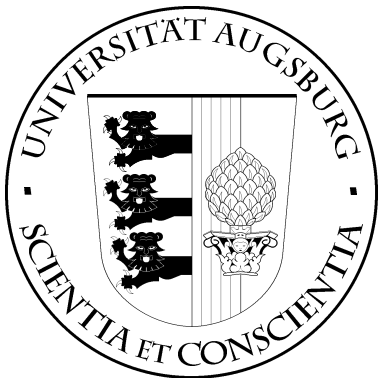
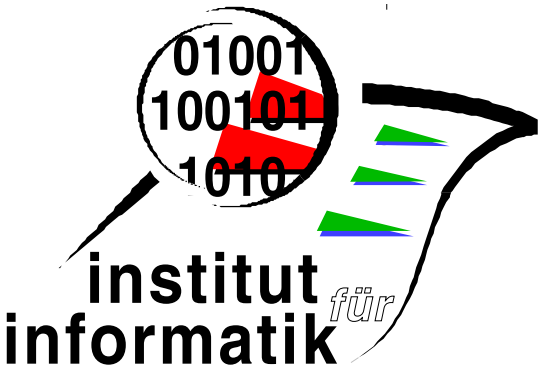
Universität Augsburg



Complete Tests do not Guarantee Domain

Bernhard Möller

Report 2005-6 März 2005



Institut für Informatik
D-86135 Augsburg

Complete Tests do not Guarantee Domain

Bernhard Möller

Institut für Informatik, Universität Augsburg,
D-86135 Augsburg, Germany

Abstract. We refute, by a counterexample, the conjecture that in a test semiring with complete lattice a domain operation can always be defined. The construction is based on ultrafilters extending the cofinite filter on a set.

1 Introduction

The algebraic structure of a domain semiring [2] has proved as quite widely applicable (see [1] for a survey). Therefore it is interesting to look for further examples of this structure.

In the present report we demarcate the class of models by showing that a certain completeness assumption is *not* sufficient to guarantee existence of a domain operation, contrary to earlier conjectures. We briefly repeat the necessary definitions.

A *semiring* is a structure $(S, +, \cdot, 0, 1)$ such that $(A, +, 0)$ is a commutative monoid, $(S, \cdot, 1)$ is a monoid, multiplication distributes over addition in both arguments and 0 is a left and right annihilator with respect to multiplication ($a \cdot 0 = 0 = 0 \cdot a$). The semiring is *idempotent* if its addition $+$ is. In this case the relation $\leq$ defined for all $a, b \in S$ by $a \leq b \Leftrightarrow a + b = b$ is a partial ordering, called the *natural ordering* on S. It induces an upper semilattice on S in which 0 is the least element and $a + b$ is the join of a and b.

A *test semiring* [3] is an idempotent semiring S with a distinguished Boolean subalgebra $\mathsf{test}(S)$ of *tests* with greatest element 1, least element 0 and join operation $+$, such that $\mathsf{test}(S)$ is closed under multiplication; then multiplication is the meet operation on $\mathsf{test}(S)$.

A *domain semiring* [2] is a test semiring S with a *domain operation* $\ulcorner\colon S \to \mathsf{test}(S)$ that satisfies for all $a, b \in S$ and $p \in \mathsf{test}(S)$

$$a \leq \ulcorner a \cdot a, \qquad\qquad \ulcorner(pa) \leq p. \tag{dom}$$

The conjunction of (d1) and (d2) is equivalent to

$$\ulcorner a \leq p \Leftrightarrow a \leq pa. \tag{llp}$$

(llp) says that $\ulcorner a$ is the least left preserver of a.

Because of (llp), domain is unique if it exists. Earlier it was conjectured that domain always exists if the test algebra is a complete Boolean algebra, since then the set of left preservers of each element has an infimum. However, as will be seen in Section 3, this infimum need not be a left preserver itself, so that the conjecture is false.

2 Ultrafilters

Since the counterexample is based on ultrafilters, we recall a few facts about them.

Definition 2.1 (1) A *filter* on a set m is a collection $F \subseteq \wp(m)$ with the following properties for all $p, q \subseteq m$:

$$\begin{array}{ll} \emptyset \notin F & \text{(F0)} \\ p, q \in F \Rightarrow p \cap q \in F & \text{(F1)} \\ p \in F \wedge p \subseteq q \Rightarrow q \in F & \text{(F2)} \end{array}$$

A filter F is *free* if $\bigcap F = \emptyset$.

