The regularity calculus: a first trial

We consider regular expressions built from a constant, letters from an alphabet and three constructors.

Axiom 0 Each letter is a regular expression .

In the sequel, a, b, and c are variables of type "regular expression".

Axiom 1 The expression $a [] b$ is regular . The infix operator $[]$ —pronounced "bar"— is symmetric, idempotent, and associative, i.e.

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

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

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

$$a \leq b \equiv a [] b = b$$

Theorem 0 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 $a \leq b \wedge b \leq a \equiv a = b$.

Proof Reflexivity follows from the idempotence of $[\!]$, transitivity follows from the associativity of $[\!]$, and antisymmetry follows from the symmetry of $[\!]$. (End of Proof.)

Theorem 1 The $[\!]$ is monotonic, i.e.

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

Proof

$$
\begin{array}{ll}
 & a \leq b \\
= & \{\text{def. of } \leq\} \\
 & a [\!] b = b \\
\Rightarrow & \{\text{Leibniz}\} \\
 & a [\!] b [\!] c = b [\!] c \\
= & \{\text{properties of } [\!]\} \\
 & (a [\!] c) [\!] (b [\!] c) = (b [\!] c) \\
= & \{\text{def. of } \leq\} \\
 & a [\!] c \leq b [\!] c \quad .
\end{array}
$$

(End of Proof.)

We introduce the constant 0 as special regular expression: it is the unit element of $[\!]$:

Axiom 2 The expression 0 is regular and satisfies $\underline{0} [\!] a = a$ or, equivalently, $0 \leq a$.

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

Axiom 3 The expression ab is regular. The (invisible) infix operator is associative, i.e.

$$(ab)c \;=\; a(bc) \quad .$$

Syntactic convention. 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.)

Axiom 4 Concatenation distributes in both directions over the $[\!]$, i.e.

$$(a\,[\!]\,b)c \;=\; ac\,[\!]\,bc$$
$$a(b\,[\!]\,c) \;=\; ab\,[\!]\,ac$$

Theorem 2. Concatenation is monotonic in both its arguments, i.e.

$$a \leqslant b \;\Rightarrow\; ac \leqslant bc$$
$$b \leqslant c \;\Rightarrow\; ab \leqslant ac \quad .$$

Corollary 0. $a \leqslant b \wedge c \leqslant d \;\Rightarrow\; ac \leqslant bd$.

Proof

$$\begin{array}{ll}
a \leqslant b & b \leqslant c \\
= \{\text{def. of } \leqslant\} & = \{\text{def. of } \leqslant\} \\
a\,[\!]\,b = b & b\,[\!]\,c = c \\
\Rightarrow \{\text{Leibniz}\} & \Rightarrow \{\text{Leibniz}\} \\
(a\,[\!]\,b)c = bc & a(b\,[\!]\,c) = ac \\
= \{\text{Axiom } 4\} & = \{\text{Axiom } 4\} \\
ac\,[\!]\,bc = bc & ab\,[\!]\,ac = ac \\
= \{\text{def. of } \leqslant\} & = \{\text{def. of } \leqslant\} \\
ac \leqslant bc \quad . & ab \leqslant ac \quad .
\end{array}$$

(End of Proof of Theorem 2.)

<u>Axiom 5</u> $0a = 0$ and $a0 = 0$.

For concatenation, a single unit element is introduced; we denote it by 1 , which will shortly be recognized as an abbreviation.

<u>Axiom 6</u> The expression 1 is regular and satisfies $1a = a$ and $a1 = a$.

(Expressions 0 and 1 differ from each other and from all the letters.)

Our last constructor, called "closure", indicated by a postfix $*$ with highest binding power and pronounced "star", is introduced by

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

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

<u>Theorem 3</u> $0^* = 1$.

<u>Proof</u> true
$= \{\text{Ax. 8 with } b := 0\}$
$(a0)^* = 1 [] a(0a)^* 0$
$= \{\text{Ax. 5, twice}\}$
$0^* = 1 [] 0$
$= \{\text{Ax. 2}\}$
$0^* = 1$. (End of Proof.)

