The regularity calculus: a second trial

(This is a successor to the incompleted 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 $a \,[\!]\, b$ is regular. The infix operator (constructor) $[\!]$ - pronounced "bar" - is symmetric, idempotent, and associative, i.e.

$$a \,[\!]\, b = b \,[\!]\, a \quad ,$$
$$a \,[\!]\, a = a$$
$$(a \,[\!]\, b) \,[\!]\, c = a \,[\!]\, (b \,[\!]\, c) \quad .$$

Syntactic convention. In view of the associativity of $[\!]$, we allow ourselves the omission of parentheses. Of the three constructors, $[\!]$ is given the lowest binding power. (End of Syntactic convention.)

On regular expressions, the relation $\leq$ —pronounced "at most"— is defined by

$$a \leq b \;\equiv\; a [] b = b \qquad .$$

<u>Theorem 0</u> The relation $\leq$ is

reflexive: $a \leq a$
transitive: $a \leq b \wedge b \leq c \Rightarrow a \leq c$
antisymmetric: $a \leq b \wedge b \leq a \Rightarrow a = b$.
Note that reflexivity and antisymmetry can be combined into $a \leq b \wedge b \leq a \;\equiv\; a = b$.

<u>Proof</u> Reflexivity follows from the idempotence of $[]$, transitivity follows from the associativity of $[]$, and antisymmetry follows from the symmetry of $[]$. (End of Proof.)

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

<u>Theorem 1</u> $a \leq a [] b$.

<u>Proof</u>

$$\begin{array}{ll} & true \\ = & \{\text{Axiom 1}\} \\ & a [] a [] b = a [] b \\ = & \{\text{definition of } \leq\} \\ & a \leq a [] b \end{array}$$

. (End of Proof.)

<u>Remark</u> Note how our syntactic convention has shortened the proof by one step. Without it, we would have been <u>forced</u> to write

$$
\begin{array}{ll}
& true \\
= & \{\text{Axiom 1, idempotence}\} \\
& (a [] a) [] b = a [] b \\
= & \{\text{Axiom 1, associativity}\} \\
& a [] (a [] b) = a [] b \\
= & \{\text{definition of } \leq\} \\
& a \leq a [] b \quad .
\end{array}
$$

(End of Remark.)

<u>Theorem 2</u> $\quad a [] b \leq c \;\equiv\; a \leq c \wedge b \leq c \quad .$

<u>Proof</u>

$$
\begin{array}{ll}
& a [] b \leq c \\
= & \{\text{Theorem 1}\} \\
& a \leq a [] b \;\wedge\; b \leq a [] b \;\wedge\; a [] b \leq c \\
\Rightarrow & \{\text{Theorem 0, transitivity twice}\} \\
& a \leq c \;\wedge\; b \leq c \\
= & \{\text{definition of } \leq\} \\
& a [] c = c \;\wedge\; b [] c = c \\
\Rightarrow & \{\text{Leibniz}\} \\
& a [] (b [] c) = c \\
= & \{\text{definition of } \leq\} \\
& a [] b \leq c \quad .
\end{array}
$$

(End of Proof.)

<u>Theorem 3</u> The $[]$ is monotonic, i.e.

$$a \leq b \;\Rightarrow\; a [] c \leq b [] c \quad .$$

<u>Proof</u>

$$
\begin{array}{ll}
& a \leq b \\
= & \{\text{definition of } \leq\} \\
& a [] b = b \\
\Rightarrow & \{\text{Leibniz}\} \\
& a [] b [] c = b [] c
\end{array}
$$

$$\begin{aligned}
&= \{\text{Axiom 1}\}\\
&\quad (a \,[]\, c) \,[]\, (b \,[]\, c) = b \,[]\, c\\
&= \{\text{definition of } \leq\}\\
&\quad a \,[]\, c \leq b \,[]\, c \qquad . \qquad \text{(End of Proof.)}
\end{aligned}$$

<u>Remark</u> As we have only used that $[]$ 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

<u>Axiom 2</u> The expression ab is regular. The (invisible) infix operator of concatenation is associative, i.e.

$$(ab)c = a(bc) \qquad .$$

<u>Syntactic convention</u> In view of the associativity of concatenation, we allow ourselves the omission of parentheses. Concatenation has a higher binding power than the $[]$, i.e. $ab \,[]\, c = (ab) \,[]\, c$. (End of Syntactic convention.)

