\ \} \\ & R \circ (S;T) \circ R\&(S;T) \\ = & \quad \{\ (1)\ \} \\ & R \circ S \circ T \circ S\&T \circ R\&(S;T) \end{array}$$

(Note that the outermost occurrence of ";" has been expanded first. Expanding the innermost occurrence leads to a larger formula.)

This is a pleasing result becauses it expresses $R;(S;T)$ in terms of a restriction on the right domain of $R \circ S \circ T$. Now for the other term:

$$\begin{array}{ll} & (R;S);T \\ = & \quad \{\ (1)\ \} \\ & (R;S) \circ T \circ (R;S)\&T \\ = & \quad \{\ \text{Applying (1) for a second time would introduce an undesirable restriction on the } \textit{left} \text{ domain of } T, \text{ not on the right. We search around for something more suitable. Aiming for (13) we apply (5)}\ \} \\ & R \circ S \circ (R;S)\!> \circ T \circ (R;S)\&T \\ = & \quad \{\ (10),\ (13),\ R,S := (R;S),T\ \} \\ & R \circ S \circ T \circ (R;S)\&T \end{array}$$

Thus $(R;S);T$ has also been expressed in terms of a restriction on the right domain of $R \circ S \circ T$ and we can infer that

$$
\begin{array}{lcl}
R;(S;T) & = & (R;S);T \\
\Leftarrow & & \\
S\&T \circ R\&(S;T) & = & (R;S)\&T
\end{array}
$$

The reader will undoubtedly have observed that only limited use of (3) has been used. The cancellation property (12) has been used but nowhere have we used the fact that $R\&S$ is the *limit* of a set of monotypes. This element of the specification will figure highly in the final proof obligation which is to show that

$$(16) \qquad S\&T \circ R\&(S;T) \;=\; (R;S)\&T$$

Demonic composition is still present in both the left and right sides of this equation. Let us try to remove it using the adjointness of the & operator. We choose to begin with the right side of (16), this choice being made because the demonic composition appears in the left argument of the & operator and we know so much more about the behaviour of that operator with respect to its left operand than with respect to its right operand.

$$
\begin{array}{ll}
 & (R;S)\&T \\
= & \quad \{\ (10)\ \} \\
 & (R;S)\!>\!\&T \\
= & \quad \{\ (14)\ \} \\
 & (S\!>\circ R\&S)\&T \\
= & \quad \{\ (15)\ \} \\
 & S\!>\!\&T \circ (R\&S)\&T \\
= & \quad \{\ (10)\ \} \\
 & S\&T \circ (R\&S)\&T
\end{array}
$$

Summarising,

$$(17) \qquad (R;S)\&T \;=\; S\&T \circ (R\&S)\&T$$

The right side of (17) is very close to the left side of (16). Only the terms $R\&(S;T)$ and $(R\&S)\&T$ differ. We now try to eliminate the demonic composition appearing in the former and simultaneously prove its equality to the latter. (It turns out that they are not equal but that is our proof strategy nevertheless.)

Since the demonic composition appears in the second operand we have little choice but to apply (9). We have, for all monotypes B,

$$
\begin{array}{ll}
 & R\&(S;T) \sqsupseteq B \\
\equiv & \quad \{ (9) \} \\
 & R\rangle \sqsupseteq ((S;T) \circ B)\langle \\
\equiv & \quad \{ (1) \} \\
 & R\rangle \sqsupseteq (S \circ T \circ S\&T \circ B)\langle \\
\equiv & \quad \{ \bullet \text{ assume } S\&T \sqsupseteq B, \text{ monotypes} \} \\
 & R\rangle \sqsupseteq (S \circ T \circ B)\langle \\
\equiv & \quad \{ \text{domains} \} \\
 & R\rangle \sqsupseteq (S \circ (T \circ B)\langle)\langle \\
\equiv & \quad \{ (9) \} \\
 & R\&S \sqsupseteq (T \circ B)\langle \\
\equiv & \quad \{ (9) \} \\
 & (R\&S)\&T \sqsupseteq B
\end{array}
$$

We have thus established that

$$
\begin{array}{ll}
 & S\&T \sqsupseteq B \ \wedge \ R\&(S;T) \sqsupseteq B \\
\equiv & \\
 & S\&T \sqsupseteq B \ \wedge \ (R\&S)\&T \sqsupseteq B
\end{array}
$$

from which it follows (since all inclusions are between monotypes) that

(18) $\quad S\&T \circ R\&(S;T) \ = \ S\&T \circ (R\&S)\&T$

Combining (17) and (18) we have established (16) and our task is complete.

3 Discussion

Our concern here has not been to *establish* a mathematical theorem — that demonic composition is associative has been known for decades — but with economy and elegance of calculation. Writing the note was prompted by discontent with the only two proofs that I know of using the axiomatic relational calculus. In this section I want to take the opportunity to compare those proofs with that given here in order to clarify my criticisms and to reinforce the lessons that I believe can be learnt form this exercise.

Both van der Woude and Berghammer use explicit, quantifier-free formulae for $R;S$ which, I complained earlier, are plucked out of the blue. Before embarking on the discussion of relative merits it is worthwhile to see how one might derive those formulae. The task is thus to derive a definition of R,S that fulfills the specification as given by (1), (2) and (3). (The formula (8) is inadequate because it is not quantifier-free.)