Theorem 3 justifies our characterization of 1 as "an abbreviation".

Theorem 4 The * is idempotent, i.e. $a^* = a^{**}$.

Proof true

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

$(a [] 0)^* = (a^* 0^*)^*$

$= \{$Axiom 2 and Theorem 3$\}$

$a^* = (a^* 1)^*$

$= \{$Axiom 6$\}$

$a^* = a^{**}$. (End of Proof.)

Theorem 4 justifies the name "closure".

Theorem 5 $1 = 1^*$.

Proof true

$= \{$Theorem 4 with $a := 0\}$

$0^* = 0^{**}$

$= \{$Theorem 3$\}$

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

Theorem 6 $a^* = 1 [] a a^*$ and $b^* = 1 [] b^* b$.

Proof From Axiom 8 by $b := 1$ and $a := 1$ respectively, and Axiom 6. (End of Proof)

Theorem 7 $a^* = a^* a^*$.

Proof true

$= \{$Theorem 6 with $a := a^*\}$

$a^{**} = 1 [] a^* a^{**}$

$= \{$Theorem 4$\}$

$a^* = 1 [] a^* a^*$

$= \{$Axiom 6$\}$

$a^* = 1 1 [] a^* a^*$

{Corollary 0 and $1 \leq a^*$ from Theorem 6}
$a^* = a^* a^*$. (End of Proof.)

Theorem 8 $a \leq a^*$

Proof true
= {Theorem 6, unfolding once}
$a^* = 1 [] a(1 [] a a^*)$
= {Axiom 4 and Axiom 6}
$a^* = 1 [] a [] a a a^*$
⇒ {Axiom 1}
$a^* [] a = a^*$. (End of Proof.)

Theorem 9 Closure is monotonic, i.e. $a \leq b \Rightarrow a^* \leq b^*$.

Proof Under the assumption $a \leq b$, i.e. $a [] b = b$, we have to prove $a^* [] b^* = b^*$. Since $b^* \leq a^* [] b^*$ is obvious (from Axiom 1), it suffices —on account of Theorem 0, antisymmetry— to prove $a^* [] b^* \leq b^*$ under the assumption $a [] b = b$. We observe for any c

$c = a^* [] b^*$
⇒ {Theorem 8}
$c \leq (a^* [] b^*)^*$
= {Axiom 7, with $a := a^*$ and $b := b^*$}
$c \leq (a^{**} b^{**})^*$
= {Theorem 4}
$c \leq (a^* b^*)^*$
= {Axiom 7}
$c \leq (a [] b)^*$
= {assumption $a [] b = b$}

$c \leq b^*$. (End of Proof.)

(The above proof is due to Rudolf H. Mak and Stefan Rönn.)

<u>Theorem 10</u> $a \leq b^* \equiv a^* \leq b^*$.

<u>Proof</u>. $a \leq b^*$
$\Rightarrow$ {Theorem 9}
$a^* \leq b^{**}$
$=$ {Theorem 4}
$a^* \leq b^*$.

$a^* \leq b^*$
$\Rightarrow$ {Theorem 8}
$a \leq b^*$

(End of Proof.)

* * *

The relation c <u>from</u> (a,b) between an expression c and a pair of variables (a,b) is defined as the strongest relation satisfying

0 <u>from</u> (a,b)
a <u>from</u> (a,b) and b <u>from</u> (a,b)
$(c [] d)$ <u>from</u> (a,b) $\equiv$ c <u>from</u> (a,b) $\wedge$ d <u>from</u> (a,b)
$(c\, d)$ <u>from</u> (a,b) $\equiv$ c <u>from</u> (a,b) $\wedge$ d <u>from</u> (a,b)
c^* <u>from</u> (a,b) $\equiv$ c <u>from</u> (a,b) .

It allows us to formulate

<u>Theorem 11</u> c <u>from</u> $(a,b) \Rightarrow c \leq (a [] b)^*$

<u>Proof</u>. The proof is by induction over the syntax. We observe for the base — mainly on account of Theorem 8 — $0 \leq (a [] b)^*$, $a \leq (a [] b)^*$, $b \leq (a [] b)^*$.