Concatenation and $[]$ are connected by

<u>Axiom 3</u> Concatenation distributes in both directions over the $[]$, i.e.

$$\begin{aligned}
(a \,[]\, b)c &= ac \,[]\, bc\\
a(b \,[]\, c) &= ab \,[]\, ac \qquad .
\end{aligned}$$

<u>Theorem 4</u> Concatenation is monotonic in both its arguments, i.e.

$$a \leq b \Rightarrow ac \leq bc$$
$$b \leq c \Rightarrow ab \leq ac \quad .$$

<u>Corollary</u> $a \leq b \wedge c \leq d \Rightarrow ac \leq bd \quad .$

<u>Proof of Theorem 4</u>

$$\begin{array}{l} a \leq b \\ = \{\text{def. of } \leq\} \\ a [] b = b \\ \Rightarrow \{\text{Leibniz}\} \\ (a [] b) c = bc \\ = \{\text{Axiom 3}\} \\ ac [] bc = bc \\ = \{\text{def. of } \leq\} \\ ac \leq bc \end{array}$$

$$\begin{array}{l} b \leq c \\ = \{\text{def. of } \leq\} \\ b [] c = c \\ \Rightarrow \{\text{Leibniz}\} \\ a(b [] c) = ac \\ = \{\text{Axiom 3}\} \\ ab [] ac = ac \\ = \{\text{def. of } \leq\} \\ ab \leq ac \quad . \end{array}$$

(End of Proof of Theorem 4.)

* * *

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

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

<u>Proof</u> Denoting the unit elements by L and R respectively and the operator by juxtaposition we observe

$$\begin{array}{l} (\underline{A}\, x, y :: Lx = x \wedge yR = y) \\ \Rightarrow \{x := R \; ; \; y := L\} \\ LR = R \wedge LR = L \end{array}$$

$\Rightarrow$ { Leibniz }
$L = R$. (End of Proof.)

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

<u>Axiom 4</u> Constant 0 is the unit element of $[\!]$, i.e.

$$a\,[\!]\,0 = a \quad , \quad 0\,[\!]\,a = a \quad . \text{ or } \quad 0 \leq a \quad .$$

<u>Axiom 5</u> Constant 1 is the unit element of concatenation, i.e.

$$1a = a \quad \text{and} \quad a1 = a \quad .$$

<u>Axiom 6</u> $ab = 0 \;\equiv\; a = 0 \vee b = 0$

<u>Corollary 1</u> $a0 = 0$ and $0b = 0$.

* *
*

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

<u>Axiom 7</u> $(a\,[\!]\,b)^* = (a^* b^*)^*$.

<u>Axiom 8</u> $(ab)^* = 1\,[\!]\,a(ba)^*b$.

<u>Theorem 5</u> $a^* = 1\,[\!]\,aa^*$ and $b^* = 1\,[\!]\,b^*b$

<u>Proof</u>. From Axiom 8 with $b{:=}1$ and $a{:=}1$ respectively, and Axiom 5. (End of Proof.)

Our next theorem connects the two constants:

<u>Theorem 6</u> $0^* = 1$

<u>Proof</u> true

$= \{$Theorem 5 with $a := 0\}$

$0^* = 1 \,[\!]\, 0\, 0^*$

$= \{$Corollary 1 with $b := 0^*\}$

$0^* = 1 \,[\!]\, 0$

$= \{$Axiom 4 with $a := 1\}$

$0^* = 1$. (End of Proof.)

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

<u>Theorem 7</u> The $*$ is idempotent, i.e. $a^* = a^{**}$.

<u>Proof</u> true

$= \{$Axiom 7 with $b := 0\}$

$(a \,[\!]\, 0)^* = (a^*\, 0^*)^*$

$= \{$Theorem 6$\}$

$(a \,[\!]\, 0)^* = (a^*\, 1)^*$

$= \{$Axioms 4 & 5$\}$

$a^* = a^* a^*$.

<u>Theorem 8</u> $a \leq a^*$

<u>Proof</u> true

$= \{$Theorem 5, unfolding once$\}$

$a^* = 1 \,[\!]\, a(1 \,[\!]\, a a^*)$

$= \{$Axioms 3 & 5$\}$

$a^* = 1 \,[\!]\, a \,[\!]\, a a a^*$

$\Rightarrow \{$Theorem 1$\}$

$a \leq a^*$. (End of Proof.)