The regularity calculus: a second trial

(This is a successor to the incompletely AvG36/EWD882: "The regularity calculus: a first trial" and consequently owes a lot to A.J.M. van Gasteren. The absence of her initials on top of this text is explained by the sad circumstance that I have to carry out my second trial without her guidance.)

We consider regular expressions built from the two constants 0 and 1, the letters from some alphabet, and three constructors.

Axiom 0 The constants 0 and 1, and the letters of the alphabet are all different regular expressions.

Unless mentioned otherwise, a, b, c, and d are in the formulae in the sequel variables of type "regular expression".

Axiom 1 The expression \[ a \parallel b \] is regular. The infix operator (constructor) \( \parallel \) - pronounced "bar" - is symmetric, idempotent, and associative, i.e.
\[
\begin{align*}
a \parallel b &= b \parallel a, \\
a \parallel a &= a \\
(a \parallel b) \parallel c &= a \parallel (b \parallel c).
\end{align*}
\]

Syntactic convention. In view of the associativity of \( \parallel \), we allow ourselves the omission of parentheses. Of the three constructors, \( \parallel \) is given the lowest binding power. (End of Syntactic convention.)
On regular expressions, the relation \( \leq \) — pronounced "at most" — is defined by
\[
a \leq b \equiv a \cdot b = b
\]

**Theorem 0** The relation \( \leq \) is reflexive: \( a \leq a \)
transitive: \( a \leq b \land b \leq c \Rightarrow a \leq c \)
antisymmetric: \( a \leq b \land b \leq a \Rightarrow a = b \).

Note that reflexivity and antisymmetry can be combined into
\[
a \leq b \land b \leq a \equiv a = b
\]

**Proof** Reflexivity follows from the idempotence of \( \cdot \),
transitivity follows from the associativity of \( \cdot \),
and antisymmetry follows from the symmetry of \( \cdot \). (End of Proof.)

**Comment** The last line of above proof reveals that "antisymmetry" is an unfortunate name for the property it denotes. (End of Comment.)

**Theorem 1** \( a \leq a \cdot b \)

**Proof** true
\[
= \{\text{Axiom 1}\}
\]
\[
a \cdot a \cdot b = a \cdot b
\]
\[
= \{\text{definition of \( \leq \)}\}
\]
\[
a \leq a \cdot b
\]
(End of Proof.)

**Remark** Note how our syntactic convention has shortened the proof by one step. Without it, we would have been forced to write...
true
= \{\text{Axiom 1, idempotence}\}
\quad (a \parallel a) \parallel b = a \parallel b
= \{\text{Axiom 1, associativity}\}
\quad a \parallel (a \parallel b) = a \parallel b
= \{\text{definition of } \leq\}
\quad a \leq a \parallel b
\quad \text{(End of Remark.)}

\textbf{Theorem 2} \quad a \parallel b \leq c \equiv a \leq c \land b \leq c

\textbf{Proof} \quad a \parallel b \leq c
\quad = \{\text{Theorem 1}\}
\quad \quad a \leq a \parallel b \land b \leq a \parallel b \land a \parallel b \leq c
\quad \Rightarrow \{\text{Theorem 0, transitivity twice}\}
\quad \quad a \leq c \land b \leq c
\quad = \{\text{definition of } \leq\}
\quad \quad a \parallel c = c \land b \parallel c = c
\quad \Rightarrow \{\text{Leibniz}\}
\quad \quad a \parallel (b \parallel c) = c
\quad = \{\text{definition of } \leq\}
\quad \quad a \parallel b \leq c
\quad \quad \text{(End of Proof.)}

\textbf{Theorem 3} \quad \text{The } \parallel \text{ is monotonic, i.e.}
\quad a \leq b \Rightarrow a \parallel c \leq b \parallel c

\textbf{Proof} \quad a \leq b
\quad = \{\text{definition of } \leq\}
\quad \quad a \parallel b = b
\quad \Rightarrow \{\text{Leibniz}\}
\quad \quad a \parallel b \parallel c = b \parallel c
= \{ \text{Axiom 1} \}
\begin{align*}
(a \parallel c) \parallel (b \parallel c) &= b \parallel c \\
= \{ \text{definition of } \leq \} \\
a \parallel c &\leq b \parallel c \quad \text{(End of Proof.)}
\end{align*}

Remark As we have only used that \( \parallel \) is symmetric, idempotent, and associative, the above is a special instance of a rather general state of affairs. (End of Remark.)

* * *

Our second constructor, called "concatenation", indicated by juxtaposition, and not pronounced, is introduced by

Axiom 2 The expression \( a b \) is regular. The (invisible) infix operator of concatenation is associative, i.e.
\[(a b) c = a (b c)\]

Syntactic convention In view of the associativity of concatenation, we allow ourselves the omission of parentheses. Concatenation has a higher binding power than the \( \parallel \), i.e. \( a b \parallel c = (a b) \parallel c \)
(End of Syntactic convention.)