For the induction step, we prove under the hypothesis

$$c \leq (a [] b)^* \;\wedge\; d \leq (a [] b)^*$$

(i) $c [] d \leq (a [] b)^*$ (Theorem 1 and Axiom 1, idempotence)

(ii) $cd \leq (a [] b)^*$ (Corollary 0 and Theorem 7.)

(iii) $c^* \leq (a [] b)^*$ (Theorem 10.)

(End of Proof.)

Combining Theorems 10 and 11 we get

<u>Corollary 1</u> c <u>from</u> $(a,b) \Rightarrow c^* \leq (a [] b)^*$

From Corollary 1, Theorem 9, and Theorem 0, antisymmetry, we conclude

<u>Theorem 12</u> $a [] b \leq c \;\wedge\; c$ <u>from</u> $(a,b) \Rightarrow c^* = (a [] b)^*$.

* * *

<u>Intermezzo</u> In the mean time we have discovered a few improvements of the above. We should add

<u>Theorem 1/3</u> $a \leq a [] b$

<u>Proof</u> true

$= \{$Axiom 1$\}$

$a [] a [] b = a [] b$

$= \{$definition of $\leq\}$

$a \leq a [] b$. (End of Proof.)

<u>Theorem 2/3</u> $a [] b \leq c \;\equiv\; a \leq c \;\wedge\; b \leq c$

<u>Proof</u> $a [] b \leq c$

$= \{$Theorem 1/3$\}$

$$a \leq a \,[\!]\, b \;\wedge\; b \leq a \,[\!]\, b \;\wedge\; a \,[\!]\, b \leq c$$
$\Rightarrow$ {Theorem 0, transitivity}
$$a \leq c \;\wedge\; b \leq c \quad .$$

$$a \leq c \;\wedge\; b \leq c$$
$=$ {definition of $\leq$}
$$a \,[\!]\, c = c \;\wedge\; b \,[\!]\, c = c$$
$\Rightarrow$ {Leibniz}
$$a \,[\!]\, (b \,[\!]\, c) = c$$
$=$ {definition of $\leq$}
$$a \,[\!]\, b \leq c \quad .$$
(End of Proof.)

In connection with Axiom 2 it would have been appropriate to recall the general

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

<u>Proof</u> $(\underline{A}\, a,b :: UL \,\$\, a = a \;\wedge\; b \,\$\, UR = b)$
$\Rightarrow$ {$a := UR$; $b := UL$}
$$UL \,\$\, UR = UR \;\wedge\; UL \,\$\, UR = UL$$
$\Rightarrow$ {Leibniz}
$$UL = UR \quad .$$
(End of Proof.)

The theorem is of equal relevance for Axiom 6.

We are tempted to replace Axiom 5 by

<u>Axiom 5'</u> $\quad ab = 0 \;\equiv\; a = 0 \vee b = 0 \quad .$

The original Axiom 5 would then get the status of a corollary.

In a similar vein we are tempted to strengthen Axiom 6 by adding to it

<u>Axiom 6½</u> $1 \leq ab \equiv 1 \leq a \wedge 1 \leq b$.

<u>Theorem 2½</u> $1 = ab \equiv 1 = a \wedge 1 = b$.

<u>Proof</u>
$$
\begin{array}{l}
1 = a \wedge 1 = b \\
\Rightarrow \{\text{Axiom } 6\} \\
1 = ab
\end{array}
$$

$$
\begin{array}{l}
1 = ab \\
= \{\text{Theorem } 0, \text{ reflexivity}\} \\
1 \leq ab \wedge 1 = ab \\
= \{\text{Axiom } 6\tfrac{1}{2}\} \\
1 \leq a \wedge 1 \leq b \wedge 1 = ab \\
= \{\text{monotonicity of concatenation and Axiom } 6\} \\
1 \leq a \wedge 1 \leq b \wedge 1 = ab \wedge b \leq ab \wedge a \leq ab \\
\Rightarrow \{\text{Leibniz}\} \\
1 \leq a \wedge 1 \leq b \wedge b \leq 1 \wedge a \leq 1 \\
= \{\text{Theorem } 0, \text{ antisymmetry}\} \\
1 = a \wedge 1 = b
\end{array}
$$
. (End of Proof.)