The calculation amounts to finding a closed form for $R\&S$ which is then substituted in (1). In broad terms the calculation of $R\&S$ consists of three steps. In the first step we reduce the problem to the calculation of $A\&S$, for monotype A, using (10). In the second step the adjoints of $<$ and $S\circ$ are composed, giving a solution to (3) but one that does not map monotypes to monotypes. In the final step the latter complication is overcome. In detail the calculation is as follows, beginning with the second and third steps. For all monotypes A and B and all specs S, we have:

$$
\begin{array}{ll}
 & A \;\sqsupseteq\; (S\circ B)< \\
\equiv & \quad \{ \text{ adjoint of } < \} \\
 & A\circ\top\top \;\sqsupseteq\; S\circ B \\
\equiv & \quad \{ \text{ adjoint of } S\circ \} \\
 & S\backslash(A\circ\top\top) \;\sqsupseteq\; B \\
\equiv & \quad \{ \text{ An adjoint has been found but is not} \\
 & \quad\ \text{a monotype transformer. We reintroduce } < \\
 & \quad\ \text{to obtain a monotype.} \\
 & \quad\ \mathit{leftcondition}.(U\backslash V) \Leftarrow \mathit{leftcondition}.V, \text{ domains } \} \\
 & (S\backslash(A\circ\top\top))<\circ\top\top \;\sqsupseteq\; B \\
\equiv & \quad \{ B = B<, \text{ adjoint of } < \} \\
 & (S\backslash(A\circ\top\top))< \;\sqsupseteq\; B
\end{array}
$$

Comparing with (11) the appropriate definition of $\&S$ for monotype A is

(19) $\quad A\&S \;=\; (S\backslash(A\circ\top\top))<$

and for arbitrary spec R (see (10))

(20) $\quad R\&S \;=\; (S\backslash(R>\circ\top\top))<$

Finally, by substitution in (1), we have

(21) $\quad R;S \;=\; R\circ S\circ(S\backslash(R>\circ\top\top))<$

The right side of (21) is an ugly formula, and direct manipulation of it is strongly discouraged. Some simplification is possible although the gain is marginal. The (equivalent) formulae used by van der Woude [2] and Berghammer [1] were, respectively,

$$(22) \qquad R;S \;=\; (R \circ S) \sqcap (\top\!\!\top \circ R)/S\cup$$

and

$$(23) \qquad R;S \;=\; (R \circ S) \sqcap \neg(\neg(\top\!\!\top \circ R) \circ S)$$

The main difference between the proof that I have presented here and those of Berghammer and van der Woude is the ubiquitous use of monotypes and the domain operators instead of right conditions/vectors. ("Right condition" is the term used by van der Woude, "vector" is the term used by Berghammer. Their meaning is the same, namely, spec R is a right condition/vector iff $R = \top\!\!\top \circ R$.)

The choice of which to use is difficult because right domains and right conditions are intimately connected — indeed Galois connected. Specifically, for all monotypes A and specs R we have

$$(24) \qquad A \sqsupseteq R\!> \;\equiv\; \top\!\!\top \circ A \sqsupseteq R$$

(which result is due to van der Woude). Moreover, this is a somewhat special Galois connection in that $(\top\!\!\top \circ A)\!>$ is *equal* to A, whereas the existence of a Galois connection predicts only an inclusion between the two.

The principle argument for the use of right conditions is that they are closed under negation whereas monotypes are not. Against that must be weighed the fact that intersection coincides with composition for monotypes and the domain operators both have adjoints for arbitrary specs rather than just for monotypes.

In my own mind I have no doubt that the emphasis on right (and left) conditions is misplaced. Those who work with them have to clutter their brains with ugly distributivity laws such as

$$(25) \qquad R \circ (S \circ \top\!\!\top \sqcap T) \;=\; (R \sqcap \top\!\!\top \circ S\cup) \circ T$$

whereas for the user of the domain operators it suffices to be aware that composition in the expression

$$(26) \qquad R \circ S\!< \circ T$$

is associative. That right conditions are closed under negation is, in my experience, rarely relevant. Indeed, one reason for preferring van der Woude's proof to Berghammer's is that negation has almost been eliminated. (In fact, by using Dedekind's rule it could have been eliminated altogether.)

The ugliness of the equational properties of right conditions is illustrative, I believe, of a more general phenomenon. When two functions are connected by a Galois connection it is often the case that one has very amenable algebraic properties whereas the other is much more difficult to work with. Commonly also one function is well-known, the other not (for example, think of composition and factors). From a calculational viewpoint a commendable heuristic would thus seem to be to limit explicit use of the algebraic properties of the "ugly sister" as much as possible by appealing instead to the Galois connection combined with the properties of its more beautiful partner. That is the tactic that has been adopted above.

A final remark on the length of the paper: I have been somewhat verbose in the presentation of the proofs in order to properly explain the important considerations at each step. Bearing this in mind, I believe that the length of the calculations compares favourably with those of van der Woude and Berghammer.

References

[1] R. Berghammer. Relational specification of data types and programs. Bericht Nr. 9109, Universität der Bundeswehr München, Fakultät für Informatik, September 1991.

[2] Jaap van der Woude. Free style specwrestling: Demonic composition and choice. In *Lambert Meertens, CWI, Liber Amicorum, 1966-1991.* Stichting Mathematisch Centrum, Amsterdam, January 1991.