Concatenation and \( \parallel \) are connected by

Axiom 3 Concatenation distributes in both directions over the \( \parallel \), i.e.
\[
\begin{align*}
(a \parallel b) c &= ac \parallel bc \\
a (b \parallel c) &= ab \parallel ac
\end{align*}
\]
Theorem 4. Concatenation is monotonic in both its arguments, i.e.
\[ a \leq b \Rightarrow ac \leq bc \]
\[ b \leq c \Rightarrow ab \leq ac \]

Corollary. \[ a \leq b \land c \leq d \Rightarrow ac \leq bd \]

Proof of Theorem 4
\[
\begin{align*}
    a \leq b & \Rightarrow b \leq c \\
    \text{(def. of } \leq) & \Rightarrow \text{(def. of } \leq) \\
    a \parallel b = b & \Rightarrow b \parallel c = c \\
    \text{(Leibniz)} & \Rightarrow \text{(Leibniz)} \\
    (a \parallel b) c = bc & \Rightarrow a(b \parallel c) = ac \\
    \text{(Axiom 3)} & \Rightarrow \text{(Axiom 3)} \\
    ac \parallel bc = bc & \Rightarrow ab \parallel ac = ac \\
    \text{(def. of } \leq) & \Rightarrow \text{(def. of } \leq) \\
    ac \leq bc & \Rightarrow ab \leq ac
\end{align*}
\]

(End of Proof of Theorem 4.)

* * *

Before introducing unit elements for the two above constructors, we recall the general

Theorem. For a binary operator with a left and a right unit element, the unit element is unique.

Proof. Denoting the unit elements by \( L \) and \( R \) respectively and the operator by juxtaposition we observe
\[
\begin{align*}
    (A \ x, y :: L x = x \land y R = y) & \\
    \Rightarrow \{ x := R ; y := L \} & \\
    LR = R \land LR = L
\end{align*}
\]
\[ \Rightarrow \{ \text{Leibniz}\} \]
\[ L = R \quad \text{(End of Proof.)} \]

For the symmetric \[ \equiv \], the theorem is only of mild interest.

**Axiom 4** Constant 0 is the unit element of \[ \equiv \], i.e.
\[ a \equiv 0 = a, \quad 0 \equiv a = a, \quad \text{or} \quad 0 \equiv a \]

**Axiom 5** Constant 1 is the unit element of concatenation, i.e.
\[ 1a = a \quad \text{and} \quad a1 = a. \]

**Axiom 6** \[ a \equiv b = 0 \equiv a = 0 \lor b = 0 \]

**Corollary** \[ a0 = 0 \quad \text{and} \quad 0b = 0 \]

* * *

Our last constructor, called "closure", indicated by a postfix \[ * \] with the highest binding power and pronounced "star", satisfies

**Axiom 7** \[ (a \equiv b)^* = (a^* \equiv b^*)^* \]

**Axiom 8** \[ (ab)^* = 1 \equiv a(ba)^* b \]

**Theorem 5** \[ a^* = 1 \equiv aa^* \quad \text{and} \quad b^* = 1 \equiv b^* b \]

**Proof.** From Axiom 8 with \[ b = 1 \] and \[ a = 1 \] respectively, and Axiom 5. (End of Proof.)

Our next theorem connects the two constants:
**Theorem 6** \( 0^* = 1 \)

**Proof** true
\[
0^* = 1 \parallel 0 0^*
\]
\[
= \{ \text{Corollary 1 with } b := 0^* \}
\]
\[
0^* = 1 \parallel 0
\]
\[
= \{ \text{Axiom 4 with } a := 1 \}
\]
\[
0^* = 1 \tag{End of Proof.}
\]

Taking Axiom 7 into account as well, we can now justify the name "closure":

**Theorem 7** The \( * \) is idempotent, i.e. \( a^* = a^{**} \).

**Proof** true
\[
(a \parallel 0)^* = (a ^* 0^*)^*
\]
\[
= \{ \text{Axiom 7 with } b := 0^* \}
\]
\[
(a \parallel 0)^* = (a ^* 1^*)^*
\]
\[
= \{ \text{Theorem 6} \}
\]
\[
(a \parallel 0)^* = (a^* 1)^*
\]
\[
= \{ \text{Axioms 4 & 5} \}
\]
\[
a^* = a^* a^*
\]

**Theorem 8** \( a \leq a^* \)

**Proof** true
\[
= \{ \text{Theorem 5, unfolding once} \}
\]
\[
a^* = 1 \parallel a(1 \parallel a a^*)
\]
\[
= \{ \text{Axioms 3 & 5} \}
\]
\[
a^* = 1 \parallel a \parallel a a a^*
\]
\[
\Rightarrow \{ \text{Theorem 1} \}
\]
\[
a \leq a^* \tag{End of Proof.}
\]