We probably need as well

<u>Axiom vi</u> $1 \leq a \| b \equiv 1 \leq a \vee 1 \leq b$

<u>Axiom vii</u> $a \leq 1 \equiv a = 0 \not\equiv a = 1$

(With $a := 1$, we derive from Axiom vii $1 \neq 0$.)

(End of Intermezzo.)

Further addition:

<u>Theorem $6\frac{1}{2}$</u> $\quad aa^* = a^*a$

<u>Proof</u>

$$
\begin{aligned}
& z = aa^* \\
= & \{\text{Theorem 6 with } b := a\} \\
& z = a(1 \,[\!]\, a^*a) \\
= & \{\text{Axioms 4 and 6}\} \\
& z = a \,[\!]\, aa^*a \\
= & \{\text{Axioms 4 and 6}\} \\
& z = (1 \,[\!]\, aa^*)a \\
= & \{\text{Theorem 6}\} \\
& z = a^*a
\end{aligned}
$$

(End of Proof.)

* * *

We observe

$$
\begin{aligned}
& x = (aa)^* \,[\!]\, a(aa)^* \qquad\qquad *) \\
\Rightarrow & \{\text{Leibniz and Axiom 4}\} \\
& 1 \,[\!]\, aa(aa)^* \,[\!]\, a(aa)^* = 1 \,[\!]\, ax \\
= & \{\text{Theorem 6}\} \\
& (aa)^* \,[\!]\, a(aa)^* = 1 \,[\!]\, ax \\
= & \{ *) \} \\
& x = 1 \,[\!]\, ax
\end{aligned}
$$

From the above we conclude that the equation

$$x : (x = 1 \,[\!]\, ax) \qquad (0)$$

is solved by $(aa)^* \,[\!]\, a(aa)^*$; on account of Theorem 6, it is also solved by a^*. Our axioms so far — see Arto Salomaa "Theory of Automata", 1969 — do <u>not</u> suffice to conclude

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

We could try to solve the problem by postulating that (0) has a unique solution, but that would be a mistake, as is shown by the following analysis.

<u>Theorem 13</u> $\quad 1 \leq a \;\equiv\; a^* = aa^*$

<u>Proof</u> $\quad a^* = aa^*$

$= \{\text{Theorem 6}\}$

$\quad 1 \,[\!]\, aa^* = aa^*$

$= \{\text{definition of } \leq\}$

$\quad 1 \leq aa^*$

$= \{\text{Axiom } 6\tfrac{1}{2}\}$

$\quad 1 \leq a \;\wedge\; 1 \leq a^*$

$= \{1 \leq a^*\}$

$\quad 1 \leq a \qquad .$ (End of Proof.)

We now show that for $1 \leq a$ equation (0) is solved by $a^* \,[\!]\, a^*c$. To this end we observe

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

$= \{\text{Axiom } 4\}$

$\quad z = 1 \,[\!]\, aa^* \,[\!]\, aa^*c$

$= \{\text{Theorem 6}\}$

$\quad z = a^* \,[\!]\, aa^*c$

$= \{1 \leq a \text{ and Theorem 13}\}$

$\quad z = a^* \,[\!]\, a^*c \qquad .$

Note that in the above observation we have not made any assumption about c . Since $1 \leq 1$, the above observation with $a := 1$ and $1^* = 1$ — Theorem 5 — tells us that the postulate that (0) has a unique solution leads to the conclusion that $1 [] c$ is unique, i.e. independent of c. From the idempotence of $[]$ we would then conclude $1 [] c = 1$, i.e. $c \leq 1$ for any c. Axiom vii then tells us that for any c we have $c = 0 \vee c = 1$. Such a universe, however, is too meagre to our taste: in view of our earlier remark that 0 and 1 differ from all the letters and — Axiom 0 — that each letter is a regular expression, we would be considering the not so interesting situation of an empty alphabet.