(2) An *ultrafilter* is a filter that additionally satisfies

$$p \in F \vee \overline{p} \in F \qquad\qquad \text{(U)}$$

Equivalently, an ultrafilter is a filter that is $\subseteq$-maximal in the set of all filters on m. Note that (F0)$\wedge$(F1) already implies

$$p \in F \Rightarrow \overline{p} \notin F.$$

By Zorn's Lemma, every filter on a set m is contained in an ultrafilter on m.

Lemma 2.2 *Let F be an ultrafilter.*

1. $p \in F \Leftrightarrow \overline{p} \notin F$. *In particular,* $m \in F$.
2. $p \cap q \in F \Leftrightarrow p \in F \wedge q \in F$.
3. $p \cup q \in F \Leftrightarrow p \in F \vee q \in F$.

Proof. 1. ($\Leftarrow$) follows from (U).
($\Rightarrow$) As noted above, this holds for arbitrary filters.
2. ($\Leftarrow$) is (F1), whereas ($\Rightarrow$) follows from (F2).
3. ($\Rightarrow$) By (1), (F1) and (1) again we have

$$p \cup q \in F \Rightarrow \overline{p \cup q} = \overline{p} \cap \overline{q} \notin F \Rightarrow$$
$$\overline{p} \notin F \vee \overline{q} \notin F \Leftrightarrow p \in F \vee q \in F \ .$$

($\Leftarrow$) By (U) and (F2) we get

$$\overline{p} \notin F \Rightarrow p \in F \Rightarrow p \cup q \in F \ .$$

Likewise, $\overline{q} \notin F \Rightarrow p \cup q \in F$, which shows the claim. □

We will need the following extension property.

Lemma 2.3 *Assume a filter F and $p \neq \emptyset$ with $p \notin F \wedge \overline{p} \notin F$. Set*

$$F' \stackrel{\text{def}}{=} F \cup \{p\} \cup \{q \cap p : q \in F\},$$
$$F'' \stackrel{\text{def}}{=} \{r : \exists\, q \in F' : r \supseteq q\}.$$

Then F'' is a filter again.

Proof. (F0) We show that F' satisfies (F0), from which it follows that F'' satisfies (F0), too. Assume that $q \cap p = \emptyset$ for some $q \in F$. But this means $q \subseteq \overline{p}$, so that (F2) for F would imply $\overline{p} \in F$, contradicting the assumption.
(F1) It is clear that F' satisfies (F1). Assume now $s, t \in F''$, say $s \supseteq q$ and $t \supseteq r$ for $q, r \in F'$. Then $s \cap t \supseteq q \cap r \in F'$, hence $s \cap t \in F''$ as well.
(F2) Assume $s \supseteq r$ for some $r \in F''$. By definition of F'' there is a $q \in F'$ with $r \supseteq q$. But then also $s \supseteq q$ and hence $s \in F''$ as well. □

If m is infinite then the set of all cofinite subsets of m is a filter $\mathrm{CF}(m)$ on m.

Lemma 2.4 *For infinite m and $p \subseteq m$ we have*

$$p = \bigcap \{q \in \mathrm{CF}(m) : q \supseteq p\}.$$

Proof. $(\subseteq)$ is clear.
$(\supseteq)$ Let $D \stackrel{\text{def}}{=} \{q \in \mathrm{CF}(m) : q \supseteq p\}$ and consider $x \in \bigcap D$, i.e., $\forall\, q \in D : x \in q$. Suppose $x \notin p$. Then for all $q \in D$ also $q - \{x\} \in D$, since $q - \{x\}$ is cofinite again. Set now $D' \stackrel{\text{def}}{=} \{q - \{x\} : q \in D\}$. Then $\bigcap D \subseteq \bigcap D'$. But $x \notin \bigcap D'$, hence $x \notin \bigcap D$, a contradiction. □

Corollary 2.5 *For every filter $F \supseteq \mathrm{CF}(m)$ and every $p \subseteq m$ we have*

$$p = \bigcap \{q \in F : q \supseteq p\}.$$

In particular, on every infinite set there is a free ultrafilter.

Proof. By $F \supseteq \mathrm{CF}(m)$ we get

$$\bigcap \{q \in F : q \supseteq p\} \subseteq \bigcap \{q \in \mathrm{CF}(m) : q \supseteq p\} = p.$$

The inclusion $p \subseteq \bigcap \{q \in F : q \supseteq p\}$ holds by definition of $\bigcap$.
Taking now $p = \emptyset$ and choosing as F any ultrafilter containing $\mathrm{CF}(m)$ shows the second claim. □

3 Counterexample

Now we are ready to give a test semiring with complete test algebra but without domain. First we give a general construction.

Lemma 3.1 *Consider a non-empty set m. For $p \in$ let $\underline{p}$ be a copy of p and let $\underline{\wp(m)}$ be the set of all these copies, ordered by $\underline{p} \leq \underline{q} \Leftrightarrow p \subseteq q$. We assume $\wp(m) \cap \underline{\wp(m)} = \emptyset$. Set*

$$S \stackrel{\text{def}}{=} \wp(m) \cup \underline{\wp(m)}.$$

Assume an ultrafilter F on m. For $p, q \in \wp(m)$ we define

$$p \triangleright \underline{q} \stackrel{\text{def}}{=} \begin{cases} \underline{p \cap q} & \text{if } p \in F, \\ p \cap q & \text{otherwise.} \end{cases}$$

Define the structure $S(F) = (S, \wp(m), +, \emptyset, \cdot, m)$ by the following tables ($p, q \in \wp(m)$):

$+$	q	$\underline{q}$
p	$p \cup q$	$\underline{p \cup q}$
$\underline{p}$	$\underline{p \cup q}$	$\underline{p \cup q}$

$\cdot$	q	$\underline{q}$
p	$p \cap q$	$p \triangleright \underline{q}$
$\underline{p}$	$q \triangleright \underline{p}$	$\underline{p \cap q}$

Then S is a test semiring. It becomes even a Kleene algebra wit tests by setting

$$p^* \stackrel{\text{def}}{=} m \qquad\qquad \underline{p}^* \stackrel{\text{def}}{=} \underline{m}$$

Proof. We write 0 instead of $\emptyset$. The commutative and idempotent monoid structure of $(S, +, 0)$ is immediate from the definitions. The annihilator property of 0 and neutrality of m w.r.t. $\cdot$ follow from (F0) and $m \in F$ (see Lemma 2.2(1)). Moreover, also $\cdot$ is commutative.

We now check multiplicative associativity. For products in which all three factors are in $\wp(m)$ or are all in $\underline{\wp(m)}$ associativity is immediate from the definitions. For the remaining ones we calculate as follows.

$$\begin{aligned} p \cdot (q \cdot \underline{r}) &= \left\{ \begin{array}{ll} p \cdot \underline{q \cdot r} & \text{if } q \in F \\ q \cdot r & \text{if } q \notin F \end{array} \right\} \\ &= \left\{ \begin{array}{ll} \underline{p \cdot q \cdot r} & \text{if } q \in F \wedge p \in F \\ p \cdot q \cdot r & \text{if } q \in F \wedge p \notin F \\ p \cdot q \cdot r & \text{if } q \notin F \end{array} \right\} \\ &= \left\{ \begin{array}{ll} \underline{p \cdot q \cdot r} & \text{if } p \in F \wedge q \in F \\ p \cdot q \cdot r & \text{otherwise} \end{array} \right\} \\ &\underset{\text{L } 2.2(2)}{=} \left\{ \begin{array}{ll} \underline{p \cdot q \cdot r} & \text{if } p \cdot q \in F \\ p \cdot q \cdot r & \text{otherwise} \end{array} \right\} \\ &= (p \cdot q) \cdot \underline{r} \end{aligned}$$

$$
\begin{aligned}
(p \cdot \underline{q}) \cdot \underline{r} &= \left\{ \begin{array}{ll} \underline{p \cdot q} & \text{if } p \in F \\ p \cdot q & \text{if } p \notin F \end{array} \right\} \cdot \underline{r} \\
&= \left\{ \begin{array}{ll} \underline{p \cdot q \cdot r} & \text{if } p \in F \\ \underline{p \cdot q \cdot r} & \text{if } p \notin F \ \wedge \ p \cdot q \in F \\ p \cdot q \cdot r & \text{if } p \notin F \ \wedge \ p \cdot q \notin F \end{array} \right\} \\
&\underset{\text{(F2)}}{=} \left\{ \begin{array}{ll} \underline{p \cdot q \cdot r} & \text{if } p \in F \\ p \cdot q \cdot r & \text{if } p \notin F \end{array} \right\} \\
&= p \cdot (\underline{q} \cdot \underline{r})
\end{aligned}
$$

By commutativity of $\cdot$ these cases cover all possibilities.

It remains to check the distributive laws. Again we only need to consider the "non-homogeneous" cases.

$$
\begin{aligned}
p \cdot \underline{r} + q \cdot \underline{r} &= \left\{ \begin{array}{ll} \underline{p \cdot r} & \text{if } p \in F \\ p \cdot r & \text{otherwise} \end{array} \right\} + \left\{ \begin{array}{ll} \underline{q \cdot r} & \text{if } q \in F \\ q \cdot r & \text{otherwise} \end{array} \right\} \\
&= \left\{ \begin{array}{ll} \underline{p \cdot r + q \cdot r} & \text{if } p \in F \ \wedge \ q \in F \\ \underline{p \cdot r + q \cdot r} & \text{if } p \in F \ \wedge \ q \notin F \\ \underline{p \cdot r + q \cdot r} & \text{if } p \notin F \ \wedge \ q \in F \\ p \cdot r + q \cdot r & \text{if } p \notin F \ \wedge \ q \notin F \end{array} \right\} \\
&= \left\{ \begin{array}{ll} \underline{p \cdot r + q \cdot r} & \text{if } p \in F \ \vee \ q \in F \\ p \cdot r + q \cdot r & \text{otherwise} \end{array} \right\} \\
&\underset{\text{L 2.2(3)}}{=} \left\{ \begin{array}{ll} \underline{p \cdot r + q \cdot r} & \text{if } p + q \in F \\ p \cdot r + q \cdot r & \text{otherwise} \end{array} \right\} \\
&= \left\{ \begin{array}{ll} \underline{(p+q) \cdot r} & \text{if } p + q \in F \\ (p+q) \cdot r & \text{otherwise} \end{array} \right\} \\
&= (p+q) \cdot \underline{r}
\end{aligned}
$$

$$
\begin{aligned}
(\underline{p} + q) \cdot r = (\underline{p+q}) \cdot r &= \left\{ \begin{array}{ll} \underline{(p+q) \cdot r} & \text{if } r \in F \\ (p+q) \cdot r & \text{otherwise} \end{array} \right\} \\
&= \left\{ \begin{array}{ll} \underline{p \cdot r + q \cdot r} & \text{if } r \in F \\ p \cdot r + q \cdot r & \text{otherwise} \end{array} \right\} \\
&= \left\{ \begin{array}{ll} \underline{p \cdot r} & \text{if } r \in F \\ p \cdot r & \text{otherwise} \end{array} \right\} + q \cdot r \\
&= \underline{p} \cdot r + q \cdot r
\end{aligned}
$$

$$
\begin{aligned}
p \cdot \underline{r} + \underline{q} \cdot \underline{r} &= \left\{ \begin{array}{ll} \underline{p \cdot r} + \underline{q \cdot r} & \text{if } p \in F \\ p \cdot r + \underline{q \cdot r} & \text{otherwise} \end{array} \right\} = \underline{p \cdot r + q \cdot r} \\
&= \underline{(p+q) \cdot r} = (\underline{p+q}) \cdot \underline{r} = (p + \underline{q}) \cdot \underline{r}
\end{aligned}
$$

Again, by commutativity of $\cdot$ these cases cover all possibilities.

So the test semiring structure is established. We now show that the additional definitions satisfy the star axioms. For elements $p \in \mathsf{test}(S)$ this follows from $p \leq 1 = m$ and general properties of test semirings.

For the other elements we first work out the meaning of $\underline{m} \cdot b$ for arbitrary $b \in S$, since that has to be the least fixpoint of $f(x) \stackrel{\text{def}}{=} b + \underline{p} \cdot x$ if the claim is true. The definitions imply

$$\underline{m} \cdot q = \left\{ \begin{array}{ll} \underline{q} & \text{if } q \in F \\ q & \text{otherwise} \end{array} \right\} \qquad\qquad \underline{m} \cdot \underline{q} = \underline{q} \qquad\qquad (*)$$

We now show that $\underline{m}$ satisfies the unfold axiom for $\underline{p}^*$:

$$1 + \underline{p} \cdot \underline{m} \underset{(*)}{=} m + \underline{p} = \underline{m \cup m} = \underline{m} \leq \underline{m}$$

For the star induction axiom we have to distinguish four cases.

Case 1. Assume $q + \underline{p} \cdot r \leq r$. We have to show $\underline{m} \cdot q \leq r$.
The assumption implies $\underline{p} \cdot r \leq r$. Hence $\underline{p} \cdot r$ cannot have the form $\underline{s}$ for some s. Therefore we must have $r \notin F$. Again by the assumption we have $q \leq r$ and (F2) shows that also $q \notin F$. Hence $\underline{m} \cdot q \underset{(*)}{=} q \leq r$ by the assumption.

Case 2. Assume $q + \underline{p} \cdot \underline{r} \leq \underline{r}$. We have to show $\underline{m} \cdot q \leq \underline{r}$.
The assumption implies $q \leq \underline{r}$, i.e., $\underline{r} = q + \underline{r} = \underline{q + r} \underset{(*)}{=} \underline{m} \cdot q + \underline{r}$ and we are done.

Case 3. Assume $\underline{q} + \underline{p} \cdot r \leq r$.
But $\underline{q} + \underline{p} \cdot r$ always has the form $\underline{s}$ for some s. So this assumption is false implies $\underline{m} \cdot q \leq r$ vacuously.

Case 4. Assume $\underline{q} + \underline{p} \cdot \underline{r} \leq \underline{r}$. We have to show $\underline{m} \cdot \underline{q} \leq \underline{r}$.
The assumption implies $\underline{q} \leq \underline{r}$ which is equivalent to the claim by $(*)$.

This establishes the Kleene algebra structure. □

Finally we can prove the main result.

Theorem 3.2 *There is a test semiring with complete test algebra but without domain.*

Proof. Consider an infinite set m and choose an infinite but not cofinite subset $p \subseteq m$. Then $\overline{p} \neq \emptyset$ and $p \notin \mathrm{CF}(m) \wedge \overline{p} \notin \mathrm{CF}(m)$. Hence we can extend $\mathrm{CF}(m)$ by $\overline{p}$ as in Lemma 2.3 and extend the resulting filter to an ultrafilter F. By construction, $\overline{p} \in F$, hence $p \notin F$. Let us now calculate the set L of left preservers of $\underline{p}$.

$$
\begin{array}{ll}
 & q \cdot \underline{p} = \underline{p} \\
\Leftrightarrow & \quad \{\!\![\text{ definition of } \cdot \ ]\!\!\} \\
 & \left\{ \begin{array}{ll} \underline{q \cap p} & \text{if } q \in F \\ q \cap p & \text{otherwise} \end{array} \right\} = \underline{p} \\
\Leftrightarrow & \quad \{\!\![\text{ simplification }]\!\!\} \\
 & q \in F \wedge \underline{q \cap p} = \underline{p} \\
\Leftrightarrow & \quad \{\!\![\text{ order isomorphism between } \wp\mathcal{O}(m) \text{ and } \underline{\wp\mathcal{O}(m)} \ ]\!\!\} \\
 & q \in F \wedge q \cap p = p \\
\Leftrightarrow & \quad \{\!\![\text{ set algebra }]\!\!\} \\
 & q \in F \wedge q \supseteq p
\end{array}
$$

Hence $L = \{q \in F : q \supseteq p\}$. But by Corollary 2.5 the infimum $\bigcap L = p \notin F$, so that L has no least element. Hence $\ulcorner p$ does not exist in $S(F)$. □

Acknowledgments. I am grateful to Jules Desharnais and Peter Höfner for helpful comments.

References

1. J. Desharnais, B. Möller, and G. Struth. Applications of modal Kleene algebra — A survey. *Journal on Relational Methods in Computer Science*, 1:93–131. `http://www.cosc.brocku.ca/Faculty/Winter/JoRMiCS/`
2. J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. *ACM Transaction on Computational Logic*, 2004. Preliminary version: Universität Augsburg, Institut für Informatik, Report No. 2003-07, June 2003.
3. D. Kozen. Kleene algebra with tests. *Trans. Programming Languages and Systems*, 19(3):427–443, 1997.